

Degree Thesis, Åland University of Applied Sciences,
Bachelor of Information Technology/Bachelor of Engineering

WHAT IS ZERO TRUST

- and How Can It Be Implemented?

André Öberg



2022:50

Publishing date: 20.12.2022
Supervisor: Björn-Erik Zetterman

DEGREE THESIS

Åland University of Applied Sciences

Degree Programme:	Bachelor of Information Technology/Bachelor of Engineering
Author:	André Öberg
Title:	What is Zero Trust - and How Can It Be Implemented?
Academic Supervisor:	Björn-Erik Zetterman
Commissioned by:	André Öberg

Abstract
<p>In this thesis I write about Zero Trust and how it can be implemented. The purpose for that is to be more knowledgeable within IAM and explain why in today's IT it is no longer as safe to use standard user credentials for sign in and why the Zero Trust model should be used in Today's IT.</p>

Keywords
Zero Trust, SSO, OIDC, SAML, Authentication

Serial number:	ISSN:	Language:	Number of pages:
2022:50	1458-1531	English	36

Handed in:	Date of presentation:	Approved:
4.12.2022	16.12.2022	20.12.2022

EXAMENSARBETE

Högskolan på Åland

Utbildningsprogram:	Informationsteknik
Författare:	André Öberg
Arbetets namn:	Vad är Zero Trust - Och hur man kan implementera det?
Handledare:	Björn-Erik Zetterman
Uppdragsgivare:	André Öberg

Abstrakt

I mitt examensarbete skriver jag om Zero Trust och hur det kan implementeras. Syftet är att förbättra mitt kunnande inom området samt förklara varför man bör använda Zero Trust inom dagens IT då standarden av inloggningsnamn samt lösenord inte längre är tillräckligt säkert.

Nyckelord (sökord)

Zero Trust, SSO, OIDC, SAML, Authentication

Högskolans serienummer:	ISSN:	Språk:	Sidantal:
2022:50	1458-1531	Engelska	36

Inlämningsdatum:	Presentationsdatum:	Datum för godkännande:
4.12.2022	16.12.2022	20.12.2022

TABLE OF CONTENTS

1. INTRODUCTION	6
1.1 Purpose	6
1.2 Background	6
1.3 Methodology	7
1.4 Definitions	7
2. CREDENTIALS IN TODAY’S WORKSPACE	9
2.1 Breaches due to leaked credentials or unauthorized access	9
2.1.1 Ticketmaster 2021: Unauthorized access	9
2.1.2 GoDaddy 2021: Unauthorized access	10
2.1.3 Verkada 2021: Unauthorized access	10
3. YESTERDAY’S IT-SYSTEMS	11
3.1 On-premise	11
3.2 Software As a Service	11
4. WHAT IS ZERO TRUST?	13
4.1 Why should organizations use ZeroTrust?	13
4.2 Never Trust, Always Verify	13
4.3 Identity	14
4.4 Authentication	14
4.4.1 Security Question	15
4.4.2 Email	15
4.4.3 One-Time Password	16
4.4.4 Authentication Applications	16
4.4.5 Biometric	17
4.4.6 Security Keys	17
4.5 Least Privilege	18
4.6 Continuous Monitoring	19
4.7 Microsegmentation	19
4.8 Stages of Zero Trust	19
4.8.1 Stage 0: Fragmented identity	19
4.8.2 Stage 1: Unified identity and access management	20
4.8.3 Stage 2: Contextual Access	20
4.8.4 Stage 3: Adaptive Workforce	20
4.9 Single Sign On	21
4.9.1 Identity Providers & Service Providers	21
4.9.2 Federated Sign-On	21
4.9.3 Secure Web Authentication	21

4.9.4 OAuth	22
4.9.5 OIDC	22
4.9.6 SAML	23
5. HOW TO IMPLEMENT ZERO TRUST USING OKTA	24
5.1 Setting Up Universal Directory	24
5.2 Setting Up Groups and Rules	24
5.3 Setting up MFA	26
5.4 Setting up SSO	29
6. WHAT COMPANIES USE TODAY	31
6.1 Statistics	31
6.2 Company 1	31
6.2.1 Stage of Zero Trust	31
6.3 Company 2	32
6.3.1 Stage of Zero Trust	32
7. CONCLUSION	33
REFERENCES	35
APPENDICES	37
FRÅGOR - INTERVJUER (svenska)	37
INTERVJU 1	38
INTERVJU 2	39

1. INTRODUCTION

The reason for this thesis is that in today's IT the standard user credentials are no longer enough. And the process of onboarding and offboarding users can leave major security risks if not handled correctly.

The process for this has mostly been building upon what I have learned from my time working with Identity and Access Management in Advania and using Okta¹ as our Identity And Access Management tool during the last year.

This thesis will also explain how you can start setting up Zero Trust with Okta in chapter 5.

1.1 Purpose

The purpose of this thesis is to explain why in today's IT it's important to update one's security model. By putting the focus on the user's identity instead of assuming that people who are on the local network are trustworthy. Which can be done by implementing the Zero Trust security model.

1.2 Background

I choose Zero Trust as my thesis due to my work, as I work daily with IAM solutions and have seen and heard how current credentials are used and how it has changed over the years. The most common thing I have read about is how many data breaches occur due to unsafe user credentials and poor management from onboarding and offboarding which results in old users still having access to a company's resources even after they have quit which can result in devastating consequences. Or how new employees have access to something they should never have.

An important thing to note is how users get managed. If the IT department needs to manage let's say 100 users that could be manageable but it might get error prone. Now let's say that you have 2000 employees: Now the chances of something going wrong rises exponentially as some users might still have access to sensitive information as they have multiple different

¹ Okta is an IAM service for managing user access.

accounts for each and every application needed for their work. Same goes if you hire a new one as they might not have access to everything on their first day at work.

1.3 Methodology

This thesis is constructed using a review of current situations in this field, defining, walking the reader through what this ‘Zero Trust’ is actually about. So in terms of methodology this is literature review complemented with interviews with anonymous stakeholders in the industry. The reason for being anonymous is the potential harm a security problem can cause in a company/organization.

