ENDPOINT PROTECTION SECURITY SYSTEM FOR AN ENTERPRISE

Petri Ruotsalainen

Master´s Thesis
May 2013

Information Technology
Technology and transportation

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s) RUOTSALAINEN, Petri	Type of publication Master's Thesis	Date 31.05.2013
	Pages 77	Language English
		Permission for web publication (X)

Title ENDPOINT PROTECTION SECURITY SYSTEM FOR THE ENTERPRISE
Degree Programme Information Technology
Tutor(s) KOTIKOSKI, Sampo
Assigned by Metso Shared Services Ltd.

Abstract

The thesis subscriber was Metso Shared Services Ltd. The objective was to find out if Microsoft Forefront Endpoint Protection 2010 (FEP) would be secure and cost-effective enough system to fulfill the requirements of the company's endpoint protection security system.

Microsoft FEP was compared and benchmarked with some other most significant endpoint protection products based on the requirements and definitions of the subscriber. The comparison and evaluation were based on investigation and data gathering of public sources, user's own experiences of the compared products and analysis of results found during the project.

As a conclusion it can be stated that Microsoft's FEP is good, however, it falls short of the integrated technical, security and management capabilities of the endpoint protection market leaders. Microsoft's security offerings are not the leading ones, nevertheless, they are reasonably priced and good enough for Microsoft-centric, cost-driven enterprises. If a company is Windows-centric, licensed under Core CAL or ECAL or has deployed and is using Microsoft System Center Configuration Manager (SCCM), FEP must at least be considered as an endpoint protection solution for Windows based endpoints.

Although this thesis has been assigned by Metso Corporation, the results of the investigations can be used for any company which considers Microsoft Forefront Endpoint Protection as protection software for their endpoint devices.

Keywords
FEP, endpoint protection, Forefront Endpoint Protection

Miscellaneous

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) RUOTSALAINEN, Petri	Julkaisun laji Opinnäytetyö	Päivämäärä 31.05.2013
	Sivumäärä 77	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
ENDPOINT PROTECTION SECURITY SYSTEM FOR THE ENTERPRISE

Koulutusohjelma
Information Technology

Työn ohjaaja(t)
KOTIKOSKI, Sampo

Toimeksiantaja(t)
Metso Shared Services Oy

Tiivistelmä

Työn tilaaja oli Metso Shared Services Oy. Työn tavoitteena oli selvittää, onko Microsoft Forefront Endpoint Protection 2010 (FEP) riittävän turvallinen ja kustannustehokas ohjelmisto yrityksen päätelaitteiden tietoturvaohjelmistoksi.

Työn aikana Microsoft FEP tuotetta vertailtiin ja arvioitiin muihin merkittäviin päätelaitteiden tietoturvaohjelmistoihin perustuen tilaajan vaatimuksiin. Vertailevaksi tuotteeksi kirjalliseen tuotokseen otettiin mukaan Symantec Endpoint Protection (SEP) ohjelmisto. Vertailu ja arviointi ovat perustuneet julkisista lähteistä saatavien tietojen keräämiseen ja tutkimiseen, omiin kokemuksiin kyseisten tuotteiden ominaisuuksista sekä saatujen tulosten analysointiin.

Tulokset osoittivat, että Microsoft FEP on riittävän hyvä tuote teknisesti mutta ei kuitenkaan markkinoiden johtavien tuotteiden veroinen teknisiltä ominaisuuksiltaan tietoturvan ja hallittavuuden osalta. Microsoftin tietoturvatuotteet eivät ole ominaisuuksiltaan parhaiden joukossa mutta ne ovat kuitenkin kohtuullisesti hinnoiteltuja ja soveltuvat riittävän hyvin Microsoft tuotekeskeisiin ja kustannustietoisiin yrityksiin. Jos yrityksessä on paljon Windows-päätelaitteita ja yrityksellä on Core CAL tai ECAL sopimus ja yritys on ottanut käyttöönsä Microsoft System Center Configuration Manager (SCCM) tuotteen, FEP 2010 ohjelmistoa on syytä harkita yrityksen päätelaitteiden tietoturvaohjelmistoksi.

Työ toteutettiin Metso konsernille mutta kehittämistyön tuloksia voidaan käyttää hyödyksi myös muissa yrityksissä, jotka harkitsevat Microsoft Forefront Endpoint Protectionin käyttöönottoa päätelaitteidensa tietoturvaohjelmistoksi.

Avainsanat (asiasanat)
FEP, endpoint protection, Forefront Endpoint Protection

Muut tiedot

TABLE OF CONTENTS

FIGURES

TABLES

1 INTRODUCTION

1.1 Motivation and background

This thesis deals with endpoint protection security system for large enterprises. This thesis investigated if Microsoft Forefront Endpoint Protection 2010 (FEP) is secure and cost-effective enough system to fulfill the requirements of those companies. Information security is discussed from various points of views, business and IT drivers for information security and risks, including information risks, are discussed on a theoretical level. Microsoft FEP is presented from technical point of view with financial aspects and also taking into account its strengths and challenges. In Analysis and collections chapter there is a summary, which discusses the suitability of Microsoft FEP for an endpoint protection security system in a large enterprise.

When talking about the endpoints, IT devices used by end users and located on a corporate network or even outside of corporate network are meant. Endpoints are typically physical desktops, virtual desktops, laptops, tablets, and possibly Windows phones. They are used as a computing device by end users and they should be centrally managed by IT department to ensure manageability, up-to-date security patches and virus definitions to name a few issues.

Any user in the company needs to have the latest antivirus, antimalware and firewall software program installed and updated on to their computer. The protection software is absolutely essential for safe and uninterrupted system usage. Endpoint protection security system software plays an important role in security, as it can protect vital documents and files from being damaged or lost forever.

Too often it can be noticed in the news or in companies’ announcements about a potential virus, worm or other realized threat that is spread via email, Internet browsing or other attack. Endpoint protection software can help minimize the overall threat that viruses, malware or similar issues cause, as computers and even company safety depend on having endpoint protection software installed in the machine. New worms and malware programs are being developed all the time. By having a secure, cost-effective and centrally managed endpoint protection software in every computer in a company, risks for business continuity can be significantly reduced.

The motivation for doing this Master’s Thesis study comes from my own work and responsibilities as a Service Delivery Manager for End User Computing area in Metso Shared Services Ltd. The job includes being responsible for endpoint security for Windows-based endpoint devices and implementing any changes done to those devices. Although this thesis was assigned by Metso Corporation, the results of the investigations can be used for any company which is considering the use of Microsoft Forefront Endpoint Protection as protection software for their computers.

1.2 Metso as a company

Metso is a global supplier of technology and services to customers in the process industries, including mining, construction, pulp and paper, power, and oil and gas. Metso employ worldwide about 30,000 professionals based in over 50 countries. In 2012 Metso Corporation's net sales were EUR 7.5 billion and nowadays 44 percent of net sales come from the Metso’s services business. There are three segments in Metso group: Mining and Construction, Automation and Pulp, Paper and Power. Figure 1 shows Metso net sales over the recent years and Figure 2 Metso personnel in the end of 2012. (Metso homepages)

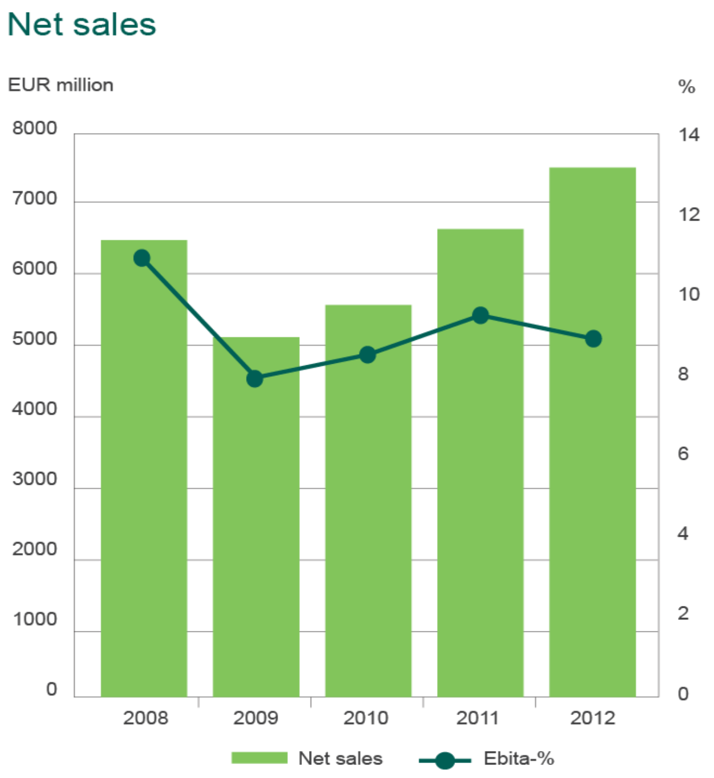


FIGURE 1. Metso net sales 2008-2012

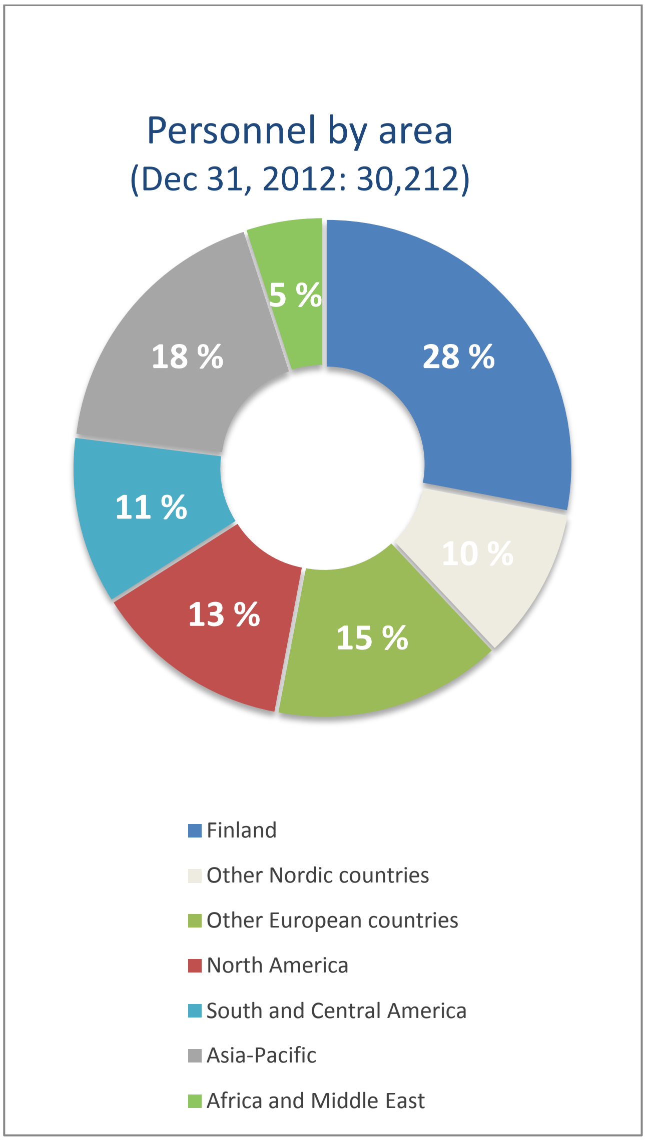


FIGURE 2. Metso personnel by area

Mining and construction

Mining and Construction delivers cutting-edge equipment, solutions and services to make a real and sustainable difference for customers' businesses. The main customers are mining industry, construction industry, quarries and contractors, scrap yards and waste-handling companies and recycling companies. Mining and construction net sales in 2012 was EUR 3.282 million where mining business line had 75%, construction 25% and recycling 6%. Employees were approximately 11 700. (Metso homepages)

Automation

Automation segment consists of three business lines; Process Automation Systems, Flow Control and Services business line. (Metso homepages)

Automation reporting segment produces following products and services:

- Process automation and information management application networks and systems
- Process measurement systems and analyzers
- Control, on-off and emergency shutdown (ESD) valves
- Intelligent positioners
- Intelligent condition monitoring
- Expert and life cycle services

The main customers are power generation industry, oil and gas industry, pulp and paper industry, mining and construction industry and selected other process industries. Automation net sales in 2012 were EUR 859 million where energy and oil & gas line had 60% and pulp and paper 40%. Employees were approximately 4 100.

Pulp, Paper and Power

Pulp, Paper and Power consists of these three business lines. They produces following products and services:

- Chemical pulping lines and equipment
- Mechanical pulping lines and equipment
- Paper and board making lines, machines and rebuilds
- Tissue making lines, machines and rebuilds
- Power boiler plants and chemical recovery boilers, evaporators, flue-gas cleaning and environmental systems, boiler rebuilds and upgrades, biomass power plants
- Expert and maintenance services
- Fabrics and filters for the pulp, paper, energy and mining industries
- Spare and wear parts

The main customers are chemical and mechanical pulp producers, paper, board and tissue producers, industrial power generators and municipalities and utility companies. (Metso homepages)

Figure 3 shows Metso's extensive sales, services and manufacturing network built over 20 years.

