Expertise
and insight
for the future

Rodolfo Loaiza Enriquez

Cloud Security Posture Management (CSPM) in Azure

Metropolia University of Applied Sciences

Bachelor of Engineering

Degree Programme in Information Technology

Bachelor's Thesis

25th June 2021

Author Title Number of Pages Date	Rodolfo Loaiza Enriquez Cloud Security Posture Management 61 pages + 4 appendices 25th June 2021
Degree	Bachelor of Engineering
Degree Programme	Degree Programme in Information Technology
Professional Major	Communications and Data Networks
Instructors	Janne Salonen, Principal Lecturer

Cloud computing is highly vulnerable to cyberattacks and threats due to inadequate change control, misconfiguration, and numerous vendors that utilize distinct strategies and policies with inadequacies for securing cloud-based infrastructure.

The advancement of security measures in cloud computing requires Cloud Security Posture Management for example to establish remote workforce management via policies as well as disaster recovery through business continuity planning by providing continuous threat monitoring and real-time risk monitoring. In this regard, the assessment involved system audit, workshops, and desk review to identify how CSPM can promote high-level configuration of the organization's cloud environment, promote security posture and enhance proactive cloud monitoring and audit to improve risk monitoring and management besides intensifying cloud management and automating deployment.

The assessment found failed security features in the following domains: Azure Defender, Azure DDoS protection, Access and Permissions and, Network Security. Consequently, the company should evaluate internal policies and protocols to identify appropriate features to install, update, and enable without constraining the established workflow, operational environment and cost management. The company should also embrace security best practices in the management and use of Azure cloud available in the industry and Microsoft Recommendation Center.

Keywords	management, recovery, monitoring, continuity, risk, policies

Contents

List of Abbreviations

ACL	Access-control list
AD	Active Directory
ADE	Azure Disk Encryption
AI	Artificial Intelligence
AKS	Azure Kubernetes Service
ARPANET	Advanced Research Projects Agency Network
AWS	Amazon Web Services
CIS	Center for Internet Security
CPPO	Consulting partner private offers
CSPM	Cloud Security Posture Management
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed denial of service
DevOps	Software development and IT operations
EC2	Elastic Compute Cloud
ECPA	Electronic Communications Privacy Act
IaaS	Infrastructure as a service
IaC	Infrastructure as Code
MMA	Microsoft Monitoring Agent

MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
NSG	Network Security Group
PaaS	Platform-as-a-service
SaaS	Software as a service
SOC	Security operations center
SQL	Sequential query language
VPNs	Virtual private networks
www	World Wide Web

List of Tables

List of Figures

1 Introduction

The Internet-connected world features IT that connects almost all facets of society. As a result, threats and breaches are numerous due to varying security measures in different systems. Cabaj et al. (2018) indicate that cybersecurity and forensic specialists are incessantly pursuing innovations for dealing with a wide range of cyber threats in real-time. In this context, human agents cannot handle all requests successfully and efficiently in real-time. Subsequently, reliable systems require inputs from machine learning techniques, big data, and threat intelligence to enhance detection, analysis, and defending (Cabaj et al. 2018). For instance, extensive data generated by monitoring solutions require advanced analytical tools for mining and interpreting to enhance its use in cyber security. Moreover, the absence of capital due to a lack of cooperation between different stakeholders is a critical challenge that hampers effective cybersecurity systems. Nonetheless, CSPM is a critical security relief in cloud computing due to its ability to enforce continuous threat monitoring and real-time risk monitoring (Cabaj et al. 2018).

One of the common security issues in cloud computing is inadequate change control and misconfiguration. Numerous vendors utilize strategies and policies that are inadequate for securing cloud-based infrastructure. In this regard, they design infrastructure that is easy to use and share data, making security a secondary consideration. Additionally, the existing architecture in cloud-based infrastructure does not provide clients complete visibility or control of resources, making them dependent on the vendor's security measures. The use of vendor-provided security controls enhances misconfiguration among clients with multi-cloud deployments due to limited knowledge on suitable mechanisms for enforcing security across all deployments. In this regard, cloud computing security architecture enhances client awareness of available measures for constraining threats and their impact on cloud-hosted data and applications. Moreover, organizations can effectively evaluate individual vendors depending on their ability to secure their infrastructure and customer data (Alshenqeeti 2014; Cabaj et al. 2018).

The use of cloud computing promotes the sheer accessibility of data. Employees can access corporate data and applications from virtually any location around the world. In this context, cloud computing is a critical tool for fostering flexible work arrangements, global procurement practices, remote workplaces, and teamwork in the global workforce.

Therefore, the advancement of security measures in cloud computing enhances remote workforce management besides disaster recovery through business continuity planning. Consequently, CSPM promotes high-level configuration of cloud storage and enhanced proactive cloud monitoring and audit. The leading achievements of the technology include improved risk monitoring and management besides intensified cloud management and deployment automation (Cabaj et al. 2018).

1.1 The Company

The company is an international company with approximately 20 000 employees distributed worldwide. The company is one of the leading suppliers of processing technologies to different industries. The company utilizes diverse technologies and information systems to manage its global workforce and operations. Meanwhile, the involvement in different industries, diversified customers, and a large number of worldwide locations necessitate effective management of the enterprise cloud services essential and critical to competitive advantage and business sustainability. The company needs regular and comprehensive assessment of the cloud environment to security posture adequate and reliable.

1.2 The Objectives of the Study

The objective is to demonstrate the advantages of employing CSPM using existing tools in Azure, while aligning the solution with the current cybersecurity architecture to help the organization improve the security posture in short term and propose and plan for long term to allow the organization gather the required resources to engage in more strategic projects for formalizing governance and security frameworks and ensuring proper management and security architecture of the cloud infrastructure and services.

1.3 The Scope

Scope of the study was to understand the cloud environment and current security practices within Azure services and platform by performing a risk assessment and map the vulnerabilities against Microsoft cybersecurity architecture and best practices. The risk

assessment was spanned across the three subscriptions currently contained under the "company.com" tenant, namely Company Microsoft Azure Enterprise, Company DMZ, Company Network. In this context, the assessment process was derived only with the aid of the following resources:

- The security findings and recommendations from Azure Security Center,
- The use of Microsoft Cybersecurity Reference Architecture as reference standard to base required gap analysis upon, and
- Active discussion through workshops, with project seniors and stakeholders to validate the security risks and related findings.

2 Current State Analysis

Current state analysis enables companies to focus and capture issues and priorities. In this regard, analyzing the current state of the company defines the project scope, visualizes the required work, identifies challenges and issues in formulation of cloud security, creates a baseline for measuring improvements, and identifies any possible bottlenecks (McKay 2019). Korban (2015) adds that current state analysis defines needs, problem, and pain points, enhances understanding of the business domain, visualizes current processes and bottlenecks, identifies causes of poor performance, recognizes integration points and principles, and describes process intensity patterns. Therefore, the company benefits with enhanced evaluation of external environment, leadership capacity, technical capacity, management capacity, and adaptive capacity. The management gains enhanced understanding of the company's ability to respond to changes, how policies and practices articulate efficient use of corporate resources, capacity of the available resources to deliver successful programs and services, and the existing strategic and decision-making capabilities (Unison Health and Community Services 2015). Therefore, current state analysis of the company articulates feasibility of determining the current capacity for successfully embracing change (Korban 2015; McKay 2019; Unison Health and Community Services 2015).

The company has reliable adaption capability to emerging technologies, but it is not incorporating security and security governance in its practices. Its financial base promotes enhanced adaptation as evidenced by the company's collaborations with companies and stakeholders in different sectors worldwide, client risk management data, and

performance scorecard. However, the company does not extensively depend on technological innovation. This explains the minimal utilization of cloud solutions in management, control, and coordination. Microsoft Office365 and Azure are currently the primary systems responsible for the provision of IT services in the company. In this context, they constitute the pillar of the entire IT and process essentials due to their role in handing and manipulating highly critical data. The embedded security mechanism constitutes the primary strategies for enforcing data integrity, confidentiality, and privacy. Moreover, Microsoft Office365 and Azure are the keys to agile collaboration with partners and customers, meaning they are responsible for business continuity and operations in the global market.

Currently, the company does not have or feature a single framework/standard for enforcing security architecture. The company relies on security mechanisms and tools issued by software and system vendors. In this context, utilization of cloud strategy across the organization is rather limited. The company leverages Azure cloud for infrastructure and SAP cloud services software for the most important part of ERP/CRM/BI business application landscape. The approach ensures that the company effectively completes essential transaction using cloud platforms without optimizing possible benefits. The current cloud strategy is for steering competitiveness rather than fostering optimum efficiency and performance. Nonetheless, the company is investing in analytics and IoT planform to leverage existing production data to optimized and improve production and assist customers.

The company has an active strategy of enhancing use of cloud computing and fostering security. For instance, Azure Enterprise subscription complements internal infrastructure, but the company is exploring possibilities of utilizing outward phasing solutions such as IoT provided through IoT platforms and Digital Customer Services accessed through analytics subscriptions. However, the organization does not have a cloud management or a cloud security specific policy for articulating cloud governance framework. The organization also lacks in-house expertise for cloud security and cloud architecture. In this regard, securing of cloud infrastructure and services follows best practices and input from the most experienced employees in IT (see Appendix 1 for departmental chart).

Currently, the company is exploring strategies for avoiding vendor locking, but the initiative is in the preliminary stages, meaning that suitable approaches are still unclear.

Moreover, initiatives to assess the security posture have not been presented to date, which were previously recommended as rapid measures of assessing the environment. In the meantime, all the migration of the on-premises IT infrastructure in the IaaS and PaaS program was done in a lift and shift way. As a result, the company is currently spending immense time and effort on refactoring, rebuilding, or replacing some previously implemented solutions. In the past IaaS and PaaS migration and current development, the engineers and project stakeholders did not understand shared responsibility model due lack of training, resulting in numerous inactivated security controls that generated significant amount of unhealthy service during assessment. Although the company is reviewing lift and shift work completed in the PaaS program to improve governance and cost management, the absence of established governance and policy framework for cloud computing at the company is challenging efficiency and performance due to enhanced demand for refactoring, rebuilding, or replacing of established solutions.

3 Research Methodology

Research methodologies foster data collection and analysis by addressing the practical how of a study. The process describes techniques use for the identification, selection, and analyzing of information about the study problem. Research methodology empowers the readers to critically evaluate the validity and reliability of findings and inference. In this context, researchers and investigators utilize research methodology to collect specific data from specific individuals using established techniques for a given purpose that favor specific analysis. In this regard, methodological choices explain and justify the design choices by describing the rationale for specific techniques and methods. An investigator illustrates that the embraced approach and strategy effectively fits research questions, aims, and objectives by providing valid and reliable results. Consequently, research methodology used in this study focused on collecting suitable data for architecting security in Azure cloud at the company (Gell 2020).

This assessment involved a qualitative research that focused on collecting and analyzing textual data dependent on descriptive reasoning and words. The primary objective of the assessment was descriptive, allowing the employment of qualitative methodology. Systematic evaluation of service was used to provide information on threats and vulnerability facing the company for utilizing Azure cloud without established security architecture. In

this context, the leading goal was to understand the current security status of the cloud environment and evaluate the perception of individuals. The assessment involved collection of primary and secondary data from reputable sources. Consequently, the employment of qualitative research provides comprehensive description of the problem and possible solution without quantification.

3.1 Desk Research

The investigation involved collection of secondary data from published sources to understand the background of the problem. In this context, desk research focused on evaluating security architecture and models used in cloud environment. Gell (2020) notes that desk research describes use of data and information collected for unique purpose that is different from the current intent. The method involves evaluation of industry reports, journals, e-books, online platforms, and web searches. In this assessment, desk research was used to evaluate the background of cloud computing, compare cloud computing and traditional computing, and cloud security and governance. The primary goal of utilizing the method was to enhance understanding of concepts and techniques that influence architecting security for Azure cloud. For instance, review of CSPM enhanced understanding of automating risk identification and remediation in cloud environment. Therefore, desk review provides adequate background for enhancing evaluation of the cloud environment besides aiding and recommending of reliable security mechanisms (Gell 2020).

Desk research focused on the collection and analysis of publicly available data on public platforms, including corporate websites, datasets, statistics, and databases. The method allowed gathering of information specific to this assessment at relatively low cost. The information was readily available in the public discourse, meaning that a computer and internet connection were sufficient to complete data gathering. The technique provided reliable background data on cloud computing and security architecture. Bhasin (2020) notes desk research is not time demanding and helps to focus research. In this context, this assessment involved minimal time investment in the collection of reliable data from secondary sources, which influenced aspects of cloud computing assessed at the company. However, desk research does not provide up-to-date information, making unreliable for solving dynamic problems. For instance, security elements and threats are

increasing changing, meaning the most reliable architecture should consider the most recent details. Moreover, considerable amount of time is spent searching and evaluating information specific to the current study problem (Bhasin 2020).

3.2 Interview

The qualitative interviews focus on describing central themes from the perspective of the subjects. According to Alshenqeeti (2014), interviews refer to guided conversation for describing the lifeworld of the interviewee in relation of a phenomena of interest. The extendable conversation between interviewee and interviewer provided in-depth information on a specific subject or topic. The utilization of interviews allows reporting of detailed informant views, analyzing of words, creating of holistic snapshot, and enabling of interviewees to speak in their voice while expressing their thoughts and feelings. (Alshenqeeti 2014). In this context, this assessment involved unstructured interviews with managers and experienced personnel responsible for maintaining the company cloud solution. The data collection technique enhanced the understanding of IT security around the organization besides describing vulnerabilities and setbacks of Azure cloud (Alshenqeeti 2014).

The absence of established security architecture for Azure encourages the use of unstructured interviews. Individual employees lacked adequate information to describe the entire systems and it is functioning, necessitating information from different resource person. In this regard, unstructured interviews allowed questions to differ per subject and advance knowledge of the topic from diverse perspectives. Hence, the data collection provided flexibility and enhanced the response rate. The interviews were conducted during the working hours without dedicating specific time or reserving elaborate sessions with interviewees. The technique allowed the judging of non-verbal behavior and spontaneity of the respondent. However, interviewing was relatively time consuming. The data collection did not involve specific data resource, meaning gathering of reliable and meaningful information took an extended time. Moreover, the interviewees were not readily available, meaning that data collection in some instance extended over several sessions. The absence of dedicated professional team for handling Azure cloud ensured that the assessment could not identify all critical resource individuals. Thus, interviewing allowed the description IT security environment at the company, but the collected information

may suffer from bias due to inability to identify all resource people and the limitations of unstructured approach.

3.3 System Audit

System analysis focused on evaluation of IT systems to determine their performance and vulnerabilities. For the assessments, different analysis tools were utilized, chiefly embedded in Azure to evaluate security performance of the company. Farooq (2020) describes system audit as the evaluation and review of computer systems, controls, security, and efficiency used in processing information in a company. Auditing determines the suitability of established arrangement for achieving corporate objectives. In this context, this assessment involved auditing of Azure cloud using internal reporting tools to identify existing security mechanisms and their effectiveness in articulating data integrity, privacy, and confidentiality Farooq (2020).

The employment of system auditing as data collection technique allowed the identification of susceptibility to threat. As a consequence, the company became aware of the security status of its cloud environment. The technique also evaluated the system, informing the company whether Azure is the appropriate technology for achieving corporate objectives. Moreover, the company identified the level of optimization of available security features. For instance, numerous security features offered in Azure cloud were not enabled enhancing vulnerability to threats. In this context, the company identified controls that require restructuring or reinforcement to improve cyber security and introduce enhanced data availability, confidentiality, and integrity. Smyth (2019) However, did not provide the company with efficiency enhancement mechanism besides facilitating data collection. The enhancement of security mechanism identified by the system audit does not guarantee improvement of reliability and efficiency. Moreover, this assessment involves system auditing from a set of tools provided by Azure, which makes the data relatively biased. A reliable audit should involve external scanning and penetration tests completed using tools from different vendors for articulating divulging purposes (Smyth 2019).

4 Cloud Computing

4.1 History

The information age involves ubiquitous cloud computing that enhances access to shared resources, lowers cost, and promotes agility. The technological innovation is rapidly becoming popular due to organizations and private individuals' continual discovery of cloud-based data and systems' benefits. (Cascio and Montealegre: 2016). Nonetheless, cloud computing is an old concept that emerged in the early 1950s to meet military demands. The development of a military mainframe in 1950 aimed at connecting several computer terminals in an internal matrix (Neto.2014). The need to contain cost necessitated sharing of technology among multiple people, creating a foundation for cloud computing. The mainframe computers were prohibitively expensive and relatively huge, ensuring organizations could only afford a limited number. Most enterprises had less than two computers and utilized time-sharing schedules, which involved connected stations without independent processing power (Neto.2014). The approach enabled individual companies to maximize return on investment and reduce payback time (Cascio and Montealegre: 2016; Neto 2014).

The main advancement of cloud computing emerged in the 1960s due to the development of the ARPANET. Foote (2017) indicates that DARPA contracted MIT in 1963 to develop a computer for simultaneous use by two or more people. The $2 million Project MAC developed a computer that used magnetic tapes for memory, which acted as the cloud that allowed two or three people to use the computer simultaneously (Foote: 2017). Bob Taylor and Larry Roberts developed ARPANET in 1969 with the assistance of J. C. R. Licklider, Goddard (2018) notes that ARPANET was a primitive version of the modern internet that allowed sharing of digital resources across computers in different locations. The technological innovation was a significant breakthrough for Licklider's vision of a world interconnected by computers and unlimited access to data from virtually all geographical locations (Foote 2017; Goddard 2018).

Virtual machines (VM) emerged and became popular in the 1970s. In this regard, IBM, in 1972, developed an operating system that enabled people to share computing resources (Neto. 2014). The technological advancement attracted several telecommunication companies that offered virtual private networks (VPNs) as a rentable service.

Bairangi and Bang (2015) indicate that VPNs reduced cost and provided high-quality services compared to previous technology of dedicated point-to-point data circuit, which significantly wasted bandwidth. In contrast, VPN allowed balanced utilization of an entire network through switching of traffic (Neto. 2014). Virtualization in the modern environment is relatively simple with tools, such as VMWare and Xen, enabling the launching of multiple virtual servers on personal computers (Bairangi and Bang 2015; Neto 2014).

The www technology invented in 1989 by Tim Berners-Lee allowed linking hypertext documents, leading to an enhanced internet expansion (Blanchard 2020). The web continues to drive numerous inventions today, including networking technology and social media. (Blanchard 2020.) Initially, available bandwidth was minimal, but the web's embracement in the 1990s and 2000s led to the development of on-premises data centers by large companies. As a result, the data center industry emerged, resulting in dedicated servers and shared hosting. In this regard, Software-as-a-Service applications emerged to utilize improved bandwidth and hosting technology in the provision of content relationship management over web browsers. Salesforce in 1999 was the first successful Cloud Computing application aimed at delivering software programs to the end-users through the internet (Jungck and Rahman, 2011). Individuals with Internet access could access and download the application, meaning that businesses could purchase it on-demand from their offices' convenience (Blanchard 2020; Jungck and Rahman 2011).

