

# MVP Dagen

mvpdagen.no



# Kjente feil og fallgruver i Microsoft sikkerhetsstacken



mvpdagen.no

# Hey!

## Vi er Anders og Truls



**Anders Kristiansen**  
**Lead Security Architect @**  
**Storebrand**

Microsoft MVP Security  
SIEM & XDR,  
Identity & Access

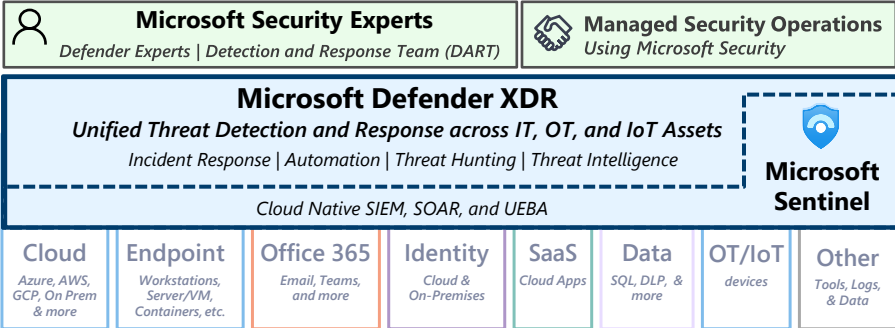


**Truls Thorstad Dahlsveen**  
**Security Architect**  
**@ Sopra Steria**

Microsoft MVP Security SIEM  
& XDR

mvpdagen.no

## Security Operations (SecOps/SOC)



## Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

April 2025 – [aka.ms/MCRA](https://aka.ms/MCRA)

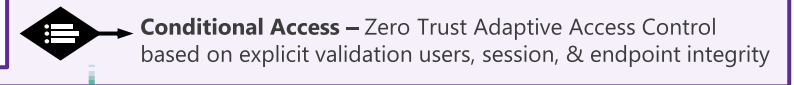
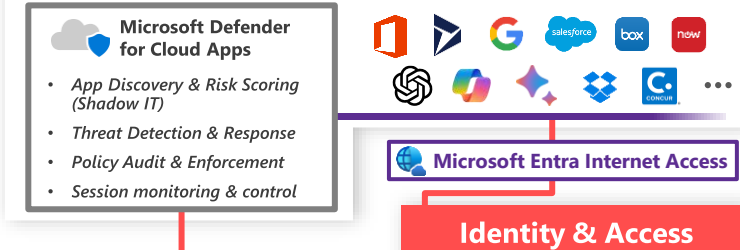
This is interactive!

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

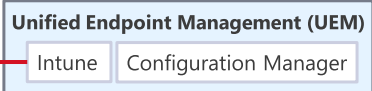
Security Guidance

1. [Security Adoption Framework](#)
2. [Security Documentation](#)
3. Cloud Security [Benchmarks](#)

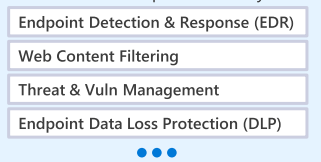
## Software as a Service (SaaS)



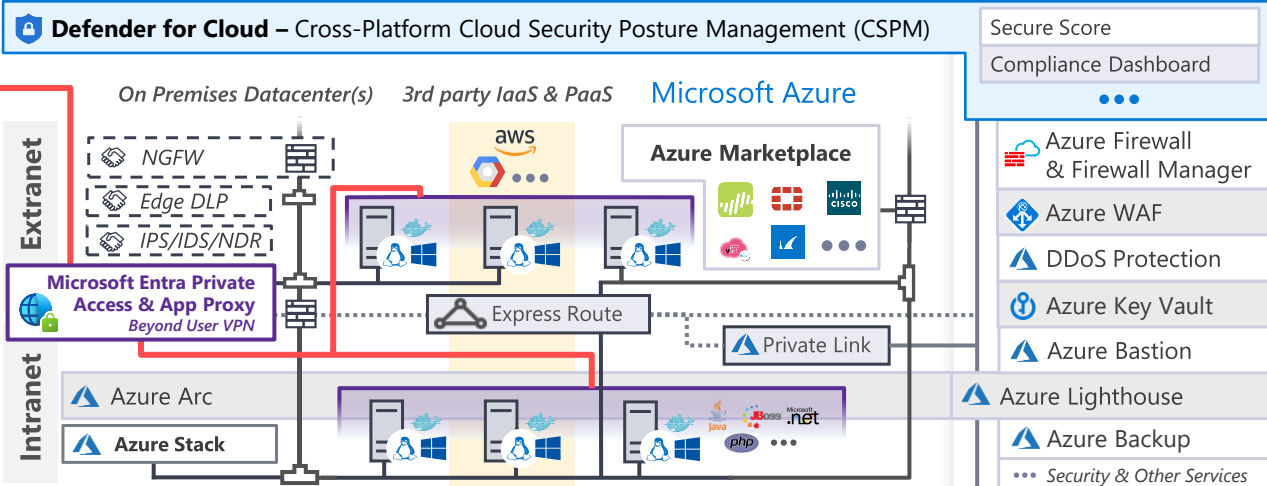
## Endpoints & Devices



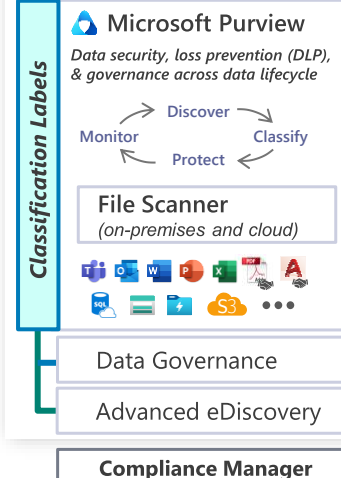
### Microsoft Defender for Endpoint



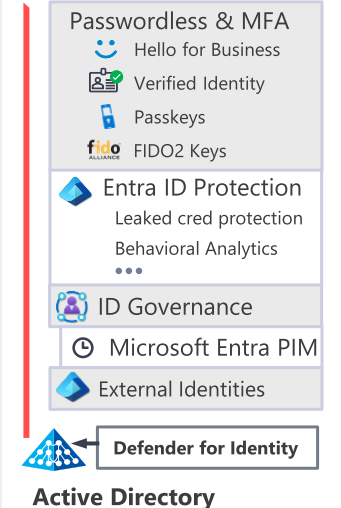
## Hybrid Infrastructure – IaaS, PaaS, On-Premises