1.4 Definitions

IT	Information Technology
On Prem	On Premises is software which is locally installed on the users computer
Cloud	Cloud means applications which are accessed through the internet
IAM	Identity and Access Management
MFA	Multi-Factor Authentication
SSO	Single Sign On
SAAS	Software As A Service
ZT	Zero Trust
IDP	Identity Provider
SP	Service Provider
SSOT	Single Source of Truth
RBAC	Role-based access control
XML	Extensible Markup Language
JSON	JavaScript Object Notation file
REST	Representational State Transfer
SWA	Secure Web Authentication

FIDO	Fast Identity Online
OTP	One Time Password
AD	Active Directory
VPN	Virtual Private Network
SAML	Security Assertion Markup Language
OIDC	Open ID Connect
OAuth	Open Authorization

2. CREDENTIALS IN TODAY'S WORKSPACE

According to Verizon's data breach report for 2022 about 80% of data breaches which target Web Applications are due to stolen passwords, which can be due to brute force attacks and weak passwords (“Verizon DBIR” 2022). And from the interviews discussed in chapter 6 it can be seen that Multi-Factor authentication is commonly used with the addition of user credentials. The use of access policies is also in use which use information about the user's location and device to determine if the users need to use additional authentication methods to gain access to a resource.

2.1 Breaches due to leaked credentials or unauthorized access

It's very common to read about damage caused by data breaches within IT. Most of the time it's due to compromised user credentials, old accounts lingering in systems and users having access to more than what's needed.

And sadly most of the time it could have been prevented with stronger authentication. Such as using Multi-Factor authentication, setting up password policies to have expiration dates on user passwords and not allowing commonly used passwords.

In the following chapters I will list some examples of this that happened during 2021.

2.1.1 Ticketmaster 2021: Unauthorized access

During early 2021 a rival company to Ticketmaster had a former employee give login credentials for several accounts to Ticketmaster. These accounts were used to manage ticket presales. The employee also showed a bug in the URL generation which allowed access to unpublished ticket pages (Goodin 2021).

This could have easily been prevented with the usage of MFA or password policies to force users to change their password periodically.

2.1.2 GoDaddy 2021: Unauthorized access

During 2021 the web host GoDaddy had discovered the 22nd November a data breach which has been compromised since August. This breach comprised more than 1 million of their user accounts.

The cause of this breach was the usage of compromised credentials(Sundaram 2021; “GoDaddy DataBreach 2021” 2021).

2.1.3 Verkada 2021: Unauthorized access

In 2021 Verkada, a security company had a data breach due to leaked admin credentials which were visible on a customer support server. This resulted in the hacker gaining access to 97 of their customers' security cameras and data as well as Verkada's sales orders (“Verkada Security Update -Incident Report” n.d.).

This like many more breaches could have been prevented by not having the credentials visible on the support server and setting up MFA for high privilege accounts or in general.

3. YESTERDAY'S IT-SYSTEMS

3.1 On-premise

Before most organizations would have their systems in their premise, hence the name on-premise or on-prem. This kind of system would work well on the assumption that all who would connect would be connected to the organization local network and would consist of traditional local credentials to sign in and a user database such as active directory or similar. This structure would have the applications run locally on the user's computer or a server and an IT team which manages the hardware and software (“On-Premise vs. Cloud Pros and Cons” 2022).

But as stated it requires you to be on the local office network to gain access to the required software and data. To be able to gain access to it remotely it required additional costs for setting up VPN which increases the chance of threats to gain access to valuable company information.

The benefits of an on-premises is that you have complete control over the system and nobody else has access to the data stored. But the problem lies in the initial costs for setting up the hardware and licenses required. There are also the additional costs for maintaining it and for personnel which are needed to manage it. Another weakness is the poor scalability of on premise due to the additional costs required for newer hardware and software (“On-Premise vs. Cloud Pros and Cons” 2022).

3.2 Software As a Service

Software as a service also known as SaaS is software which is in the cloud and has been on the rise, as it doesn't require the initial costs of needing hardware and personnel for maintenance. Some examples of as a service is Google Workspace and Office 365 where the user data can be synced to the internal Active Directory.

These programs are usually easy for the users to access as there is no need for the programs to be installed on their computer and instead are accessed through a web browser. This means that the user can access these programs through their own devices or outside the local network in their organization.

So instead of spending money on hardware you just need to pay a fee for the users who need to access the program and it's easily scalable as you just add more users for your subscription. This also usually leads to less costs as you don't need to have an internal IT support to manage the software as the ones who deliver support it and update it ("What Is SaaS? Defining Software as a Service" n.d.).

4. WHAT IS ZERO TRUST?

Zero Trust is a security model whose core principle is to move the defense away from trusting devices and users in the organization's network to instead be focused on the users. The model also continuously requires that the users identify themselves when they attempt to access more sensitive resources ("Cloudflare: Zero Trust Security" 2022).

This is done by granting users the least privilege required and always verifying that the user is who they say they are by validating their current location, device, using MFA and continuously monitoring for suspicious activity or threats (Syed et al. 2022).

As a model Zero Trust isn't new as it was introduced in 2009 by John Kindervag who worked at Forrester during this time. Who explained that threats could also be within the company perimeter and not just outside. This could be users who have more access than they need and might accidentally remove important information. It could also be accounts that former employees have had after they left but they still linger within the systems without being deleted or deactivated. ("Okta-Whitepaper-Getting-Started-Zero-Trust_2021" 2021).

4.1 Why should organizations use ZeroTrust?

As stated in chapter 2.1 the most common breaches today are weak, repeated or commonly used passwords. It also doesn't help as remote work has become more popular which has resulted in the internal systems within organizations needing to be changed to allow remote work with some solutions such as VPNs.