The term "cloud" emerged in the mid-1990s to discuss the new digital sphere. A practical and reliable cloud computing emerged in 2002 with Amazon's introduction of web-based retail services and subsequent establishment of AWS in 2006 to offer online services, including human intelligence, computation, and storage, to clients and other websites (Foote 2017). Mohamed (2018) notes that Amazon launched EC2, which fostering renting of virtual computers and deployment of private applications, while Google launched Google Docs in 2006, resulting in ability to save, update, edit and share documents online. In 2007, private companies and institutions of higher learning in the United States developed a server farm, which hosted several research projects requiring high processor power and large datasets. Again, in that year, Netflix started an online video streaming service. Meanwhile, other significant enhancements of cloud computing include a compatible platform for distributing private Clouds by Eucalyptus, iCloud by Apple for storing personal information, and open-source software by OpenNebula for deploying Private and Hybrid Clouds (Foote 2017). Oracle Cloud by Oracle emerged in 2012 with

software-as-a-service, platform-as-a-service, and infrastructure-as-a-service (Jungck and Rahamn, 2011). Thus, cloud computing is increasingly becoming popular since 2000 in government, finance, healthcare, and entertainment services (Foote 2017; Jungck and Rahman 2011; Mohamed, 2018).

4.1.1 Cloud Computing vs Traditional Computing

Modern businesses understand the value of data storage and record-keeping in a competitive operational environment. As a result, data management is a critical process for articulating ethical and sustainable models due to its role in creating growth and efficiency insights. DMS Technology (2017) indicates that company traditionally stores files on individual devices or on a local server to promote information availability in the future. The main difference between traditional computing and early on-site storage, which involved a physical registry, is computer technologies, such as hard disks and servers for backup. (DMS Technology (2017.) In this regard, traditional data centers involve assorted hardware connected by a remote server installed on the business premises to a network. Employees using the hardware have access to stored applications and data (DMS Technology, 2017).

Businesses privately and individually own traditional computing infrastructure. As a result, individual companies aiming to scale up data storage and services for an enhanced number of users, purchase additional hardware or initiate and pay for require upgrades. In this regard, established departments install and maintain computing resources to promote reliability and efficiency (Pandey 2018). Nonetheless, traditional computing is a highly secure data hosting solution because individual businesses maintain absolute control over data and applications stored in a local server (Pandey 2018). Moreover, companies can customize IT infrastructures to meet unique demands, chiefly when running numerous applications. DMS Technology (2017) notes that the technological approach is relatively cheap and effective for businesses with unreliable Internet connections. Thus, limited capital does not constrain businesses and individuals from computing benefits (DMS Technology 2017; Pandey 2018).

The emergence of computers as mainstay devices of homes and workplaces encouraged innovators to search for ways effectively utilizing technology. In this regard, computer capabilities have been advancing in the last two decades while their sizes have

been becoming smaller and smaller (DMS Technology 2017). Consequently, cloud computing is a new model of enhancing the storage of increasing data from corporates and individuals. The distributed decentralized architecture replaces centralized resources in traditional computing by providing storage, software, and software development platforms over the internet (Nicholas 2018). Consequently, cloud computing is a utility enhancement strategy by distributing some computing services way from the local infrastructure by an external entity (DMS Technology 2017; Nicholas 2018).

Cloud computing involves diverse hardware and software components that facilitate different utilities to clients. According to Nicholas (2018), hardware and software entail communicating components for the delivery of computing services, networking, software analytics, storage databases, and intelligence. Thus, cloud computing provides economies of scale and innovation flexible resources that enhance organizational efficiency and performance. DMS Technology (2017) associates cloud computing with measureable services, high elasticity, shared infrastructure, extensive dependence on networks, and selective service delivery to clients. Individual businesses utilize the innovation selects preferred services and pays for them only. (DMS Technology (2017.) Therefore, cloud computing fosters unlimited access to services by users with compatible devices, involves multiple hardware platforms besides client devices, allows modulations at any time depending on the consumer's needs, and offers measurable and limitable services (Nicholas, 2018). In this regard, the technology lowers lower upfront cost, improve performance and scalability, and allows an organization to focus on core businesses rather than computing needs and infrastructure. Hence, cloud computing promotes a data-driven world by fostering online and offsite data storage, processing, and access (DMS Technology 2017; Nicholas 2018).

Flexibility and Scalability

Traditional computing is inflexible and non-scalable because individual organizations can only use available resources. In this context, the exhaustion of storage space demands the purchase or renting of another server. (Nicholas 2018.) The approach is highly cost-oriented because business owners incur expenditure on service provision contracts, staff and support overheads, data storage, hardware purchase and management, power overheads, and maintenance and support. In contrast, cloud computing features several

server resources with unlimited storage space, meaning that it can scale up or down depending on the traffic customer receives. Meanwhile, customers can install software to meet the changing or growing needs of a business. Cloud computing is a service-oriented approach because business owners have access to data storage, application server, and telephone platform as core utilities (Nicholas 2018).

Resilience and Elasticity

Cloud computing provides high resilience and elasticity compared to traditional computing due to the distribution of information and applications across several servers. The employment of several servers increases server resources and storage space, resulting in enhanced computing power (Pandey 2018). In contrast, traditional computing does not guarantee superior server performance due to capacity limitation and downtime susceptibility (Pandey 2018).

Automation

Traditional computing requires extensive in-house administration that is expensive and time-consuming. Consequently, businesses require diverse professionals to offer a wide range of services, including monitoring, control, maintenance, configuration among others required for efficiency and reliability of in-house data storage (Pandey, 2018). In contrast, cloud computing involves a dedicated service provider who maintains hardware and implements security measures (Pandey 2018). Table 4.1 presents the main differences between traditional and cloud computing during the automation process. The approaches have significant distinctions in the acquisition, access, business, and technical models (Pandey 2018).

Table 4. 1 Difference between traditional and cloud computing (Nicholas, 2018).

Model	**Traditional computing**	**Cloud computing**
Acquisition	Customer purchases assets and builds technical architecture.	Customer buys services that include architecture.

Business	A client pays for assets and administrative overheads.	Customer pays for use, resulting in reduced administrative functions.
Access	Users rely on the internal network and corporate desktops and laptops.	Users rely on the internet, meaning they can utilize a wide range of devices.
Technical	Businesses have static and non-shared systems authorized to a single tenant.	The systems are elastic, scalable, dynamic, and multi-tenant.
Delivery	Systems are costly and involve lengthy deployment. Businesses must pay for land and expand staffing.	Systems have reduced deployment times and swift return on investment.

The differences in the automation models result in distinctiveness in characteristics. Table 4.2 shows that traditional and cloud computing have features unique to each of them. The approach used to address different utilities vary with the computing approach (Nicholas 2018).

Table 4. 2 Characteristics difference between traditional and cloud computing.

Character	**Traditional computing**	**Cloud computing**
Consumption	Applications	Software-as-a-service
Creation	Development tools	Development-as-a-service
Orchestration	Middleware	Platform-as-a-service
Infrastructure	Infrastructure and hardware	Infrastructure-as-a-service
Cost	Incremental capita expenditure	Pay per use
Provisioning	Months	Minutes
Availability	Manual repair of system failures	Automated recovery

Scaling	Manual addition of new services	Scale on demand
Ease of use	Traditional hardware procurement	Self-service
Consumption	Dedicate	Shared

The automation of business using traditional and cloud computing have distinct differences (Nicholas, 2018.) In this regard, cloud computing features standardized services, shared resources, unlimited capacity, secured computing environment, and partial control. In contrast, traditional computing offers customized services, limited capacity, full control, dedicated resources, and a high-security level (Nicholas 2018). In this regard, cloud computing is disadvantaged against traditional computing due to high latency, offers servers on the internet, lacks user-defined security, is vulnerable to attacks, features multiple hops, and does not have data location awareness (Nicholas 2018).

Running Costs

The pay-per-use model in cloud computing ensures that businesses pay for used services rather than unjustified lump sum amount, which sometimes involve unnecessary or unused services. Figure 4.1 shows the services managed by a client compared to the administrative functions in traditional computing. The decreased downtime ensures businesses have high productivity and maximized profits. Nicholas (2018) notes that cloud computing saves time and enhances return on investment due to minimal setup time, eliminates upfront costs for procuring hardware and software, and allows vendors to host several clients on shared resources (Nicholas 2018).

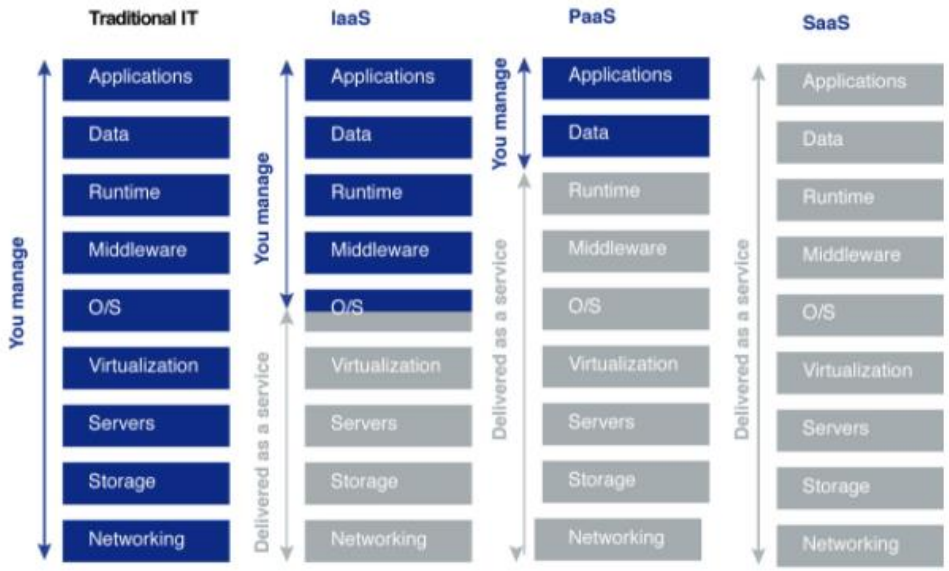


Figure 4. 1 User-managed functions in the cloud and traditional computing.

The traditional computing model is relatively expensive to acquire and maintain compared to cloud computing. In this regard, it is vulnerable to hardware outages and underutilization of processor and computing resources. The supporting infrastructure is not scalable, meaning businesses pay for unused or underutilized services, leading to unnecessary maintenance costs. Nicholas (2018) indicates that traditional computing involves expensive cycling of hardware and software licenses, in-house maintenance staff, regular retraining of staff due to upgrades, complex budgeting, and bookkeeping due to the oscillation of IT expenditures. Therefore, traditional computing has considerable costs avoided by embracing cloud computing (Nicholas 2018).

4.1.2 Advantages and disadvantages of Cloud Computing

Cloud computing involves simplified administration with providers handling extensive activities and operations. Abdalla and Varol (2019) indicate that setting up cloud-based applications is less demanding as the vendor handles all management complexities. The model is cost-effective because businesses do not purchase the hardware components or pay for their maintenance. Moreover, storing information in remote servers reduces operational costs by eliminating the need for physical storage devices and maintenance tasks associated with regular backup and purchase of storage devices. Abdalla and Varol (2019) posit that cloud computing has low impact failures and upgrades due to

hardware redundancies that ensure scheduled or unplanned breakdown are invisible to clients. Abdalla and Varol (2019.) Cloud computing also features flexible solutions that ensure clients pay for used services. The approach enables customers to pay for additional services when a scale-up is needed. In this context, users have unlimited computing powers because they do not rely on computers in their business premises. Moreover, the model reduces administration demands enabling the reallocation of resources to core business operations (Abdalla and Varol 2019).

The use of cloud computing enhances flexibility and data safety. Workers can access different resources hosted on the cloud remotely. The only prerequisite for utilizing corporate resources is reliable internet access. In this context, employees or individuals in different geographical locations can collaborate using highly convenient and secure models. NCC Group (2019) reports that cloud computing fosters flexibility by allowing organizations to choose different service models. NCC Group (2019.) Moreover, businesses do not incur costs and strains of recruiting and retaining security experts. Consequently, cloud computing offers numerous benefits ranging from web-based control and interfaces, low-cost software, pay-per-use, multi-tenancy, effective virtualization to advanced online security (NCC Group 2019).

Cloud computing is highly dependent on reliable internet connections. Users must have an internet connection to use cloud computing services. (Abdalla and Avarol, 2019.) Moreover, the Internet connectivity speed must be high because web-based applications require a lot of bandwidth to complete transactions. Nonetheless, the connectivity speed does not guarantee swift access to resources. The need to download and upload documents ensures the access is slow compared to utilizing a local server. The independence of users and data storage facilities arouse fear over the handling of confidential data. Abdalla and Varol (2019) indicate that some servers have leaks and unauthorized data access between virtual devices, resulting in confidentiality breaches. Additionally, errors lead to incorrect handling, management, and saving of sensitive data (Abdalla and Varol 2019).

The enhanced utilization of cloud computing to manage critical organizational operations is enhancing dependence on online resources. According to Abdalla and Varol (2019), cloud services occasionally tend to be unavailable for extended periods due to internal issues, particularly among vendors who do not replicate data and applications across

multiple sites. As a result, organizations cannot recover from unexpected disruptions, leading to constrained performance and profitability (NCC Group 2019). Cloud computing concentrates massive resources and data, creating attractive targets, enhancing organizations' vulnerability to and shared technology issues, denial of service, data loss, and data breaches. In this context, when hackers enter client's applications may access, destroy, distribute, or disclose sensitive data, leading to loss of competitive edge, legal suits, and reduced trust in consumer segments. Abdalla and Varol (2019) report that some vendors cannot maintain data integrity, which reduces data value to organizations. Meanwhile, cloud computing is challenging compliance because clients do not have information about their data's storage location. Thus, it is challenging to articulate localized data protection regulation (Abdalla and Varol 2019; NCC Group 2019).

4.2 Cloud Security and Governance

The enhanced utilization of IT in the business world is creating new and unique challenges (Mukundha and Vidyamadhuri, 2017). Organizations have unprecedented burden of satisfying enhanced need for reliable, fast, and secure services. The attempt to enhance IT systems by increasing storage capacity and processing power expose individual companies to prohibitively expensive investment. Meanwhile, cloud computing is the new alternative fostering robust, scalable, and secure IT services without massive investment in additional hardware and software. Mukundha and Vidyamadhuri (2017) indicates that pay-per-use principle, on-demand changing scalability, and use of distributed environment make cloud computing attractive and competitive to organizations with changing workload regardless of their size. In this regard, cloud computing involves distinct services that address unique set of business requirements to enhance efficiency, accessibility, throughput, and reliability (Mukundha and Vidyamadhuri 2017).

4.2.1 Cloud Governace

The adoption of cloud computing in an enterprise requires consideration of a host of factors. In this context, companies do not utilize internal data center for hosting applications, management need to adopted cloud models, demand and capacity require revised planning cycle, and companies need flexible budgets with on-demand models and new

set of policies and controls (Agarwal 2011). The new phenomenon in the IT environment requires company to adopt or change the existing workflow and processes. (Agarwal 2011.) Consequently, a requisite cloud governance with set of rules for handling costs and efficiency issues besides effectively integrating third-party in internal operations and managing relationships is highly essential. In this regard, the rules dictate amounts department can spend, appropriate policies for cloud security, and suitable departmental programs and applications (Agarwal 2011).

The implementation of rules in a business organization requires monitoring for compliance to enhance efficiency. Individual companies can utilize different types of cloud management software to view all cloud activities. (Price, 2018.) The monitoring for compliance identifies aspects of organizational rules that require improvement to enhance cost-efficiency or performance. Thus, amendment of policies is crucial for accommodating new products and services besides sustaining competitive advantage in consumer segments. In this context, Price (2018) perceives cloud governance as the development and deployment of controls for managing compliance, budget, and access in corporate cloud workloads (Price 2018).

Principles of Cloud Governance

Cloud governance is a set of principles for dictating and managing the use of cloud computing services. Parveen (2020) notes that primary goal is safeguarding remote data by utilizing people, processes, and technology as the primary solutions. Thus, cloud governance focuses on managing operational efficiency, optimizing finances, and promoting compliance to reduce risks. (Parveen, 2020.) Effective cloud governance has reliable cost management strategies, security controls, established identity requirements, consistent resource configuration, and centralized, standardized, and consistent approach of articulating effective deployment. In this regard, cloud governance operates under the principles of cost optimization, financial management, performance management, operational governance, asset and configuration management, and security and incident management (Parveen 2020). Nonetheless, organizations need to vary the content of each principle to match governance necessities and specific circumstances in operational environment. In this regard, Figure 4.2 presents components of a good cloud governance. The design for each component depends on organizational needs and constraints (Parveen 2020).

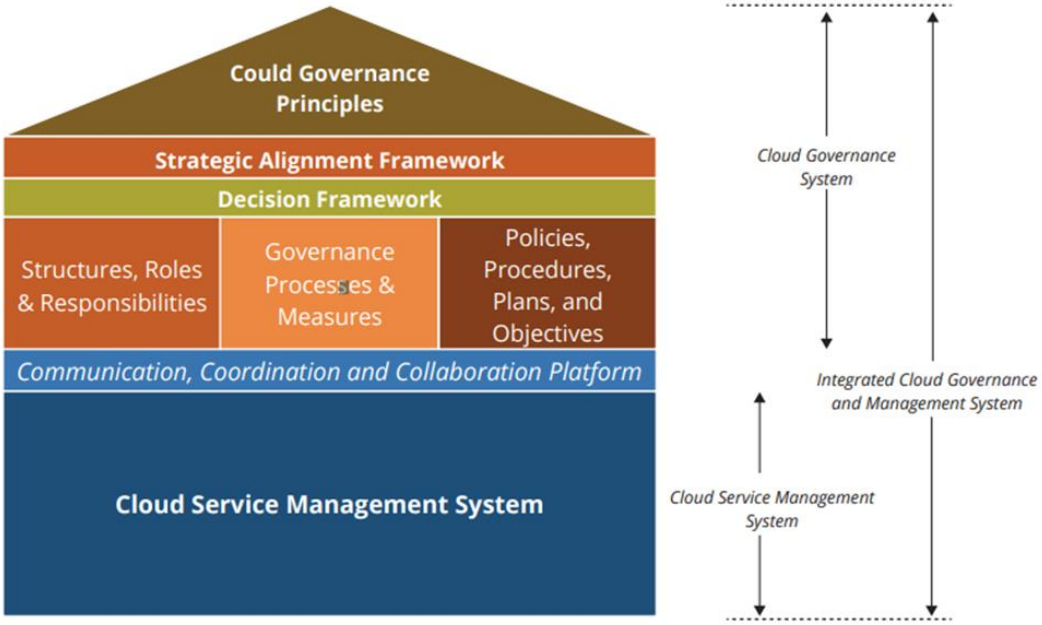


Figure 4. 2 Effective cloud governance (Everett 2017).