## Information Protection



## Microsoft Entra



**Securing Privileged Access** – [aka.ms/SPA](https://aka.ms/SPA)

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

**Privileged Access Management (PAM)**

**Cloud Infrastructure Entitlement Management (CIEM)**

**Microsoft Security Exposure Management** – Provides unified view of security posture + attack surface across organization, enabling you to investigate security insights, identify critical assets, reduce attack surfaces and security risk

## Windows 11 & 10 Security



## IoT and Operational Technology (OT)



**Microsoft Defender for IoT (and OT)**

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

**Defender for Cloud** – Cross-Platform, Multi-Cloud XDR  
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises

**Defender for APIs**

## People Security

Attack Simulator

Insider Risk Management

Communication Compliance

**GitHub Advanced Security & Azure DevOps Security**  
Secure development and software supply chain

**Microsoft Security Copilot**

**Threat Intelligence** – 78+ Trillion signals per day of security context

**Service Trust Portal** – How Microsoft secures cloud services

**Security Development Lifecycle (SDL)**

# Dagens fokus

Microsoft Sentinel



Microsoft Defender XDR




Entra ID



[mvpdagen.no](https://mvpdagen.no)

# Entra ID Applikasjoner

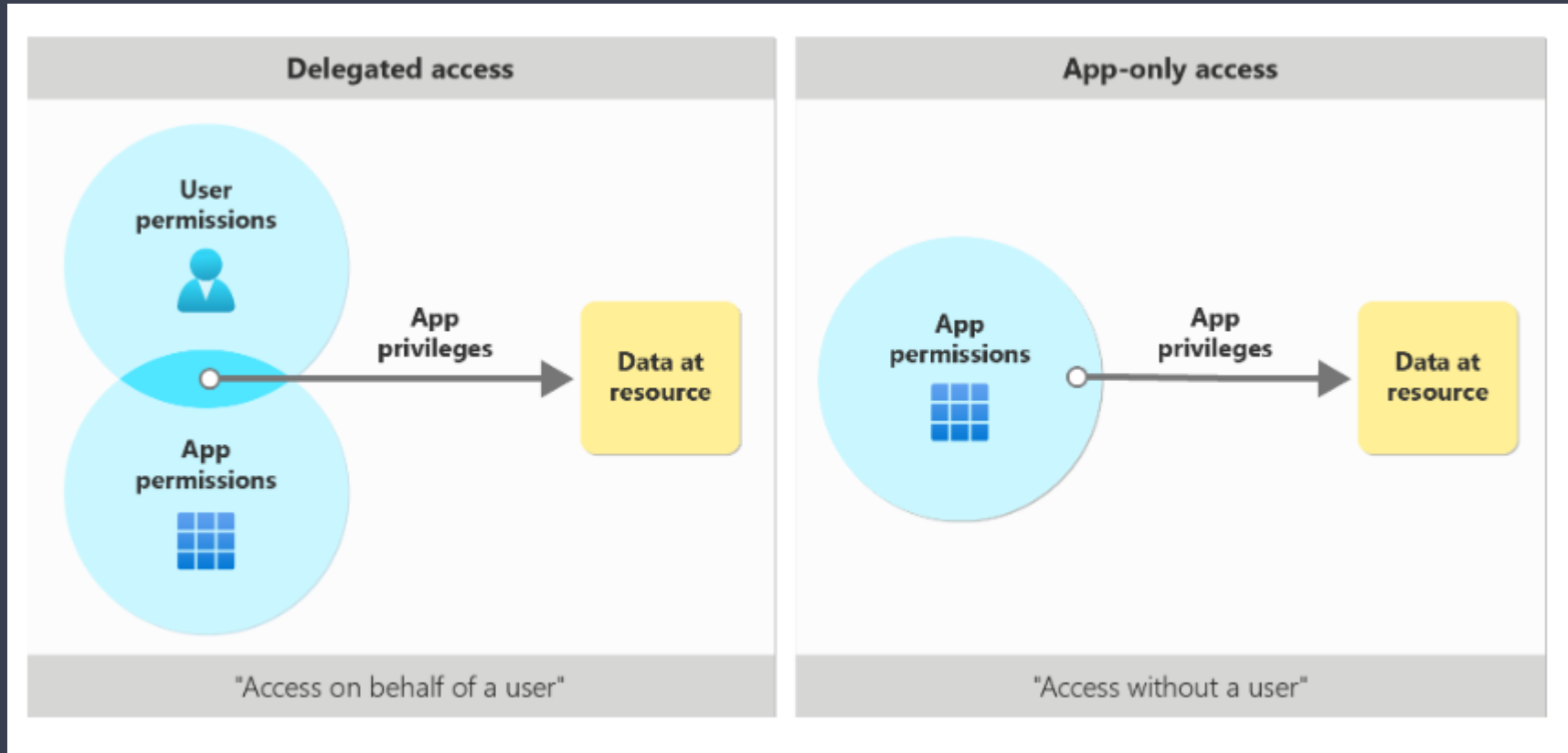
- Mye rom for feilkonfigurasjon
- Egne applikasjoner og tredjeparts applikasjoner
- Applikasjons governance settings er 
- Deteksjon på høyt privilegerte apps

## Warning

Microsoft-user-default-recommended is a Microsoft managed policy. The conditions included in the policy are automatically updated based on Microsoft's latest security recommendations for end-user consent.



# Entra ID: Consents



# Innsikt:

- Innebygde verktøy:

- Entra ID portal: Microsoft Entra application activity and workbooks

- Security portal: App Governance

- MSIdentityTools

- AzADServicePrincipalInsights - <https://aka.ms/azadspi>

- Aztier.com

- graphpermissions.merill.net

- Maester- Entra ID Config analyzer



# XDR – Hva er det?

Trenger vi msportals.io fortsatt?

Prøver å lage en portal for pre og post breach portal for bedrifter.

Sentinel vil bli fjernet 1. Juli 2026.