4.2 Never Trust, Always Verify

The concept of "Never Trust, Always Verify" is common for Zero Trust. This is due to Zero Trust being completely built around it. Which can be observed as anytime an user attempts to access an application or resource they must authenticate. ("Okta The State of Zero Trust Security 2021" 2022)

So how does it work? Previously most companies would be safe due to their on premise security which would protect them from threats which came from outside. However during 2020 remote work became more common which in turn caused companies to move towards cloud based technologies which forced them to also support remote work from outside the corporate network. This caused problems when most systems were built up like a castle that didn't let anyone in from the outside. In return this would require a change of security as users would need to be able to access the company resources either remotely or from private devices (“Cloudflare: Zero Trust Security” 2022).

4.3 Identity

So the question then was how would you be able to verify who were your users and who were the outside threats, and the solution would be to move the security to be focused on the user identity.

This means that it wouldn't matter if a user would be inside or outside of the company network as they would still need to identify themselves if they would want access to any of the company resources. This concept would also remove one of the major problems with the previous method caused by granting users complete access within the company network as long as they were inside the company perimeter, as it meant if any threat would be able to get inside it would mean they would most likely be able to access anything (“Securing Identity with Zero Trust” n.d.).

4.4 Authentication

The general rule for authenticating users in a Zero Trust architecture is to verify them through the process of either something they know something they have or something they are, this is done by MFA (“What Is Multi-Factor Authentication (MFA)?” 2022).

Something an user knows refers to user credentials and security questions. This is the most common type of authentication as it's used everywhere in the form of username and password.

Something you have refers to certificates and tokens which get generated or received when a user attempts to access a resource. This is usually done with authenticators or one time passwords.

Something you are, which is the last authentication method which requires either a fingerprint, facial recognition or similar methods in order to authenticate.

But not every authentication method has the same level of security so this section will discuss the different kinds of authentication methods there are in order of security (“About Multifactor Authentication” n.d.).

4.4.1 Security Question

Security questions would fall under the something you know category and are not much safer than standard user credentials. This is due to the fact that it can get guessed and depending on the security question could get figured by you being the target of spear phishing attacks. (Sham 2022).

Spear phishing is a phishing attack with a clear target in mind to acquire the login credentials from the target or infect their device or devices with malware. The way it works is that the ones doing the attack research gather information about their potential target to then send them convincing emails, phone calls or sms from what looks like real senders (Paying close attention to the sender's email or potential URL's can help reveal that it's not a trustworthy source.) (“What Is Spear Phishing? Definition with Examples” 2020).

4.4.2 Email

MFA that would send an email to the users mail would be of higher security than the security question, but would be harder to rank in terms of security as it would depend on the user. This is due to the fact that the user might use repeated passwords when signing in or could have different credentials for every application and use MFA when accessing their mail. It would then be harder to breach due to the added security from the MFA.

4.4.3 One-Time Password

One-Time Passwords is the type of authentication where a random password is either sent to you as a sms or a voice call. Email would also belong here but as stated previously is more volatile based on the user (“One-Time Passwords (OTPs)” n.d.).

4.4.4 Authentication Applications

This refers to applications such as Google Authenticator, Okta Verify and comes in two different types: either push or a constantly generated password (OTP).

The authentication which generates passwords is less secure than its counterpart as it can get brute forced but it’s significantly harder than a normal password as it constantly gets changed(““Banking Grade’ Authentication Often Means a Weak OTP” 2019). The authentication method which requires push verification is the more secure one as it requires the user's validation by them accepting the sign on attempt. It also usually displays information regarding the device and location from where the sign on was started from (Robinson 2020). Figure 1 displays two authenticators, Okta Verify and the Google Authenticator.

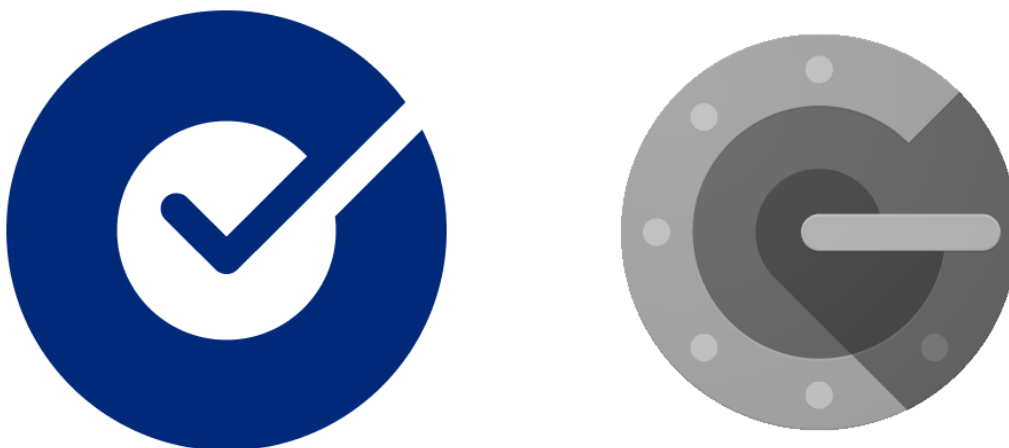


Figure 1. Logos for the Okta Verify and Google Authenticator

4.4.5 Biometric

Biometric authentication is very secure as it requires either fingerprint, facial or vocal verification from the user to verify the identity of the user. This causes it to be very convenient for the users as instead of entering a PIN or password they would just need to identify themselves by scanning their fingerprint or face. But this does not mean that it's impossible for someone else to authenticate as you. This is because some AIs can generate fingerprints. And facial recognition can get tricked by using photos. ("Biometric Authentication: Good, Bad, & Ugly" n.d.).

4.4.6 Security Keys

Security keys are one of the most secure authentication methods as it requires an external physical key which is required for signing in and optionally requires another verification method such as a PIN or fingerprint to allow authentication. This key will randomly generate a string which is used for authentication each time the user plugs it into their computer via the USB port and pushes the button on it, after signing in with the key for the specific application it's also possible to authenticate without the security key ("How the YubiKey Works" 2021).

The security keys are most commonly built on the FIDO protocol which uses key pairs for authentication ("How FIDO Works" 2017). A key pair is two items which are linked together: A key which is a unique identifier for and the value for said identifier which contains the data for the key. Some examples of security keys on the market are the Yubikey and the Google Titan. In figure 2 the Yubikey series five is displayed.