The variance of operational environment creates specific demand for cloud computing, resulting in uniqueness of operating principles. For instance, Oman Governance and Standard Division (2016) notes that cloud governance involves six principles, including enablement that allows organizations to consider cloud computing as a strategic enabler, enterprise risk that enforces enterprise risk management approach in the adoption and utilization of cloud, and trust that allow organization to trust organizations involve in provision of cloud computing. (Oman Governance and Standard Division, 2016.) Moreover, cost/benefit ensures that individual companies have comprehensive understanding of all possible costs compared to costs of other technologies, while accountability require companies to define internal and provider responsibilities. The capability principle focuses on utilizing internal resources to the optimum by integrating possible extent of capabilities from cloud providers. In this regard, principle of cloud governance ensures organizations obtain efficiency and improved performance from cloud computing (Oman Governance and Standard Division 2016).

Importance of Cloud Governance

Cloud governance policies involve set of protocols with established framework. According to Parveen (2020), the presence of backup recovery services, programming

standards, security policy, infrastructure and application monitors, and design standards for infrastructure enable executives, managers, and IT professionals to create or regularly review cloud governance. (Parveen, 2020.) Therefore, the concept is under the control of decision-makers in business to ensure it promotes desired interests and goals. Figure 4.3 shows design and implementation process that enhance organizational control over deployment and use of cloud governance. Meanwhile, cloud governance operates in virtualization platform, application, and operating systems, which enable access restriction to sensitive information and data. Organizations access their cloud features with proper permission level checks and authentication (Parveen 2020).

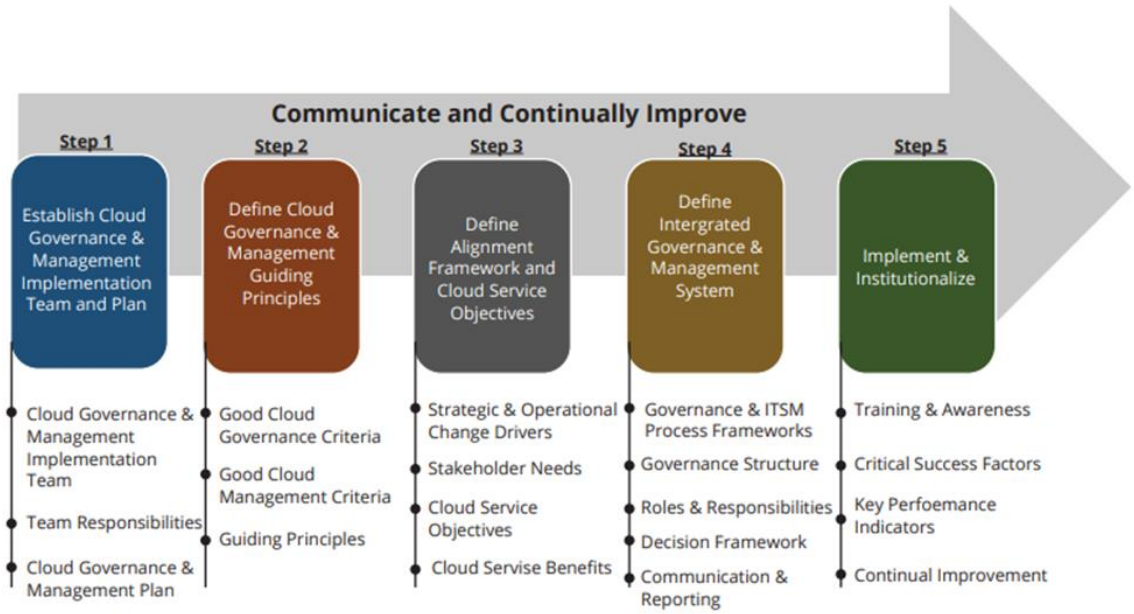


Figure 4. 3 Design and implementation of an effective cloud governance (Everett 2017).

Cloud governance enhances management of cloud resources. Price (2018) indicate that leading cloud service providers advise customers to use distinct account for managing multiple-tenant workloads for enhanced cost management, precise access control, limiting security and financial blast radius during breaches. Gandhi (2020) notes that the utilization of single cloud account enhance management of numerous accounts besides enabling visibility of activities and trends. Meanwhile, cloud governance enables quick access to cloud resources within compliance and budget constraints. In this regard, companies obtain enhanced efficiency through reduction of manual processes for tracking accounts, cost, and compliance besides eliminating need for follow-up actions after receiving alerts (Gandhi 2020; Price 2018).

Cloud Governance Models

The Guo's governance model is one of the reliable models for standardizing management of operational risks in cloud computing. Saidah and Abdelbaki (2014) indicate that it describes the necessary components cloud governance using four objectives, including compliance, risk, policy, and service management. Guo's governance model categorizes cloud governance into management, operational, and policy activities (see Figure 4.3). In this regard, each category provides structure and details related to information security in cloud computing (Saidah and Abdelbaki 2014).

Figure 4. 4 Guo's governance model (Saidah and Abdelbaki 2014).

Guo's governance model exhibits significant gap with the real world. Saidah and Abdelbaki (2014) applied controls in Cloud Controls Matrix (CCM) extracted from real Cloud business and found that differences between IT and organizational alignment hinder adoption of cloud computing. (Saidah and Abdelbaki 2014.) In this regard, IT teams need to become information and business experts, while individual businesses need to understand contribution and influences of cloud computing on established practices, resources, and workflows. In this regard, Table 4.3 presents an applicable Guo's governance model with practical strategies for implementing cloud governance (Saidah and Abdelbaki 2014).

Table 4. 3 New governance model (Saidah and Abdelbaki 2014)

Policy Model	**Operational Model**	**Management Model**

Business Process Management Policy	Metadata repository	Change management
Service Policy	Transformation	Risk Management
Data Policy	Monitoring	Service Management - Auditing and Logging - Errors and exceptions management - Service Delivery - Service Discovery (Saidah and Abdelbaki 2014)
Exit Policy	Audit	Security Management - Roles and responsibilities - Jurisdiction - Access - Privacy - Integration (Saidah and Abdelbaki 2014)
	Authorization	Policy Management - Policy Specification Service - Policy Repository - Application specification Ontology - Generic Policy Ontology (Saidah and Abdelbaki 2014)
	Authentication	Asset Management - Capacity planning - Configuration and documentation - IT Assets - Employees (Saidah and Abdelbaki 2014)

The primary goal of the new model coverts Guo's model is to enhance system reliability and efficiency. In this regard, an effective governance model considers all business stakeholders and processes in a secure way to guarantee that cloud computing supports established strategies and objectives besides promoting service value, service quality, and security (Saidah and Abdelbaki 2014).

4.2.2 Cloud Security

Cybersecurity in the information age is a critical concept that focuses on sustaining and enhancing the welfare of IT users, data, and assets. According to Pardini et al. (2017), it describes all the approaches for protecting networks, systems, and data from accidental or deliberate attacks (Kaur and Kaur 2014). Makeri (2017) indicates that cyber security involves a combination of innovation, practices, guidelines, training, activities, and risk management approaches used to protect assets in the cloud environment. Meanwhile, advancement in technology increasingly encourages cloud computing, mobile computing, and E-commerce to achieve different corporate objectives, enhancing the demand for cybersecurity (Kaur and Kaur 2014.) Although the technological innovations are relatively new and widely accepted in different industries, the available security models are inadequate and unreliable. Therefore, companies and private individuals face increasing vulnerability to cyberattacks due to the adoption of cloud computing, mobile computing, and E-commerce. In this regard, the attainment of global security and economic wellbeing requires enhanced cybersecurity for conventional and emerging technologies (Kaur and Kaur 2014; Makeri 2017; Pardini et al. 2017).

The cloud computing policies and technologies limit the innovation from effectively articulating security and control. NCC Group (2019) notes that security in the model involves protecting the systems and infrastructure besides formulating policies for controlling and protecting access to the cloud. In this regard, organizations are experiencing security breaches with data compromise and malware due to their employees violating cloud security policies NCC Group (2019.) Although customers require established measures for strengthening security and managing the impact of security breaches, vendors need to improve infrastructure and customer data protection. Therefore, the assessment of architecture security of cloud computing is essential for enhancing protection against threats. Moreover, it allows identifying suitable models for inducing customer's self-protection when interacting with shared resources in a multi-tenancy environment (NCC Group 2019).

Cloud computing operates on a global scale, meaning that vendors have clients distributed worldwide. In this regard, the industry lacks conventional policies on data handling and storage. Most vendors have unique data formats that are highly limiting. As a result, they tend to lock clients from migrating using unstandardized data formats, making data transformation, and transferring difficult and expensive affairs (Chaudhary 2020). In this

regard, individual clients cannot migrate despite their dissatisfaction with their vendor services and excessive reliance on their proprietary tools. Chaudhary (2020) notes that numerous organizations continue to rely on suppliers with an inappropriate security architecture that cannot withstand cyberattacks due to errors in decision-making during selecting a reliable vendor to handle highly sensitive, personal, or financial data (Harkut 2020). Therefore, assessing the security of cloud computing suppliers is highly essential to prevent enhanced vendor lock-in of business entities. The corporate decision-making processes on cloud computing need improved awareness of prevailing security issues vendors' architecture (Chaudhary 2020; Harkut 2020).

The cost of managing security breaches is relatively high. Stevens (2019) indicates that companies with average operation accrued $3.8 million loss due to cyberattacks in cloud computing, while American companies that take an average of 196 days to detect breaches accrued $7.9 million. The United Kingdom government in 2017 found that large businesses experienced losses amounting to £19,600 compared to £1,570 for small to medium-sized businesses due to cyberattacks (Seemma et al. 2018). In this context, cloud security threats constrain client's control over personal data. Thus, the assessment of cloud computing vendors' architectural security, primarily Azure, enhances customers' protection against security breaches. Makam (2020) notes that clients require enhanced awareness of emerging cloud security threats amid sophisticated technology and infrastructure. In this regard, decisions on cloud computing operations require extensive consideration of popular and emerging security threats (Makam 2020; Seemma et al. 2018; Stevens 2019).

In the past two decades, unscrupulous computer users distributed worldwide have been increasingly using IT to commit crimes and perpetrate fraud. Ayofe and Irwin (2010) indicate that cybercrimes' main motivation includes pursuit for recognition, urge to make quick money, gathering information about operations, attempting to interrupt technology infrastructures, and revenge or fight for a specific cause of interest to the perpetrator. As a result, people have a fascination with mixed feelings of fear and admiration for cybercrimes due to possible losses to victims and potential gains by the hackers. Nonetheless, sophisticated cyberattacks have unprecedented increase with enhanced penetration of the internet worldwide and ease of access to hacking tools and tutorials. For instance, hackers can manipulate hospital prescriptions and cause physical harm to targets (Ayofe and Irwin 2010). In this regard, cloud security requires a combination of legal

frameworks, system tools, and professionalism to thwart or minimize their social, psychological, financial, and physical effects on cyberspace and its users (Ayofe and Irwin 2010).

Cloud computing technologies emerged in environment with complex regulatory frameworks. As a result, cloud computing stakeholders need to evaluate existing legislation and regulatory framework to enhance data security. Blaisdell (2012) notes that Health Insurance Portability and Accountability Act restrains cloud providers from disclosing protected health information without appropriate authorization, while the Gramm-Leach-Bliley Act requires financial institution to inform clients about information collected about, its storage location, current uses, and enacted security measures. Blaisdell (2012.) The Family Educational Rights and Privacy Act require learning institutions and cloud vendors to obtain student's consent before disseminating their personal data, while Payment Card Industry Data Security Standard enforces layered security, data privacy, and perimeter security among MasterCard and Visa merchants. The ECPA requires cloud vendors to protect electronic communications from disclosure during transit and storage. Patriot Act requires security organs, such as Federal Bureau of Investigation to obtain court orders before accessing business records stored in the cloud. In this regard, cloud providers and customers need to consider their industry and country of operation to identify crucial legislation and policies (Blaisdell 2012).

4.3 CSPM

With the advancement of technological innovation, enhanced computing integration is becoming popular, leading to the utilization of IT in virtually all aspects of society. Trappe and Straub (2018) indicate that computing and communication technologies are responsible for advancement and innovations in different industries, including healthcare, recreation, manufacturing, logistics, and transportation. The enhanced utilization of cyber technologies in different domains eliminates separation barriers due to intensified data sharing, leading to improved cost control, capacity development, and heightened efficiency. Meanwhile, intensified communication and interaction of different industries ensure that cyber threats are universal rather than specific to one industry or area (Trappe and Straub 2018). In this context, the enhanced adoption of cloud in business operation is commensurate with number of unmanaged risks. Subsequently, CSPM

emerges in the business world to enforce security. According to Crowd Strike (2020), CSPM is responsible for automating risk identification and remediation in IaaS, SaaS, and PaaS (Crowd Strike 2020; Trappe and Straub 2018).

4.3.1 What is CSPM

Effective and working cloud computing services require numerous configurations and considerations to provide recommendable level of security to client data and operations. In this context, clouds tend to connect and disconnect numerous networks, challenging the development of effective security models. Crowd Strike (2020) notes that traditional model is highly ineffective due to the absence of protection perimeter, inability of manual processes to deliver required scale or speed, absence of centralization, which limit visibility. KPMG (2018) notes that unique attributes of Cloud computing require distinct security framework and approach. Hence, CSPM describe continuous process for adapting and improving cloud security to reduce effectiveness or success of cyberattacks (Gartner Research 2019). The process provides unique security concept for addressing threats in distributed cloud infrastructure with high level of dynamism. In this regard, CSPM security tools continuously monitor cloud environments to identify issues with security posture and thwart them before occurrence (Crowd Strike 2020; Gartner Research 2019; KPMG 2018).

The deployment and use of cloud computing deliver cost advantage to businesses. However, the need to manage different components and services, including serverless functions, Kubernetes, and microservices, shrink return on investment. Moreover, cybersecurity skills gap is rapidly expanding beyond proportion because new technologies are emerging at higher rate than security professionals. Fugue (n.d.) notes that IaC is becoming prevalent in the marketplace, enabling definition files that are machine-readable to manage and provision infrastructure. In this context, organizations can effectively program in misconfigurations and constrain environmental vulnerabilities that constituted 95% of all security breaches 2018 and 2019, while costing companies approximately $5 trillion (Gartner Research 2019). Meanwhile, typical enterprise cloud is complex and fluid due to lack of visibility, which makes vulnerabilities arising from misconfigurations almost undetectable without sophisticated automation. CSPM emerges in the cloud environment to address cyber threats by intensifying risk monitoring through established

behaviors, such as predicting, responding, detecting, and preventing attacks on assets (Fugue n.d.; Gartner Research 2019).

CSPM focus on specific activities in the cloud computing environment. Fugue (n.d.) indicates that the innovation assesses available encryption on databases, data storage, application traffic, and sensitive data besides identifying liberal account permissions, misconfigured network connectivity, and improper encryption key management. Moreover, CSPM can identify absence of multi-factor authentication in critical system accounts and data storage susceptible to internet threats and network flows. Crowd Strike (2020) notes that CSPM allows management of several virtual networks, projects or accounts through a single console, which foster automatic discovery of change activity, security, networking, metadata, and misconfigurations. CSPM also cloud application configurations with established industrial standards for identification and remediation of security risks in real-time. Thus, the innovation continually monitors database for encryption, backups, and availability to ensure proper authentication is active. Additionally, CSPM constrains developers' mistakes by establishing previews in controlled environment besides automatically remediating unauthorized modifications and erroneous misconfigurations that expose systems to risks (Crowd Strike 2020; Fugue n.d.).

Security teams utilize CSPM to identify cloud threats before their circulating in the entire enterprise environment. As a result, CSPM effectively centralizes visibility and cloud resource control, leading to minimal friction and complexity in accounts or providers, besides reducing operational overheads. Crowd Strike (2020) posits that CSPM unceasingly monitors cloud environment for risks framed by malicious activities through its real-time detection systems (Crowd Strike.) The approach reduces threats and alerts by focusing on vulnerable areas, prioritizing environmental susceptibility, and preventing vulnerable code from progressing in the application development lifecycle. Thus, CSPM is a reliable tool for enforcing real-time threat detection by instituting continuous monitoring and targeted threat identification (Crowd Strike 2020).

4.3.2 AWS and Azure CSPM

AWS CSPM

The migration of organizations to cloud involves distinct decisions on different factors. For instance, the selection of a cloud with suitable CPMS requires the security team to visibility into accounts. AWS allows organizations to embrace multiple account strategies, which allow separation of production, development, and sandbox accounts for limiting blast radius (Dickinson 2019:2). In this regard, security team should evaluate how the AWS provisions will scale with growth. Additionally, organizations need to evaluate other CSPM provisions available through AWS, such as consulting partner opportunities, managed services, licensing, and SaaS (Dickinson 2019:2).

SaaS in AWS allow companies to focus on risks reduction and prevention without incurring significant costs on managing configuration files. Organizations can acquire AWS CSPM licenses from different channels, including private sales by vendors, bring-your-own-license, and AWS Marketplace, but should ensure that the license accommodates required resources or monitored accounts (Dickinson 2019:2). The partners enable organizations to fill knowledge or resources gap in their workforce profiles. The managed security service providers are AWS security subject-matter experts who assist organizations with customization, training, and integration of CSPM into existing AWS accounts (Dickinson 2019:2). Therefore, AWS CSPM features distinct services and capabilities that influence selection and benefits to clients (Dickinson 2019).

AWS CSPM has an extensive range of capabilities, which organizations should ensure meets their security demands. Dickinson (2019:3) notes that AWS CSPM features a feedback mechanism that reports risks associated with work under development, reports for executives, compliance checks to monitor risks associated with cloud footprint, modification tracking of changes in AWS accounts, and inventory for assets. Dickinson (2019.) In this context, individual organizations utilizing AWS CSPM require asset inventory for all running endpoints, enhanced understanding how to add and maintain accounts, DevOps principles for monitoring workloads, understanding of functionality of CSPM providers, and analyst with appropriate authentication and authorization. Consequently, effective selection and deployment of AWS CSPM require potential clients to evaluate its vendor support models, scaling, third-party integrations, ability to customize alerts, and reporting with alternatives available in the market (Dickinson 2019).

Azure CSPM

Azure CSPM provides clients with security and risk management to avoid misconfigurations. Butt (2019) indicates that Azure CSPM is responsible for protecting workloads at scale, continuously assessing, and monitoring security state, and reviewing security recommendations in workloads. Butt (2019) notes that analysis of cloud environment allows description of threat detection, endpoint protection enablement, misconfigured security settings, and missing updates, which enable organizations to prioritize work, reduce vulnerability, and strengthen security posture. Thus, Azure CSPM offers a combination of processes, tools, and technologies for enforcing control and enhance risk management in cloud environment (Butt 2019).

The prevalent threats in the cloud environment include insufficient access control, resource misconfiguration, data leakage, insider threats, compromised accounts, and cloud resources abuse. (Sagir 2021.) Azure features built-in anomaly detection policy, which detects and notifies organizations about multiple delete VM activities, data exfiltration to unsanctioned apps, multiple failed login attempts, and unusual Power BI report sharing, administrative, impersonated, and file sharing activities. Consequently, organizations need Azure CSPM to identify their security posture, track suspicious activities, evaluate security compliance status, and automate policy enforcement, governance control, and protection (Sagir 2021). The enforcement of CSPM in Azure cloud involves collaboration with several stakeholders who offer diverse services for the formulation of consistent and reliable security layer (Sagir 2021).