- [Microsoft Defender for Endpoint](#)
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Defender for Cloud
- Microsoft Entra ID Protection
- Microsoft Data Loss Prevention
- App Governance
- Microsoft Purview Insider Risk Management

# XDR Unified RBAC

Med unified RBAC Roller kan vi fjerne bruk av security admin rolle som altfor ofte brukes. (Security Admin ses på som tier 0)

Microsoft states that Unified RBAC is now the default permissions model for new tenants, existing tenants need to activate Unified RBAC

Med Unified RBAC vil man en rolle man PIMer seg opp til (om nødvendig) så har man tilgang på tvers av produkter.

## Workloads

### Endpoints & Vulnerability Management

☒ Active

### Email & Collaboration

Enforcing Exchange Online permissions will impact the Email & Collab capabilities that were previously configured in the Exchange admin center. [Exchange admin center](#).

☒ Active - Defender for Office 365

☒ Active - Exchange Online permissions ⓘ

### Identity

Enabling this setting will also enforce these permissions on the Microsoft Defender for Identity portal. [Learn more about role groups for MDI](#).

☒ Active

### Cloud Apps

Turning on this setting will apply these permissions to Microsoft Defender for Cloud Apps experiences, with the exception of app governance. Note: built in roles such as discovery admin, discovery report admin, app/instance admin and user group admin will no longer be supported once this setting is activated. [Learn more about the existing cloud apps roles](#).

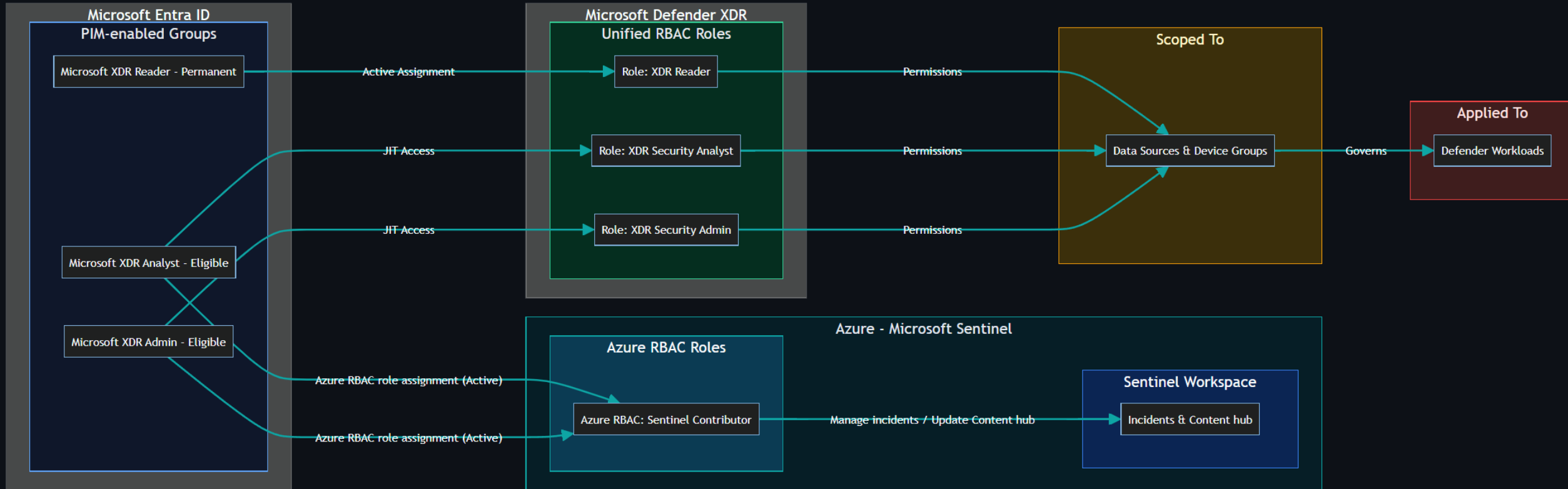
☒ Active



Demo – show and tell

[mvpdagen.no](http://mvpdagen.no)

# XDR Design





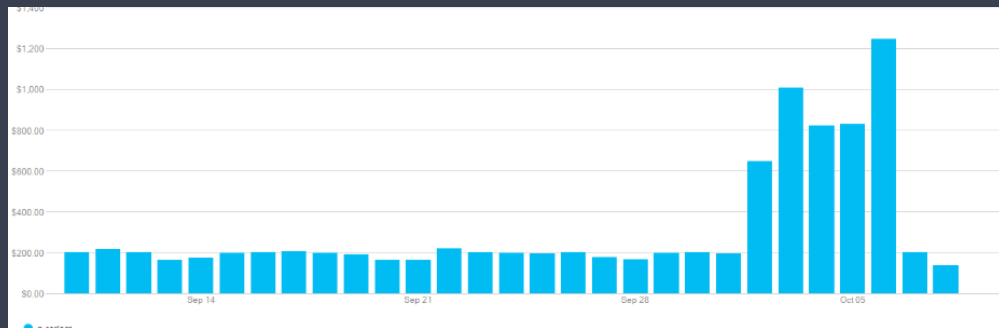
# Sentinel kostnader

# Sentinel Cost use Case

Hei Anders, vi må spare noe penger, sentinel koster for mye.

Pls fix asap!

1. Du må klare oppdage en kostendring



# Mail

## Subscription summary

Anomaly detected	Yes
Delta compared to expected range	527.14 %

## Resource group summary

- Cost up 79.05% from 5 new resource group(s).
- Cost changed 9.09% from 3 existing resource group(s).

## Most significant changes in resource group(s) during this period


Name	Cost change %	Percent of total
mc_mvpdagen_mvpdagen-aks_westeurope	88.43	51.94
t-aks-np	20.3	16.21
t-aks	39.66	9.09
defaultresourcegroup-weu	196.88	4.98
mvpdagen	79.22	4.82

Review additional details in the Azure portal.

# Hvordan?

## 1. Undersøk hvor du kan "spare" eller filtrere bort data\*

- **Security Portal** → **Sentinel** → **Threat Management** → **Workbooks**
- **Or Content Management- content hub**

 Microsoft Sentinel Optimization Workbook

## 2. Grav videre ned i tabell som generer mye ingest

- Avhengig av hva slags tabell dette er, finn ut om det er mønster eller om det er enkelte servere, løsninger, ressurser som "spammer" ned tabellen

## 3. Hva er egentlig denne loggkilden og hva slags data inneholder den?

Trenger vi dette i det hele tatt? ( Eksisterende deteksjon, planlagte deksjoner)

Trenger vi det pga compliance/Dora?