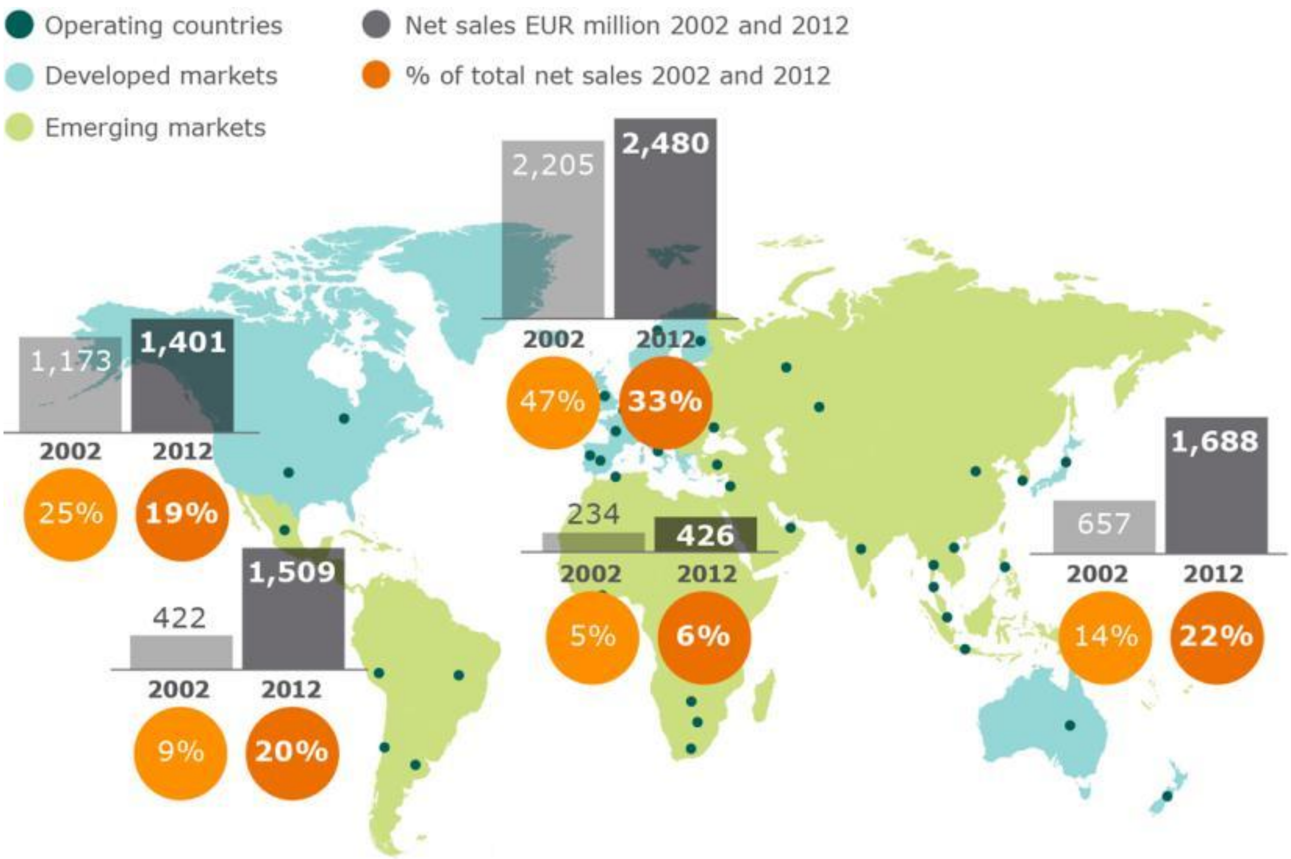


FIGURE 3. Metso's extensive sales, services and manufacturing network over 20 years

1.3 Metso information technology environment

Metso has IT resources in its own company Metso Shared Services Ltd. (MSS) which is called Metso IT. Metso IT is responsible for the development and delivery of Metso's global IT infrastructure and shared application services. Businesses are responsible for the development of business specific application services. Application support is globally harmonized and user support is provided as a common global service by Metso IT. Procurement in all IT related matters is centralized and managed globally by Metso IT. (Metso intranet, Metso Information Technology (IT) policy.)

Metso has a common IT infrastructure across the enterprise. IT is using standard and mainstream technologies to consolidate technology and infrastructure across the enterprise. IT supports growing and globally expanding business with reusable and scalable services which include common wide area network services, server management services, end user computing services and common application services. (Metso intranet, Metso Information Technology (IT) policy.)

IT service delivery is organized with mix of own capability and sourced services. Internal IT resource focuses on business relationship management, service development, IT service management and vendor management. Common corporate level processes and services are applied in IT sourcing. Outsourced services are sourced from a limited number of service providers. (Metso intranet, Metso Information Technology (IT) policy.)

IT risks are major part of Metso`s business continuity risks. Therefore IT risk management process is a key focus area in Metso IT. IT risks will be managed through Metso Risk and Compliance programs throughout the solution lifecycle. IT function actively incorporates risk management practices in all IT related operations. (Metso intranet, Metso Information Technology (IT) policy.)

2 THEORETICAL FRAMEWORK

2.1 Definition of knowledge

There is many kind of knowledge: heard, learned, read from books and newspapers and other similar kinds. People interpret things in different ways and create interpretation on incidental observations and previous experiences. Everyday findings often do not constitute matters of objective truth, because everyday philosophy is based on the individual's own observations. As on opposite to everyday knowledge, scientific knowledge is justified, produced and proven in the scientific community.

Criticality is characteristic for scientific thinking. The results will become science when they have undergone a critique of the research community and are proven to be sustainable. Scientific thought is characterized by articulated and reproducible methods. Science strives to organize the results for a systematic entirety, in other words for descriptive and explanatory theory of the target. (Uusitalo, 1991.)

The pragmatic theory of knowledge is based on an extended concept of knowledge. Charles Peirce, who established pragmatism, believed that the best information about the reality can be reached by acting and that information is the most important criterion of effectiveness. Scientific research seeks to form a new and better theory, while the professional research and development activities aims to create improved practice based on new knowledge. This is the difference between these functions. In practice, modeling is trying to be created instead of theoretical analysis of the phenomenon. Modeling can be carried out verbally, mathematically or digitally (virtual models). (Räsänen, Scientific reference of research and development projects). This thesis is based on action research and it is very suitable for the development work in companies.

2.2 Security as governance concern

When talking about the governance, the question of the definition of governance arises. What does it mean and how can company leaders use governance to keep adequate security in a continuously changing business, customer, risk, and technology environment? Enterprise security is important to almost all organizations, however what kind of priority should be assigned to enterprise security?

Governance could be simplified so that organizations are doing the right things and doing things right, and at the right time. “Right things” and “things right” are relative, not absolute concepts and they can change as the organization’s goals change. It includes specifying a framework for decision making, with assigned decision rights and accountabilities, and its meaning is to continuously produce desired behaviors and actions in organizations. Another aspect of effective governance is to ensure that the right leaders are making the right decisions targeting the right outcomes and results. Governance relies on well-informed decision making and it is most effective when it is systematical. IT governance consists of the actions required to align IT with enterprise objectives and ensure that IT investment decisions and performance measures show the value of IT in meeting these objectives. (Allen 2005, 5.)

Enterprise security must be addressed at a governance level by organizational leaders and not be relegated to technical specialists in the IT department. If the responsibility for enterprise security is relegated to people that lacks the authority and resources to act and enforce, enterprise security will not be optimal. Most senior executives and managers know what governance means and their responsibilities to it. In addition, they should expand their governance perspectives to include security, and include enterprise-wide security thinking into their own and their organizations' day-to-day governance actions. (Allen 2005, 5.)

How much security is enough?

Determining adequate security depends on what an organization needs to protect. It is largely synonymous with determining and managing risk. An organization should implement controls that satisfy the security requirements for its critical business processes and assets. Where this is not possible, security risks to such processes and assets are identified, mitigated, and managed at a level of remaining risk that is acceptable to the organization. A useful way to address the question "How much security is enough?" is to first ask "What is our definition of adequate security?" What are the critical assets and business processes that support our organizational goals? What is the organization's risk tolerances and risk appetite? Adequate security is about managing risk. Governance and risk management are linked to each other — governance is an expression of responsible risk management, and effective risk management requires efficient governance. (Allen 2005, 23-25.)

2.3 Definition of information security elements

There is a common understanding for basis of information security: the most important asset in companies is data. It has to be reliable and available quickly, in correct format and available only for authorized people. Information security provides the basis for handling the data. In classical definition information security consists of three elements which are confidentiality, integrity and availability. Availability is often called also usability. (Hakala et al 2006, 4-5.)

An asset is anything valuable to a company. Assets include information such as enterprise strategies and plans, product information, and customer information; technology such as hardware, software, and IT-based services; and supporting assets such as facilities and utilities. Critical assets are those which, in case of losing them, compromise the ability of the organization to gain its business objectives. (Allen 2005, 24).

Confidentiality means that data is available only for authorized people. Availability or usability means that data is available in correct format and fast enough from the data system; integrity means that the data is correct and does not contain intentional or unintentional errors. (Miettinen 1999, 25.)

Classical definition is quite reduced to fulfill all information security issues in companies because identity of data owner or creator is not observed enough. Also the value of information systems and data network systems is not included in classical definition. The most common extended definition comprises five elements: confidentiality, availability/usability, integrity, non-repudiation and access control. (Hakala et al 2006, 5.)

In practice confidentiality means to protect the data from unauthorized usage and protect the privacy of company’s data. The data is meant only for people with access to the data. Maintaining the confidentiality requires protecting the devices physically and data by user accounts and passwords. Different kind of ciphering methods can be used also to protect very critical data. It is very important that especially customer and identity management, research and development (R&D), corporate planning, financial, trade secret or national defense related data is confidential. If the confidentiality is lost, it can cause significant financial or public image losses for the company. (Miettinen 1999, 25.)

Availability means that company data is available for the users whenever the data is needed and can be used from the start to the end for the daily working. If that it is not true, the availability is lost. To maintain the availability the data system devices and telecommunication devices have to be effective enough and applications used are most suitable to handle the data. Devices should be also reliable, secured and back upped. Information processing should be automatized to provide the data for the end users as ready-made reports. (Hakala et al 2006, 4-5.) When talking about the availability, the data should be also useful. If data cannot be used for some reason at all, the data is not useful. The data might be saved for the format that it cannot be used. (Miettinen 1999, 28.)

Integrity means that the data in the data system is correct and does not contain intentional or un-intentional errors. (Hakala et al 2006, 4.) It guarantees for the users that data remains as invariable in every phase of its lifecycle and usage. (Miettinen 1999, 25.) Integrity will be tried to be kept with using checking or restrictions during the data inputs or with checksums during the data savings or data transitions. Devices will be planned to prevent errors by using memories and channels with the error correction. In telecommunication, error detection and error correction is used in protocols and devices. Different kind of ciphering methods can be used for integrity also. (Hakala et al 2006, 5.)

Non-repudiation means the ability to identify the user and save reliably the identity of the user who uses the data system. It is often based on legislation. There are two reasons for the non-repudiation: to ensure the origin of the data and to verify the unauthorized usage of existing data. Different kind of methods can be used when trying to achieve the non-repudiation: passwords, smart cards, identity cards, certificates and biometric identifiers. (Hakala et al 2006, 5, 86.) If the non-repudiation of data is lost, it can lead for the wrong decisions in companies. As an example wrong decisions can be made daily when recruiting new people, making business alignments or in acquisitions. This can cause huge losses for the companies. (Miettinen 1999, 27.)

Access control means those methods which are used to restrict the usage of computing infrastructure. Companies want that the infrastructure and telecommunication systems are used for business usage only, not for any unauthorized usage. Unauthorized usage overloads the systems and leads for a weak availability. It provides also a possibility for malware and viruses to spread out in company's network. Access control is used also to prevent the usage of company's computing infrastructure by external people. When planning the access control, the authorized usage of devices and e.g. server rooms and cross linking rooms has to be defined. (Hakala et al 2006, 5-6, 85.)

2.4 Information security sections

When defining information security, it should be defined as a part of company's overall security. The overall security should be defined for whole organization in company and should be lead to business security. Overall security consists of physical security and information security components. Those components shouldn't be defined and developed separately, otherwise the overview for overall security is too narrow and restricted.

Physical security is build to protect organization people and assets from the risks such as violence, thefts, fire or some other accidents. Information security in turn protects organization data and data systems and prevents unauthorized use of computing devices and data networks. Both components of overall security often use same computing infrastructure if there only would be knowledge in the company to exploit that. Overlapping work and contradictory solutions could be avoided with good planning of overall security. (Hakala et al 2006, 14-16.)

Information security is often viewed through its sections. It helps to understand which it consists of and how does it affects for daily working in company. (Miettinen 1999, 15.)

2.4.1 Administrative security

The company's management creates prerequisites with an administrative security to manage and develop information security. It combines all the aspects of information security to one entirety which is easy to lead and manage like IT, financial management, human resources or other functions. (Miettinen 1999, 18.) Very important part of administrative security is evaluating the effects of legislation, agreements and licenses for organization daily practices. Administrative security is often managed by IT.

2.4.2 Physical security

Physical security protects spaces and devices in company's building from vandalism and thefts, fire and water accidents and from electricity or heating malfunctioning. It is important for IT people to participate for planning and managing physical security because company data is behind the physical spaces and nowadays access control systems are tight part of company's computing infrastructure. (Hakala et al 2006, 11.)

2.4.3 Personal security

Personal security is part of company's overall security and it has many confluences for information security. As a part of information security it means protecting the company's data and data computing from intentional an unintentional threats. With personal security actions company tries also to protect personnel activities in information security part. Personal security concerns company's own people, partners, quests and other people. (Miettinen 1999, 18.) To ensure data computing systems performance by personnel and to restrict access only to authorized systems, different kind of substitute arrangements, education, defining the responsibilities and rights and clarifying the background information of people is used. Normally human resources is responsible of personal security together with IT and security department. (Hakala et al 2006, 11.)

2.4.4 Data security and data communication security

Data security contains all the actions that are used for storing, backup, restoring and destroying the data. Data contains both digital and traditional data. (Hakala et al 2006, 11.) The basis for data security is confidentiality; what kind of data is used in company, how important the data is, how confidentiality is defined and subscribed and how it affects data lifecycle. The purpose is to ensure the correct data only for those people who need it. (Miettinen 1999, 22-23.) With data communication security target is to protect company's continuous and trouble-free data communication both in local area network and in wide area network.

2.4.5 Software security

With software security companies try to ensure that all software are permissible and licensed, they are planned for their use, all software are compatible and they are reliable and flawless. (Hakala et al 2006, 11., Miettinen 1999, 21-22.)