The enforcement of CSPM involves guided activities in Azure Defender. Diogenes (2021) notes that organizations should begin defining the scope for CSPM by identifying critical requirements, such as roles, data collection, PaaS workloads, operating systems, VMs, and administrative and read access. (Diogenes 2021.) The 30 days trial period for Azure Defender ensure organizations can evaluate its capabilities and efficiencies before actual purchase and deployment. Subsequently, clients should measure success to ensure they have appropriate levels expectation with Azure CSPM. Diogenes (2021) indicates that preparation enables companies to acquire required resources besides changing the operational environment to achieve successful deployment of the Azure CSPM. The implementation and validation include threat detection and response, reducing the attack surface, and security posture management. Therefore, successful deployment and utilization of Azure Defender as the primary Azure CSPM requires coordination of internal and cloud activities (Diogenes 2021).

4.3.3 Capabilities

CSPM providers express varying capabilities in different contexts. As a result, organizations need to evaluate the capabilities to select the most suitable vendor, depending on corporate needs and objectives. Dickinson (2019:4) notes that data retention describes contract language and anonymization of data, which influence storage of indexed data by the CSPM vendor. Organizations should ensure retention policies align with corporate policies while long-term commitments do not adversely affect data or internal systems. Meanwhile, licensing significant influence cost and services received. In this context, customers should consider licensing policies to determine whether CSPM provider offers license per feature used, per resource monitor, or per account monitored. (Dickinson 2019.) Moreover, vendors should ensure administrative costs are minimal because CSPM is a SaaS platform. The administrative responsibility on the client requires evaluation of teams connected with security effort and required internal knowledge (Check Point n.d.). Consequently, CSPM should possess capacity to monitor operations, manage incidences, classify and inventory assets, perform risk identification, and assess compliance policies continuously (Check Point n.d.; Dickinson 2019).

The technical capabilities of CSPM vendors involve account integration, authentication, and API. Clients should evaluate cloud account authentication process and configuration of resources for CSPM to function for assurance that cloud footprint does not enhance cyber risks. Dickinson (2019:4) indicates that federated identity integration and supported authentication standard guarantee secure access to the CSPM. Organizations can effectively disable users when unauthorized to access enterprise cloud environment. Additionally, CSPM vendors should have APIs with appropriate logging, documentation, and access control to ensure clients can access functionality and programmatic data. Meanwhile, CSPM providers should also possess operational and investigational capabilities to promote clients' interests and objectives. (Dickinson 2019.) In this context, CSPM vendor should have adequate functionality monitoring to prevent integration fail, custom alerts to notify customers about certain activities of interest, and reporting and dashboards to articulate the security posture. Users of the enterprise cloud environment should access different reports and granular analytic tool to achieve specific objectives. Additionally, the establishment of vendors' acceptable-use policy and authority to request an investigation promote legality of operations (Dickinson 2019:4). Customers should be familiar with technologies involved in investigation of operations, activities, and processes. Therefore, effective CSPM should feature a combination of business,

technical, operational, and investigational capabilities to promote resilience, efficiency, competitiveness, and sustainability in the market (Dickinson 2019).

4.3.4 Benefits

With enhanced cloud computing in the business world, security breaches are becoming increasingly popular. (Crow Strike, 2020.) As a result, cloud providers focus on securing infrastructure cloud stack while clients are responsible for securing applications and data. CSPM coordinates the activities of cloud providers and clients to achieve heightened cloud security. Moreover, the technological innovation continuously checks for misconfigurations that enhance data leakage and breaches in cloud environment. In this context, companies can identify cloud misconfiguration vulnerabilities and continually amend their security provisions to enhance protection of their data besides reducing their vulnerability to cyberattacks (Crowd Strike 2020).

Organizations are vulnerable to intentional and unintentional risks. Although unintentional mistakes expose businesses to significant risks, CSPM chiefly focuses on malicious insiders and outside attacks. Crowd Strike (2020) indicates that CSPM automatically prevents misconfigurations, leading to accelerated time-to-value in addition to facilitating unified visibility across multi-cloud environments that promote protection of critical cloud services and continuous compliance with established standards. As a result, organizations do not need to check multiple consoles from different vendors to enforce data normalization (Crowd Strike 2020).

CSPM is highly effective for reducing distraction and alert fatigue. The use of AI in the cloud environment minimizes false positives responsible for distracting users from constructive activities and generating numerous unnecessary alerts. Additionally, security teams obtain alerts from a single system, leading to enhanced SOC productivity. Crowd Strike (2020) notes that threat detection induces automatic corrective actions because CSPM is unceasingly monitoring and evaluating cloud environment for compliance. Moreover, CSPM's scans of cloud infrastructure effectively identify concealed threats, resulting in shortened times for remediation (Crowd Strike 2020).

CSPM promotes access to diverse security tools and measures, which effectively enhance data protection. Brooks (2020) notes that CSPM promote compliance with

standards, such as PIC, SOC2, and HIPAA besides automatically remedying some misconfigurations. The continuous monitoring of the cloud environs detects policy violations. Additionally, the integration of security procedures into DevOps processes enable IT team to simultaneously address service configurations and security settings (Brooks 2020).

4.4 Reference Architectures

Reference architectures utilizes the essence of established architectures, current needs, and evolution to develop new and unique systems. Cloutier et al. (2010:14) describe reference architectures as set of patterns partially or completely instantiated for use in technical and business context for supporting distinct use. In this regard, the concept comprises design pattern which describe appropriate technology and architectural principles, which are rules and guidelines for governing scalable designs (Lai 2002). Additionally, supporting software tools for describing available product solution options, underlying architecture framework that defines the logical and physical components constituting developmental processes and business services, and verified process for depicting architecture. Consequently, CSPM features distinct reference architecture for enforcing security in cloud environment (Cloutier et al. 2020; Lai 2002).

4.4.1 Microsoft Cybersecurity Reference Architecture

The Microsoft Cybersecurity Reference Architecture (MCRA) is a conglomeration of cybersecurity capabilities issued by Microsoft and how they interrelate with each other to enforce cyber security. Figure 4.4 presents the reference architecture. Al-Beruni (2020) notes that critical components include Azure Sentinel, Azure Monitoring, Azure Log, Azure Information Protection, Intune, Azure Active Directory, Azure Key Vault, and Azure Policies. In this regard, elements of MCRA have specific roles in threat detection, protection, and cross platform visibility (Al-Beruni 2020).

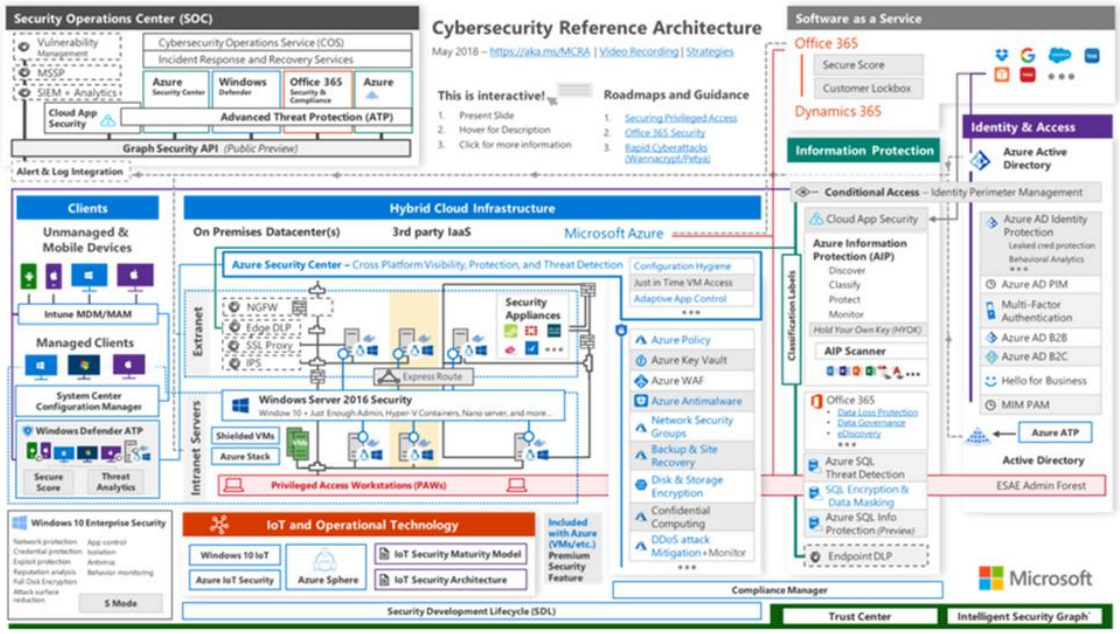


Figure 4. 5 MCRA

MCRA provides the basic template for implementing an effective security architecture in cloud computing. Organizations utilize MCRA to define the target state for existing and planned cybersecurity capabilities (Simos 2018). In this regard, the architecture enables businesses to identify all operation aspects, leading to effective protection operational environment spanning from IoT, operational technology, clouds, mobile devices, to premises. Meanwhile, MCRA is a comprehensive description of Microsoft capabilities in cybersecurity. (Simos 2018.) As a result, organizations can utilize it as comparison reference for security capabilities to enhance their security understanding. With information on current cybersecurity status, companies effectively identify duplication of efforts besides identifying aspects that require enhancement. Thus, MCRA enhances resource optimization by ensuring individual organizations invest in appropriate security measures, policies, and tools without duplication (Simos 2018).

MCRA presents Microsoft capabilities using an approach that enhances learning and in-depth understanding. MCRA provides an interface that focuses on customer empowerment through eased learning. Moreover, MCRA's learning tool prepare individuals for career in cyber security. Simos (2018) notes that the architecture uses visual to highlight crucial integration points where Microsoft requires or embraces partner capabilities. For instance, customers can enforce conditional access, advanced threat protection, SQL data masking, DDOS attack mitigation, disk and storage encryption, and backup and

recovery sites at instances, such as DLP integration, Security Appliances in Azure, and SIEM/Log integration (Al-Beruni 2020; Simos 2018). In this context, customers can save time and cost during integration of additional layers or software in MCRA (Al-Beruni 2020; Simos 2018).

4.4.2 Azure Security Benchmark v2

The Azure Security Benchmark (ASB) is security tool provided by Microsoft for improving services, data, and workload security on Azure by prescribing recommendation and best practices. (Balwin, 2020.) The benchmark includes Microsoft Security Best Practices, Azure Well-Architected Framework, and Cloud Adoption Framework. In this regard, ASB effectively formulates recommendations and guides users on workload security in cloud-centric control areas. The prescribed controls align with NIST and CIS Controls Version 7.1. Baldwin (2020) notes that ASB features network security responsible for securing and protecting Azure networks from external threats. The controls focus on constraining cyberattacks and formulating secure connections. The subsequent identity management utilizes Azure Active Directory to protect identity through established practices. In this context, ASB is a crucial tool for enforcing cybersecurity through policies and control practices (Baldwin 2020).

ASB fosters cloud security through asset management, data protection, privileged access, incident response, and threat detection. (Balwin, 2020) The privileged access involves controls for regulating access to Azure tenant and resources, while data protection safeguards data during storage or transit using authorized access mechanisms. Asset management in ASB promote security visibility and governance through management of approval for resources and services. Baldwin (2020) threat detection and logging controls of ASB collect and store critical logs for effective remediation, investigation, and detection of cyberattacks and threats. Meanwhile, incident response focuses on containing, analyzing, detecting, and preparing appropriate containment measures. Baldwin (2020). Vulnerability management improves Azure security posture by enhanced trailing, recording, and fixing susceptibility. Meanwhile, endpoint security provides anti-malware service and endpoint detection and response, while backup and recovery perform, validates, and protects data and backup configuration. ASB also involves governance and strategy that provide coherent security strategy and sustain security assurance (Baldwin 2020).

4.4.3 AWS Well Architected Framework

AWS Well-Architected Framework enables customers to understand the benefits and costs of developing systems on AWS. (Amazon Web Services 2021.) In this regard, customers can effectively compare their architectures with established standards to identify aspects that require enhancement. Consequently, organizations intending to utilize AWS rely on the framework to avoid intuitions on capacity needs, test systems at production scale, ease architectural experimentation, embrace evolutionary architectures, improve security through game days, and drive architectures using data (Amazon Web Services 2021:5). Therefore, AWS Well-Architected Framework is a combination of diverse tools, including AWS Well-Architected Tool, AWS Well-Architected Labs, AWS Cloud Compliance, and AWS Partner Network, for adding design and operation of cloud workloads (Amazon Web Services 2021).

AWS Well-Architected Framework focuses on recognized for establishing operational excellence. According to Amazon Web Services (2021), operational excellence enables organizations to run workloads, support development, continuously improve supporting processes, and gain insight into internal operations be formulating best practices, design principles, and questions that deliver business value. The security pillar for AWS Well-Architected Framework focuses on data protection strong identity foundation, enhanced traceability, automated security best practices, preparation for security events. Amazon Web Services (2021) indicates that reliability focuses on the ability of workload to function correctly and consistently due to automatic recovery from failure, tested recovery procedures, managed change in automation, and horizontal scaling. (Amazon Web Services 2021.) Meanwhile, performance efficiency fosters the proficient use of computing resources to marinating efficiency with changing demand and evolving technologies due to use of serverless architectures, democratization of advanced technologies, and enhanced experimentation. Cost optimization in AWS Well-Architected Framework delivers business value at minimal cost due to adoption of consumption model, implementation of cloud financial management, and measurement of overall efficiency (Amazon Web Services 2021).

5 CSPM Practical Assessment

5.1 Assessment

5.1.1 Microsoft Azure Services and Platform Assessment

This assessment evaluated Azure and Microsoft Office 365 for threats and vulnerability. The initial goal was to identify the current status of the cloud environment. However, the assessment addressed the gaps and security risks for Azure services and platform only because no critical or medium security threats were found for Microsoft Office 365 during the evaluation. All feasible threats on Security Center for remediation identified and reported.

5.1.2 Pre-Assessment State

Microsoft's Cybersecurity Architecture was set to default for the assessment. Figure 5.1 presents the initial interface of Microsoft's Cybersecurity Architecture. The interface combines all services from Microsoft both active and inactive. In this context, running an audit for Azure describes vulnerability levels of all the activated services. The embedded auditing tools also evaluates integrated third-party services to provide a comprehensive analysis of the cloud environment.

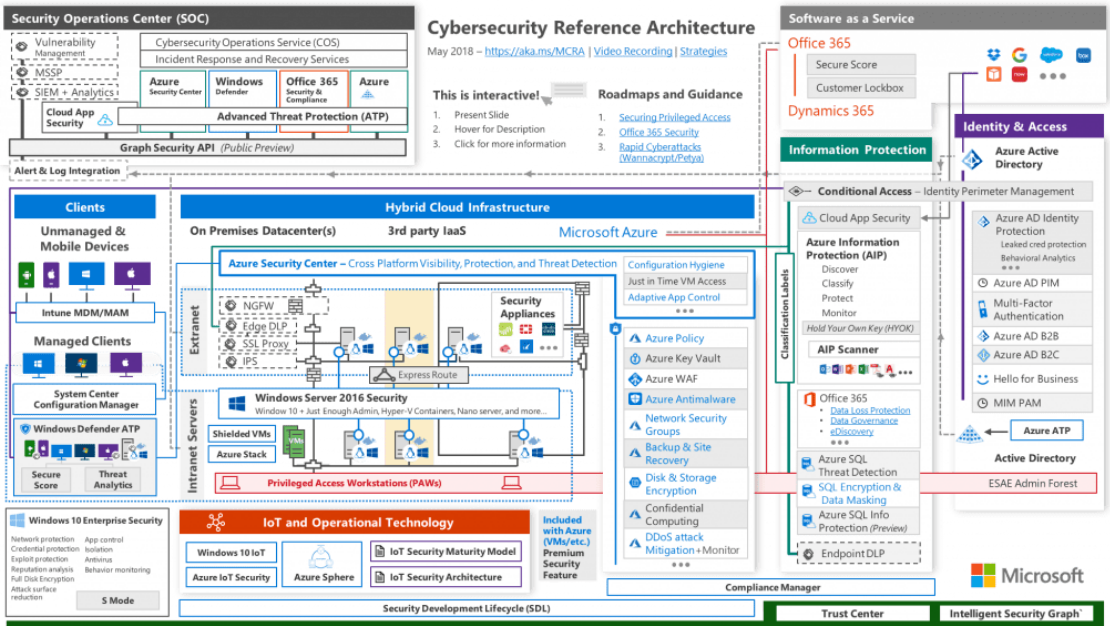


Figure 5. 1 Pre-assessment state

5.1.3 Post-Assessment State

The assessment of the company cloud environment generated a comprehensive report on vulnerabilities and threats. Figure 5.2 shows post assessment state according to Microsoft's Cybersecurity Architecture. The interface describes all the services evaluated during the audit. In this context, the report on Microsoft's Cybersecurity Architecture interface describes Azure Sentinel, clients, operating system, hybrid cloud infrastructure, SaaS, IoT and operational technology, information protection, and identity and access. In this case, the assessment considered enabled features and default features marked with green buttons on Microsoft's Cybersecurity Architecture interface. The assessment includes all the security features and recommends the enablement of those that were disabled to be enabled as per Microsoft best practice. Consequently, the assessment was informative and descriptive to the readers to enhance informed decision-making on suitable security models and mechanisms.

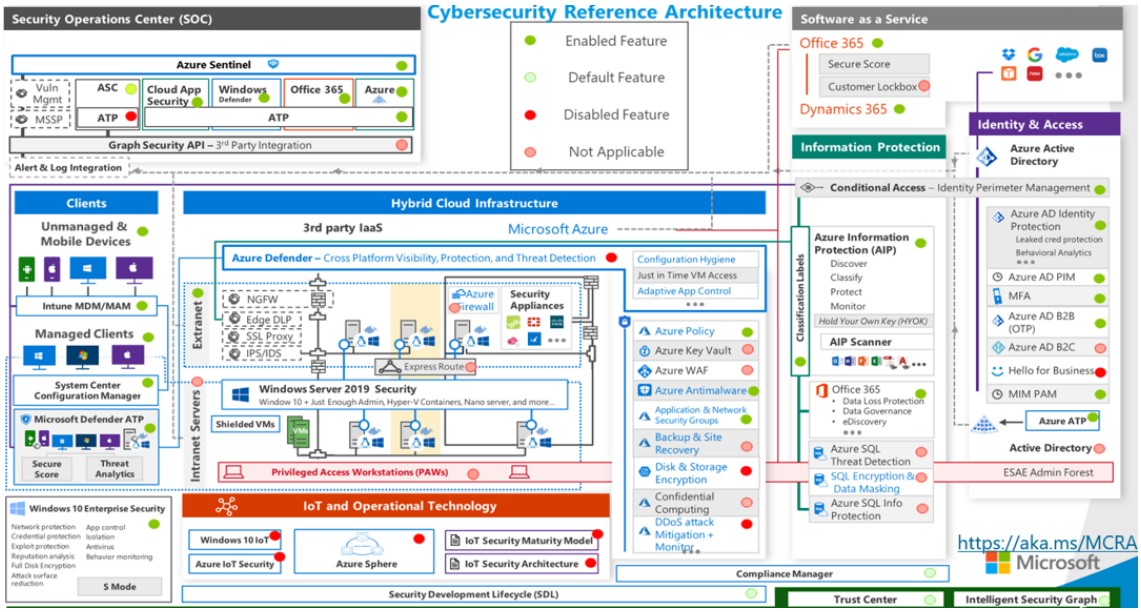


Figure 5. 2 Post-assessment state

5.1.4 Security Score Classification Security Center

The assessment tool identified the security score and the Azure status of the entire cloud environment. Figure 5.3 shows the security score and compliance level of Azure resources and services with Microsoft security recommendations. However, the low score does not necessarily translate to highly vulnerable system. In this context, some of those recommendations might not be implemented as per design and/or with reasonable business justification provided by the company. The company chooses the most appropriate security feature for its data and system rather than solely relying on Microsoft security recommendations.