Lag deg en matrise på hvordan du analyser de typiske spørsmålene.

Del informasjon med stakeholders, åpent før du gjør tiltak ( gjerne ADR)



# Use case ADR: Nsg resource logs

Within the Diagnostics settings we noticed these a certain resource type was about 40 % + of the logs.

Status	COMPLETED
Owner	@Anders Kristiansen
Contributors	@Anders Kristiansen @Eirik Sveen
Approved	Approved by Security Architecture Group Sep 25, 2024
Created On	Sep 24, 2024
Decision Outcome	1 : Stopp logging these events completely. <a href="#">Proof of meeting</a>
On this page	<ul style="list-style-type: none"><li>• ? Problem statement</li><li>• 💡 Research insights</li><li>• 📊 Solution hypothesis</li><li>• 🌈 Design options</li><li>• 😊 Criteria for voting</li><li>• ☀️ Results</li><li>• ✅ Follow up</li><li>• 💎 Examples and links</li></ul>


# Mye logger, er det verdt det?

Results			Chart
Category	Count	Percent	
> NetworkSecurityGroupEvent	24918956	22	
> NetworkSecurityGroupRuleCounter	24917188	22	
> ApplicationGatewayAccessLog	16368602	14	
> WorkflowRuntime	10631111	9	
> ApplicationGatewayFirewallLog	9529821	8	
> kube-apiserver	8607653	8	
> EventHubVNetConnectionEvent	6841746	6	
> AuditEvent	6439714	6	
> SQLSecurityAuditEvents	1824422	2	
> guard	1675761	1	
> RuntimeAuditLogs	801291	1	
> Engine	550393	0	
> OperationalLogs	199790	0	
> ActivityRuns	110818	0	
> Service	74419	0	
> Blocks	50036	0	

Categories

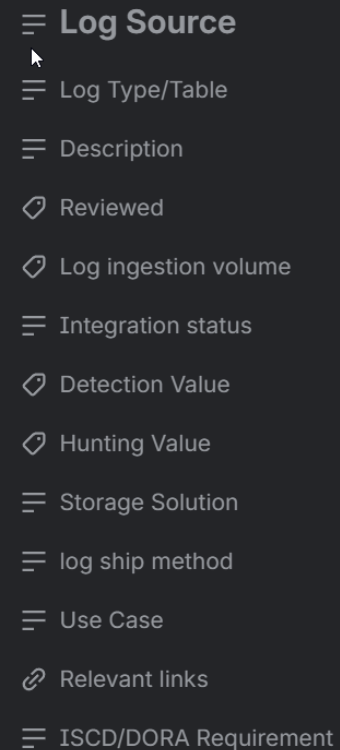
☒ Network Security Group Event

☒ Network Security Group Rule Counter

 Storage retention via diagnostic settings is being deprecated and new rules will no longer be configured. To maintain your existing retention rules please migrate to Azure Storage Lifecycle Management by September 30th 2025. [What do I do?](#)

# Evaluering av loggkilde

Bruker vi disse til deteksjoner?  
Har vi andre måter å se denne  
type informasjon på?  
Legal?

A screenshot of a dark-themed user interface showing a list of configuration options for a log source. The options are listed vertically, each preceded by a small icon: a hamburger menu icon for expandable sections and a key icon for individual settings.

- ≡ Log Source
- ≡ Log Type/Table
- ≡ Description
- 🔑 Reviewed
- 🔑 Log ingestion volume
- ≡ Integration status
- 🔑 Detection Value
- 🔑 Hunting Value
- ≡ Storage Solution
- ≡ log ship method
- ≡ Use Case
- 🔗 Relevant links
- ≡ ISCD/DORA Requirement
















# Design opsjoner

	↓	Option 1	Option 2	Option 3
Overview		Stopp logging these events completely.	Log to storage account.	As is, Do nothing
Benefits and risks		<ul style="list-style-type: none"><li>+ saving about 70 K SEK each month.</li><li>+ Aligned with log management evaluation schema.</li><li>- no monitor to detect anomalies and high spikes in deny/allow hits.</li></ul>	<ul style="list-style-type: none"><li>+ cost effective solution</li><li>+ Keep logs for possible audit, post mortem incident</li><li>- Most likely waste of money and never used.</li><li>- Time spent on implementing and documenting should be used on other areas.</li></ul>	<ul style="list-style-type: none"><li>+ All logs in sentinel ready for use with live detection.</li><li>- high cost</li><li>- Wrong tier modell on this log.</li></ul>
Criteria/Decision drivers		These logs give little added value from both a hunting and incident response. The	If these logs are required for compliance and audit we should store them in storage account.	As is solution, no required job, just pay as is.


# Microsoft Sentinel Logging

## Feil tiering

Ofte setter man opp  
Sentinel og sender all logg  
– uansett bruksområde –  
direkte inn i analytic tier

<input type="checkbox"/> Table name ↑↓	Type ↑↓	Plan ↑↓
<input type="checkbox"/>  ABAPAuditLog	Azure table	Analytics
<input type="checkbox"/>  ABAPAuthorizationDetails	Azure table	Analytics
<input type="checkbox"/>  ABAPChangeDocsLog	Azure table	Analytics
<input type="checkbox"/>  ABAPTableDataLog	Azure table	Analytics
<input type="checkbox"/>  ABAPUserDetails	Azure table	Analytics
<input type="checkbox"/>  ADAssessmentRecommendation	Azure table	Analytics
<input type="checkbox"/>  ADReplicationResult	Azure table	Analytics
<input type="checkbox"/>  AggregatedSecurityAlert	Azure table	Analytics
<input type="checkbox"/>  Alert	Azure table	Analytics
<input type="checkbox"/>  AlertEvidence	Azure table	Analytics
<input type="checkbox"/>  AlertInfo	Azure table	Analytics
<input type="checkbox"/>  Anomalies	Azure table	Analytics
<input type="checkbox"/>  AppCenterError	Azure table	Analytics
<input type="checkbox"/>  ASimAuditEventLogs	Azure table	Analytics
<input type="checkbox"/>  ASimAuthenticationEventLogs	Azure table	Analytics

# Microsoft Sentinel Logging



**Manage table**



Type: Any Tier: Any  Add filter

Table name	Tier
<input checked="" type="checkbox"/>  AlertInfo	Analytics

## Manage AWSNetworkFirewallAlert

After you've set up Microsoft Sentinel data lake, all new data ingested into this table is automatically available in the data lake regardless of tier. To access archived data ingested prior to setup, use search and restore. [Learn more about data retention](#)

After you've set up Microsoft Sentinel data lake, all new data ingested into this table is automatically available in the data lake regardless of tier. To access archived data ingested prior to setup, use search and restore. [Learn more about data retention](#)

### ☒ Analytics tier

Analytics data supports real-time monitoring, detection, and hunting. To place data into longer-term storage that you can query, extend the total retention period.