2.4.6 Hardware security

In hardware security part a computer and other devices are viewed from appropriate design, functionality testing, service and aging point of view. Also, taking care of risk factors is a part of hardware security. (Hakala et al 2006, 12.) With hardware security only reliable devices will be provided into daily use. (Miettinen 1999, 21.)

2.5 Information security planning

Hakala et al (2006) says that modern information security planning is based on business security and company's overall security, which in strategy level defines targets for information security as a part of bigger ensemble. Organization structure should support overall security and all departments or units responsible for security in somehow, should operate under same management. Otherwise there will be different kind of security cultures in the same company and that leads to overlapping work, overlapping or separated systems for access control, locking systems and building automation even when existing ICT systems could be used. (Hakala et al 2006, 14, 17.)

According to Hakala et al, first of all the overall security should be defined for whole organization in a company. If there are any plans made earlier for physical security and information security, those plans will be combined and all discrepancies and overlapping will be removed. Business processes and their security demands will be separated and which is very important, owners of business processes will be find out. That is the basis for process matrix and gives also answer who is responsible for each process in security manner. (Hakala et al 2006, 15- 16.)

Information security planning should never be done by only ICT people or by physical security people, says Hakala et al. Good planning take into consideration people and their functions and needs in different organization level. It requires strong commitment from process owners and commits people into overall security definition in every level. Security planning is usually done in workshops or in projects. In those workshops or projects there should be members from every level of organization: top management representative to support planning, progression and decision making, security managers, process owners, employees, experts from ICT, occupational safety and health representative and also other experts if needed. This ensures comprehensive security planning and awareness of overall security for whole company in its every organization level. (Hakala et al 2006, 18.)

By clarifying the responsibilities and making co-operation in overall security planning, clear and simple picture of security needs will be achieved. It is the basis for combining the practices, and what is also very important for company and its top management, significant cost savings will be achieved because of removing overlapping systems. (Hakala et al 2006, 14-18.)

2.6 Information security management

Miettinen states that leading the information security is not separated from other management functions in company. It is based on same models, methods and tools like in other functions but it takes into consideration special features of information security. The basic elements for information security management are (Miettinen 1999.):

1. Risk identification
2. Determining the protection level
3. Protection planning
4. Protection implementation
5. Monitoring
6. Development

Miettinen states also the key issues to develop information security are risk identification and level of risks. They are basis for defining the level of protection for several parts of security, such as data, people, and spaces or similar. That will lead for the planning, how to protect all the risks which has been identified in every level. Planning requires very professional and intensive management in every phase to fulfill all the requirements for protection. Planning has to be done very comprehensive.

When basic work with risk identification, protection level determination and protection planning has been done with care, the implementation phase can be done successfully. Implementation phase should be controlled by professional management to ensure high quality.

Miettinen states that information security has to be monitored, so it is just like other functions in company too. Monitoring is essential part of management and information security is not an exception. Only the methods are focused on information security to ensure adequate protection level. The company has to monitor its systems to find out possible shortages and weaknesses and also to find out new, unknown threats. There are several parties who are monitoring information security in companies and in bigger companies there are both internal and external inspection parties.

According to Miettinen, protection level has to be evaluated and measured regularly because threats, used protection methods and company actions are changing when time goes by. Indicators has to be developed to evaluation and measuring just like in other functions in company, e.g. in quality department. Evaluation and measuring are basis for developing protection level and so far so information security. (Miettinen 1999, 95-98.)

2.7 Information security policy

Information security planning leads to the functional information security policy in the company. It is collection of management accepted practices which help to achieve and maintain information security level in demand. It is compiled as a generic level to describe the data security degree, methods to use and how information security is managed and developed. Top management is responsible for creating company’s information security policy. (Hakala et al 2006, 7.)

Information security policy is created as a written form and it is often created for five or even ten years. That is why it cannot contain very specific details of information security implementation in companies. It has to be checked yearly to match company’s operations and security needs. (Hakala et al 2006, 7.)

It is very important to understand the purpose of information security policy. Company’s information security policy is always public and meant to own personnel, customers and other partners to show and convince company’s aspiration to protect its own and stakeholder’s information. It should be always written to the form which is understandable for every employee and other people, not only for IT or administrative experts. It should not be too generic though and should contain following components according to Hakala et al (Hakala et al 2006, 8.):

- Definitions of company’s own information security policy, the major targets, scope and especially the importance for organization operations.
- Management support to achieve and follow the targets and principles as a part of company’s business strategy.

- Frames to recognize the risks and especially frames to control the risks.
- Summary of information security rules, followed standards and general principles.
- Summary of legislation, agreement and trade practices requirements.
- Summary of methods and training for security approach.
- Description of business continuity with information security.
- Definitions of responsibility areas in information security and reporting of security incidents.
- Consequences of information security violations.
- Catalog of more specific instructions and standards.

2.8 Information security plan and instructions

According to Hakala et al, information security plan and instructions are created by security responsible people together with ICT experts. They contain detailed information about technical systems and used methods in written form, and thus they are classified confidential or secret. There are practices in concrete mode to full fill security requirements based on required level of information security. Information security policy defines boundary conditions for information security plan, but the plan is normally made for two to five years and it has to be checked more often. It has to be checked after each change in the systems but at least once in a year. Based on information security plan more detailed instructions are created for specific systems or processes. Those instructions should be made so, that end users will understand them and are able to use them whenever they are needed. (Hakala et al 2006, 9-10.)

2.9 Business requirements for information security

This chapter describes the business requirements for an IT endpoint security and compliance management. There are certain drivers that influence why and how IT endpoint security and compliance management must be done in a certain business context. Most projects are driven by both business and IT drivers, however, business drivers are likely always the most important drivers.

2.9.1 Business drivers

Business drivers measure value, risk, and economic costs that affect their approach to IT security. Business drivers also present issues and consequences of significance to the stakeholders. They represent a relationship between the IT organization and the rest of the business and business drivers refer to business values that must be supported by the IT security infrastructure. (Buecker, Campos, Cutler, Hu, Jeremiah, Matsui & Zarakowski 2012, 4.)

These are the business drivers that influence security (Buecker et al 2012, 4-6.):

- **Correct and reliable operation**. Correct and reliable operation is the key factor for the business. Correct operation means that the operations perform the correct response or function without errors. Reliable means that the same result occurs all the time.

- **Service-level agreements.** Service-level agreements (SLAs) include acceptable conditions of operation within an organization. Availability of systems, data, and processes are conditions commonly referenced within SLAs.

- **IT asset value.** From the business perspective, the IT asset value directly relates to the value of the business transactions that it supports.

- **Protection of the business asset value or brand image.** This driver captures the desire of the firm to protect its image. The loss of goodwill from a security incident or attack has direct consequences to the business.

- **Contractual obligation.** Depending on the structure and terms of the contract, the consequence might lead to financial loss or liability because of security attacks. For example, when security incidents are encountered, the business might be unable to fulfill its contractual obligations of providing goods or services.

- **Financial loss and liability.** Direct or indirect financial loss is a consequence to the business as a result of a security incident, such as theft of an asset, theft of a service, or betrayal. Indirect loss might include loss based on civil or criminal court ruling, loss of good will, or re-prioritized budget allocation.

- **Critical infrastructure.** Security threats or threat agents can have a huge impact on services or resources that are common. Examples include telecommunications, electrical power, transportation systems, and computing. An important part of risk analysis is identifying critical infrastructure.

- **Safety and survival.** Security threats and threat agents can have a major impact on aspects of human life, government function, and socio-economic systems.

2.9.2 IT drivers

IT drivers present operational constraints in the general IT environment. For example, the complexity of a system, including its environment, that is exposed to internal and external threats presents risks that the organization must address. IT drivers represent technical considerations that affect the trustworthiness of the IT environment and likely the business systems as a whole. The combination of business and IT drivers represents the key initiatives for security management. (Buecker et al 2012, 4.)

These IT drivers influence the security according to Buecker et al (Buecker et al 2012, 7-9.):

- **Internal threats and threat agents.** An example of an internal threat is a poorly designed system that does not have the appropriate controls. An example of an internal threat agent is a person who uses an ability to access the IT system or influence business or management processes to carry out a malicious activity. These threats and threat agents might be associated with technology or people.

- **External threats and threat agents.** Examples of external threats are single points of failure for one or more business or management processes that are outside the enterprise boundary, such as a power system grid or a network connection, or a computer virus or worm that penetrates the system. An example of an external threat agent is a malicious hacker, or someone who gets the ability to act as an insider, by using personal electronic credentials or identifying information. These threats and threat agents are also associated with technology or people.

- **IT service management commitments.** Poor operation of the IT system might result in security exposures to the business. This driver can be divided into two categories: IT service delivery and IT service support.

    - **Service delivery commitments**
      An example of security exposure for service delivery is when IT operations processes cannot respond to critical events in a timely manner. Another example is when IT processes cannot recover from a denial of service attack in a timely manner.
    - **Service support commitments**
      The failure of the business or IT management system to meet its service level agreements (SLAs) can be viewed as a security exposure to business or management processes. An example of security exposure for service support is a situation in which the customer relationship processes do not add, modify, or remove users from access control lists in a timely manner.

- **IT environment complexity.** An environment with a larger number of systems, varied network access paths, or a complex architecture, is a complex IT environment and any IT environment that is connected to the intranet or extranet is exposed to internal or external threats or and requires specific security responses. Data system connected with other systems and other firms represents a more complex environment.

- **Business environment complexity.** Because most businesses rely on IT, most business environments are an interconnected set of businesses, each with its own complex IT environment, business processes, and IT management processes. This complexity might contribute to the security or insecurity of the IT system.

- **Audit and traceability.** This identifies the need for the IT system to support an audit of information contained within the system, whether it is associated with management data or business data.

- **IT vulnerabilities: Configuration.** Configuration vulnerabilities are potentially present in every IT system, providing an opening to a potential attack based on the system and how it is designed and set up.

- **IT vulnerabilities: Flaws.** Software flaws potentially exist in every IT system. These flaws represent vulnerabilities that were not detected and are not evident in the design documents. An example is a defect in an operating system or application that is discovered after implementation.

- **IT vulnerabilities: Exploits.** The basic design of software in any IT system might be exploited by threats or threat agents as a part of an attack on the IT system, the business, or the management processes. The exploits can also be viewed as the openings or avenues that an attacker can use.

2.10 Endpoint security and compliance management

According to Buecker et al (2012), organizations can have thousands of endpoints that must be tightly controlled to effectively manage risk. As an endpoint, varieties of servers, desktops, notebooks and mobile IT devices are known, and the amount of those devices is growing at unprecedented rates. Endpoints need to be kept secure to effectively manage risk. Protection of the endpoints can be costly, complex, and time-consuming, stretching IT staff thin and driving costs even higher. (Buecker et al 2012, 16.)

After security infrastructure is in place, many organizations must prove compliance with internal policies, security standards, laws and government regulations. After compliance levels are achieved, organizations must ensure that the compliance levels are continuously maintained. Controlling costs is high on the priorities of IT leaders, affecting IT teams that are being asked to do more with less. That leads to requirement for the organizations to have a tool that is simple and scalable. The tool must automate management capabilities so that costs and complexity are controlled, while still being able to meet compliance requirements. (Buecker et al 2012, 16.)

Endpoint security and compliance management are important to the management of IT security. It is important to plan an approach that can be an effective for the entire company. Organizations must build services that are secure by design, not added afterward. This allows organizations to securely and safely adopt new forms of technology that run on new endpoint devices. Also various business models, such as outsourcing can be used more safely for instance for cost benefit. (Buecker et al 2012, 19.)

2.11 Overview of information security risk management process

SFS-ISO/IEC 27005 standard says that “A systematic approach to information security risk management is necessary to identify organization’s needs regarding information security requirements and to create an effective information security management system (ISMS).” This approach should be in line with overall enterprise risk management and risks should be handled in an effective and timely manner where ever and whenever they are needed. Information security risk management should be an essential part of all information security management activities, both in implementation and in operation phases. (SFS-EN ISO/IEC 27005, 2009, 15-19.)

Finnish Ministry of Finance has released an issue ‘Risk Assessment Instruction to Promote Government Information Security’ where it is stated, that normally it is thought that information risks are probabilities which focus on data and data usage. The issue is created by government information security management group, called VAHTI (Valtionhallinnon tietoturvallisuuden johtoryhmä). The issue says that information risk is the situation when the data or data system is not in use, data has been transformed because of some incident, or data has ended up for external people. Those risks are always the risks of injury, which lead to losses, both economical and image.

According to VAHTI issue information risks can be caused by people, technical failures or a weather phenomenon and they can be intentional or unintentional. Professional attack is equally likely unintentional mistake and because of that, both scenarios have to be prepared for. It has to be prepared for those scenarios because of data confidentiality, usability and integrity.

Also, in the issue is said that managing the information risks is one part of normal decision making which is chargeable by organization management and it should be a continual process. The target is the continuity of business operations. Finding the correct level for information risks is very important because organization’s data is one of the protected targets and it can also affect other organizations, such as customers, partners or similar. The process should establish the context, assess the risks and treat the risks using a risk treatment plan to implement the recommendations and decisions.

In a risk survey the target is to find the probability of threats and the seriousness of threats consequences. The same methods can be used to evaluate information risks like other risks too; however, special features of information risks cannot be forgotten. Because information and data are not concrete issues, there are challenges with data networks, storage formats and information security wide-ranging. When the risks have been surveyed and evaluated, the organization knows the recognized risks. With a management plan the organization decides how to react to the information risks. (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, Foreword.)

2.12 Management activities of information security management system

According to SFS-ISO/IEC 27005 standard following parts are included in the “plan” phase of an ISMS: establishing the context, assessing risks, developing risk treatment plan and accepting risks. In the “do” phase of the ISMS, the actions and controls required to reduce the risk to an acceptable level are implemented according to the risk treatment plan. In the “check” phase managers determine the need for revisions of the risk assessment and risk treatment, in case of incidents and changes in circumstances. In the ”act” phase, any actions required are performed. (SFS-EN ISO/IEC 27005, 2009, 19. SFS-EN ISO/IEC 27001, 2006, 7.)