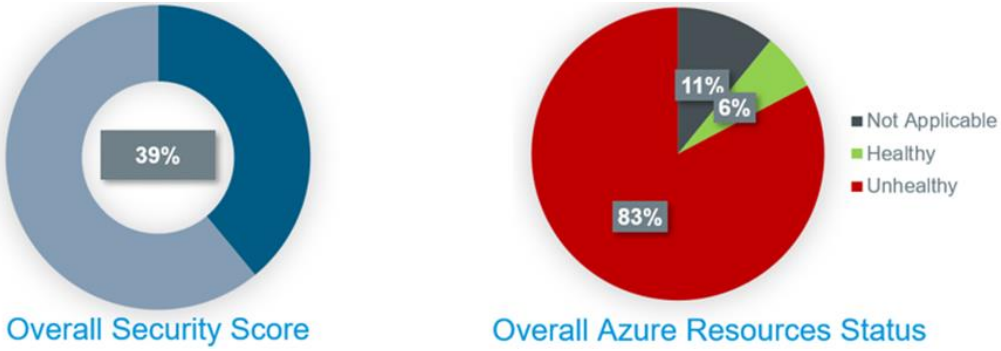


Figure 5. 3 Security score of the company's cloud environment

5.1.5 Findings Overview

The established security features and threat detection mechanism involves multifaceted strategy. Figure 5.4 describes the security components found on Microsoft's Cybersecurity Architecture. Microsoft recommends the enabling and utilization of all the services. However, individual demands of a company and the required security level dictate the activated services. Therefore, the assessment considered all the services independently to determine whether the individual vulnerability level has significance on the company's cloud environment. In this context, workshops explained and justified the need to disable some services or disregard their recommendation.

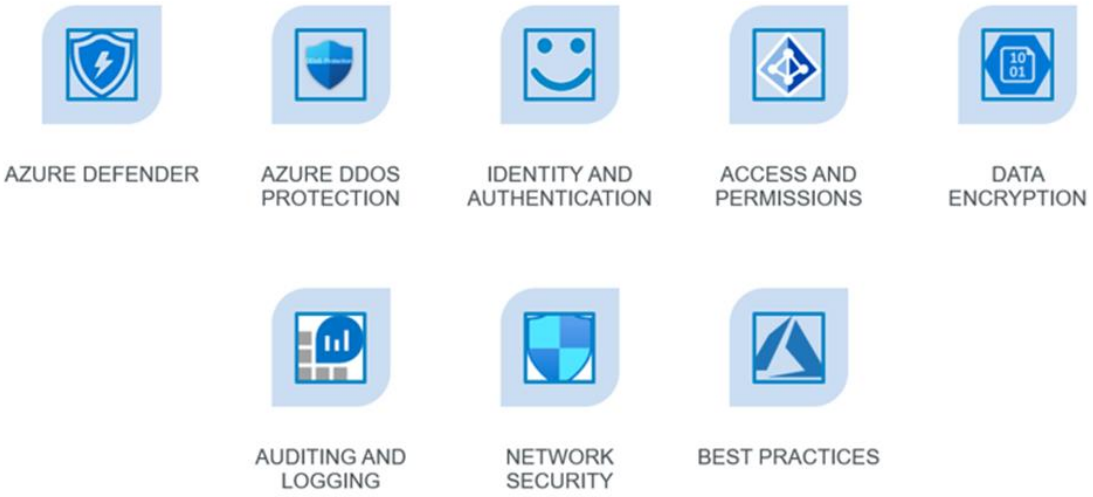


Figure 5. 4 Overview of assessment findings

5.1.6 Azure Defender and SIEM

The assessment found that the company had a disabled Azure Defender for servers. Figure 5.5 shows that disabling the service made the threat to servers unmitigated. The assessment tool considered the action severe with high impact on server security. The company can remediate the situation by enabling Azure Defender.

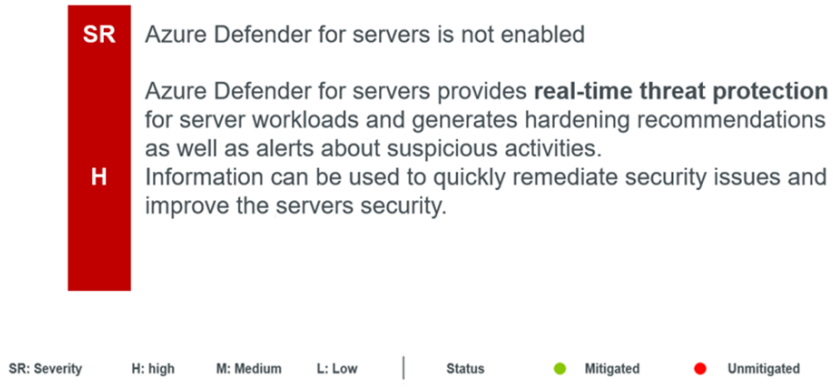


Figure 5. 5 Azure Defender for servers

The company had disabled Azure Defender for App Services during assessment. Figure 5.6 illustrate the phenomenon had was severe and exposed web apps to high risk of

attack. Thus, the disabling of Azure Defender for App Services made threat to common web apps unmitigated.

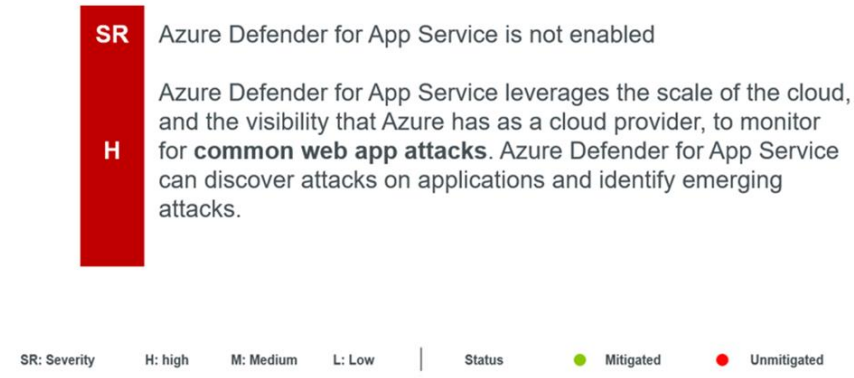


Figure 5. 6 Azure Defender for App Services

The company had not enabled Azure Defender for App Services for container registries, exposing them to severe threats with high impact. Figure 5.7 illustrates that the missed scan for security vulnerabilities in the registries, using Azure Defender made common risks unmitigated.

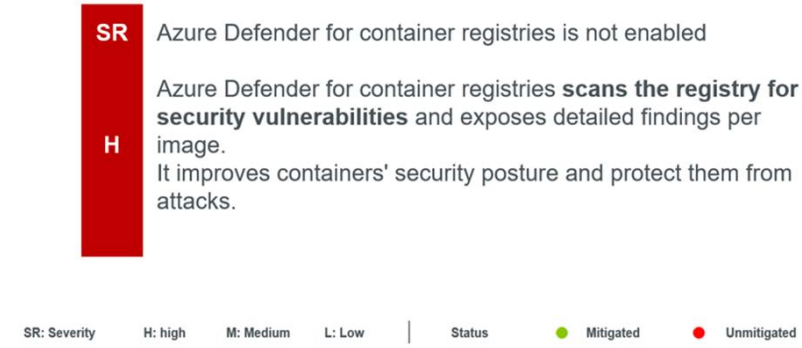


Figure 5. 7 Azure Defender for container registries.

The cloud environment for the company had not enabled Azure Defender for Kubernetes. The absence of real-time protection for the containerized environment featured unmitigated risks with significant severity and high risks. Figure 5.8 shows the risk factor to the cloud environment due to disabled Azure Defender for Kubernetes. The company can enhance container security by enabling the service.

Figure 5. 8 Azure Defender for SQL and SQL database server.

5.1.7 Azure DDoS Protection

The company had not enabled Azure DDoS Protection Standard, resulting in unmitigated risks with high severity on the operation of the business. Figure 5.10 illustrates that the failure to enable the service exposes virtual networks with firewalls and applications to significant threats. By enabling the service, the company secure cloud environment by mitigating protocol and volumetric attacks.

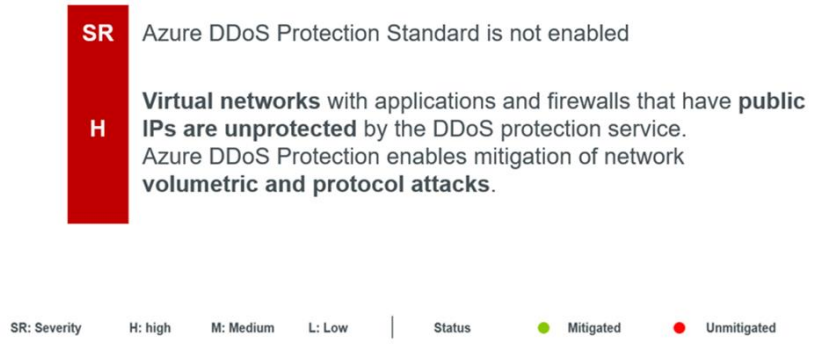


Figure 5. 9 Azure DDoS Protection Standard.

5.1.8 Identity and Authentication

The company had not enabled Windows Hello for Business during the onset of the assessment. Figure 5.11 shows the company was exposed to medium severity and attracted a significant level of unmitigated risks. In this regard, the company lacked substantial assurance level and usefulness of administrator authentication. Thus, the cloud environment was vulnerable to phishing and replay attacks due to password reuse. In some instance, Azure cloud fails to request passwords.

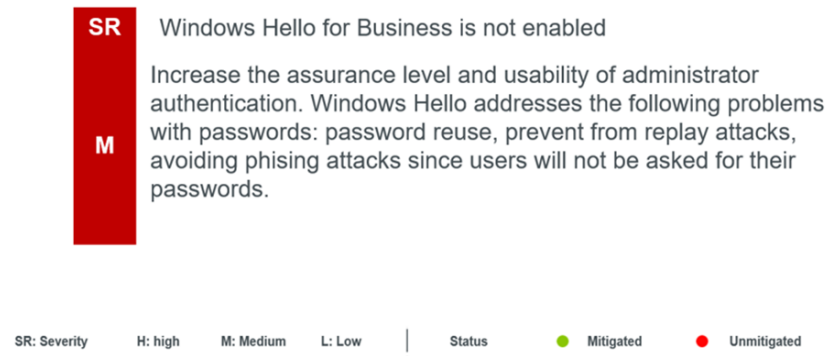


Figure 5. 10 Window Hello for Business.

5.1.9 Access and Permissions

The cloud environment for the company allowed public access to storage account. Figure 5.12 shows that the permission generated medium severity due to considerable level of unmitigated risks. The company focused on convenience instituted by anonymous public read access to blobs and containers, while disregarding risks created by anonymous access. In this context, unauthorized user or hacker could masquerade as genuine user without identification due to the public access.

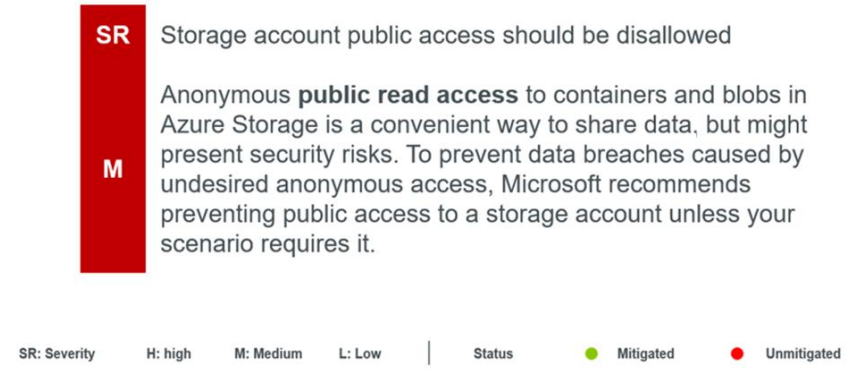


Figure 5. 11 Public access to storage account.

The company does not have established strategy for managing identity on the web app. As a result, the cloud environment is exposed to medium severity by the unmitigated risks (see Figure 5.13). Meanwhile, identity management on Azure cloud abolishes the need for credential management in Azure AD, leading to enhanced time saving among developers when utilizing cloud services.

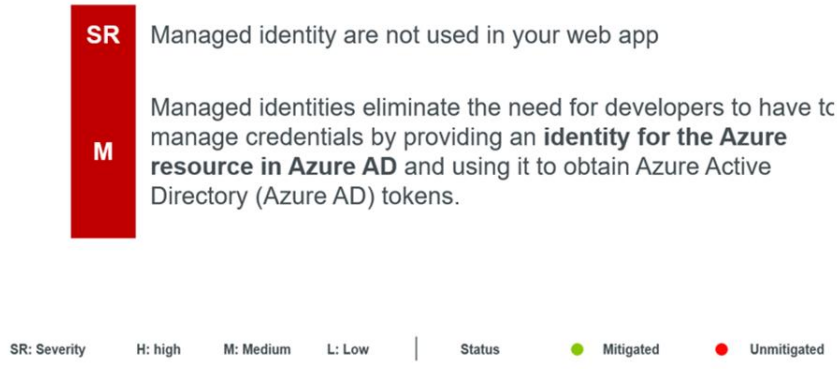


Figure 5. 12 Identity management in the web app.

The company does not remove deprecated accounts from its subscription. Figure 5.14 presents the medium severity emanating for substantial unmitigated risks. In this context, the failure to remove or delete user accounts blocked from signing in creates enhanced vulnerability to cyber threats. Hackers can target the accounts to gain access to the enterprise cloud environment without being detected.

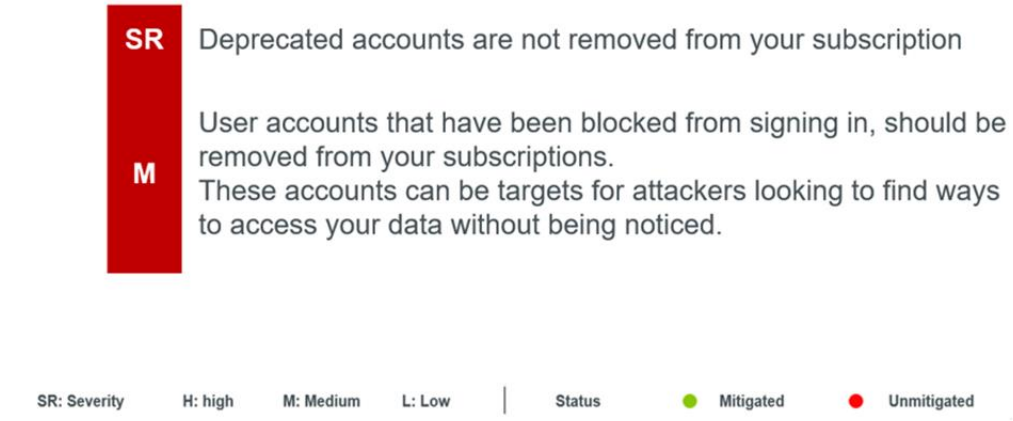


Figure 5. 13 Removal of deprecated accounts from subscription.

Data Encryption

The company had not standardized disk encryption on virtual machine during the assessment. The failed encryption instituted numerous vulnerabilities with high severity (see Figure 5.15). Azure cloud relies on ADE for encrypting Windows and Linux virtual machines to protect data and enforce integrity. Moreover, it articulates end-to-end data encryption using Linus' DM-Crypt system and BitLocker Device Encryption for Windows.

Figure 5. 14 Disk encryption on virtual machines.

The company during the assessment did have standards for encrypting automation account variables. The unmitigated risks had high severity due to exposure of sensitive to

threats (see Figure 5.16). Meanwhile, the encryption requires declaration during the creation of automation account variables. Hence, the company should delete the variables and declare encryption during recreation.

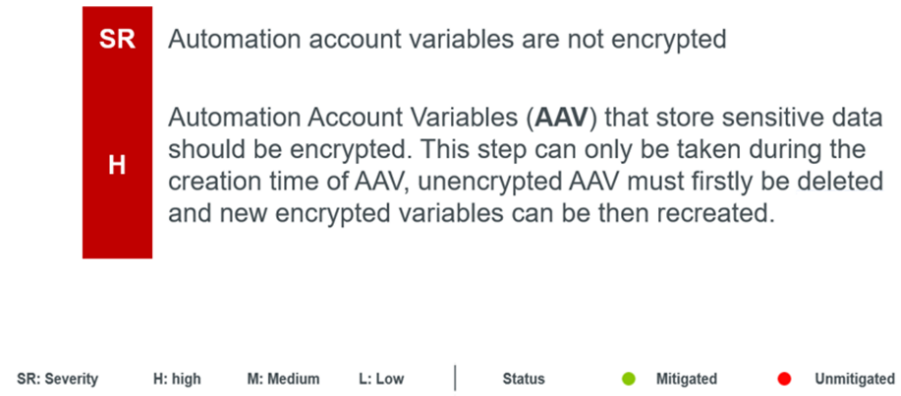


Figure 5. 15 Encryption of automation account variable.

Company does not have enabled secure transfer to storage accounts. Figure 5.17 shows that disabled feature exposes the cloud environment several unmitigated risks with high severity. By enabling secure transfer, the company will enhance data protection from network threats, such as eavesdropping.