Figure 2. Yubikey 5 Series security keys (“Discover YubiKeys” 2020).

4.5 Least Privilege

As said previously at the beginning of this chapter, least privilege means that people and applications should only be allowed to have the lowest required access needed to perform their tasks, there’s multiple reasons why you would want to do this (“Principle of Least Privilege” 2020).

The first and most important one is that if any data would be breached then not everything would be compromised as the user would most of the time not be able to access everything as the attack surface is reduced depending on user role. (The higher access required would require a stronger authentication method such as a security key.)

For users who need administrative privileges it's a good idea to give them an additional account which has the administrative privileges, and only sign them into it when needed ("What Is Least Privilege & Why Do You Need It?" 2021).

The second reason is to reduce the amount of damage an user could do by mistake to a system by deleting sensitive data.

4.6 Continuous Monitoring

So what is continuous monitoring and how does it work? When nobody is given implicit trust in a Zero Trust architecture it also means everything will get monitored and logged for oddities and discrepancies to notice if any account is compromised or a breach is being attempted. This means that you will be able to actively watch and control access requests to your organization's resources with the additional information of the location, the time the access was triggered, and what triggered it (Harrington 2022).

4.7 Microsegmentation

To make the resources more secure, Zero Trust divides the organization network into sections, each being capable of having different security policies. This is what's called microsegmentation and leads to the effect that anyone who accesses one of these sections will only be able to access the data on said section, and if they want to access another section they will need to authorize again ("Cloudflare: Zero Trust Security" 2022),

4.8 Stages of Zero Trust

Currently you can categorize what stage organizations are at in regards to Zero Trust depending on their current configurations ("Okta-Whitepaper-Getting-Started-Zero-Trust_2021" 2021).

4.8.1 Stage 0: Fragmented identity

First let's discuss what a fragmented identity is to get a better understanding of what it means for an organization to be at this stage. Fragmented identity means that users have multiple applications on prem and in the cloud which are necessary for their work which are not

integrated together. This causes the IT administrators to need to manage all the identities for each application the users might have, and for the user it means more passwords to remember and manage which in return increases the risk of repeated passwords.

This produces multiple entry points for attackers to exploit (“Okta-Whitepaper-Getting-Started-Zero-Trust_2021” 2021).

4.8.2 Stage 1: Unified identity and access management

So how do we solve the problems caused from the previous stage? You integrate all data from the applications and services under one IAM system to create a single source of truth to store all necessary user data in one place to be used. This will then enable the usage of SSO (see chapter 4.9) so that all users only need to use a single password instead of multiple like previously to gain access to all their required applications. It will then allow the configuration of access policies (“Okta-Whitepaper-Getting-Started-Zero-Trust_2021” 2021).

4.8.3 Stage 2: Contextual Access

When stage 1 is complete the groundwork for access policies is done. This then means that the next stage is to gather and log information about the users in regards to who they are, the applications they use, the devices that are used, from where they sign in, what network they are signing in from. This is done to start the creation of access policies with regards to the information gained, which can be used to determine if the user needs to verify with MFA or not.

With the data collected you can lastly set up onboarding and offboarding flows to automate the process to onboard new users by giving them access to what they need day 1 or revoke their access when they leave or change position in the company (“Okta-Whitepaper-Getting-Started-Zero-Trust_2021” 2021).

4.8.4 Stage 3: Adaptive Workforce

With stage 3 the authentication of users no longer just occurs when users sign in but continuously as they are authenticated. This means that no trust is given, instead every action gets monitored for potential threats and risks (“Okta-Whitepaper-Getting-Started-Zero-Trust_2021” 2021).

4.9 Single Sign On

Single Sign On, also more commonly known as SSO, is the process of being able to access multiple applications with a single login. This means that after the user has signed in they can with a single click access multiple applications without providing any credentials (unless the application in question is using SWA (see chapter 4.9.3) when they need to provide credentials for the first sign in). There are multiple ways to implement SSO and this chapter will walk through the most common ones in today's IT (“What Is SSO?” n.d.).

4.9.1 Identity Providers & Service Providers

To start off with this chapter it's important to understand what Identity Providers and Service Providers are. An Identity provider (IDP) is a service which stores and manages user identities, this makes it possible to use said data for a multitude of applications or resources. Instead of creating a new identity for every resource you can just refer to the data within an IDP or sync data within an external resource to the IDP depending on say email or personal id (“What Is an Identity Provider (IdP)?” n.d.).

A Service provider (SP) is a service that offers solutions or service to users and organizations. This is also what's mostly known as a cloud service (“Service Provider” 2012).

4.9.2 Federated Sign-On

Federated Sign-On builds upon the IDPs and SP by building a mutual trust between them. If the trust is then established, when the user is signed into the IDP and tries to access the SP the SP will then send the request to the IDP. The IDP will then wait for an response which if accepted will return the necessary user information and authenticates them (“What Is Federated Identity” n.d.).

4.9.3 Secure Web Authentication

One of the possible ways to sign in with SSO is to use Secure Web Authentication also known as SWA. SWA is used by Okta when an application doesn't allow federated sign-on, this means that when a user attempts to SSO to an application with Okta they need to enter their credentials for said application, those credentials then get encrypted and saved in Okta.

This means that for future uses of the application you will no longer need to sign in as the credentials will be sent to the application login (“Okta Help Center (Lightning)” n.d.).

4.9.4 OAuth

Before moving on to OIDC we must first discuss OAuth as OIDC is built on top of it.

OAuth is an authorization protocol that means that it is the part which grants users access to the different resources.

It does it through what’s known as access tokens which usually are in the format of JWTs (JSON Web Token). This token is then used to gain access to requested resources.

The way this works is that when an user attempts to access lets say an application the application sends an authorization request to an authorization server. This server then asks for four things: a client id, a client secret that is used for identification the last two things are the required scopes and the endpoint URI which usually is the login page for the application. If the authorization succeeds it will send the access token to the endpoint URI and allow access to the application.