Table 1 summarizes the management activities in case of information security risk relevant to the four phases of the Information Security Management System process (SFS-EN ISO/IEC 27005, 2009, 19. SFS-EN ISO/IEC 27001, 2006, 7.):

TABLE 1. Information security risk management activities and processes

Information Security Management System Process	Information Security Risk Management Process
Plan (establish the ISMS)	• Establish ISMS policy, objectives, processes and procedures • Risk assessment • Developing risk treatment plan • Risk acceptance
Do (implement and operate the ISMS)	• Implementation of risk treatment plan • Implement and operate the ISMS

	policy, controls, processes and procedures
Check (monitor and review the ISMS)	• Continual monitoring and reviewing of risks • Assess and measure process performance against ISMS policy, objectives and practical experience • report the results to management
Act (maintain and improve the ISMS)	• Maintain and improve the Information Security Risk Management Process • Take corrective and preventive actions, based on the internal audits

2.13 Risk analysis

Hakala et al state that starting point for the risk analysis is always an organization's overall security. Risk management and documentation of other than data systems have to be familiarized with before doing any risk analysis for data systems. Data systems and data protection needs have to be prioritized by data classification system and data system based risk analysis will be done in the order or precedence given by those systems. (Hakala et al 2006, 79-82.)

According to Hakala et al a risk analysis can be divided into two phases: risk survey and risk evaluation. The risk survey tries to find out all the risks and threats concerning a company's operations. In the risk evaluation, effects for found risks and threats are evaluated with correct indicators. Normally indicators are classification systems and criteria of them, and usually risk analysis begins with qualitative investigation of threats and risk factors. The analysis can be continued with the consequences of the most significant threats and event frequency survey, if any more detailed information is needed for decision making. Consequences can be described by different kind of calculation methods for disturbances. (Hakala et al 2006, 79-82.)

2.14 Risk survey

About risk survey Hakala et al states that in risk survey it is important to deal with both current situation and future threats. If there is a comprehensive and well structured documentation about organization's data systems, risks can be handled together with system definitions. Otherwise it is better to use mind mapping to survey the risks. If whole personnel are to be involved in the risk survey, better results can be expected. To find out any possible risks and threats, IT expertise, management and end user know-how will be needed all together. (Hakala et al 2006, 79-82.)

Data problems encountered should be taken as a starting point for the risk survey. If there have been any serious problems or damages with the data systems, users often remember those cases. Cases are written down and will be placed to the correct category of risks. Also any other possible risks will be scanned: some kind of damages, problems or events which have not been realized yet but are potential. These are also placed to the correct category of risks. Finally, also the future will be viewed and potential threats with technology and environment are tried to be found out. (Hakala et al 2006, 79-82.)

2.14.1 Common risk survey

Before making the risk survey for various data systems, it is better to make a general risk survey, state Hakala et al. The purpose is to find out any general risks and threats which could happen and threaten data security anywhere in the data systems. Mind mapping is very good method to find out risks and threats from every personnel group involved into risk survey. (Hakala et al 2006, 79-82.)

2.14.2 Data system specific risk survey

Hakala et al also state, that after finding out common risks for the data systems, the risk survey for various data systems can be made and common risk survey can be used as a help for that. Data system specific survey can reveal risks not found in common risk survey and vice versa. Also, other data systems have to be reviewed if there are any connections to the systems under survey. Especially data communication risks have to be reviewed, not only internally but also between organization and suppliers. (Hakala et al 2006, 79-82.)

2.15 Risk assessment

According to Hakala et al, when the risks and threats of data system have been clarified, the risk assessment can be started. Essential targets of assessment are risks which affects to the operations of organization. Probability of happening of risks is also essential in risk assessment. Data will be located in the data classification system and that is the basis for thinking, how serious damages integrity, usability and confidentiality risks cause to the organization. Seriousness and probability of risks are reviewed simultaneously. The bigger and more likely the damage, the more prepared the organization has to be for the risks. (Hakala et al 2006, 79-82.)

2.16 Risk management

The first phase in risk management is to recognize the threats. When this is done and probability and the severity of consequences have been evaluated, planning and deciding of actions can be carried out to manage the risks. There are many ways to do that and the main actions, which are described in VAHTI issue, are (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 21.):

- Avoiding the risk. Often this is only possible if action with risk is totally refrained.

- Removing the risk. Individual risk can be removed but that might cause totally new risks.
- Reducing the risk. First of all it is important to try to prevent any damages happening or to reduce the consequences of them.
- Transferring the risk by agreements or by insurances.
- Keep the risk at one's own risk. Some of the risks has to be kept or is worth of keeping at one’s own risk. It means that organization is aware of risk that threat can be happen.

Actions to reduce the risks can be (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 21-22.):

- Technical actions like new device rooms or workspaces, developing the computer protection, technical backups, alarm systems and service and maintenance improvements.
- Actions of organization like agreeing the common rules, creating directives, developing of controlling and monitoring, improving the flow of information and work planning and agreeing of responsibilities.
- To improve the functioning of individual’s opportunities, like buying new tools, making guidelines, orientation and training, new working time arrangements or working pair arrangements.

All the risks cannot be removed. In the ‘Risk Assessment Instruction to Promote Government Information Security’, risk management measures have to be started from the largest of the estimated risks and extend as widely as possible. Risk management is always associated with the cost of the evaluation measures, so it has to be thought how much to invest in insurance and in the various actions to reduce the risks. (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 41)

In the end of the risk analysis, it has to be agreed how to go forward and implement measures proposed in the risk assessment. At the same time the responsible persons and a rough schedule have to be agreed upon. Progress will be monitored in the regular meetings, e.g. every six months. (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 47)

All developed improvement measures cannot be implemented immediately. With risk evaluation the biggest risks has been identified. Usually it is better to start by removing or reducing them. Sometimes, improvement measures require further study, additional planning and investment. However, it is not worth of waiting for the removal of the main risks, but at the same time small improvements can be done to manage minor ones. Often the actions can be implemented easily with a small investment, e.g. with new practices and training. (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 47)

A practical tool for risk assessment is described in Table 2, which is presented in Risk Assessment Instruction to Promote Government Information Security' issue. There are three different levels in the table for the threat probability and the severity of consequences. Based on the concluded statements the severity of consequences is chosen first from the table's first row. After that the probability of the issue is chosen from the first column. The risk is the value in the point of intersection of selected items. So it can be that 1 the lowest (insignificant risk) and 5 peak (unacceptable risk). (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 43.)

TABLE 2. Risk assessment

Criticality		**Severity of consequences**		
		Minor (1)	Serious (2)	Very serious (3)
Threat probability	High (3)	3. Moderate risk	4.Significant risk	5.Unacceptable risk
	Average (2)	2.Minor risk	3.Moderate risk	4.Significant risk
	Low (1)	1.Insignificant risk	2.Minor risk	3.Moderate risk

In the Ministry of Finance issue it is stated that results of the review have to be brought to the attention of every party. The management of the office and personnel have to be informed about the results and told about the follow-up. Informing can be done by arranging information sessions, informing in the meetings, by publishing the results in the house journal or by creating the separate information letter.

Risk management training is one way to plan the organization's activities in different threat situations. As a part of the further development of measures, the organization's preparedness to act in a situation such as a virus attack can be tested. In the actual exercise, the different actors operating in the special scenario will be gone through. After the exercise the results will be reviewed and corrective action plans will be done.
(Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 47-48)

2.17 Information Security Standards as a part of the risk management

In recent years, according to ‘Risk Assessment Instruction to Promote Government Information Security’, several security standards have been created and with those standards organizations can develop their own information security and evaluate the efficiency and effectiveness of their own systems. In this chapter four key standards has been introduced. These represent somewhat different approaches to security risk management and control.

BS 7799 (ISO 17799) is published by British Standard Institution’ in (BSI) and contains information security management system standard, which is published in two parts:

- BS 7799-1: Systems of practice for information security management
- BS 7799-2: Systems requirements for information security management

The standard provides a model of information security management system for the construction and management. The standard requires the organization to identify safety first source of risk analysis, which identifies the threats to securable objects and to assess susceptibility to damage, the likelihood of accidental injury and the potential impacts.

When creating a standard for information security management system, the organization shall determine the scope of the management system and a systematic risk assessment approach. It has to recognize and evaluate the risks and options to process them, select the control objectives and security mechanisms of risk handling. The organization has to also prepare an implementation plan.

Common Criteria for Information Technology Security Evaluation (ISO 15408) is the information security evaluation, and classification of evaluation criteria, developed for the strength of information and information technology products. Systems and products may be developed security profile, which describes information security functional requirements for the system. The criteria can be also used to develop own systems and to make award decisions. Evaluation can be used when thinking if data system can fulfill the information security requirements. These requirements are normally recognized in risk analyses and in the information security policy.

Common criteria is divided into three parts (Risk Assessment Instruction to Promote Government Information Security, VAHTI 7/2003, 22-23):

1. Introduction and general model. Defines the general concepts and principles for the assessment of information technology products and systems.
2. Security functional requirements. Presents a set of functional components, which are expressed in a standardized way to evaluate the functional requirements of the object. Requirements are tabulated by component, by family and by category.
3. Information security confidential requirements. Presents a set of confidential components, which are expressed in a standardized way to evaluate the confidential requirements of the object.

ISO/IEC 27005:2008 ”Information technology. Security techniques. Information security risk management” standard provides guidelines for information security risk management in a company, supporting the requirements of an ISMS according to

ISO/IEC 27001. However, the standard does not provide any specific methodology for information security risk management. This standard is relevant to managers and personnel concerned with information security risk management in a company, and in some cases also for external parties supporting information security functions.

ISO/IEC 27005:2008 standard contains the description of the information security risk management process and its activities. The following information security risk management activities are presented (SFS-EN ISO/IEC 27005:2008, 2009.):

- Context establishment
- Risk assessment
- Risk treatment
- Risk acceptance
- Risk communication
- Risk monitoring and review.

Additional information for information security risk management activities is presented in the annexes of the standard.

What can be achieved with the help of this standard (SFS-EN ISO/IEC 27005:2008, 2009.):

- Risks are identified
- Risks are assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of the risks are communicated and understood
- Priority for risk treatment
- Priority for actions to reduce risks
- Stakeholders are involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risks and the risk management process are monitored and reviewed regularly
- Information has been captured to improve the risk management approach

- Managers and personnel are educated about the risks and the actions are taken to reduce them.

“ISO/IEC 27001:2005 ”Information technology. Security techniques. Information security management systems. Requirements” standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS. It specifies requirements for the implementation of security controls in a company or in a part of company. The ISMS is designed to ensure the selection of adequate security controls that protect information assets and give confidence to the stakeholders.

This international standard adopts a process approach for ISMS. The process approach for information security management presented in this standard encourages its users to emphasize the importance of following issues(SFS-EN ISO/IEC 27001:2005, 2006, 9.):

- understanding an organization’s information security requirements
- implementing and operating controls to manage an organization's information security
- monitoring and reviewing the performance and effectiveness of the ISMS
- continual improvement based on objective measurement.

The standard presents the "Plan-Do-Check-Act" (PDCA) model and Figure 4 shows how ISMS takes as input the information security requirements and expectations of the interested parties or stakeholders, and through the actions and processes produces information security outcomes that meets those requirements and expectations. Figure 4 also shows the links in the processes. (SFS-EN ISO/IEC 27001:2005, 2006, 9.)

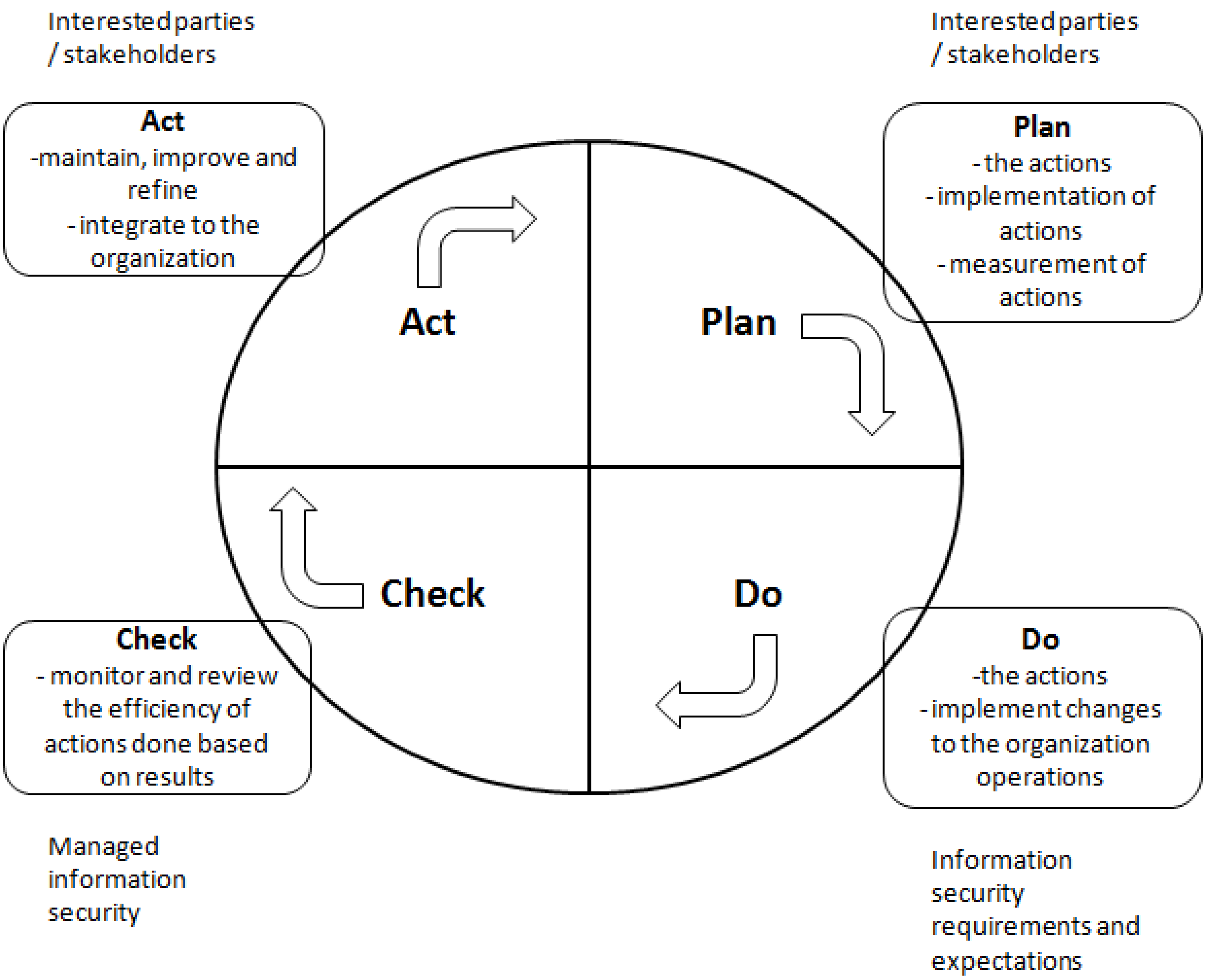

Interested parties / stakeholders
Act
-maintain, improve and refine
-integrate to the organization
Interested parties / stakeholders
Plan
-the actions
-implementation of actions
-measurement of actions
Act
Plan
Check
Do
Check
- monitor and review the efficiency of actions done based on results
Do
-the actions
-implement changes to the organization operations
Managed information security
Information security requirements and expectations

FIGURE 4. PDCA model applied to ISMS processes (SFS-EN ISO/IEC 27001:2005, 2006, 9.)