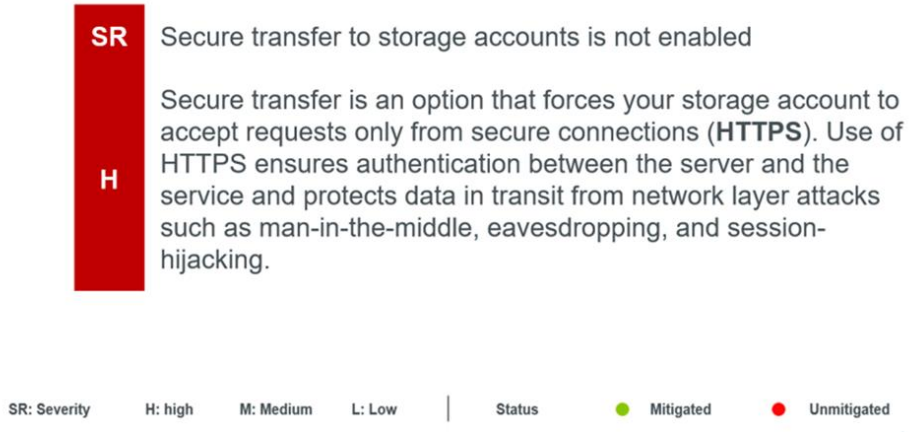


Figure 5. 16 Secure transfer for storage accounts.

The company during the assessment had not enabled secure transfer for web applications. The absence of the feature exposed the cloud environment to high severity from the unmitigated risks (see Figure 5.18). As a result, the company is not using HTTP to secure connection and authentication.

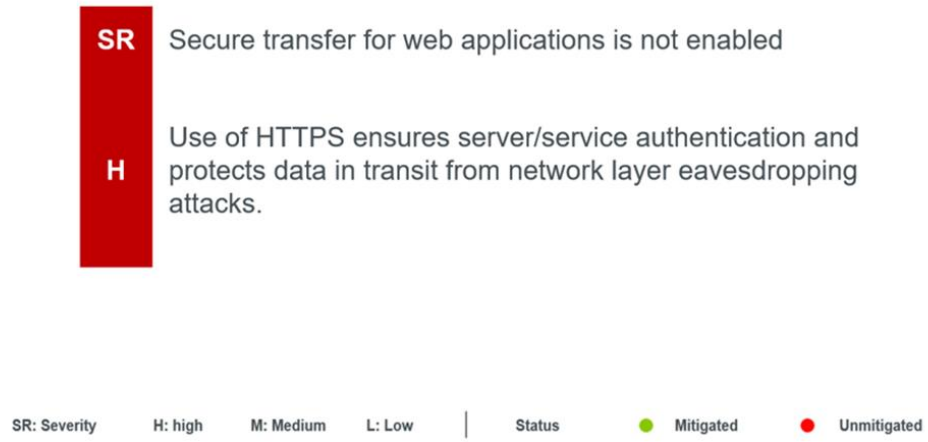


Figure 5. 17 Secure transfer for web applications.

5.1.10 Auditing and Logging

The company had not installed Log Analytics for collecting log and metric data from security configurations and events for analysis and automation using SIEM. As a result, the cloud environment was highly vulnerable to numerous unmitigated risks (see Figure 5.19). The company should install Log Analytics manually on the provisioned servers because they are not installed automatically.

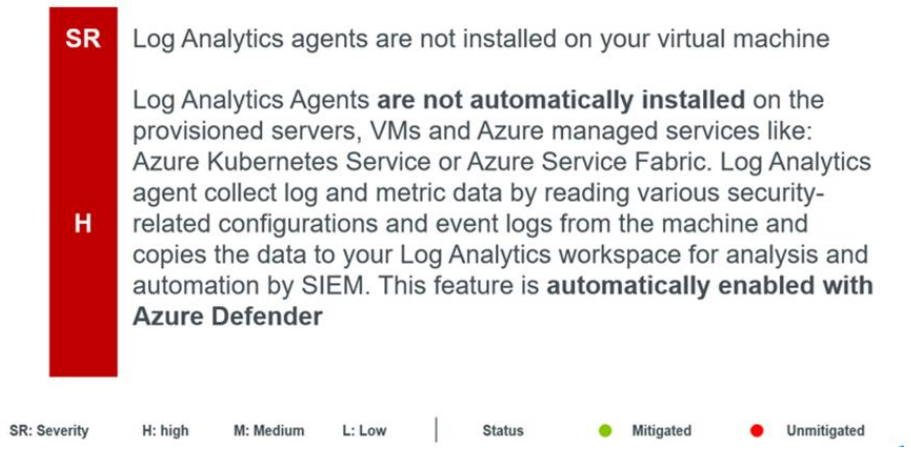


Figure 5. 18 Log Analytics agents.

Company had not enabled diagnostic logs in App Service. As a result, Figure 5.20 shows that the unmitigated risks exposed Azure cloud to medium severity. The enabling of diagnostic longs allows recreation of trail during incidents that compromises the network.

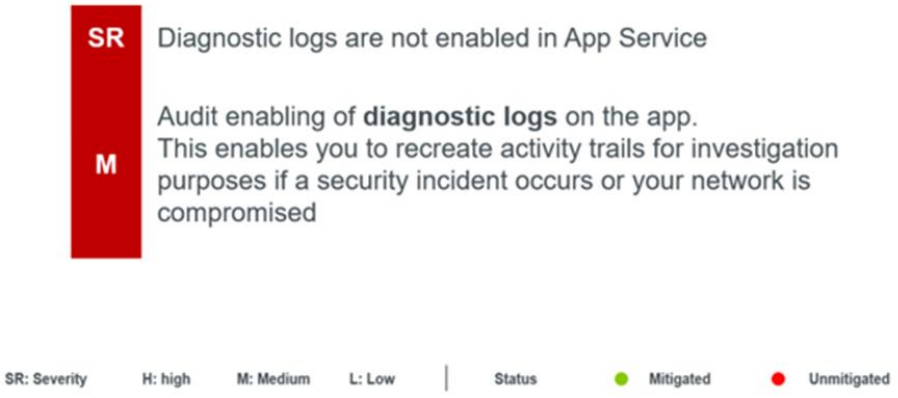


Figure 5. 19 Diagnostic logs.

5.1.11 Network Security

The company had not protected all virtual networks with Azure Firewall. Consequently, the cloud environment was exposed to low risks (Figure 5.21). Azure Firewall restricts access to private networks.

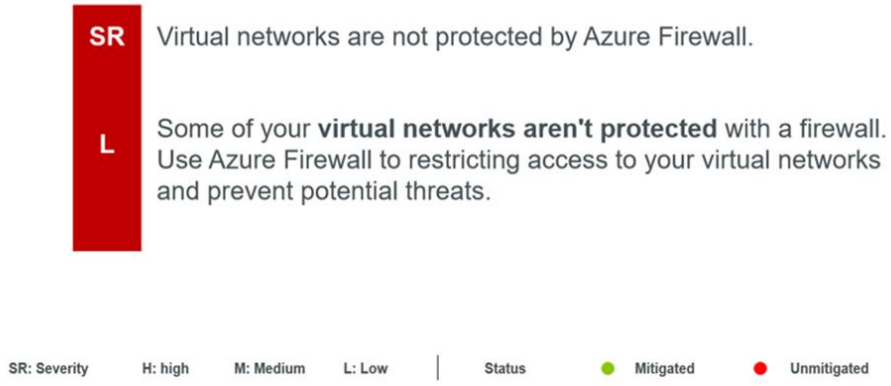


Figure 5. 20 Azure Firewall on virtual networks.

The company had its cloud environment vulnerable to high severity from unmitigated risks. Figure 5.22 shows that the company had not installed Endpoint Protections on VMs leading to high susceptibility of the internet-facing virtual machines. In this regard, the company lacked NSG that provide access-control lists.

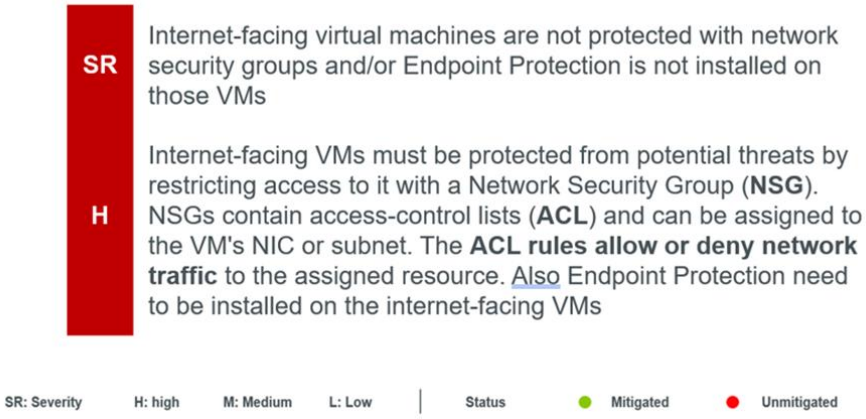


Figure 5. 21 Endpoint protection of internet-facing VMs.

The company maintained open management ports. The feature exposed the cloud environment to high risks because opened remote management ports attract numerous unmitigated internet-based attacks (see Figure 5.23). Hackers tend to use brute force to gain administrator's access rights.

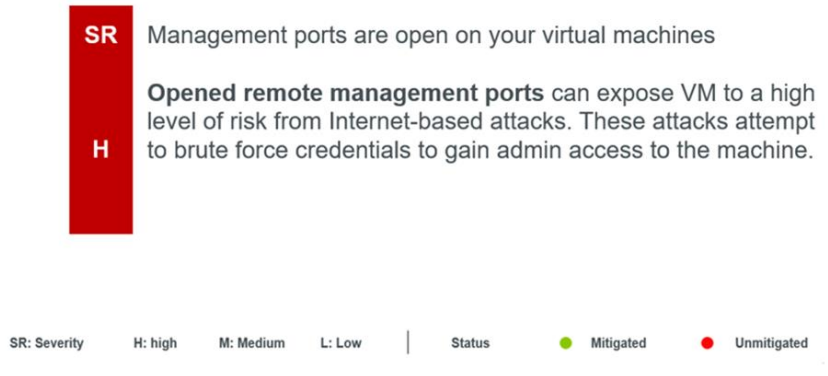


Figure 5. 22 Management ports in VMs.

The company had several instances of permissive network ports. The company is highly vulnerable to numerous risks due to unmitigated risks (see Figure 5.24). In this regard,

the company should ensure all network ports are restricted to network security groups for in-house VMs.

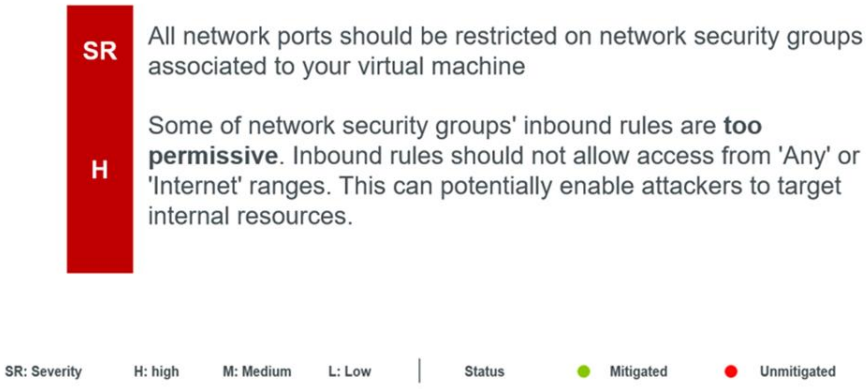


Figure 5. 23 Permission on network ports.

5.1.12 Best Practices

The assessment of the cloud environment found that the company had several instances of best practices. For instance, Figure 5.25 shows the cloud environment had enable MFA, Figure 5.26 shows remote debugging was, Figure 5.27 shows successful migration of VMs and storage accounts to new Azure Resource Manager, Figure 5.28 shows protection of non-internet facing VMs, and Figure 5.29 shows disabled IP forwarding on VMs. Consequently, the company had reliable level of mitigation of threats in the cloud environment.

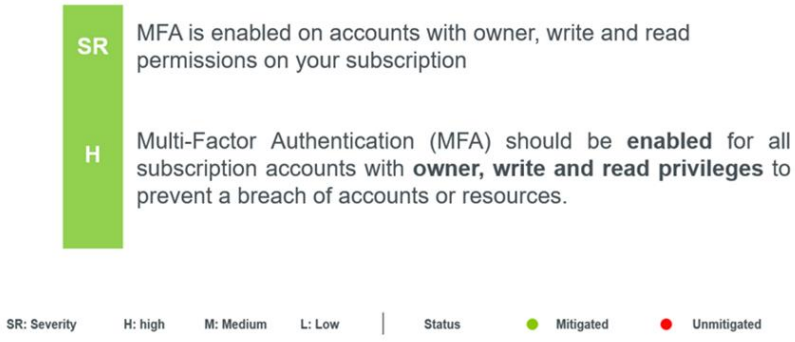


Figure 5. 24 MFA accounts read and write permissions.

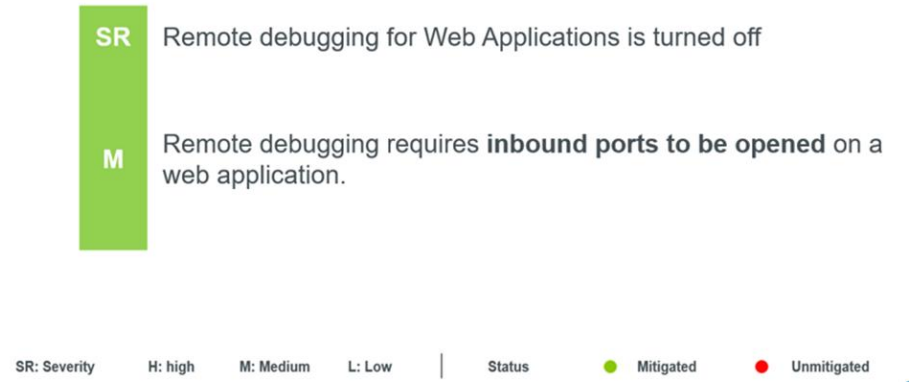


Figure 5. 25 Remote debugging for web applications.

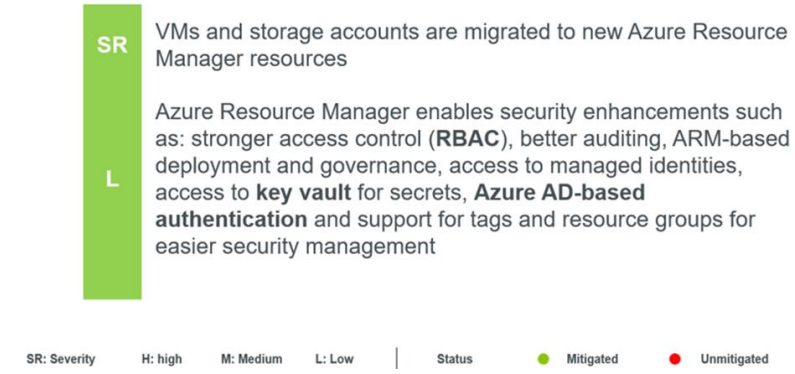


Figure 5. 26 Migration of VMs and storage accounts to new Azure Resource Manager.

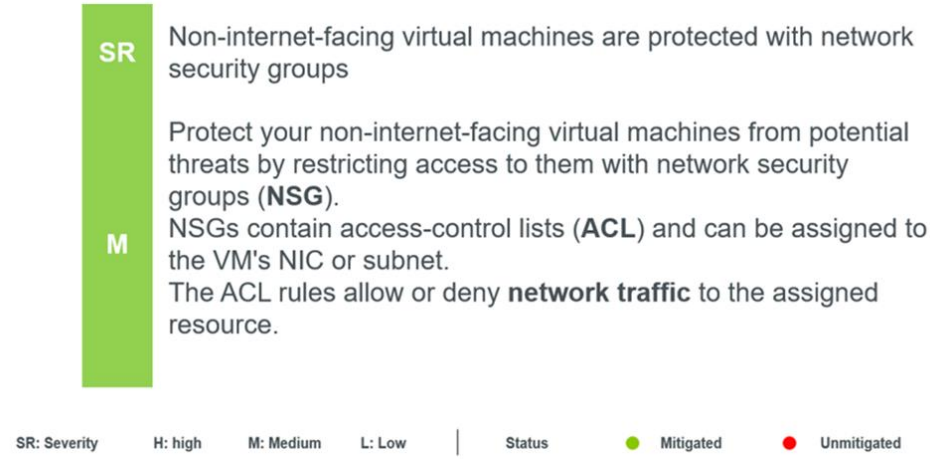


Figure 5. 27 Protection of non-internet facing VMs.

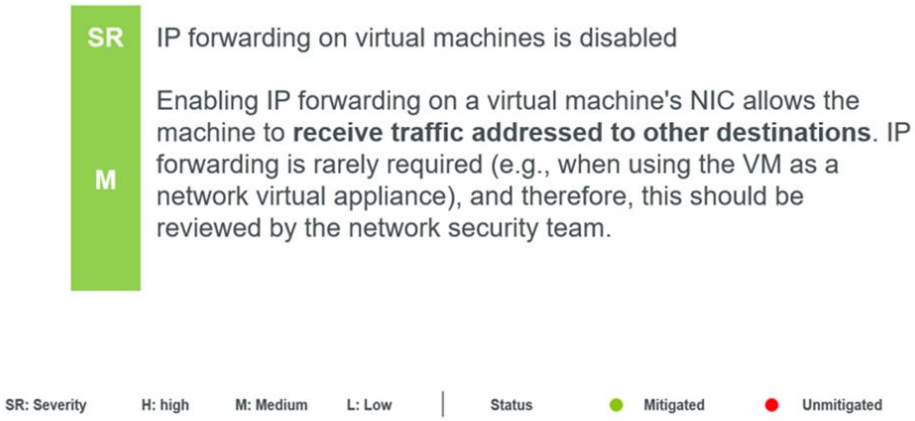


Figure 5. 28 IP forwarding on VMs.

5.2 Remediation Plan

The assessment of the company's Azure cloud identified the main vulnerabilities. Subsequently, the remediation plan focuses minimizing susceptibility by embracing the best practices. The assessment report guides the formulation and implementation of a set of actionable remediation aiming to leverage the security level for Microsoft Azure services and tools readily available and accessible to the company. Moreover, other recommendations in the remediation plan introduce necessary Azure security upgrades and/or bundles that deliver the desired security level suitable for the company's current operations in the cloud. Meanwhile, the assessment report did not identify security threats and gaps in Microsoft Office 365, meaning that the remediation activities and practices focus on the security risks identified for Azure services and platform through assessment and gap analysis.

Azure services and platforms illustrated significant exposure to diverse risks in distinct domains. Table 5.1 shows the assessment results of the company's Azure cloud security risks grouped into the identified risk domains. The vulnerabilities have unique severities to the company's cloud environment.

Table 5.1. Risk domains and their severities.

Domain	Severity
Azure Defender	High
Azure DDoS Protection	High
Access and Permission	Medium
Network Security	High
Auditing and Logging	High
Miscellaneous	High
Data Encryption	High
Identity and Authentication	Medium
IoT Security	High

The risk assessment for Azure cloud spanned across three subscriptions currently contained under the “company.com” tenant, namely the company Microsoft Azure Enterprise, the company DMZ, the company Network. Consequently, the assessment relied on the established resources in the company’s IT environment, including the security findings and recommendations from Azure Security Center, Microsoft Cybersecurity Reference Architecture as the reference standard for basing the required gap analysis, and active discussion through workshops involving project seniors and stakeholders to validate the security risks and related findings.