#### Analytics retention \* ⓘ

90 days

#### Total retention \* ⓘ

Same as Analytics retention (90 days)

[Hide Data retention settings](#)

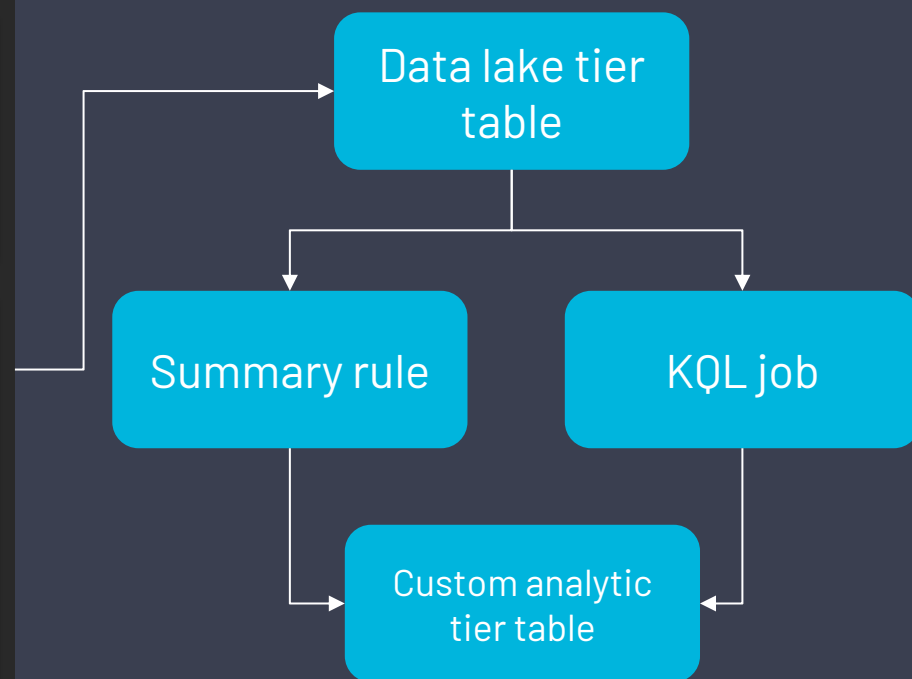
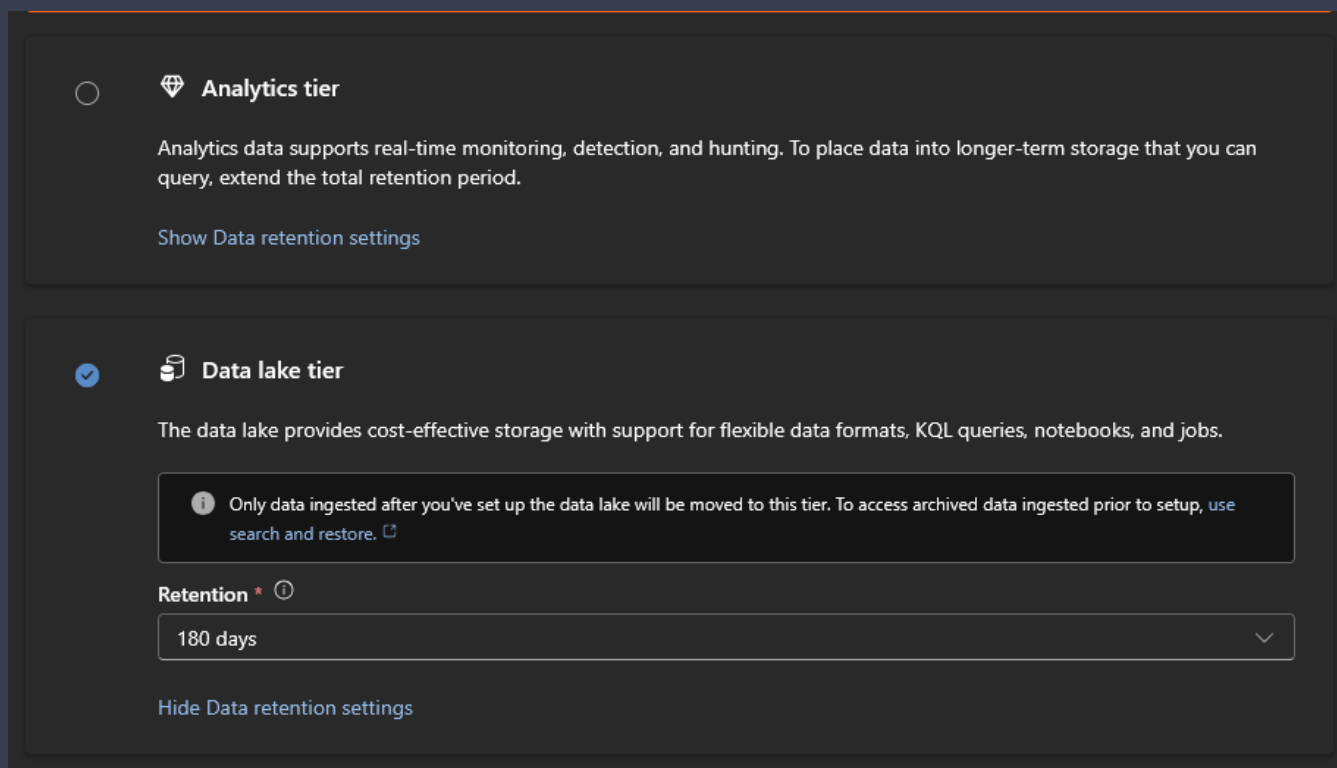
### ☐ Data lake tier

(auxiliary table tier)

The data lake provides cost-effective storage with support for flexible data formats, KQL queries, notebooks, and jobs.