There is another way to authorize users instead of using access tokens which is using something called an authorization code flow where instead of returning a access token directly you instead gain a one time use authorization code which is sent to the OAuth authorization server and returns an Access token. This is a more secure way to authorize users as the code is single use only (“What Is OAuth 2.0 and What Does It Do for You?” n.d.).

4.9.5 OIDC

OpenID Connect, also known as OIDC, is an authentication layer built upon OAuth which uses JSON or REST for federation. This is done through ID tokens which are sent in as JSON Web Tokens (JWT). These ID tokens contain information about the user. This data in the token is most commonly known as claims. So compared to OAuth which returns an authentication token OIDC returns both an authentication token as well as an ID token.

Some examples of OIDC is when you sign in to an application with either Google or Facebook which I'm quite sure most people have seen. When you sign in with either IDP they

will return the ID token discussed earlier which contains the necessary data the application you are attempting to access needs (Teleport n.d.).

4.9.6 SAML

Compared to OIDC, Security Assertion Markup Language (SAML) isn't built on top of any protocol, instead it does the authorization and authentication itself. The main difference between them is that it uses XML and at its core more focused on IDPs and SPs this makes SAML most commonly used for corporate SSO (Teleport n.d.).

The way SAML works is that when a user attempts to sign in to the SP from the IDP the SP generates an SAML request, this request is then sent to the IDP and gets parsed depending on the configuration done within the IDP. What happens is then that the required attributes are mapped to the relevant user attributes within the IDP. The IDP then sends back the response with the attributes mapped back to the SP so that it can get verified. If the data is then valid the user will get signed into the SP (Manager 2016).

5. HOW TO IMPLEMENT ZERO TRUST USING OKTA

One way to implement Zero Trust is through Okta which is one leading product on the market for IAM solutions. Okta is a cloud program which can serve as a Identity Provider (IDP) or Service Provider (SP) and stores the required information about your users in what's called Okta Universal Directory.

5.1 Setting Up Universal Directory

To set up the universal directory it's necessary to follow the stages from chapter 4.8 where we first must determine what the single source of is in regards to the data from users. This could either be information from a Human Resources system or an Active Directory running on a server.

If it's on a HR system it's highly likely it's within Okta's Integration Network (OIN) which contains over 7000 already made application integrations some examples are Microsoft Office 365, Google Workspace, Workday.

If the user data is in an AD you will need to install the Okta AD Agent on the server which contains the AD by using what's called a service account. This is an account which isn't associated with any user as the company will need to be able to access said account even if the owner leaves the company. After you have set up the server agent you will need to define how the user data is imported into Okta such as the username and when the data should get imported.

5.2 Setting Up Groups and Rules

Following stage 1 in chapter 4.8 you can now set up how users get added to groups.

First you will want to create the user groups you want if you didn't import groups from the AD. Figure 3 displays the okta groups interface which lists all groups in the okta tenant.

Groups

All Rules




Group name	People	Applications
 IT IT Department	0	0
 Everyone All users in your organization	5	0
 Sales Group for sales people	2	0

Figure 3. How Okta displays all groups within the tenant. If a group would come from a separate source it displays a different logo.

One way that however requires more administration is just to add users to groups manually. From personal experience the best way to do it is to set up group rules within Okta which allows you to add users to groups depending on a multitude of attributes such as title, where they work, which country they work from and many more. You can also exclude users from rules but it only allows 100 users to be excluded from the select rule. This is done through Group Rules which is displayed in figure 4..

Add Rule

Name: Sales Group Rule

IF: Use basic condition Use Okta Expression Language (advanced)

User attribute | department | string | Equals | IT

THEN Assign to: IT x

This rule will not add users to a group they've been manually removed from.

EXCEPT The following users: Bob Tester (bob.test@testmail.ax) x

Preview: Enter an Okta user to preview this rule

Save Cancel

Figure 4. How adding a group rule looks within Okta. In the if statement you can select which attributes are the deciding factor for assigning a user to a group or groups.

For an even more complex system you could use what's called Okta Workflows.

5.3 Setting up MFA

In Okta you can select which types of authentication are allowed to be used. Some examples are Okta Verify, SMS Authentication, Security Question, Google Authenticator and Yubikey. And in some of them you can set additional settings such as push notifications on Okta Verify which can be seen in figure 5.

Factor Types Factor Enrollment

Okta Verify	<h3>Okta Verify</h3> <p>After configuring this factor, users signing in to Okta see that extra verification is required. If Okta Verify is selected they will be instructed to download the Okta Verify App. Once installed, the user will be prompted to enter the generated six digit number to gain access.</p> <p>Okta Verify Settings</p> <ul style="list-style-type: none"><input type="checkbox"/> Enable Push Notification<input type="checkbox"/> Require Touch ID or Face ID for Okta Verify (only on iOS)
SMS Authentication	
Google Authenticator	
FIDO2 (WebAuthn)	
Symantec VIP	
On-Prem MFA	
RSA SecurID	
Email Authentication	

Figure 5. How it looks when you set up a factor in Okta.

Lastly, regarding MFA in Okta is that you can set up policies for specific user groups which defines which MFA the group needs to use when they attempt to sign in, this can be seen in figure 6.

Add Policy

Policy name
Sales_Okta_Verify

Policy description
Description

Assign to groups
Sales x

Effective factors

<input checked="" type="checkbox"/> Okta Verify	Required
<input type="checkbox"/> Google Authenticator	Optional

[Create policy](#) [Cancel](#)

Figure 6: Setting up a MFA policy in Okta. Observe the effective factors as Okta Verify is Required for users within the Sales group while Google Authenticator is Optional.

It's also possible to set up rules for each MFA policy so that the MFA would only get prompted if the user would attempt to access an sensitive application from outside the company network as seen in image 7.

Add Rule

Rule name

Exclude users

IF User's IP is ▼
Manage configuration for [Networks](#)

All Zones

THEN Enroll in multi-factor ▼

Figure 7: Setting up a MFA rule for the previous policy, where MFA would only get triggered if the user would attempt to sign in when outside the company network

5.4 Setting up SSO

As stated in chapter 4.9 there are multiple ways to set up an SSO between IDPs and SPs. Okta allows for quite simple setup of SSO through what's called Okta Integration Network also known as OIN which contains over 7000 integrations. Figure 8 displays the OIN where you can filter applications by name, functionality such as SWA, OIDC,SAML to help you find the application you are looking for.