2.18 Endpoint security definition

What is endpoint and what does endpoint security or protection mean? What is Windows desktop endpoint security? What comes into one's mind when talking about the endpoint security? Endpoint security is essential for every corporation. With new vulnerabilities, new attacks, new data leaks every day, endpoint security should get a high attention in companies. Endpoint security is a collection of security features and solutions that protect the key areas where endpoints become an attack vehicle, can be attacked, or become a risk to the entire network.

Endpoint security is not just antivirus or firewall functionality but also endpoint password policy, endpoint least privilege, and endpoint data leak protection. In this thesis those three areas are not viewed but mainly a product which will provide antivirus and firewall functionality with centralized management in a large company IT environment.

Usually when talking about the endpoints, some IT devices which are used by someone outside of the IT department are referred to, and which are located on a corporate network somewhere. Mr. Derek Melber discusses in his two part article that when talking about the Windows computers, over 90% of all worldwide endpoints are running Windows XP or Windows 7. Windows 9x, Windows 2000, and Windows Vista are no longer that popular and in the typical corporation these operating systems are often considered legacy. The scope of this thesis is computers with Windows operating system and specially Windows 7 computers.

The endpoint device is typically joined to a Windows Active Directory domain, or some other type of enterprise directory. They are typically physical desktops, virtual desktops, laptops, tablets, and possibly Windows phones, continues Melber. (Melber 2012.)

2.19 Malware, spyware and viruses as a threat

Today‘s cybercriminals have huge resources and advantages over end-users of personal computers. Their ability to develop, mutate and launch a myriad of attacks — ranging from phishing and malware, exploits – appears significant. In too many cases, vulnerabilities in a PC‘s software can be exploited when a user visits an infected web site — silently, without the user‘s knowledge. Socially-engineered malware attacks trick users into downloading and running malicious programs disguised as movie files, codecs, and other utilities. Detecting and preventing these threats continues to be a challenge as criminals become more aggressive. There is a widely-held belief that as long as a user does not visit the doubtful parts of the Internet, he/she is not at risk from attacks. This is obviously false; end users are at risk no matter where they surf. (NSS Labs, Consumer anti-malware products, Group test report 2010.)

According to Mell, Kent and Nusbaum (2005) malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually secretly, with the intent of compromising the confidentiality, integrity, or availability of the data, applications, or operating system or otherwise disrupting the victim. Malware has become the most significant threat to most systems, causing widespread damage and disruption, and requiring large recovery efforts within most organizations. Spyware — malware intended to violate a user's privacy — has also become a major concern to organizations. Although privacy-violating malware has been in use for many years, it has become much more widespread recently. Spyware invade systems to monitor personal activities and conduct financial fraud. Organizations also face similar threats from a few forms of non-malware threats that are often associated with malware. One of these forms that has become commonplace is phishing. Another common form is virus hoaxes, which are false warnings of new malware threats. (Mell, Kent & Nusbaum 2005.)

As an example, client-side exploits count on users visiting infected websites in order to exploit web browsers, browser plug-ins, and add-on applications such as Adobe Acrobat and Flash. Once the PC has been hijacked, the attacker uses that machine to attack others — either remotely as part of a "bot" or locally to gain corporate secrets including personal and financial information, such as credit cards, bank account access, passwords, social security numbers, etc. These exploits represent the newest and most serious threats, since they occur silently, without user awareness, when a user visits a malicious website. Figure 5 shows how client-side exploits work. (NSS Labs, Consumer anti-malware products, Group test report 2010.)

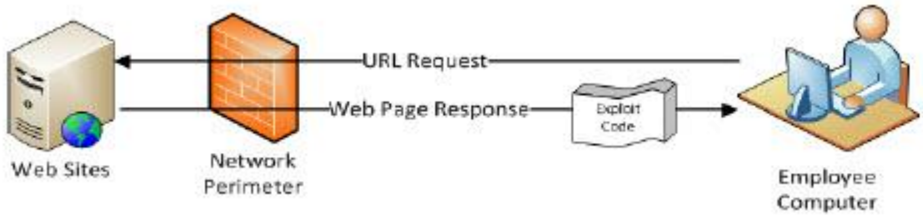


FIGURE 5. Client-side exploit

In their "Guide to Malware Incident Prevention and Handling " guide, Mell, Kent and Nusbaum states, that organizations should perform threat mitigation efforts to detect and stop malware before it can affect its targets, and that the most commonly used threat mitigation technical control is antivirus software. They strongly recommends that organizations deploy antivirus software on all systems for which satisfactory antivirus software is available, including workstations, servers, mobile devices, firewalls and various kind of servers. Additional technical controls that are helpful for malware threat mitigation include intrusion prevention systems (IPS), firewalls, routers, and certain application configuration settings. (Mell et al 2005.)

Because new malware threats appear continuously, organizations should establish malware incident prevention and handling capabilities that are robust and flexible enough to address the threats. Both malware and the defenses against malware continue to evolve, so it is continuous race against each other in response to improvements in the other. For this reason, organizations should stay up-to-date on the latest types of threats, the security products against the threats and methods to mitigate and remove them. Because the effectiveness of prevention techniques may vary depending on the environment (i.e. a technique that works well in a managed environment might be ineffective in a non-managed environment), organizations should choose preventive methods that are well-suited to their environment and systems.

3 IMPLEMENTATION OF STUDY

3.1 Qualitative and quantitative analysis

Basically, quantitative research and analysis are objective; qualitative are subjective. In quantitative analysis (research) there is always numerical data matrix where material is capsulized. The analysis in quantitative research is based on that capsulized data. The objectivity is gained by staying outside of the interviewed subject, so the research worker is like an outsider. Questions or meters are justified based on theory.

(Tilastokeskus). Measurement must be objective, quantitative and statistically valid. Simplified, quantitative research is numbers, objective hard data (Anderson 2006).

> *Qualitative Research is collecting, analyzing, and interpreting data by observing what people do and say. Whereas, quantitative research refers to counts and measures of things, qualitative research refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things.(Anderson 2006.)*

In qualitative research different kind of methods are used to collect the information, for example in-depth interviews (Anderson 2006). Today qualitative research means a whole series of different researching methods; however, the material point of view is essential for all of those methods. The quality of the findings from qualitative research is dependent on the skills and experience of the research worker. The objectivity of qualitative research is gained by researcher not to include his or her own beliefs, attitudes and values with the research. During the analysis phase the material collected is seeking to organize and understand. Theory is the starting point for reading, analyzing and thinking the material (Tilastokeskus).

Within the same research there is possibility to use different kind of theories, methods and material, both qualitative and quantitative material, to solve the same research question. In this thesis both methods, qualitative and quantitative, are used. Using those both methods is very suitable for this thesis like development work in companies.

3.2 Development work and question

This thesis investigates and compares different kind of endpoint protection security products as an enterprise wide solution for enterprise endpoint devices. Two chosen products for the comparison are Microsoft Forefront Endpoint Protection 2010 (FEP) and Symantec Endpoint Protection 11 (SEP). Because of financial aspects related to Microsoft licensing model changes 2011, Metso corporation has considered if it would be reasonable to change endpoint protection product totally for the new one. The functionality of the new product has to be known and it has to fulfill security requirements of the company for malware, spyware and virus protection in company endpoints. Because SEP 11 has been used in Metso for years, a following development question arise:

1. Would Microsoft Forefront Endpoint Protection 2010 be secure and cost-effective enough system to fulfill the requirements of security in Metso and in other similar kind of companies?

3.3 Analysis methods

The theoretical part of this thesis consists of reviewing relevant literature and utilizing already existing analysis and comparisons made on the products. The analysis methods used in this thesis are literature research and the table of the comparison with weighted scores. So the research is combination of qualitative and quantitative analysis where scores represent quantitative research, and evaluation and comparison represents qualitative research.

4 RESULTS OF STUDY

4.1 Product overview

Microsoft has invested in the security area for its products over the last several years. They have invested in a fair amount of money in the Security Development Lifecycle (SDL), improved the security of Windows desktops and servers, SQL is more secure as an example as well as Microsoft Office products. They have an effective monthly patch publishing method for the supported operating systems and for core products. However, companies try to avoid putting too many eggs in any one basket. They consider that by balancing the risk between Microsoft (operating system itself) and another vendor (e.g.: Symantec, McAfee, Trend Micro) for endpoint security, they are expanding their protection capabilities.

Prerequisites for Deploying Forefront Endpoint Protection on a Client

Table 3, provided by Microsoft, is a list of the prerequisites for deploying the Endpoint Protection on client computers. (Microsoft Technet 2012.)

TABLE 3. Prerequisites and requirements of FEP client

Prerequisite	**Requirement**
Configuration manager	A Microsoft System Center Configuration Manager 2007 site that has Endpoint Protection server installed.
Operating system	Windows 7 (x86 or x64) Windows 7 XP mode Windows Vista (x86 or x64) or later versions Windows XP Service Pack 2 (x86 or x64) or later versions Windows Server 2008 R2 (x64) or later versions Windows Server 2008 R2 Server Core (x64) Windows Server 2008 (x86 or x64) or later versions Windows Server 2003 Service Pack 2 (x86 or x64) or later versions Windows Server 2003 R2 (x86 or x64) or later versions For the following operating system, you can deploy the Endpoint Protection client and deploy Endpoint Protection policies, but the client will not be able to report status back to the Endpoint Protection dashboard. Windows Server 2008 Server Core (x86 or x64)
Available disk space	255 MB
Additional requirements	Windows Installer 3.1 or later versions Secondary Logon service must not be disabled Filter manager rollup package for Windows XP Service Pack 2 (x86) KB914882

Competitive uninstall	The client installation checks for and uninstalls the following existing antimalware clients: Symantec Endpoint Protection version 11 Symantec Corporate Edition version 10 McAfee VirusScan Enterprise version 8.5 and version 8.7 and its agent Forefront Client Security version 1 and the Operations Manager agent TrendMicro OfficeScan version 8 and version 10

Forefront Endpoint Protection Builds on Security Essentials

Mr. Derek Melber discusses in his article ‘Microsoft Forefront Endpoint Protection 2010 - Is Microsoft Anti-virus Good Enough’, that Microsoft released Security Essentials in November, 2008 and that was Microsoft’s first real coming into the anti-virus space. Microsoft Security Essentials was targeted for consumers and it was the first product from Microsoft to offer a complete anti-virus and anti-spyware solution that was free. Advertising itself as lightweight, efficient and accurate anti-malware solution that ‘stays out of the way’, Security Essentials rapidly took share in the consumer anti-virus space, Melber continues.

Microsoft claims that Security Essentials does not compete with other “for-pay” anti-virus software, states Melber, but is instead targeted towards the 50-60% of PC users who do not have (or will not pay for) anti-virus and anti-malware protection. Security Essentials and Forefront Endpoint Protection share the same Microsoft Anti-Malware engine. (Melber 2011.)

What is FEP?

In his article about Microsoft Forefront Endpoint Protection 2010, Mr. Kurt Shintaku states, that Microsoft Forefront Endpoint Protection 2010 (FEP) provides endpoint protection for business environments, including not only antimalware, but behavior monitoring and firewall management protections. Forefront Endpoint Protection also includes central deployment, configuration, and reporting features needed for ensuring protection are maintained across the enterprise.

Also, Shintaku claims that Forefront Endpoint Protection, the next generation release of Forefront Client Security, simplifies and improves endpoint protection while greatly reducing infrastructure costs. Built on Microsoft System Center Configuration Manager 2007, it will allow customers to use their existing client management infrastructure to deploy and manage endpoint protection. This shared infrastructure lowers ownership costs while providing improved visibility and control over endpoint management and security.

Key features included in FEP include:

- **Integration with Configuration Manager.** Single interface for managing and securing endpoints reduces complexity and improves troubleshooting and reporting insights.
- **New Antivirus Engine.** Highly accurate and efficient threat detection protects against the latest malware and rootkits with low false positive rate.
- **New behavioral threat detection.** Protection against “unknown” or “zero day” threats provided through behavior monitoring, emulation, and dynamic translation.
- **Windows Firewall management.** Ensures Windows Firewall is active and working properly on all endpoints, and allows administrators to more easily manage firewall protections across the enterprise.