[Show Data retention settings](#)

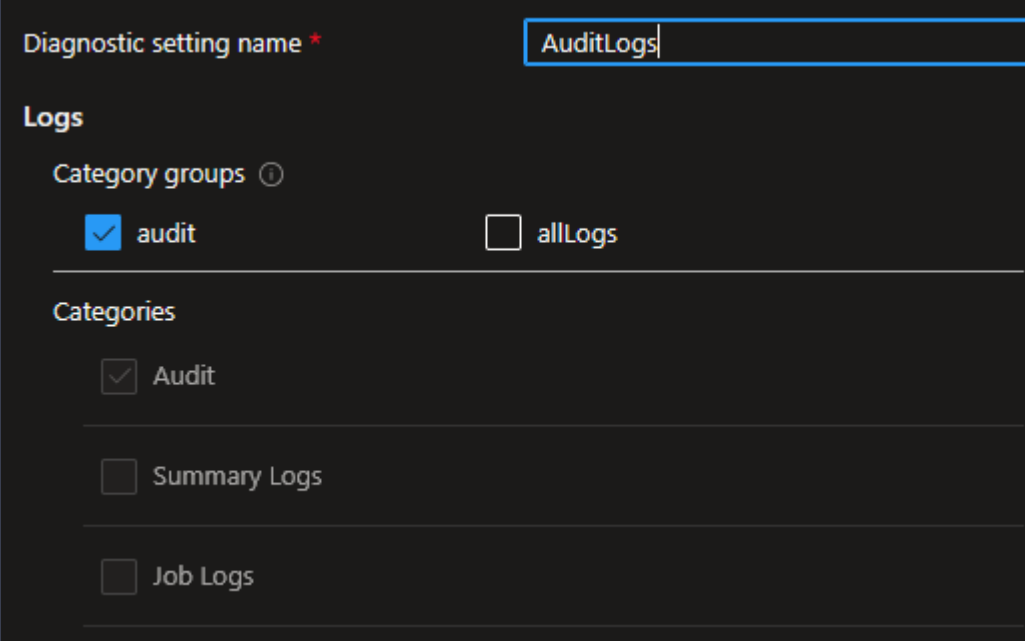
# Microsoft Sentinel Logging



# Microsoft Sentinel Audit

## LAQueryLogs

Mange glemmer å slå på  
Audit-logging direkte på  
log analytics workspacet  
som kreves for å bruke  
LAQueryLogs



The screenshot shows the configuration interface for a diagnostic setting named 'AuditLogs'. Under the 'Logs' section, the 'Category groups' are configured with 'audit' selected (checked) and 'allLogs' unselected. Under the 'Categories' section, 'Audit' is selected (checked), while 'Summary Logs' and 'Job Logs' are unselected.

Category groups
<input checked="" type="checkbox"/> audit
<input type="checkbox"/> allLogs

Categories
<input checked="" type="checkbox"/> Audit
<input type="checkbox"/> Summary Logs
<input type="checkbox"/> Job Logs



# Microsoft Sentinel Health

## SentinelHealth

Samme historie her –  
SentinelHealth kan være  
ekstremt nyttig for å  
feilsøke komponenter som  
analytic rules, automation  
rules og playbooks

mvpdagen.no

### ^ Auditing and health monitoring

#### What is it?

With the Microsoft Sentinel health and audit feature, you can keep an eye on the availability and health of system resources.

#### How to enable it?

Select **Enable** to enable health monitoring for all resources, or select **Configure diagnostic settings** for advanced configuration. [Learn more >](#)

Enabled

[Configure diagnostic settings >](#)

### Logs

#### Category groups ⓘ

☒ allLogs

#### Categories

☒ Analytics

☒ Automation

☒ Data Collection - Connectors

# Microsoft Sentinel Logging

## Workspace retention

Glemmer man å konfigurere retention på workspacet har man bare 30 dager med data – selv om 90 er «gratis»

### Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be [configured individually for specific data types](#).

Data Retention (Days)

90

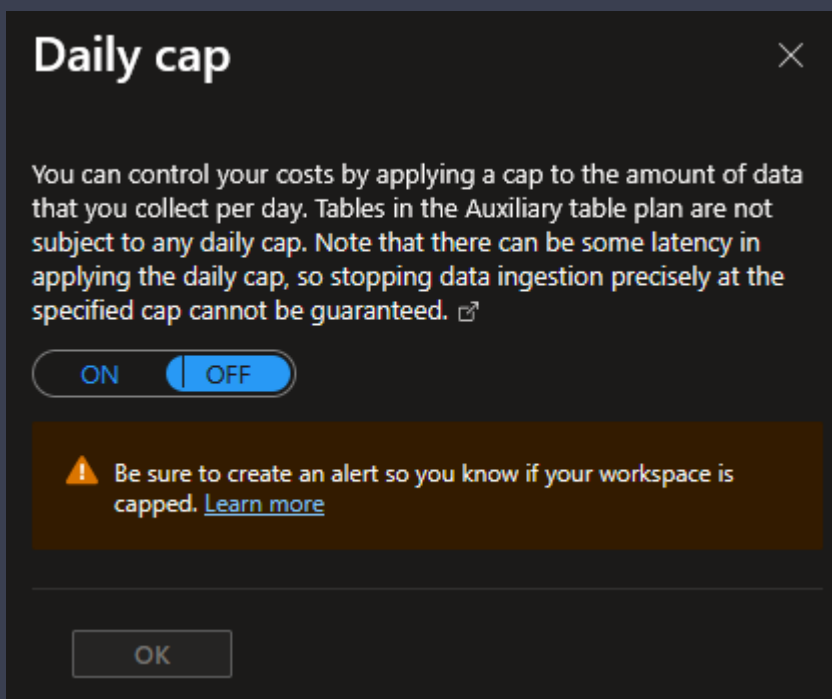
Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. [Learn more](#).

In addition to setting the default retention for tables in this workspace here, you can configuration data retention and data archive on a per-table basis on the [Tables](#) page of this workspace.