Browse App Integration Catalog

Create New App

The screenshot displays the 'Browse App Integration Catalog' interface. On the left, there is a sidebar with two sections: 'Use Case' and 'Functionality'. The 'Use Case' section lists various categories with their respective counts: All Integrations (7453), Apps for Good (8), Automation (23), Centralized Logging (11), Directory and HR Sync (14), Bot or Fraud Detection (2), Identity Proofing (7), Identity Governance and Administration (IGA) (5), Lifecycle Management (534), Multi-factor Authentication (MFA) (22), Risk Signal Sharing (5), Social Login (18), Single Sign-On (6935), and Zero Trust (46). The 'Functionality' section has three checkboxes: Workflows Connectors, Workflow Templates, and SAML, all of which are currently unchecked. The main content area features a search bar at the top with the text 'Search...'. Below the search bar, the text 'All Integrations' is displayed, followed by a 'Sort by: Default' dropdown menu. A 'FEATURED' section is highlighted, with a 'See all' link to its right. This section contains four application integration cards arranged in a 2x2 grid. Each card includes the application's logo, its name, a brief description, and a list of supported protocols. The cards are: 1. Salesforce.com (Single Sign-On): Sign into salesforce.com and automate onboarding and offboarding processes. Supported protocols: SAML, SWA, Workflow Templates, Workflows Connectors, SCIM. 2. ServiceNow UD (Single Sign-On): Sign into servicenow.com and automate onboarding and offboarding processes. Supported protocols: Workflow Templates, Workflows Connectors, SAML, SWA, SCIM. 3. Microsoft Office 365 (Single Sign-On): Sign into Office 365's suite of products and automate onboarding and offboarding processes. Supported protocols: Workflow Templates, Workflows Connectors, SWA, SCIM. 4. Workday (Single Sign-On): Sign into Workday and automate onboarding and offboarding processes. Supported protocols: SAML, SWA, SCIM.

Figure 8: Okta Integration Network with preconfigured applications which can be used.

If the application doesn't exist within OIN you can create the integration manually but it will require knowledge of several URLs, what attributes are needed and more.

6. WHAT COMPANIES USE TODAY

For some real data I interviewed two companies to learn if they have adapted to the Zero Trust model or what their current solution is. From the information I will then relate to chapter 4.8 so see which stage of Zero Trust they currently are at.

6.1 Statistics

According to Okta, after reviewing Zero Trust with 700 leaders within IT security around the world during 2022 to get data on how large of a percentage of companies use or intend to use Zero Trust it was revealed that 55% of the respondents used Zero Trust within their organizations and 42% plan on implementing it for the future.

This, compared to their last report during 2021, showed an increase of 31% more orgs who use Zero Trust and a decrease of 11% of orgs who plan to implement it (Terry 2022).

6.2 Company 1

The first company I interviewed had their application both on prem and in the cloud. So it would be what would be called a hybrid cloud environment. For access to the cloud applications it requires authentication through MFA either through notification prompt in Google or SMS. But for the on prem applications you only need to sign in with standard user credentials which have an expiration date and a password complexity. In a few cases to gain access to an application you need to have a certification installed on the pc.

However, to change a password the user needs to be signed in, and if the expiration date happens and the user hasn't updated their password they need to make a phone call to change it. The sources for user access rights are split in three different places but they have been updating their access management especially since 2020 when Covid hit. Lastly the company uses a few applications which allow for SSO where they go to an SP.

6.2.1 Stage of Zero Trust

It's hard to evaluate at what stage exactly they are at since they do have some access management depending on user roles as well as applications which use SSO so I would say

according to chapter 4.8 the company is around Stage 1 and Stage 2 but leaning more towards stage 1.

6.3 Company 2

The second company I interviewed was quite far in Zero Trust judging from the answers I got. Currently their users need to authenticate through AzureAD with SSO and then gain access depending on the attributes set on their account which is synchronized from a single source of truth. This is managed by Cloud Flare which is their IAM of choice from what I understood. The user's access rights are continuously monitored and to gain more access they need to send a request to the system owners which needs to be approved. And in regards to the multi-factor authentication all users must authenticate through it and in some cases they need to use Yubikey. This all depends on if they attempt to access a resource on a trusted device, location and have a valid certification.

In terms of their applications everything is a Cloud Application and to gain access to them they SSO with SAML. This seems accurate based around chapter 4.9.6 where it's written that SAML is the most common SSO type for organizations.

Lastly in regards to user password policies they need to follow a set password complexity and change their password at least once a year per NIST guidelines.

6.3.1 Stage of Zero Trust

Based around the answers I got they are currently at stage 3 as they get continuously monitored as they access software and resources. They also have quite a strict way of granting high access to users as they need to get verified through an official request which must be approved by the system's owners as I mentioned.

As they are on stage 3 it means that they also fulfill all previous stages as the users access is based on their attributes, current location and device. Lastly, as they have a SSOT and use an IAM system they fulfill the requirements for stage 1 as they allow their users to SSO to their applications, which means that stage 0 is also fulfilled. I would have liked to know how their onboarding and offboarding process looks but from the way it looks I would assume it's done automatically.

7. CONCLUSION

After researching how Zero Trusts works and what's needed to properly set it up, it can be difficult to revamp an existing system for a big company to Zero Trust. Due to deprecating all hardware that might be in use I definitely can see why you should do it especially if the organization has a lot of users and data that needs to be secure and is spread across multiple applications.

As just using standard credentials for sign in without any MFA in today's IT feels very unsafe due to how easy it has become for hackers to be able to gain user credentials through either phishing attempts or trying to bruteforce a way in. Then that problem start to scale if the user uses the same password across multiple applications.

With Zero Trust you could then mitigate said damage by requiring users to use different kinds of authenticators and mitigate the potential damage in worst case scenarios due to microsegmentation.