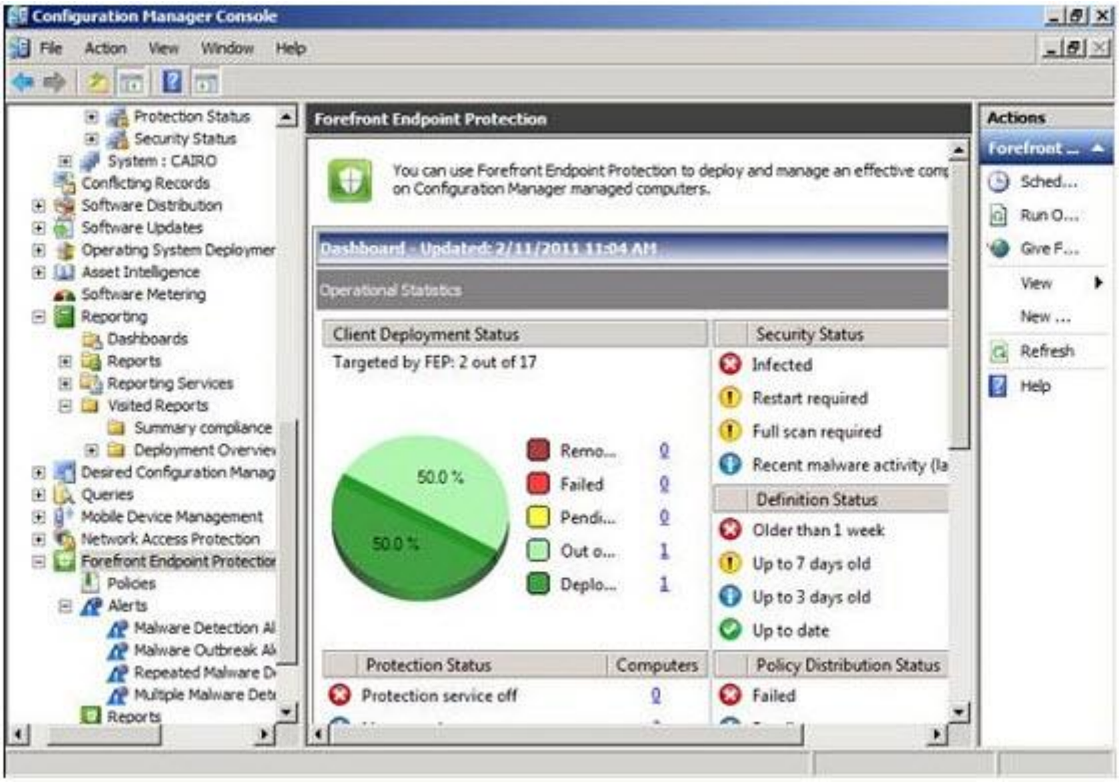
According to Shintaku, one of the major inclusions within Forefront Endpoint Protection is Host Intrusion Prevention capabilities. Host intrusion prevention includes a wide variety of technologies that help prevent unwanted activity on endpoint and server operating systems. These protections are spread across the application, file system, and network layers. Forefront Endpoint Protection incorporates several Host Intrusion Prevention technologies.

- Application: Behavior monitoring
- File System: Antimalware (known threats) and Dynamic Translation and Emulation (unknown threats)
- Network: Windows firewall management

There is an additional vulnerability shielding technology, known as Network Inspection System (NIS), which is also in the Forefront Endpoint Protection 2010. Based on a similar technology found in Forefront Threat Management Gateway Web Protection Service, it is designed to protect endpoints against application-layer threats through signatures and a deep protocol and application analysis, states Shintaku. (Shintaku 2012.)

Forefront Endpoint Protection with System Center Configuration Manager

Forefront Endpoint Protection is tightly integrated into System Center Configuration Manager (SCCM) 2007. If a company already has SCCM environment in place, they now have an integrated anti-virus solution that leverages the SCCM agent already deployed onto desktops, laptops or servers. FEP client license is now included in System Center Configuration Manager Client Access Licenses (CALs). The FEP interface is shown in Figure 6.



You can use Forefront Endpoint Protection to deploy and manage an effective comp on Configuration Manager managed computers.

Client Deployment Status	
Targeted by FEP: 2 out of 17	
Remo...	0
Failed	0
Pendi...	0
Out o...	1
Deplo...	1

Security Status
Infected
Restart required
Full scan required
Recent malware activity (la

Definition Status
Older than 1 week
Up to 7 days old
Up to 3 days old
Up to date

Protection Status	Computers
Protection service off	0

Policy Distribution Status
Failed

FIGURE 6. SCCM Console with FEP integrated in it

Microsoft’s approach with FEP and SCCM is to integrate management and security into a single environment, claims Derek Melber. Along with patch management, application distribution and configuration management, companies can now use a single console to manage anti-virus while integrating their infrastructure for management and security. Deploying an anti-virus solution with no additional infrastructure can be very appealing for companies, Melber continues. (Melber 2012).

Also, he says that FEP uses the SCCM client for updates and client-server communication. The existing SCCM distribution points are used for distributing engine updates, definition updates and updates to the client itself and this is a huge benefit for companies which already have SCCM environment in place. Integrating anti-virus updates into SCCM infrastructure will most likely cut down on bandwidth usage because SCCM distribution points use the BITS (Background Intelligent Transfer Service) protocol to download updates. FEP also has interesting delta definition update capability to only give the client the definitions it needs, not push a large definition package each time. Also, with traditional anti-virus solutions, there has been a cost of additional SQL Servers, additional management nodes etc. By removing those additional components, significant savings can be achieved, Melber says. (Melber 2012).

SCCM synchronizes the definition updates from the Microsoft Update catalog, so clients which are away from the corporate network, can check for definition updates directly from Microsoft Update. This allows clients to stay up to date and protected even they are outside of company’s network connected to the Internet. By deploying FEP clients, it is possible to use the wizard-driven SCCM interface to automatically remove competitive anti-virus solutions (e.g.: Symantec and McAfee) before installing the FEP agent. This provides almost seamless migration, especially when using the SCCM targeting groups that have probably already been built for patch distribution, application deployment, to name a few. (Melber 2012)

4.2 Other endpoint protection products in evaluation process

The endpoint protection platform provides a collection of security utilities to protect PCs, tablets, mobile devices and other endpoint protection devices. Vendors in this market compete on the quality of their protection capabilities, versatile of features, and the ease of administration. Any security solutions can still, in theory, be bypassed.

Buyers should look for good repair tools, as well as the capability to alert administrators about threats that may have had a longer dwell time or more aggressive infections. Administrators should be able to perform their own manual inspections for missed components of more-complex infections. Solutions should provide a holistic security state assessment and a prioritized action plan to remediate potential security gaps. Also, solutions should include mobile device management (MDM) capabilities and data protection for mobile devices and employee-owned devices (BYOD=Bring Your Own Device). (Gartner 2011.)

Server platforms are commonly supported by EPP vendors; however, optimal server protection may require additional features and protection mechanisms, such as file integrity monitoring or Web application firewalls. The enterprise endpoint protection platform (EPP) market is a composite market primarily made up of collections of products. These include:

- Anti-malware
- Anti-spyware
- Personal firewalls
- Host-based intrusion prevention
- Port and device control
- Full-disk and file encryption, also known as mobile data protection
- Endpoint data loss prevention (DLP)
- Vulnerability assessment
- Application control
- Mobile device management (MDM)

Due to lack of resources and enough time in Metso, only two other endpoint protection solutions were considered to be a security solution for Metso Windows based computers. Those products were McAfee and Symantec. McAfee was included because it is one of the leading providers of endpoint security platforms. Symantec was included because Symantec Endpoint Protection (SEP) is a product used in Metso over the years and that is why Metso knows the features and capabilities of that product.

After the comparison of McAfee and Symantec it was decided that only Symantec and Microsoft would be the products which to make a choice for Metso endpoint protection platform. Based on the investigations of Metso, McAfee would provide technically quite similar infrastructure than Symantec and the costs of the new product, in case of McAfee, would not be significantly lower. With McAfee product Metso should also build totally new management infrastructure. Metso could exploit neither Symantec infrastructure, nor Microsoft infrastructure which is already used for software distribution, patch management and operating system deployment.

Also, according to Magic Quadrant for Endpoint Protection Platforms (Gartner 2010) and Magic Quadrant for Endpoint Protection Platforms (Gartner 2013) McAfee is just behind of Symantec in the Leaders quadrant.

According the latest research Microsoft with its Forefront Endpoint Protection product was categorized to 'Challengers' in Gartner's research. Symantec was categorized to 'Leaders'. So why not to choose Symantec because it is one of the leading providers of EPP solutions? The answer is not so simple. A leading vendor is not a default choice for every buyer, and clients should not assume that they must buy only from vendors in the Leaders quadrant.

What does it basically mean when the product is categorized to Leaders, Challengers, Visionaries or Niche Players categories in Gartner's researches? Gartner defines: **Leaders** capabilities in advanced malware protection, data protection and/or management features raise the competitive bar for all products in the market, and they can change the course of the industry. **Challengers** have solid anti-malware products that address the foundational security needs of the mass market. They are good at competing on basic functions, rather than on advanced features. **Visionaries** invest in the leading-edge features — such as advanced malware protection, data protection and/or management capabilities — that will be significant in the next generation of products. **Niche Players** offer viable, uncomplicated anti-malware solutions that meet the basic needs of buyers or that focus on a specific protection capability. Clients tend to pick Niche Players when the focus is on a few specific functions and features that are important to them. (Gartner homepage.)

Symantec Endpoint Protection 11 features

Symantec Endpoint Protection 11.0 includes following key features which were already known from previous versions (Symantec 2008):

- Antivirus and Antispyware
- Personal Firewall (includes new technology features)
- Intrusion Prevention (includes new technology features)
- Proactive Threat Scanning (includes new technology features)

- Device and Application Control (includes new technology features)

In addition the following features were added to the 11.0 version (Symantec 2008):

- New client software user interface
- Kernel-level rootkit protection
- New management console
- Roles based administration
- Group Update Provider
- Location awareness
- Policy Based settings
- Domains
- Failover and load balancing
- SQL Database support
- Enhanced LiveUpdate

4.3 Product comparison and evaluation

Sneering about Microsoft unsecure products can often be heard and it is quite a public opinion that Microsoft does not invest at all in to security of the products it produces. It is true that Microsoft has made many failures with its products and has not responded to security requirements during the early years. However, during the latest years Microsoft has significantly improved its ability and processes to produce more secure products and has taken responsibility to publish regular patches into supported operating systems and core products like Office products, Internet Explorer, SQL etc.

In this chapter Microsoft Forefront Endpoint Protection is compared and evaluated against the other endpoint protection products. Is FEP secure enough as a company's centrally managed endpoint protection product? Because of limited time it has not been possible to compare all possible products in this thesis, but based on the requirements and definitions of the subscriber, some of most significant candidates has been taken into comparison. Comparison and evaluation are based on own experiences and investigation of public sources and data gathering and analysis of them.

The author of the thesis has tried to find the strengths and challenges of FEP and for what types of organizations FEP makes sense. Because of financial pressures, many IT security professionals will be asked to consider FEP as a replacement for the current endpoint protection platform (EPP). Financial aspects have been also one of the key drivers for this thesis subscriber. However, there are some limitations which have to be acknowledged before making the migration.

Strengths of FEP

The very considerable reason, that many organizations are considering FEP, is a licensing change announced in March of 2011. Client Access Licenses (CALs) for FEP are included with Enterprise Client Access License (ECAL), and from August 2011, with Core CAL. For organizations that have already purchased Core CAL, FEP is practically free and very interesting when looking for opportunities to reduce overall IT security costs, especially in those companies where SCCM is already in use. (Gartner 2011.)

According to Gartner research company (Gartner 2011), Microsoft's labs are regularly in the top quartile for responsiveness and coverage for malware which are targeted for Windows. Microsoft also has wide visibility into malware from multiple sources across consumers. Its relatively small footprint and the fast performance of its core anti-malware engine are assets.

FEP leverages common SCCM environment for the delivery of the FEP agent, engine updates and ongoing malware signature updates. For organizations that already have SCCM installed, estimated 60% of the PC life cycle management (PCLM) product market, this is very useful because of servers and agents already deployed, states Gartner. The SCCM backbone is used as a common distribution infrastructure for patches and software distribution, as well as malware engine distribution and signature updates. The FEP console within SCCM can manage also the Windows firewall. (Gartner 2011.)

From a security protection perspective, FEP includes multiple non-signature-based protection techniques, including behavior monitoring, emulation and dynamic translation. Microsoft also provides a dynamic signature service to enlarge periodic signature file updates. Actions from unknown sources, such as unexpected network connections attempting to modify privileged parts of Windows or downloading known malicious content trigger requests for updates from the Dynamic Signature Service. Microsoft has added vulnerability-facing HIPS protection in FEP 2010 so that attacks on known Windows vulnerabilities can be proactively shielded until patches can be applied. FEP also monitors some system behaviors and file reputation data to identify and block attacks from previously unknown threats. Vulnerability-facing HIPS capabilities were added with FEP. (Gartner 2011.)

According to Gartner (2011), here are some key strengths as a list:

- CALs for FEP are included with ECAL, and as of August 2011, with Core CAL.
- Microsoft's labs are consistently in the top quartile for responsiveness and coverage for malware targeting Windows.
- Microsoft's labs have large visibility into malware from multiple sources across consumers and enterprise offerings.
- Its relatively small footprint and the fast performance of its core anti-malware engine are assets.
- It leverages common SCCM plumbing for agent distribution and signature updates.
- The FEP console within SCCM can manage the Windows firewall.
- Vulnerability-facing HIPS capabilities were added with FEP.
- Internet-based users can be managed with SCCM's Internet-based client management.
- Templates are provided for common server roles.
- Existing enterprise Microsoft technical support contracts extend to include FEP.