OK

# Microsoft Sentinel Logging

Slås kanskje på for å få  
kostnadskontroll uten å  
være klar over  
konsekvensen – man er  
effektivt blind fra man når  
cap



# Microsoft Sentinel Deteksjon



## Manglende deteksjon

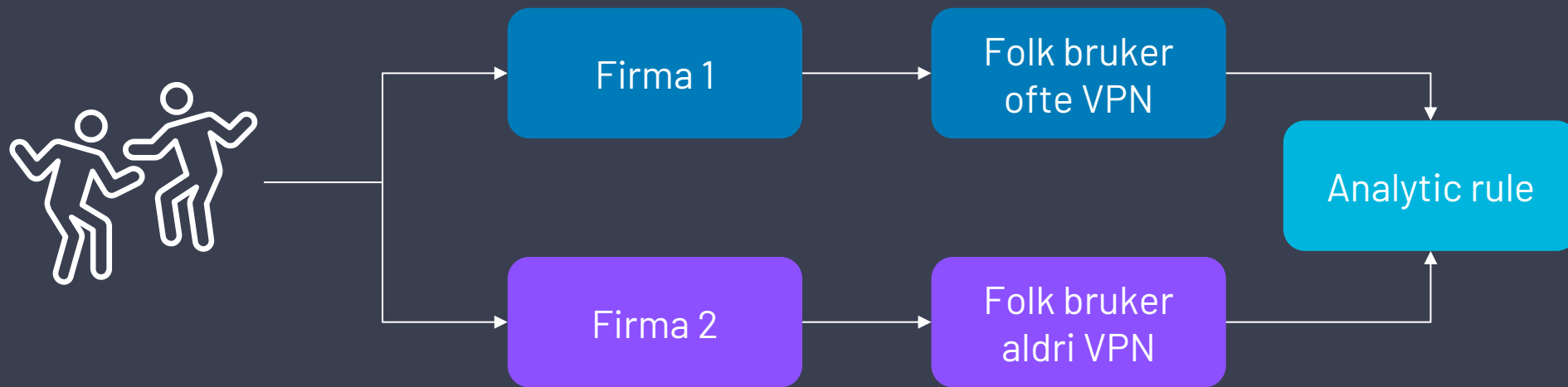
Ingen eller få alarmer til tross for «mange» regler kan bety en av to ting – enten har man *lite aktivitet*, ellers har man for *dårlig dekning*.

## Dårlig deteksjon


Begrep som falske positive og alert fatigue er velkjente i security operations – skyldes ofte at man belager seg på standardmaler som ikke egner seg for alle.

# Microsoft Sentinel

## Deteksjon



# Microsoft 365/Azure Audit logging



Data Source	# Unique Actions	% of Activities Covered
Purview Audit Search (Unified Audit Log)	190	99,5%
Defender For Cloud Apps CloudAppEvents Logs	170	89,5%
Sentinel OfficeActivity Logs	76	40,0%
Total Unique Actions	191	100%

# Microsoft 365/Azure Unified Audit Log



The **Unified Audit Log (UAL)** is a Microsoft 365 feature that consolidates user and administrator activity across various services into a single, searchable log.



```
PS C:\Program Files\PowerShell\7> Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled  
  
UnifiedAuditLogIngestionEnabled : False  
  
PS C:\Program Files\PowerShell\7> Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

Start recording user and admin activity

Searches completed | Active searches | Active unfiltered searches  
0 | 0 | 0


Date and time range (UTC) \*

Start    


End    

Keyword Search

Admin Units




Activities - friendly names



Activities - operation names ⓘ

Record Types















Search name

Users

ObjectId (File, folder, or site) ⓘ

Workloads



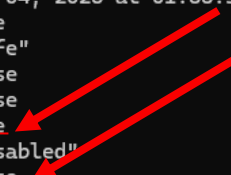
 Copy this search  Delete  Refresh					0 items	
Search name 		Job status 	Progress (%) 	Search time 	Total results 	Creation tim...   Search performed by 



# Defender for Linux

## Standard configuration

```
root@mde-test-tux:/home/mdetest# mdatp health
healthy : true
health_issues : []
licensed : true
engine_version : "1.1.25070.4000"
engine_load_status : "Engine not loaded"
app_version : "101.25082.0003"
org_id : "e66378e2-49cb-4233-a97e-ea70652bcf23"
log_level : "info"
machine_guid : "1585eed5-8b04-42b6-a4ee-e33207ac486f"
release_ring : "Production"
product_expiration : Jun 04, 2026 at 01:55:31 PM
cloud_enabled : true
cloud_automatic_sample_submission_consent : "safe"
cloud_diagnostic_enabled : false
cloud_pin_certificate_thumbs : false
passive_mode_enabled : true
behavior_monitoring : "disabled"
real_time_protection_enabled : false
real_time_protection_available : true
real_time_protection_subsystem : "fanotify"
supplementary_events_subsystem : "ebpf"
automatic_definition_update_enabled : true
definitions_updated : Sep 30, 2025 at 07:36:28 AM
definitions_updated_minutes_ago : 265
definitions_version : "1.437.227.0"
definitions_status : "up_to_date"
edr_early_preview_enabled : "disabled"
edr_device_tags : [{"key": "AzureResourceId", "value": "/subscriptions/6558eb22-631e-4ae8-9858-3c60595050e5/resourceGroups/mde-test/providers/Microsoft.Compute/virtualMachines/mde-test-tux"}, {"key": "SecurityWorkspaceId", "value": "6558eb22-631e-4ae8-9858-3c60595050e5"}]
edr_group_ids : ""
edr_configuration_version : "30.199999.main.2025.09.28.26-456999a3392a7b494c50cd4b88e64e540c495082"
edr_machine_id : "8e7abfe9ea5494dbb992cf7fecdd602d9e5fe31dd"
conflicting_applications : []
network_protection_status : "stopped"
network_protection_enforcement_level : "disabled"
```



#### Configuration status

✔ Configuration updated

#### Real time protection/RTP

✔ Enabled

#### Behavior monitoring/BM

✔ Enabled

#### Device health status

### Defender Antivirus not active +2 more issues

Type	State	Date & time
Last full scan	● No scan performed	
Last quick scan	● No scan performed	
Security intelligence	✔ Version 1.437.227.0	Sep 30, 2025 9:36:28 AM
Engine	✔ Version 1.1.25070.4000	Sep 30, 2025 9:36:25 AM
Platform	✔ Version 101.25082.0003	Sep 30, 2025 9:36:20 AM
Defender Antivirus mode	● Passive	Sep 30, 2025 8:57:16 PM


#### Device health status

### Security intelligence is not up to date +4 more issues

Type	State	Date & time
Last full scan	● No scan performed	
Last quick scan	● No scan performed	
Security intelligence	● Version 1.409.120.0	Apr 8, 2024 10:25:08 AM
Engine	● Version 1.1.24030.4	Apr 8, 2024 10:25:08 AM
Platform	● Version 4.18.24020.7	Sep 3, 2025 1:47:24 PM
Defender Antivirus mode	✔ Active	Sep 30, 2025 8:59:17 PM

# Defender for Linux

## Endpoint Security Policies

**Linux AV**  
Antivirus

[Overview](#) [Policy settings values](#) [Policy settings status](#) [Applied devices](#) [Assigned groups](#)

Settings

Cloud delivered protection preferences

Enable cloud delivered protection

Enabled

Enable automatic sample submissions

Safe

Diagnostic data collection level

optional

Automatic security intelligence updates

Enabled

Configure cloud block level

High

Antivirus engine

Enable real-time protection (deprecated)

Enabled

Enable passive mode (deprecated)

Enabled

Exclusions merge

admin\_only

Threat type settings merge

admin\_only

Enable scanning of archives

Enabled

Enable scanning after definition update

Enabled

Enable file hash computation

Enabled

Enable behavior monitoring

Enabled

Network protection

Enforcement Level

block

# mdatp\_managed.json