5.2.1 Overall Security Score

The current overall security score reported by Azure Security Center during the assessment was 39%, reflecting an enhanced need to consider remediation activities and procedures for mitigating security-related risks in the vulnerable domains. Meanwhile, the assessment findings list a detailed description of the security risks and name the “unhealthy” Azure resources for each domain. In this regard, the remediation plan focuses on recommending solutions rather than their implementation. Although the application of the recommended remediation should elevate the overall security score to an average of 75%, it will not address resources in an unhealthy state. The assessment reported illustrated that 83% of the used resources are in an unhealthy state. Nonetheless, the referred security score implies how compliant are the currently used Azure resources and services with Microsoft security standards and recommendations. In this context,

some recommendations might not be implemented per the design and/or with a reasonable business justification that the company embraces in its operations and IT infrastructure management. Hence, the company needs a multifaceted strategy for minimizing vulnerabilities to the lowest possible level, which aligns with established operational and management standards.

5.2.2 Risk Level

The overall security risk for the company is high. Although some of the baselines are already in place, such as Azure AD tiering, Defender ATP plans for Office 365, Windows, MFA best practices, MCAS, SIEM, and AIP labeling, some operational risks need addressing to minimize the effectiveness of possible attack vectors. Moreover, some operational risks require the upgrading of distinct Azure functional security tools to articulate effective monitoring and logging capabilities to the current the company's platform.

5.2.3 Remediations

The remediation activities and procedures require an investment of time and resources. the company should commit optimum resources to obtain the best results and consequently reduce vulnerabilities of its Azure cloud. Table 5.2 summarizes the estimates of required remediation effort across the risk domains in terms of use impact, required man-days, and workstream. The successful coordination and articulation of the remediation efforts will provide the company with short-term, medium-term, and long-term benefits.

Table 5.2. The required remediation efforts to enhance the company's Azure cloud.

Domain	Severity	User Impact	Man-Days	Workstream	Roadmap
Azure Defender	High	Low	15	Short-Term	Recommended as a next step or successor project (proposed as 90 Man-Days project extension)
Azure DDoS Protection	High	Low	13		
Access and Permission	Medium	Low	12		
Network Security	High	Low	13		
Auditing and Logging	High	Low	10		
Miscellaneous	High	Low	11		
Data Encryption	High	Medium	16	Mid-Term	
Identity and Authentication	Medium	High	>90	Long-Term	Future Projects
IoT Security	High	High	>90		

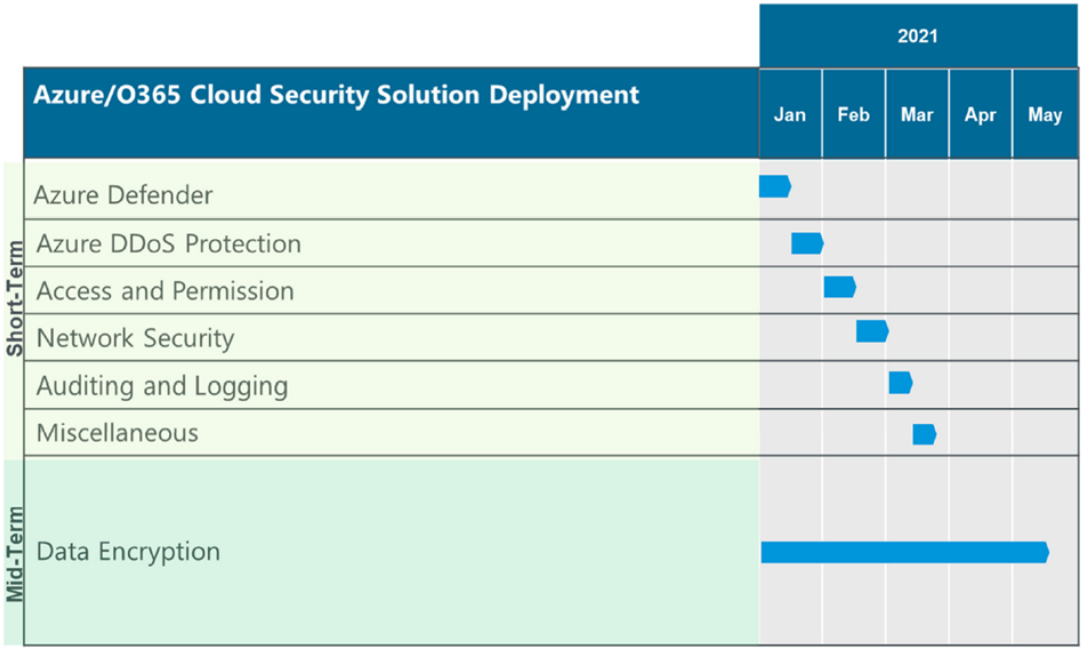
Practical solutions for reducing computing and cloud vulnerabilities require enhanced time planning. Reliable timing considers available resources and requires implementation efforts to ensure the project is successful without increasing susceptibility. In this regard, the remediation action for the company involves three workstreams that present an estimation of the time needed to achieve the best results (see Table 5.3). The workability of the workstream relies on the company's commitment to providing the required resources without delays or coordination breakdown.

Table 5.3. Workstream for implementing remediation actions at the company.

Workstream	Man-Days	Description
Short-Term	30 – 60 Days	This group of remediating actions shall ensure mitigating risks with high security impact and less user impact in a short time to boost the security score by gaining the quick wins. Outcomes shall be reached **in 60 days** after applying the remediation actions.
Mid-Term	60 – 90 Days	This group of remediating actions shall enhance the overall security score. They ensure mitigating security risks with high security impact and medium user impact in a moderate amount of time. Outcomes shall be reached **in 90 days** after applying the remediation actions.
Log-Term	6+ Months	Those are the remediating actions that might require Enterprise-wise hardware, software and/or service licenses purchases. They might also involve relatively higher costs and hence a slightly longer process for planning or decision-making.

Effective coordination of resources and effort produces optimum benefits. In this context, combining both short-term and mid-term remediation into one implementation project and proposing a 90-Man-Days extension to get them simultaneously delivered, as illustrated in Table 5.4, provide tangible benefits with moderate budgeting. The implementation roadmap ensures the company considers all remediation actions as components of a single multifaceted strategy rather than distinct projects.

Table 5.4. Implementation roadmap for short-term and mid-term remediation actions.



The effort estimation for implementation of mid-term remediation actions shall not extend for the entire 90-Man-Days period. In this regard, Table 5.4 shows an early starting point to address the expected “Medium” user impact. The implementation shows suggested remediation plans fit into one 90-Man-day project by describing the latest completion time.

5.2.4 Issue Level

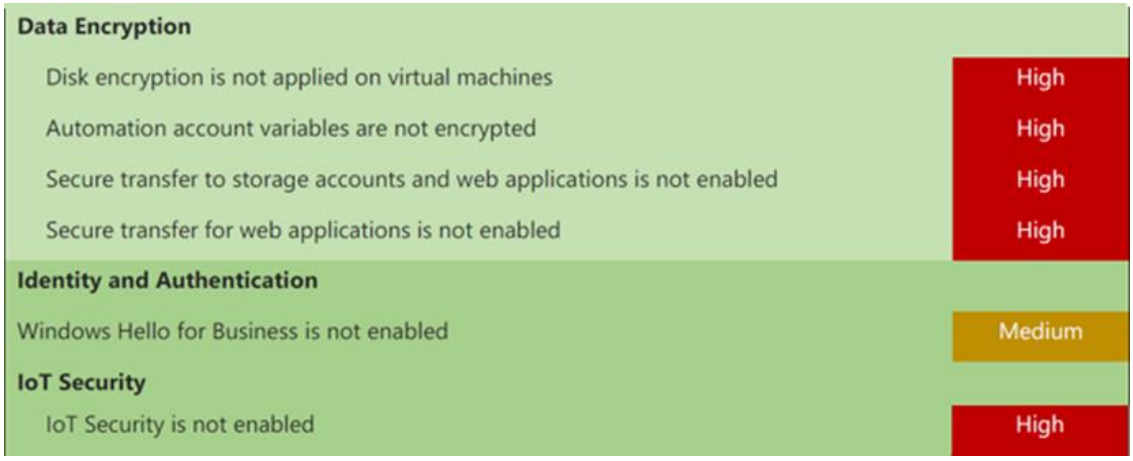
The company’s Azure cloud attracted different levels of risks in each domain. Table 5.5 describes severity levels identified in the assessment across all the considered domains. The security risks associated with each risk domain guided remediation actions.

Table 5.5. Risk domains and their severity levels.

The company's Azure cloud attracted different levels of risks in each domain. Table 5.5 describes severity levels identified in the assessment across all the considered domains. The security risks associated with each risk domain guided remediation actions.

Table 5.5. Risk domains and their severity levels.

Risk	Severity
Azure Defender	
Azure Defender for servers is not enabled	High
Azure Defender for App Service is not enabled	High
Azure Defender for storage is not enabled	High
Azure Defender for container registries is not enabled	High
Azure Defender for Kubernetes is not enabled	High
Azure Defender for SQL, SQL database servers and SQL servers on machines is not enabled on managed instances	High
Azure DDoS Protection	
Azure DDoS Protection Standard is not enabled	High
Access and Permissions	
Storage account public access should be disallowed	Medium
Managed identity is not used in your web app	Medium
Deprecated accounts are not removed from your subscription	Medium
Network Security	
Virtual networks are not protected by Azure Firewall	Low
Some internet-facing virtual machines are not protected with network security groups	High
Management ports are open on some virtual machines	High
All network ports should be restricted on network security groups associated to some virtual machine	High
Auditing and Logging	
Log Analytics agents are not installed on your virtual machine	High
Diagnostic logs are not enabled in App Service	Medium
Miscellaneous	
A vulnerability assessment solution should be enabled on your virtual machines	Medium
Vulnerability assessment should be enabled on your SQL managed instances	High



5.2.5 Short Term Remediation Actions

The short-term remediation actions describe quick fixes with low complexity and user impact for mitigating some of the operational and functional risks. Most corrective actions involve upgrading some of the used Azure Services tiers from free or basic tiers to standard ones. The actions involve limited expertise and resource investment. More details on the short-term remediation actions can be found in appendix 2.

5.2.6 Mid Term Remediation

The remediation action in this assessment adds an extra security layer to address technical information and data protection. The introduced features enhance overall the company defenses and harden Azure cloud security level. The goal is to reduce vulnerability and increase the reliability of cloud computing at the company. More details on the mid-term remediation actions can be found in appendix 3.

5.2.7 Long-Term Remediation

The recommended remediation at the long-term level covers a broader spectrum of the company security posture. Although companies cannot attain perfect security for all their IT and cloud computing needs, the outcomes of this phase fulfill most of the up-to-date recommendations of Microsoft's Cybersecurity Reference Architecture. In this context, long-term remediation adds more security capabilities to the Azure cloud and moves

defenses into a proactive posture. More details on the long-term remediation actions can be found in appendix 2.

6 Conclusion

The increased penetration of internet-based applications and use is creating new challenges in all social facets. The Internet-connected world attracts numerous threats and breaches with varying effects on different systems. One of the most affected areas is cloud computing due to inadequate change control, misconfiguration, and numerous vendors that utilize distinct strategies and policies with inadequacies for securing cloud-based infrastructure. The advancement of security measures in cloud computing enhances remote workforce management besides disaster recovery through business continuity planning. In this regard, CSPM is a critical security relief in cloud computing due to its ability to enforce continuous threat monitoring and real-time risk monitoring. CSPM promotes high-level configuration of cloud storage and enhanced proactive cloud monitoring and audit, leading to improved risk monitoring and management besides intensifying cloud management and automating deployment.

The implementation of rules in a business organization requires monitoring for compliance to enhance efficiency. Individual companies require different types of cloud management software to view all cloud activities. The monitoring for compliance identifies aspects of organizational rules that require improvement to enhance cost-efficiency or performance. Thus, amendment of policies is crucial for accommodating new products and services besides sustaining competitive advantage in consumer segments. This assessment found that cloud governance is one of the effective methods of enhancing management of cloud resources. The concept provides distinct account for managing multiple-tenant workloads for enhanced cost management, precise access control, limiting security and financial blast radius during breaches. Moreover, governance enhance management of numerous accounts besides enabling visibility of activities and trends. Meanwhile, cloud governance enables quick access to cloud resources within compliance and budget constraints. In this regard, companies obtain enhanced efficiency through reduction of manual processes for tracking accounts, cost, and compliance besides eliminating need for follow-up actions after receiving alerts.

The company is an international company with an enhanced need for a secure cloud environment to promote reliability and competitiveness of operations. The deployment of CSPM using existing tools in Azure improves cybersecurity architecture as the integration of these tools within Microsoft's backbone allows the consolidation of results and recommendations from Microsoft security best practices to help the organization improve the security posture and gather the required resources for formalizing governance and security frameworks. In this regard, the assessment of Azure cloud at the company involved security findings and recommendations from Azure Security Center besides Microsoft Cybersecurity Reference Architecture for gap analysis. Nonetheless, the company does not extensively utilize technological innovation to complete different management, control, organization, and coordination activities. the company utilizes Microsoft Office 365 and Azure for agile collaboration with partners and customers in the cloud environment, meaning they are responsible for business continuity and operations in the global market.

The company uses unsecured cloud computing due to numerous instances of risk vulnerabilities. The company lacks a single framework/standard for enforcing security architecture, whereby it relies on security mechanisms and tools issued by software and system vendors for ERP/CRM/BI business application landscape. The company also lacks cloud management or a cloud security-specific policy for articulating cloud governance framework and in-house expertise for promoting cloud security and architecture. In this context, the company completed the migration of on-premises IT infrastructure in the IaaS and PaaS program in a lift and shift. As a result, the company had an overall security score of 39%, with 83% unhealthy resources characterized by high-level disabling of critical security features and tools. For instance, the company had disabled Azure Defender for servers, Azure Defender for App Services, Azure Defender for Kubernetes, Azure Defender for SQL, SQL database servers, and SQL server machines, Azure DDoS Protection Standard, and Windows Hello for Business. Therefore, the company's cloud computing environment was highly vulnerable to threats with severe impacts on operations, competitiveness, and data privacy.

The company needs to enhance the security features of its Azure cloud. In this context, the company should enable all the disabled features as per Microsoft recommendations. However, the enabling of the feature should align with internal standards, operations, and protocols to ensure some security tools and features remain disabled to articulate

the company's interest. Moreover, the company should restrain public access to storage account; establish a strategy for managing identity on the web app; regularly remove deprecated accounts from its subscription; standardize disk encryption on VMs; encrypt automation account variables; enable secure transfer to storage accounts and web applications and install Log Analytics for collecting log and metric data. The company needs also to enable diagnostic logs in App Service, protect all virtual networks with Azure Firewall, install Endpoint Protections on VMs, close management ports, and restrict all network ports to NSGs for in-house VMs. Therefore, the company should embrace best practices in the management and Azure cloud to enforce enhanced security and reliability.

References

Abdalla, P.A., and Varol, A. 2019. Advantages to Disadvantages of Cloud Computing for Small-Sized Business. In proceeding of 7th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-6.

Al-Beruni, R. 2020. Cybersecurity Reference Architecture: Security for a Hybrid Enterprise [Online]. Available at: <https://araihan.wordpress.com/2020/06/15/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/> [Accessed 12 March 2021].

Alshenqeeti, H. 2014. Interviewing as a Data Collection Method: A Critical Review. English Linguistics Research, 3(1), pp. 39-45

Amazon Web Services. 2020. AWS Well-Architected Framework: AWS Well-Architected Framework. Amazon Web Services, Inc.

Agarwal, A. 2011. Navigating the Clouds: Fortifying ITIL for Cloud Governance. HCL Technologies

Ayofe, A. N., and Irwin, B. 2010. Cyber Security: Challenges and the Way Forward. GESJ: Computer Science and Telecommunications, 6(29), 56-69.

Baldwin, M. S. 2020. Overview of the Azure Security Benchmark (V2) [Online]. Available at: <https://docs.microsoft.com/en-us/azure/security/benchmarks/overview> [Accessed 12 March 2021].

Bhasin, H. 2020. Desk Research: Definition, Importance and Advantages [Online]. Available at: <https://www.marketing91.com/desk-research/> [Accessed 17 April 2021].

Blaisdell, R. 2012. Laws and Regulations Governing the Cloud Computing Environment [Online]. Available at: <https://rickscloud.com/laws-and-regulations-governing-the-cloud-computing-environment/> [Accessed 11 March 2021].

Blanchard, J. 2020. The History of Cloud Computing [Online]. Available at: <https://blog.servermania.com/the-history-of-cloud-computing/> [Accessed 5 March 2021].

Brook, C. 2020. What is CSPM (Cloud Security Posture Management)? [Online]. Available at: <https://digitalguardian.com/blog/what-cspm-cloud-security-posture-management> [Accessed 11 March 2021].

Butt, R. J. 2019. Azure Security Center – Cloud Security Posture Management Available at: < https://msexperttalk.com/azure-security-center-cloud-security-posture-management/> [Accessed 12 March 2021].

Cabaj, K., Kotulski, Z., Księżopolski, B., and Mazurczyk, W. 2018. Cybersecurity: Trends, Issues, and Challenges. EURASIP Journal on Information Security, 10.

Cascio, W. F. and Montealegre, R. (2016). How technology is changing work and organizations. *Annual Review of Organizational Psychology and Organizational Behavior,* 3(1), 349-375.

Chaudhary, A. 2020. Cloud Security Challenges in 2020 [Online]. Available at: <https://cloudsecurityalliance.org/blog/2020/02/18/cloud-security-challenges-in-2020/> [Accessed 5 March 2021].

Check Point. What is Cloud Security Posture Management (CSPM)? [Online]. Available at: <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cspm-cloud-security-posture-management/> [Accessed 11 March 2021].

Cloutier, R., Muller, G., Verma, D., Nilchiani, R., Hole, E., and Bone, M. 2010. The Concept of Reference Architectures. Systems Engineering, pp. 14-27.

Crowd Strike. 2020. What Is Cloud Security Posture Management (CSPM)? [Online]. Available at: <https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-posture-management-cspm/> [Accessed 11 March 2021].

Dickinson, K. 2019. JumpStart Guide to Investigations and Cloud Security Posture Management in AWS. Barracuda.

Diogenes, Y. 2021. How to Effectively Perform an Azure Security Center PoC [Online]. Available at: <https://techcommunity.microsoft.com/t5/azure-security-center/how-to-effectively-perform-an-azure-security-center-poc/ba-p/516874?ocid=AID754288&wt.mc_id=azfr-c9-scottha&wt.mc_id=CFID0548> [Accessed 12 March 2021].

DMS Technology. 2017. Cloud Computing vs. Traditional OnSite Storage. New York, NY: DMS Technology.

Everett, R. 2017. Cloud Governance & Management Success Plan. Viderity.

Farooq, U. 2020. What is Systems Audit and What are the Objectives of System Audit? [Online]. Available at: <https://www.businessstudynotes.com/finance/auditing/systems-audit/> [Accessed 17 April 2021].