But that doesn't mean that Zero Trust is completely secure as there is always a risk of an outside actor gaining access, but then the idea is to instead reduce the chance of it happening in the first place and minimizing the impact by limiting what an user actually can gain access to if they would get in.

Lastly you create a seamless user experience by using SSO by allowing the user to only need to sign in once and then have access to all their required apps. Some IAM's like Okta even allow the users to add their own applications for potential SSO with the only disturbance being said authenticator apps if they don't use push notifications or biometrics.

This in return will reduce the amount of work that the IT support would need to do if they manage the users passwords.

As a last word would give a response to a question I got at work in regards to Zero Trust after writing this thesis.

Why would I use Okta, isn't it safer to use multiple complex and unique passwords?

I personally would rather just remember one password and authenticate with MFA to gain access to all apps I need instead of trying to remember a unique password for each app.

Also not all users will have strong passwords and will instead repeat either their one password across multiple apps which then causes a security risk.

REFERENCES

- “About Multifactor Authentication.” n.d. Accessed December 3, 2022.
<https://help.okta.com/en-us/Content/Topics/Security/mfa/about-mfa.htm>.
- “Banking Grade Authentication Often Means a Weak OTP.” 2019. *nextAuth* (blog). March 29, 2019.
<https://www.nextauth.com/banking-grade-login-often-means-weak-otp/>.
- “Biometric Authentication: Good, Bad, & Ugly.” n.d. Accessed December 3, 2022.
<https://www.onelogin.com/learn/biometric-authentication>.
- “Cloudflare: Zero Trust Security.” 2022. Cloudflare. 2022.
<https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/>.
- “Discover YubiKeys.” 2020. Yubico. October 26, 2020. <https://www.yubico.com/products/>.
- “GoDaddy DataBreach 2021.” 2021. 2021.
<https://www.sec.gov/Archives/edgar/data/1609711/000160971121000122/gddyblogpostnov222021.htm>.
- Goodin, Dan. 2021. “Ticketmaster Admits It Hacked Rival Company before It Went out of Business.” *Ars Technica*. January 4, 2021.
<https://arstechnica.com/information-technology/2021/01/ticketmaster-pays-10-million-criminal-fine-for-hacking-a-rival-company/>.
- Harrington, David. 2022. “What Is Zero Trust? A Comprehensive Guide & Security Model.” *Varonis*. September 9, 2022. <https://www.varonis.com/blog/what-is-zero-trust>.
- “How FIDO Works.” 2017. FIDO Alliance. January 21, 2017.
<https://fidoalliance.org/how-fido-works/>.
- “How the YubiKey Works.” 2021. Yubico. January 26, 2021.
<https://www.yubico.com/why-yubico/how-the-yubikey-works/>.
- Manager, Holly Guevaradeveloper Content. 2016. “What Is SAML and How Does SAML Authentication Work.” *Auth0 - Blog*. December 5, 2016.
<https://auth0.com/blog/how-saml-authentication-works/>.
- “Okta Help Center (Lightning).” n.d. Accessed December 3, 2022.
https://support.okta.com/help/s/article/What-is-Secure-Web-Authentication-SWA?language=en_US.
- “Okta The State of Zero Trust Security 2021.” 2022.
- “Okta-Whitepaper-Getting-Started-Zero-Trust_2021.” 2021.
https://www.okta.com/sites/default/files/2021-11/Whitepaper-Getting-Started-Zero-Trust_2021.pdf.
- “One-Time Passwords (OTPs).” n.d. Accessed December 3, 2022.
<https://www.beyondidentity.com/glossary/one-time-passwords>.
- “On-Premise vs. Cloud Pros and Cons.” 2022. Morefield. Morefield Communications. May 27, 2022.
<https://www.morefield.com/blog/on-premises-vs-cloud/>.
- “Principle of Least Privilege.” 2020. CyberArk. CyberArk Software. January 29, 2020.
<https://www.cyberark.com/what-is/least-privilege/>.
- Robinson, Kelley. 2020. “Understanding Push Authentication.” *Twilio Blog* (blog). Twilio. December 10, 2020. <https://www.twilio.com/blog/understanding-push-authentication>.
- “Securing Identity with Zero Trust.” n.d. Accessed December 3, 2022.
<https://learn.microsoft.com/en-us/security/zero-trust/deploy/identity>.
- “Service Provider.” 2012. Techopedia.com. What is a Service Provider? - Definition from Techopedia. November 26, 2012. <https://www.techopedia.com/definition/22021/service-provider>.
- Sham, Swaroop. 2022. “Security Questions: Best Practices, Examples, and Ideas.” *Okta Inc*. November 17, 2022. <https://www.okta.com/blog/2021/03/security-questions/>.
- Sundaram, Karishma. 2021. “GoDaddy Data Breach 2021: What Happened and How It Affects You.”