```
{
  "antivirusEngine":{
    "enforcementLevel":"real_time",
    "threatTypeSettings":[
      {
        "key":"potentially_unwanted_application",
        "value":"block"
      },
      {
        "key":"archive_bomb",
        "value":"audit"
      }
    ]
  },
  "cloudService":{
    "automaticDefinitionUpdateEnabled":true,
    "automaticSampleSubmissionConsent":"safe",
    "enabled":true,
    "proxy": "<EXAMPLE DO NOT USE> http://proxy.server:port/"
  }
}
```

- Make sure it's valid json
- Set realtime monitoring on
- Enable cloud block mode
- Enable cloud protection
- Set all merge policies to admin\_only!

<https://learn.microsoft.com/en-us/defender-endpoint/linux-preferences>

# Defender for Cloud Apps

## Standard configuration

### Blokkering av applikasjoner

For å blokkere applikasjoner som er markert unsanctioned må man sette på integrasjon mot Defender for Endpoint

#### Microsoft Defender for Endpoint

##### Microsoft Defender for Endpoint Integration

☐

Enforce app access

Enabling this will Block access to apps that were marked as Unsanctioned and will deliver a Warning on access and allow bypass to apps marked as Monitored.

# Defender for Endpoint

## Standard configuration

### Oppdagelse og blokkering av applikasjoner

Må også sette på integrasjonen fra Defender for Endpoint sine settings mot MCAS



On

#### Microsoft Defender for Cloud Apps

Forwards Microsoft Defender for Endpoint signals to [Defender for Cloud Apps](#), giving administrators deeper visibility into both sanctioned cloud apps and shadow IT. It also gives them the ability to block unauthorized applications when the custom network indicators setting is turned on. Forwarded data is stored and processed in the same location as your Cloud App Security data. This feature is available with an E5 license for [Enterprise Mobility + Security](#) on devices running Windows 10 version 1709 (OS Build 16299.1085 with KB4493441), Windows 10 version 1803 (OS Build 17134.704 with KB4493464), Windows 10 version 1809 (OS Build 17763.379 with KB4489899) or later Windows 10 versions.

# Defender for Endpoint

## Standard configuration

### Custom network indicators

MCAS legger inn domener, URL og IP her når man markerer som unsanctioned – så dette må også stå på



On

#### Custom network indicators

Configures devices to allow or block connections to IP addresses, domains, or URLs in your [custom indicator lists](#). To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform ([see KB 4052623](#)). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender for Endpoint data.

# Defender for Endpoint

## Standard configuration

### EDR i blokkeringsmodus

Når Defender ikke er hovedpersonen på en server er blokkeringsmodus nyttig for ekstra beskyttelse – ingen grunn til å ha det slått av (*utenom oppdukkende kompatibilitetsproblemer*)



On

#### Enable EDR in block mode

When turned on, Microsoft Defender for Endpoint leverages behavioral blocking and containment capabilities by blocking malicious artifacts or behaviors observed through post-breach endpoint detection and response (EDR) capabilities. This feature does not change how Microsoft Defender for Endpoint performs detection, alert generation, and incident correlation. To get the best protection, make sure to apply [security baselines in Intune](#). See [EDR in block mode](#) for more details.



# Defender for Endpoint

## Standard configuration

### Automatisk lukking av alarmer

Har en tendens til å lukke alarmer med f.eks URL-klikk på phishing-lenker uten å faktisk få verifisert om brukeren har gitt fra seg info.



On

#### **Automatically resolve alerts**

Resolves an alert if Automated investigation finds no threats or has successfully remediated all malicious artifacts.

# Defender for Endpoint

## Standard configuration

### Automation uploads fra automated investigation

#### File Content Analysis

Content analysis submits suspicious files identified by Automated investigation to the cloud for additional inspection. Only files with the specified extension names will be submitted.

##### Content analysis

☐ Off

##### File extension names ⓘ

","air,bat,cmd,com,cpl,dll,elf,exe,gadget,inf,job,js,ko,ko.gz,msi,pl,ps1,py,rb,reg,rgs,scr,sh,sys,tcl,url,vb,vbe,vbs,ws,wsf

#### Memory Content Analysis

If you would like Microsoft Defender for Endpoint to automatically investigate memory content of processes, please enable the Memory Content Analysis. When enabled, memory content might be uploaded to Microsoft Defender for Endpoint during an Automated investigation.

##### Enabled

☐ Off

# Takk!

## Spørsmål?

Du finner oss på:

- **Anders** - @linkedin.com/in/akristiansendotcom
- **Truls** - @linkedin.com/in/truls-dahlsveen/

mvpdagen.no