Microsoft’s fragmented technical capabilities are presented in Appendix 1.

Challenges of FEP

Gartner says that although there are plenty of benefits for organizations to implement FEP and the product itself has many strengths, organizations has to take into consideration also limitations and challenges of FEP. CALs for FEP are included with Core CAL but Core CAL is not free and organizations should perform a cost-benefit analysis. A fully functional SCCM infrastructure must be in place and SCCM may require more servers for management than comparable infrastructure to support alternative endpoint protection solution. (Gartner 2011.)

The single biggest operational limitation of FEP is lack of support or partnerships to fulfill the security needs of heterogeneous platforms, says Gartner. FEP runs on Windows XP and higher, and Windows Server 2003 and higher, 32-bit and 64-bit operating systems, however there is no support for Macintosh, Linux or other platforms, including mobile devices. Organizations with heterogeneous platform that choose FEP will be required to implement some other solution for non-Windows platforms. (Gartner 2011.)

According to Gartner, there are also technical challenges. FEP does not include an integrated firewall. Instead, the FEP console within SCCM now manages Microsoft's own Windows firewall. Also, FEP does not include and manage full drive and removable device encryption. Microsoft has these capabilities; however not managed within FEP, because these capabilities come out with separate products, like AppLocker, BitLocker, BitLocker To Go and so on. Some group policy settings for these Windows security capabilities may be managed in other areas of SCCM or with Group Policies (GPOs). However, there is still no unified console for security policy, management and reporting across all security policies. Maybe it is because Microsoft's organizational and cultural issues prevent it from providing a unified console for that.

According to Gartner (2011) , here are some key challenges as a list:

- There is no heterogeneous platform support, including mobile devices.

- FEP requires SCCM (or Windows update) for signature distribution, which is duplicative if an alternative PCLM infrastructure is in place.
- Historically, the product releases have been slow.
- There is no single security policy management console across all of Microsoft's security policy products.
- The management console, reporting and alerting capabilities are not so good compared to the market leaders.
- There is no integrated application or device control.
- Data loss prevention capabilities are lacking.
- There are limited rule-based behavioral HIPS capabilities.
- There are no integrated NAC (Network Access Control) capabilities.
- Integrated encryption is not included, although a third party or BitLocker could be used.
- There is limited tamper resistance.
- In the event a mobile user cannot reach the enterprise SCCM servers, signature updates should be retrievable directly from Microsoft and have this reflected in the management console.
- While FEP protects servers, no server-specific protection mechanisms, such as file integrity monitoring or rule-based behavioral HIPS, are provided.
- There is no cross-VM optimization for more efficient scanning in hosted virtual desktop environments, nor can FEP see into AppV containers.
- SCOM may be required for complete monitoring.

Strengths of Symantec

According to Gartner, Symantec Endpoint Protection provides a full-featured EPP solution, including anti-malware protection, device control and engine for behavioral heuristics. Encryption capabilities and Data Loss Prevention (DLP) are available as separately charged offerings. For protection from zero-day and targeted attacks, Symantec was a pioneer introduced with SEP 12 which is the latest version of SEP. Furthermore, Insight technology inside of SEP shares information and cooperates with Sonar to reduce false positives. (Gartner 2013.)

An innovative free plug-in to the Symantec Protection Center (SPC) provides IT analytics capabilities and offers data cubes for the analysis of SEP data. For server-based Host-based Intrusion Prevention System (HIPS), Symantec Critical System Protection has broad platform support. Symantec has solid MDM capabilities from its acquisitions of Odyssey and Nukona, which again provides application isolation. Symantec is rated a Challenger in the MDM software Magic Quadrant. Symantec Power Eraser is a good tool for scrubbing hard-to-remove infections and provides a free alternative to Malware, Gartner states. (Gartner 2010.)

Challenges of Symantec

Because of multiple acquisitions, Symantec administrators have to interact with multiple consoles through the SPC, claims Gartner. For example, Symantec Critical System Protection uses a different console from SEP. Newer products (such as encryption) are integrated directly at the SPC level, but have not yet been integrated for reporting. The Insight file reputation technology only works on file downloads and is not a full application control solution. Although it has some vShield integration to remove critical processing from each virtual machine, Symantec still does not offer the agentless anti-malware scanning. Removable device encryption requires a confusing set of policies across Symantec's encryption products and SEP's device control functionality, states Gartner. (Gartner 2013)

Economic impacts of Microsoft FEP 2010

Total economic impact and potential return on investment (ROI), which companies could achieve by deploying FEP 2010, can be calculated in many different ways with different kind of variables. The following list presents the components which could be included into cost calculation:

- PC application tests
- Microsoft FEP pilot program costs
- Microsoft FEP deployment costs
- Training fees
- Microsoft FEP annual administration costs

- Licensing costs
- Business critical support costs
- Server management costs

By including all components into cost calculation, costs would significantly increase the ROI and by outscoping some components, costs would significantly lower the ROI. Also, it has to be taken into account that the costs to test, pilot, deploy and administer FEP 2010 will vary with the number of PCs, the amount of testing performed, and the complexity of the IT environment in the company. This thesis presents some basic tables to include basic cost components regarding endpoint protection security product management and implementation project.

Figures in the Table 4 are not from the real world, so the readers can change their own figures based on their own IT environment. Still they are based on experience of Metso's environment with Metso's amount of PCs, amount of management servers, network topology and domain structure. Table 4 below shows basic cost components regarding endpoint protection security product management.

TABLE 4. Cost components for endpoint protection security product management

Cost item	**Microsoft FEP 2010**	**Symantec SEP 11**
Management / administration costs	50 000€	75 000€
License costs	0 €	150 000€
Business critical support	40 000€	40 000€
Server management costs	50 000€	80 000€
TOTAL	140 000€	345 000€
Costs / month	11 667€	28 750€
Savings / month	17 083€	

Savings / year	204 996€	

Table 4 above shows significant savings annually for the company when using FEP 2010 instead of SEP 11. It is based on the knowledge that FEP 2010 clients can be managed with lower server amount and benefit the same environment where the whole endpoint environment can be managed. Also, the management itself can be conducted with lower amount of personnel because of synergy of SCCM and FEP management environment. The most significant savings can be reached via licensing costs because of licensing changes by Microsoft during 2011. It is really so that if a company is Windows-centric and licensed under Core CAL or ECAL and has deployed SCCM for PC management, FEP must be strongly considered as an endpoint protection solution for Windows based computers.

Table 5 shows, as an example, one time project cost if Symantec Endpoint Protection were to be changed to Forefront Endpoint Protection. The figures in the table are not from the real world, so the reader can change his/her own figures based on the own IT environment.

TABLE 5. Project (from Symantec to FEP) payback time

Project manager cost / hour	100 € / hour
Workload	75%
Months	10
Hours / month	160 (20 day x 8 hours)
€ / month	12 000€
Total €	120 000€
SEP 11 cost / month / PC	0,40 €
PCs	30 000

SEP 11 € / month	12 000€
Project payback time	**10 months**

As a result it can be seen that the project payback time for the product change can be quite short. If using resources from off shoring countries, project payback time can be even shorter because personnel costs per hour are significantly lower than in Western countries.

Product key features of compared endpoint protection products

Product key features for the comparison table were chosen based on endpoint product key features, and experience about the endpoint protection security products and their centralized management in the large enterprise over the years. It has been noticed that antivirus comparative tests does not illustrate the whole picture of product features overall. They are often based on consumer products and even if based on business products, the pure detection rate does not resolve the product superiority. When cross-tested products in practice, the product which has had poor results in the test, has managed to find malware or other threats when product with better results has not, and vice versa.

Product analysis of Gartner (2010, 2011, 2013) has been used also as a basis for choosing the features for the table as well as 'Performance test (AV Products), Impact of Anti-Virus Software on System Performance' (AV Comparatives 2012), 'Summary Report 2012, Awards, winners, comments' (AV Comparatives 2012), 'Performance Test, Impact of Anti-Virus Software on System Performance, Microsoft Forefront Endpoint Protection (Release Candidate)' (AV Comparatives 2010), 'Comparative Analysis on Endpoint Security Solutions' (Indusface 2010) and 'Consumer anti-malware products, Group test report' (NSS Labs, 2010).

Single console for endpoint management and security. Management and downloading virus definitions can be done from one single management console which reduces the work of administrative people.

Central policy creation. Policies for endpoint protection clients can be defined and deployed from one single management console which reduces the work of administrative people and makes reacting to security threats faster.

Enterprise scalability. System has to be scalable technically and from management point of view from hundreds of endpoints in the organization to tens of thousands endpoints.

Efficient threat detection. Endpoint protection product has to recognize efficiently malware, spyware, viruses and other threats. Also, efficiency means that client agent does not overload CPU and memory and basic work, such as copying files, launching applications and downloading files to name a few, can be done with the computer when protection client is enabled. Efficient security features are the most important features in the endpoint protection product.

Behavioral threat detection. Endpoint protection product has to recognize malware, spyware, viruses and other threats based on their typical behavior. Live system behavior monitoring identifies new threats by tracking unknown processes and known "good" processes gone infected. This type of protection is sometimes referred to as zero-day protection. Efficient security features are the most important features in the endpoint protection product.

Network vulnerability shielding. Known also as a Network Inspection System (NIS). NIS detects and blocks Conficker-style network vulnerability exploits. It inspects inbound and outbound network traffic and blocks detected exploits. Efficient security features are the most important features in the endpoint protection product.

Signature updates. Signature updates delivers protection for new threats. If the file is known infected, a new signature is delivered in real-time to the client requesting it. Efficient security features are the most important features in the endpoint protection product.

Customized alerts. Ability to configure customized alerts regarding various security threats.

Automated agent replacement. Possibility to automatically detect and remove the most common endpoint security agents in case of product change. This feature reduces the time needed to deploy new protection product.

Windows firewall management. This feature ensures that Windows Firewall is active and working properly to protect against network-layer threats.

Amount of management servers. By reducing the amount of management servers a company can achieve potential savings.

Detailed reports. Detailed and customized reporting capabilities creates company an opportunity to gain comprehensive picture about the endpoint security level and offers possibilities to react fast to threats.

Licensing costs. Licensing model and licensing costs are the most important cost factor when calculating costs of the endpoint protection product.

Table 6 presents some key features of compared endpoint protection products with scores and weighted scores. There is one row for each criterion and one column for each alternative. Columns are subdivided to record scores and weighted scores. Weighting factors are used to define the level of importance of criteria. Assigning meaning to weighting factors is subjective. A category score is calculated by summing the weighted scores for each criterion in the category and dividing by the sum of the weights for the criteria in the category. Table 6 can be used to evaluate any endpoint protection product.

Six weighting factors are used with the following meaning:

- 5 - Very high importance
- 4 - High importance
- 3 - Medium importance
- 2 - Low importance
- 1 - Very low importance
- 0 - Not important

Scores are from 1 to 5 and given based on experiences about both products used in Metso IT environment.

TABLE 6. Weighted matrix for product comparison

		Microsoft Forefront Endpoint Protection 2010		**Symantec Endpoint Protection 11**	
Criteria	**Weight**	**Score**	**Weighted**	**Score**	**Weighted**
Single console for endpoint management and security	3	5	15	3	9
Central policy creation	3	4	12	4	12
Enterprise scalability	4	5	20	4	16
Efficient threat detection	5	3	15	3	15
Behavioral threat detection	5	3	15	3	15
Network vulnerability shielding	5	3	15	3	15
Signature updates	5	4	20	3	15

Customized alerts	3	4	12	3	9
Automated agent replacement	3	4	12	2	6
Windows firewall management	4	4	16	4	16
Amount of management servers	4	5	20	4	16
Detailed reports	3	4	12	4	12
Licensing costs	5	5	25	3	15
TOTAL	52	53	**209**	43	**171**
SCORE			**4,0**		**3,3**

Based on the Table 6 with weighted scores, it can be seen that Microsoft FEP 2010 is worth of considering as an enterprise wide endpoint protection product.

4.4 Analysis and conclusions

Gartner Inc. is an American information technology research and advisory company providing technology related insight. The research provided by Gartner is targeted at CIOs and senior IT leaders in industries to deliver the technology-related insight necessary for their clients to make the right decisions. Gartner research and compares regularly different players on EPP protection platform market. The latest results are from January, 2013. (Gartner homepage.)

According to Gartner (2011), Microsoft's FEP is good, but falls short of the integrated technical, security and management capabilities of the endpoint protection market leaders. However, organizations that choose FEP are not at increased risk because of worse protection capabilities. Also, Microsoft's labs are strong, and the underlying FEP engine has a small footprint and performs well. Gartner claims that Microsoft's security offerings are not the leading ones, however, they are reasonably priced and "good enough" for Microsoft-centric, cost-driven enterprises, which do not have a high degree of heterogeneity and that do not require an integrated, risk based view of the security state of their endpoints. (Gartner 2011.)

Gartner recommends that if a company is Windows-centric, is licensed under Core CAL or ECAL or has deployed and is using SCCM for PC life cycle management (PCLM), FEP must at least be considered as an endpoint protection solution for Windows based computers. The limitations of FEP must be weighed against the cost savings if FEP will be chosen, especially if the organization already has a solution for disk encryption. (Gartner 2011.)

Where explicit cost savings are a heavily weighted component of the evaluation, FEP will provide a reasonable replacement for core anti-malware protection capabilities, Gartner says. However, there are implicit costs of switching to FEP, including the cost of retraining security administrators, removal of the competitive offering, and testing and deployment of the FEP agent, Gartner reminds. There are also hidden costs if shortcomings in FEP management and reporting make administrators less effective. (Gartner 2011).