- Malcare. December 9, 2021. <https://www.malcare.com/blog/godaddy-data-breach/>.
- Syed, Naeem Firdous, Syed W. Shah, Arash Shaghghi, Adnan Anwar, Zubair Baig, and Robin Doss. 2022. "Zero Trust Architecture (ZTA): A Comprehensive Survey." *IEEE Access* 10: 57143–79. <https://doi.org/10.1109/ACCESS.2022.3174679>.
- Teleport. n.d. "What Is OIDC." Accessed December 3, 2022. <https://goteleport.com/blog/how-oidc-authentication-works/>.
- Terry, Ryan. 2022. "5 Important Insights From Our 2022 State of Zero Trust Report." Okta Inc. August 16, 2022. <https://www.okta.com/blog/2022/08/state-of-zero-trust-report-2022-takeaways/>.
- "Verizon DBIR." 2022. <https://www.verizon.com/business/resources/Tfa7/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>.
- "Verkada Security Update -Incident Report." n.d. Accessed December 3, 2022. <https://www.verkada.com/security-update/report/>.
- "What Is an Identity Provider (IdP)?" n.d. Cloudflare. Accessed December 3, 2022. <https://www.cloudflare.com/learning/access-management/what-is-an-identity-provider/>.
- "What Is Federated Identity." n.d. Accessed December 3, 2022. <https://www.onelogin.com/learn/federated-identity>.
- "What Is Least Privilege & Why Do You Need It?" 2021. *BeyondTrust* (blog). February 19, 2021. <https://www.beyondtrust.com/blog/entry/what-is-least-privilege>.
- "What Is Multi-Factor Authentication (MFA)?" 2022. CrowdStrike.com. CrowdStrike. June 22, 2022. <https://www.crowdstrike.com/cybersecurity-101/multifactor-authentication-mfa/>.
- "What Is OAuth 2.0 and What Does It Do for You?" n.d. Auth0. Accessed December 3, 2022. <https://auth0.com/intro-to-iam/what-is-oauth-2>.
- "What Is SaaS? Defining Software as a Service." n.d. Accessed December 3, 2022. <https://www.okta.com/identity-101/saas/>.
- "What Is Spear Phishing? Definition with Examples." 2020. CrowdStrike.com. CrowdStrike. June 16, 2020. <https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/>.
- "What Is SSO?" n.d. Cloudflare. Accessed December 3, 2022. <https://www.cloudflare.com/learning/access-management/what-is-ssol/>.
- Syed, Naeem Firdous, Syed W. Shah, Arash Shaghghi, Adnan Anwar, Zubair Baig, and Robin Doss. 2022. "Zero Trust Architecture (ZTA): A Comprehensive Survey." *IEEE Access* 10: 57143–79. <https://doi.org/10.1109/ACCESS.2022.3174679>.
- "Verizon DBIR." 2022. <https://www.verizon.com/business/resources/Tfa7/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>.
- "Zero Trust Security." n.d. Cloudflare. Accessed November 27, 2022. <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/>.

APPENDICES

FRÅGOR - INTERVJUER (svenska)

Respondenterna är anonyma, men svaren dokumenteras i bilagor, som numrerad intervju.

1. Vilket sätt autentiseras era användare?
2. Hur bestäms en användares behörigheter?
3. Hur granskas behörigheterna samt hur uppdateras de kontinuerligt?
4. Hur arbetar ni med MFA?
5. Känner du till ZeroTrust och dess nivåer?
6. Hur arbetar ni med utvecklingen av it system kring behörigheter?
7. Om ni har flera olika behörighets databaser, hur synkroniseras de?
8. Har användare flera olika behörighetssystem till olika applikationer?
9. Hur hanterar ni lösenordsbyten, då någon glömt sitt lösenord?
10. Hur hanterar ni löpande lösenordsbyten, policy?
11. Används IAM eller liknande system för att hantera SSO?
12. Vilka tekniker används för att åstadkomma SSO, p SWA, OIDC, WS-FED eller SAML?
13. har ni olika behörigheter/nivåer som kräver strängare försäkran om användares autencitet? (tex skillnad på location, trusted devices, olika funktioner i system)
14. Finns det krav från organisationens ledning(styrelse,VD...) för hur identitet och behörighet hantera?
15. Vilken utveckling har skett de senaste åren inom detta område på din arbetsplats?

INTERVJU 1

1. MFA via gmail samt telefon
2. Manuellt
3. -
4. MFA via mail används för alla användare
5. Har kännedom om hur ZeroTrust generellt dock inte specifikt de olika nivåerna om zero trust
6. Manuellt bulk
7. haka, science sese i finland , zunet funet
8. -
9. Finns tillgång för användare att byta sitt lösenord dock så kräver det att man är inloggad på systemet. Annars hanteras det i nuläget externt via telefon samtal.
10. -
11. edurow, logga in med skol inloggning, installering av certifikat. Få system använder sig av SSO.
12. -
13. Viss åtkomst av tjänster kräver certifiering som installeras på användarens datorer.
14. Styrelsen har ord om hur det skall hanteras (Personen i fråga satt tidigare i ledningen)
15. Under 2015 - 2018 var utvecklingen kring användarautentisering snabb men började sakta av till 2020 (Covid) som ledde till ökat tempo igen

INTERVJU 2

1. Via SSO (AzureAD)
2. Via rollen (RBAC), vi har fördefinierade rättigheter beroende på vad man jobbar med
3. Vi är ISO27001 certifierade, och där ingår kontinuerlig granskning av behörigheter.
Dessa rättigheter uppdateras men då måste det finnas en officiellt "request" att få behörigheter och system ägare måste godkänna detta. Allt detta måste dokumenteras, och vi har portaler och case system som hanterar detta.
4. Vi har MFA på allt, främst genom Google Authenticate appen men t.ex Yubikey's används också
5. Ja, majoriteten av det vi körs är via ZeroTrust, vi har olika leverantörer av Zero Trust med den frästa är Cloudflare
6. Samma som vanlig utveckling, vi definierar eventuella flaskhalsar eller förbättringar och implementerar dessa.
7. Vi har ett ställe som är "single source of truth (SSOT)", därifrån så synkroniseras det utåt för alla miljöer och system. De flesta system har färdigbyggda integrationer man kan använda
8. Ja, i vissa applikationer så måste man "assume role" för att få högre rättigheter
9. InternallIT hanterar detta om användaren glömt lösenordet, användaren får då sätta ett nytt som internallIT inte känner till. Vi mailar aldrig ut lösenord
10. Vi har en Password Policy som berättar hur ofta lösenord måste bytas + komplexitet, detta hanteras automatiskt.
Min password length är 12 och byte minst en gång / år, där följer vi NIST guidelines
11. AzureAD och GoogleSSO används för SSO
12. oftast SAML
13. Ja, vi har kombinationer av certifikat, location, trusted devices och Biometric Yubikey utöver vanliga user/password
14. Ja, reglerade marknader där vi har tjänster har krav på oss och vår ISO27001 har dessa krav och vi auditeras kontinuerligt att vi följer dessa
15. Ingenting hostas själva, allt köra i Cloud tjänster, så som AWS, Cloudflare, Google osv (t.ex vår ZeroTrust är från Cloudflare)