Foote, K.D. 2017. A Brief History of Cloud Computing [Online]. Available at: <https://www.dataversity.net/brief-history-cloud-computing/#> [Accessed 5 March 2021].

Fugue. Cloud Security Posture Management [Online]. Available at: <https://www.fugue.co/cloud-security-posture-management> [Accessed 11 March 2021].

Gartner Research. 2019. Innovation Insight for Cloud Security Posture Management [Online]. Available at: <https://www.gartner.com/en/documents/3899373/innovation-insight-for-cloud-security-posture-management> [Accessed 11 March 2021].

Gell, T. 2020. Desk Research | What It Is and How You Can Use It [Online]. Available at: <https://www.driveresearch.com/market-research-company-blog/desk-research-what-it-is-and-how-you-can-use-it/> [Accessed 17 April 2021].

Goddard, W. (2018). The Evolution of Cloud Computing – Where's It Going Next? [Online]. Available at: <https://itchronicles.com/cloud/the-evolution-of-cloud-computing-wheres-it-going-next/> [Accessed 12 March 2021].

Harkut, D.G. 2020. Cloud Computing Security: Concepts and Practice. IntechOpen.

Jungck, K and Rahman, S. M. (2011). Cloud computing avoids downfall of application service providers. *International Journal of Information Technology Convergence and Services (IJITCS)*, 1(3), pp. 1-20.

Kaur, R., and Kaur, A. 2014. A Review Paper on Evolution of Cloud Computing, its Approaches and Comparison with Grid Computing.) International Journal of Computer Science and Information Technologies, 5(5), pp. 6060-6063.

Korban, S. 2015. Why Is the Current State Analysis Important? [Online]. Available at: <https://www.linkedin.com/pulse/why-current-state-analysis-important-sergey-korban> [Accessed 17 April 2021].

KPMG. 2018. Cloud Governance and Security: Helping Organizations Adopt Cloud Solutions [Online]. Available at: <https://assets.kpmg/content/dam/kpmg/ca/pdf/2017/10/cloud-governance-services-kpmg-canada.pdf> [Accessed 12 March 2021].

Lai, R. 2002. J2EE Platform Web Services. Prentice Hall PTR

Makam, V. 2020. Why Organizations Need to Pay Attention to Cloud Security [Online]. Available at: <https://www.red-gate.com/simple-talk/cloud/security-and-compliance/how-organizations-can-optimize-cloud-security/> [Accessed 5 March 2021].

Makeri, Y. A. 2017. Cyber Security Issues in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering, 7(4), pp. 315-321.

McKay, A. 2019. Why your project needs a current state analysis [Online]. Available at: < https://clarit-e.com.au/business-analysis-current-

state/#:~:text=Current%20state%20analysis%20is%20key&text=By%20develop-ing%20a%20baseline%20of,the%20current%20and%20future%20states.> [Accessed 17 April 2021].

Mohamed, A. 2018. A History of Cloud Computing [Online]. Available at: < https://www.computerweekly.com/feature/A-history-of-cloud-computing > [Accessed 12 March 2021].

NCC Group. 2019. Advantages and Disadvantages of Cloud Hosted Software. NCC Group.

Neto, M. D. (2014). A brief history of cloud computing. [Online] Available at: <https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-com-puting-3/> [Accessed 5 March 2021].

Nicholas. 2018. Traditional Computing Vs Cloud Computing [Online]. Available at: <https://quantumcomputingtech.blogspot.com/2018/08/traditional-computing-vs-cloud-computing.html> [Accessed 5 March 2021].

Pandey, U.N. 2018. An Informative Guide On Cloud Computing Vs Traditional It Infra-structure [Online]. Available at: <https://highlightstory.com/informative-guide-cloud-computing-vs-traditional-infrastructure/> [Accessed 5 March 2021].

Pardini, D.J., Heinisch, A.M., and Parreiras, F.S. 2017. Cyber Security Governance and Management for Smart Grids in Brazilian Energy Utilities. Journal of Information Systems and Technology Management, 14(3), pp. 385-400.

Parveen. 2020. Cloud Governance: The Big Challenges and Best Practices [Online]. Available at: <https://www.xenonstack.com/blog/cloud-governance/> [Accessed 12 March 2021].

Price, B. 2018. 4 Reasons Why Cloud Governance Matters [Online]. Available at: <https://www.cloudtamer.io/4-reasons-why-cloud-governance-matters/> [Accessed 12 March 2021].

Oman Governance & Standards Division. 2017. Cloud Governance Framework Gov-ernance & Standard Division. Sultanate of Oman Information Technology Authority

Reddy, G.N., and Reddy, G.J. 2014. A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies [Online]. Available at: <https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf> [Accessed 5 March 2021].

Sagir, S. H. 2020. How Cloud App Security Helps Protect Your Azure Environment [Online]. Available at: <https://docs.microsoft.com/en-us/cloud-app-security/protect-az-ure> [Accessed 12 March 2021].

Saidah, A. S., and Abdelbaki, N. 2014. A New Cloud Computing Governance Framework. CLOSER 2014-4th International Conference on Cloud Computing and Services Science, pp. 671-678.

Seemma, P.S, Sundaresan, N., and Sowmiya, M. 2018. Overview of Cyber Security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), pp. 125-128.

Simos, M. 2018. Cybersecurity Reference Architecture: Security for a Hybrid Enterprise [Online]. Available at: <https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/> [Accessed 12 March 2021].

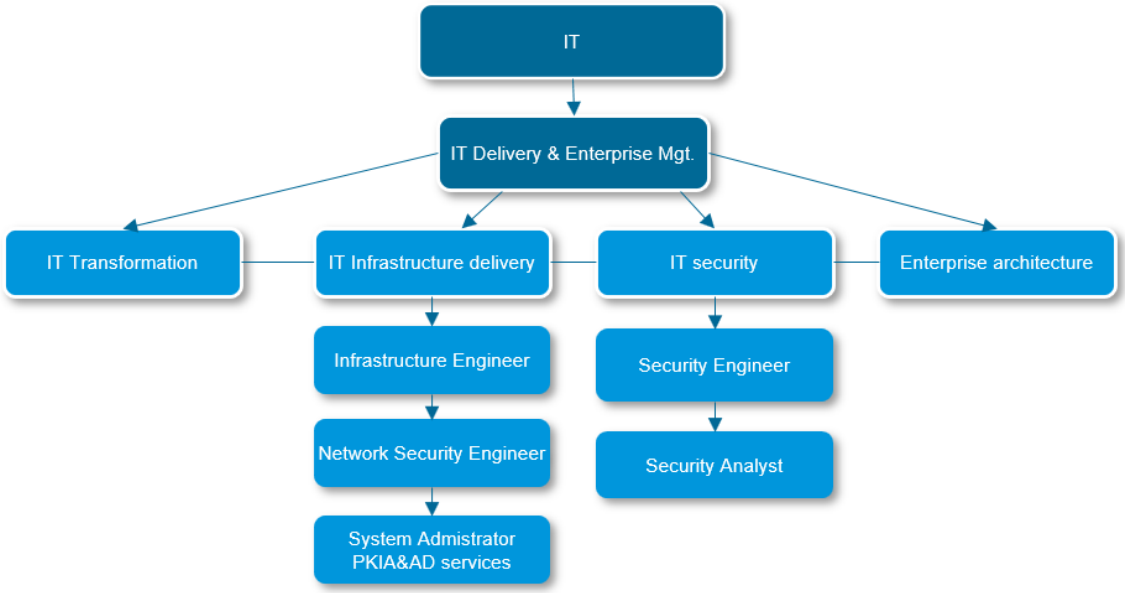
Smyth, D. 2019. Advantages & Disadvantages of a System Based Audit [Online]. Available at: <https://bizfluent.com/info-8782978-advantages-disadvantages-system-based-audit.html> [Accessed 17 April 2021].

Stevens, J. 2019. 5 Reasons Why Cloud Security Is Important for All Businesses [Online]. Available at: <https://www.cyberdefensemagazine.com/5-reasons-why-cloud-security-is-important-for-all-businesses/> [Accessed 5 March 2021].

Trappe, W., and Straub, J. 2018. Journal of Cybersecurity and Privacy: A New Open Access Journal. Journal of Cybersecurity and Privacy, 1, pp. 1-3.

Unison Health and Community Services. 2015. Current State Analysis Report. Toronto, ON: Unison Health and Community Services.

Appendix 1: Departmental chart



Appendix 2: Short Term Remediation Actions

Enable Azure Defender	Motivations	Recommended Mitigations
Upgrade to Azure Defender	Azure Defender for servers is highly crucial in the management and protection of data and resources servers in cloud environment. The enabling of the security tools fosters real-time threat protection, generation of recommendations for strengthening protection, and alerting users of suspicious activities in cloud environment. Thus, enabled Azure Defender improves threat detection and advances defenses for Windows and Linux machines. Azure Defender in Windows machine works alongside Azure services to extend monitoring, recommendations on security enhancement, and protection against popular threats. The security mechanism utilizes “audit” to advance protection against threats.	The company should Azure Defender for servers
Enable Azure Defender for App Service	Azure App Service is a critical tool on cloud computing for enabling organizations to build and host the applications online. The service provide cheap APIs compared to traditional computing, which requires acquisition of infrastructure. In this regard, enabling Azure Defender for App Service enhancing the company compliance, security, and performance by providing critical insights into effective management of development resources in the cloud. The security feature focuses on the identification of threats targeting cloud application or their weaknesses. A change in the pattern and behaviors arouses suspicious and activation of threat containment measures. The methodology used in threat detection includes widespread scanning for distributed attacks. The attacks search for a vulnerability page or plugin and cannot be identified from the standpoint of a single host.	The company should Enable Azure Defender on all subscribed App Services.
Enable Azure Defender for Storage	The activation of Azure Defender for storage protect data during its storage or retrieval from loss of integrity due to corruption. In this regard, the security tool enforces protection measure on storage accounts to safeguard data store in different cloud environment. In this context, enabled Azure Defender for storage generates security alerts due to the activation of specific triggers. • Suspicious activity – for example, data access using the storage account identified as threat to cloud computing resources and environment. • Anomalous behavior – for example, changes in the access pattern to a storage account. • Potential malware uploaded – hash reputation analysis indicates that an upload file contains malware. The provided security alerts include details of the incident that triggered them and recommendations on investigating and remediating threats.	The company should subscribe and enable Azure Defender for storage.

Enable Azure Defender for Container Registries	The containerized workloads in cloud environment are highly susceptible to threats and cyberattacks. Thus, users and systems must ensure that used images are secure and do not expose systems to enhance vulnerabilities. In this regard, enabled Azure Defender protects container registries by continually scanning images for threat and susceptibility. Qualys enforces the security feature by scanning threats and reporting or displaying them on Azure Defender dashboard as notifications. Thus, enabling the security tool for container registries allow users and security experts to identify suitable approaches of resolving threats.	The company should enable Azure Defender on all container registries in the subscriptions.
Enable Azure Defender for Kubernetes	AKS is a Microsoft product that enhance application development by supporting management, development, and deployment. Enabled Azure Defender to provide enhanced security to Kubernetes by continually monitoring them for threats and reporting any suspicious activity Azure Defender and AKS form cloud-native Kubernetes security together provide environment hardening, workload protection, and run-time protection. Thus, the company should enable Azure Defender on all Kubernetes for threat detection in Kubernetes clusters.	Azure Defender on all Kubernetes should be enabled in the subscriptions.
Enable Azure Defender for SQL, SQL servers, and SQL Servers on Machines	Azure Defender package that focusses on SQL its servers and machines focus on maintaining data integrity. Enabled Azure Defender identifies possible threats and classifies the before generating reports. In this regard, the security feature provides enhanced protection and confidentiality to sensitive data held by a company.	The company should enable Azure Defender for Azure SQL Database/SQL servers in the subscriptions.
Upgrade to DDoS Protection Standard	The absence of DDoS Protection Standard in a cloud environment creates numerous vulnerabilities. In this regard, its upgrade and activation ensure system and data are free from risky or volatile IP addresses. DDoS Protection Standard blocks or limit their interaction with other network nodes or accounts within an enterprise cloud environment.	The company should enable Azure DDoS protection for VNets on all subscriptions by upgrading to the standard tier.
Access and Permissions		
Protect Virtual Network with Azure Firewall	The assessment identified that the company did not have comprehensive protection of all VM with Azure Firewall. The security mechanism is highly effective for protecting cloud environment regardless of scalability. In this regard, Azure Firewall secures all virtual networks across all subscriptions of an enterprise. The tool integrates with Azure Monitor, responsible for generating analytics and logging.	The company should deploy Azure Firewall to subscriptions
Protect Internet Facing VMs Are with NSGs	Companies should protect VMs with NSGs responsible for restricting their access. Network Security Group (NSG). NSGs involves an ACL for denying or allowing access to controlled resources. Thus, VMs need embedding in NSGs for controlled network access.	the company should protect VM's with an NSG.
Open Management Ports on Some VMs	The company has several open management ports that expose VMs to enhanced vulnerability. The open ports allow internet-based hackers and attackers to target VMs with brute force for unauthorized manipulation and control of machines. As a result, companies should harden the network security	The company needs to edit inbound rules of some VMs

	group of the virtual machines to restrict access to management ports.	
All Network Ports Need Restriction on NSGs Associated to Some VMs	The company had NSGs that were too permissive, leading to enhanced susceptibility of VMs threats. Inbound rules should be highly restrictive to provide a reliable level of protection for remote attackers who target security lapses in cloud environment. Thus, restricting access through constraining rules helps to harden the network security groups of the internet facing VMs.	The company should restrict access to VMs.
Audit and Logging		
Install Log Analytics Agents on VMs	Security Center collects telemetry data from Windows and Linux machines in any cloud or on-premises machines to monitor for security vulnerabilities and threats. The data collected using Log Analytics agents provide comprehensive description of a company's security posture. The tool navigates the entire cloud environment searching and collecting critical information that can be used to enhance established security.	The company should Install Log Analytics Agent
Enable Diagnostics Logs in App Service	Companies should enable logs and retain them for up to a year. The security feature recreates is responsible for creating a trail used to investigate breaches, vulnerabilities, or established security posture. In this regard, Diagnostics Logs maintain security and performance history of a cloud environment for successful troubleshooting and enhancement of security status. Diagnostic logs are also helpful for auditing purposes.	The company should enable App Service diagnostics
Miscellaneous		
Enable Vulnerability Assessment Solution on VMs	Organizations should install the Qualys agent (included in Azure Defender) to enable a vulnerability assessment solution on virtual machines. A 3RD party vulnerability assessment solution can also be deployed as an extension to virtual machines.	The company should deploy a vulnerability assessment solution on VMs.
Vulnerability Assessment Disenabled on SQL Managed Instances	The formulation of vulnerability assessment focuses on identifying threats and susceptibility of cloud environment to known risks. The activation of Vulnerability Assessment enables a company to identify divergence from best practices of maintaining health infrastructure and cloud-based resources. In this regard, enabling Vulnerability Assessment at the company will identify common practices and activities that create or enhance susceptibility of Azure cloud to threats.	The company should enable vulnerability assessment on SQL-managed instances.

Appendix 3: Mid Term Remediations

Data Encryption	Motivation	Recommended Remediations
Enable Azure Disk & Storage Encryption	Encrypting storage disks on Windows and Linux virtual protect them from unauthorized access besides promoting privacy and confidentiality in data access and manipulation. ADE used in Windows' world employs standard BitLocker Device Encryption while Linux utilizes DM-Crypt system. The employment of ADE provides cloud environment with end-to-end data encryption.	The company should enable Azure Disk Encryption.
Encrypted Automation Account Variables	Enabled encryption during storage of sensitive data is highly essential to enforce confidentiality and privacy. Companies should ensure sensitive data in their possession is encrypted during storage to reduce attack susceptibility.	The company should encrypt Automation Account Variables that store sensitive data.
Disenabled Secure Transfer to Storage Accounts	HTTPS provides networks with high-level data security by ensuring that nodes only accept requests from secure connections. Thus, enabling secure transfers requires nodes and resources to emphasis HTTPS connections during communication or data transmission.	The company should ensure that secure transfer is always enabled.
Enabled Secure Transfer for Web Applications	The enabling of secure transfer for web applications ensures that they value and emphasizes HTTPS connection during communication and transmission of data.	The company should redirect all HTTP traffic to HTTPS.

Appendix 4: Long Term Remediations

Identity and Authentication	Motivation	Recommended Mitigations
Enabled Windows Hello for Business	Enabling Windows Hello for Business increases the assurance level and usability of administrator authentication. Windows Hello Addresses the following problems with passwords, including password reused on different sites and profiles, breaches to established server security, and inadvertent exposure of passwords through phishing attacks.	the company should deploy Windows Hello for Business across all its computing operations.
IoT Security		
	The IoT and ICS devices are initially designed to maintain safety and availability rather than security which is on top of their design priority. Moreover, networking concepts usually use specialized protocols and offer minimal visibility to security risks. In most cases, IoT devices are designed to act for a very long period without rooms for intrusively upgrading them. As a result, designers, and users of IoT devices should proactively practice security. Azure IoT security provides a preventive edge against most current IoT attacks, such as Stuxnet, NoPetya, WannaCry, and LockerGoga. The solutions also embed defenses with proactive abilities to protect IoT assets from suspicious traffic. Meanwhile, Azure IoT easily integrates into SIEM systems to generate alerts and provide detailed logs of its findings.	
Enable Azure Sphere	Azure Defender for IoT has deep knowledge of specialized IoT protocols and devices from diverse IoT and ICS vendors. Moreover, the non-invasively integration of Defender for IoT with zero performance impacts the running systems. The security component can also be integrated with native IT Security SIEM stacks, such as Azure Sentinel, Splunk, and Service Now.	The company should enable Azure Defender for IoT.
Upgrade to Windows 10 for IoT	Windows 10 for IoT redesigns the security concept for IoT windows-based devices. The operating system is offered in various versions and bundles depending on the desired use. Windows 10 IoT Core is the preferred version due to enhanced optimization for small headless devices that run on ARM and x86/64 devices. However, Windows 10 IoT Enterprise is highly reliable due to provision of specialized features to creating	The company should upgrade to Windows 10 IoT.

	dedicated lock for devices to a given application or peripheral support. In the meantime, Windows 10 Pro leverages technologies, such as containers, Artificial Intelligence, Machine Learning, and cloud computing, to provide users with optimum benefits in performance and efficiency.	
Cloud Computing Strategies and Standards		
	The evaluation considered the recommendation to engage in a more strategic project to ensure proper management and security of the cloud infrastructure and services. Therefore, the remediation actions should include the following. • Users of the cloud need to understand the shared responsibility model before migrating and developing applications in the cloud. • Formalizing a governance and security framework to ensure proper management and security of the cloud infrastructure and security, • Deriving documentation on cloud management policy and a cloud-specific security policy and implementing and testing the impact of enabling security features derived from findings. • Dedicated professional team to manage the different aspects of the cloud. • Consider Microsoft disciplines of governance as a starting point to support corporate policy and guide future migrations and cloud designs.	