Companies could achieve significant savings annually after changing Symantec Endpoint Protection to Forefront Endpoint Protection 2010. FEP 2010 clients can be managed with lower management server amount and even with lower administrative people because of single management console for the whole endpoint environment. Single management console for PC management totally (software distribution, patch management, operating system deployment and endpoint security management) decrease requirement of administrative people because there do not have to be separate persons for endpoint security administration and management. The most significant savings can be reached via licensing costs because of licensing changes by Microsoft during 2011. Licensing costs are straight costs and there are some indirect costs, such as testing, piloting, training and deploying costs, which has to be taken into account in advance.

FEP is a new product for most of the organizations, however, it is so tightly integrated to SCCM that companies having deployed SCCM, should not have major difficulties to take FEP features into use. Of course, there are some prerequisites at least technically to deploy FEP into corporate environment. FEP is extremely attractive choice if company has SCCM in use and has tens or even hundreds of distribution servers to distribute software packages and security patches into their endpoints (desktops, laptops, tablets, mobile devices, servers). That same server infrastructure can be used to distribute also antivirus definitions to those same endpoints. That might help to reduce network traffic which has been problem with the SEP product. If SEP client has corrupted, in some cases it has caused huge network traffic over wide area network (WAN) links by downloading gigabytes of definition data from the SEP management servers which are typically located in the datacenters over the WAN links. In case of FEP, client definition data can be downloaded from the nearest distribution server which is in most cases located in the same local area network (LAN) with the endpoint client.

For organizations that have a high degree of heterogeneity, or that do not use SCCM, FEP is not a good solution, and alternatives should be considered. And even if Microsoft's FEP is not a serious consideration, it should be used as a threat to get better pricing from Microsoft's competitors endpoint protection solutions. Finally, it has to be also remembered, that FEP and MSE (Microsoft Security Essentials which is Microsoft's free product for consumers and small businesses), use the same core anti-malware engine, so the core engine is proven on tens of millions of computers and has been deployed for several years.

How to make FEP more attractive?

According to Gartner (2011), companies should pressure Microsoft to partner with some endpoint protection vendor for non-Windows platforms. However, leading endpoint protection vendors are not likely willing to partner with Microsoft because Microsoft competes with these same vendors for companies and consumers. Organizations should also pressure Microsoft to improve FEP so that it is able to manage all of the security features of the Windows operating system from one single security policy management console — most notably BitLocker, AppLocker and USB device control policies. Improvements in the management console are also needed, says Gartner. Administration of security policy should be a separate function from the ongoing operational management of the security policy. The FEP administrator dashboard should be customizable; also reporting options should be more customizable and wider, including the ability to get alerts and security information more quickly without requiring the use of System Center Operations Manager (SCOM). (Gartner 2011.)

Companies should also require tighter integration with SCCM. In the event of a malware outbreak or attack, it would be useful to click on an infected machine to quickly view patch status and inventory and quickly identify the high-risk computers. And finally, companies should also demand improved integration with Microsoft's mobile device management to securely manage mobile devices (including non-Microsoft OS-based devices) at a policy level, e.g. password strength, encryption policies or similar. (Gartner 2011.)

The total economic impact of Microsoft FEP 2010 can be studied from the document 'The Total Economic Impact Of Microsoft Corporation's Forefront Endpoint Protection (FEP) 2010' made by Forrester consulting in February, 2011. The financial results calculated in the document can be used to determine the return on investment, net present value, and payback period for the company's investment in FEP. Forrester did a study of the benefits achieved by organizations using System Center Configuration Manager by deploying Forefront Endpoint Protection (FEP) 2010 and integrating their desktop management and security infrastructure. Their study indicates a total Net Present Value (NPV) of almost $300k for a reference customer with 5000 seats. (Forrester 2011.)

5 CONCLUSIONS

The main target of this thesis was to find out if Microsoft FEP would be an applicable solution as an enterprise endpoint protection security system for Metso Windows based computers. Microsoft's 2010 release of FEP leverages its System Center Configuration Manager (SCCM) platform, and licensing changes make the offering effectively free for most organizations. Because of ongoing financial pressures in Metso, also, the end user computing service delivery managers and information security professionals were asked to consider FEP as a replacement for the current endpoint protection platform (EPP) solution. However, IT experts should find out, understand and acknowledge the limitations of the current FEP offering before a migration is undertaken.

FEP was started to be investigated as a replacement for the SEP product with this thesis, which would help to make a final decision if FEP could be the next endpoint protection product for Metso over the several years. Investigating and writing this thesis simultaneously with everyday work was not so easy task. How to find enough time and how to find the most correct information about the products for the basis of decision and this thesis? Proof of Concept (PoC) of FEP management environment installation and client installations was made to Metso during the spring 2012. That helped a great deal because basic knowledge of the product itself, its features and problems, was already there.

Very often for a specific purpose, like some task or a thesis, an information retrieval is limited in time and scope. Information retrieval is a self-correcting and guiding process, which will guide future sources found. Therefore, the findings often take surprisingly a lot of time and obtained results may change the preconceived or forced to abandon them altogether. That was one the major difficulties found out in this thesis. Another problem was to out scope some information and aggregate only necessary information, because after all, there was so much interesting information which might be included.

After all the overall picture was getting to take a shape and information from various sources began to accumulate. Then I encountered a problem how to analyze and present the information in the shape, which could be appropriate especially for Metso but also for other organizations. By going through dozens of sources the clear conformity was starting to be found, and confidence for the various comparisons of the competitive products was improved. After making quite clear picture about the products it was time to write the results into this thesis.

Working in Metso Shared Services (Metso IT), which offers end user computing, server infrastructure and network infrastructure services for all Metso businesses globally, for over seven years, has given a strong and wide view for the enterprise ICT technology. Also, it has helped a great deal making and writing this thesis. Businesses, contact persons and tools are all familiar, so those issues have not been a problem. Challenges come from the fact that the thesis cannot be quite specific only for Metso. Altogether writing this thesis has been interesting and it has widened the view for making the evaluation and seeking the theory and practical information for the basis of the results and this thesis.

REFERENCES

Allen, J. 2005. Governing for Enterprise Security. Referred 26.5.2013. http://www.sei.cmu.edu/library/abstracts/reports/05tn023.cfm.

Anderson, J. 2006. Qualitative and Quantitative research. Referred 1.6.2013. http://www.icoe.org/webfm_send/1936.

Comparative Analysis on Endpoint Security Solutions 2010. Indusface. Referred 30.5.2013. http://la.trendmicro.com/media/report/officescan-indusface-comparative-report-en.pdf.

Consumer anti-malware products, Group test report 2010. NSS Labs. Referred 27.5.2013. https://www.nsslabs.com/reports/2010-q3-consumer-anti-malware-products-group-test-report.

Firstbrook, P., Girard, J. & MacDonald, N. 2010. Magic Quadrant for Endpoint Protection Platforms. Gartner RAS Core Research Note G00208912. Referred 13.5.2013. http://www.elmtree.com.au/Portals/elmtree/Gartner_MQ_endpoint_protection_platforms_17Dec10.pdf.

Firstbrook, P., Girard, J. & MacDonald, N. 2013. Magic Quadrant for Endpoint Protection Platforms. Referred 13.5.2013. http://www.gartner.com/technology/reprints.do?id=1-1DPWLS1&ct=130122&st=sb.

Hakala, M., Vainio, M., & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Docendo.

Laadullisen ja määrällisen tutkimuksen erot. Tilastokeskus. Referred 1.6.2013. http://tilastokeskus.fi/virsta/tkeruu/01/07/.

MacDonald, N. 2011. Microsoft's Forefront Endpoint Protection: Good, but Not Great. Referred 13.5.2013. http://www.gartner.com.

Melber, D. 2011. Enhancing Endpoint Security for Windows Desktops (Part 1). Referred 20.4.2013. http://www.windowsecurity.com/articles-tutorials/misc_network_security/Enhancing-Endpoint-Security-Windows-Desktops-Part1.html.

Melber, D. 2011. Enhancing Endpoint Security for Windows Desktops (Part 2). Referred 20.4.2013. http://www.windowsecurity.com/articles-tutorials/misc_network_security/Enhancing-Endpoint-Security-Windows-Desktops-Part2.html.

Melber, D. 2011. Microsoft Forefront Endpoint Protection 2010 - Is Microsoft Anti-virus Good Enough. Referred 20.4.2013. http://www.windowsecurity.com/articles-tutorials/viruses_trojans_malware/Microsoft-Forefront-Endpoint-Protection-2010-Microsoft-Anti-virus-Good-Enough.html.

Mell,P., Kent, K., & Nusbaum, J. 2005. Guide to Malware Incident Prevention and Handling. Referred 26.5.2013. http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

Metso homepages. Referred 15.4.2013. Http://www.metso.com.

Microsoft technet 2012. Prerequisites for Deploying Forefront Endpoint Protection on a Client. Referred 28.4.2013. http://technet.microsoft.com/en-us/library/ff823900.aspx.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Kauppakaari.

Performance test (AV Products), Impact of Anti-Virus Software on System Performance 2013. AV Comparatives. Referred 30.5.2013. http://www.av-comparatives.org/performance-tests/.

Performance Test, Impact of Anti-Virus Software on System Performance, Microsoft Forefront Endpoint Protection (Release Candidate) 2010. AV Comparatives. Referred 30.5.2013. http://www.av-comparatives.org/single-product-reviews-tests/page/2/.

SFS-EN ISO/IEC 27005. 2009. Information technology. Security techniques. Information security risk management. Helsinki: Finnish Standards Association. Referred 2.5.2013. Metso intranet, SFS Online.

SFS-EN ISO/IEC 27001:2005, 2009. Information technology. Security techniques. Information security management systems. Requirements. Helsinki: Finnish Standards Association. Referred 2.5.2013. Metso intranet, SFS Online.

Summary Report 2012, Awards, winners, comments 2012. AV Comparatives. Last revision 5.1.2013. Referred 30.5.2013. http://www.av-comparatives.org/summary-reports/.

Räsänen, H. Tutkimus-ja kehittämishankkeiden tieteellinen viitekehys. Referred 27.5.2013. http://portal.hamk.fi/portal/page/portal/HAMK/koulutus/Ylempi_AMK_tutkinto/kudos/menetelmat/3_Tutkimus-_ja_kehittaemishankkeet.pdf.

Shintaku, K. 2012. WHITEPAPER: Forrester Research study on the Total Economic Impact of Forefront Endpoint Protection 2010. Referred 20.4.2013. http://download.microsoft.com/download/A/F/3/AF3EB4CF-B683-4816-A107-DFAF508EB61A/TEI%20of%20Microsoft%20FEP2010%20FINAL.pdf.

Uusitalo, H. 1991. Tiede, tutkimus ja tutkielma – johdatus tutkielman maailmaan. Helsinki: WSOY.

VAHTI 2003.Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtiovarainministeriö. Referred 20.4.2013.

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf.

What's new in Symantec Endpoint Protection 11.0, 2008. Symantec. Referred 30.5.2013. http://www.symantec.com/docs/TECH102401.

APPENDICES

Appendix 1. Microsoft's fragmented technical capabilities.

Security Capability	**Product included**	**Client support**	**Licensing Requirements**	**Managed by**
Forefront anti-malware engine — includes antivirus, anti-spyware and nonsignature-based protection capabilities	Add-on to SCCM	Windows XP Service Pack 3 (SP3) and higher	Bundled with Core CAL	Forefront console within SCCM
Windows Defender — anti-spyware only; subsumed by Forefront Endpoint Protection if it is used	Windows Vista and higher	None	Included in base OS	Individually
Windows firewall	Windows XP, Vista, 7 (bidirectional in Windows Vista and higher)		Included in base OS	Individually, group policy objects (GPOs) or optionally managed by Forefront plug-in for SCCM as of Forefront 2010

Security Capability	**Product included**	**Client support**	**Licensing Requirements**	**Managed by**
Memory protection/buffer overflow protection — Data Execution Prevention	Windows XP SP2 and higher		Included in base OS	Individually or GPOs
USB port control	Windows Vista and higher	None	Enterprise Edition — requires purchase of Software Assurance on the Windows OS	Individually or GPOs
BitLocker — full drive encryption	Windows Vista and higher	None	Enterprise Edition — requires purchase of Software Assurance on the Windows OS	Individually, GPOs or BitLocker Management Pack (available with Microsoft Desktop Optimization Pack, which is only available if Software Assurance is purchased for the Windows OS)

Security Capability	Product included	Client support	Licensing Requirements	Managed by
BitLocker To Go — removable device encryption	Windows 7	Reader for XP	Enterprise Edition — requires purchase of Software Assurance on the Windows OS	Individually or GPOs
Software Restriction Policies (basic application control)	Windows XP and higher		Included in base OS	GPOs
AppLocker (more-advanced Application Control)	Windows 7	None	Enterprise Edition — requires purchase of Software Assurance on the Windows OS	GPOs
Windows Network Access Protection (NAC)	Windows Vista and higher	None	Included in base OS, but requires Windows Server 2008 to function as the health certificate server	GPOs

Security Capability	**Product included**	**Client support**	**Licensing Requirements**	**Managed by**
URL Reputation Service	Internet Explorer 8 (IE8) and higher	Runs on XP SP3 and higher	Included with IE8 and higher, which works on Windows XP SP2 and higher	Individually or GPOs
File Reputation Service	Internet Explorer 9 (IE9)	None	Included with IE9, which only works on Windows 7 and higher	Individually or GPOs
User Account Control	Windows Vista and higher	None	Included in base OS	Individually or GPOs
Windows Services Hardening (whitelisting of Windows Services — a form of host-based intrusion prevention)	Windows Vista and higher	None	Included in base OS	Controlled by application manifests provided by the developer
Windows Security Configuration Management	SCCM — Desired Configuration Management	Runs on XP SP3 and higher	Part of SCCM	Not managed by Forefront console within SCCM
Windows patch management	SCCM — Software Update Management	Runs on XP SP3 and higher	Part of SCCM	Not managed by Forefront console within SCCM