Að viðhalda öflugu öryggi í skýjaumhverfinu

Notkun Defender for Cloud og Microsoft Sentinel til að styrkja öryggisstöðu þína og verjast ógnum

- Ragnar Sigurðsson, ráðgjafi hjá Advania

Öryggislausnir í Azure

- Alhliða skýjaöryggislausnir
- Greina og styrkja heildar öryggisstöðu
- Vernda gegn nútíma ógnum
- Draga úr áhættu um allt skýið
- Styðja fjölda skýja umhverfi (Azure, AWS, Google) og hybrid umhverfi

Microsoft Defender for Cloud

DevSecOps
DevOps Security

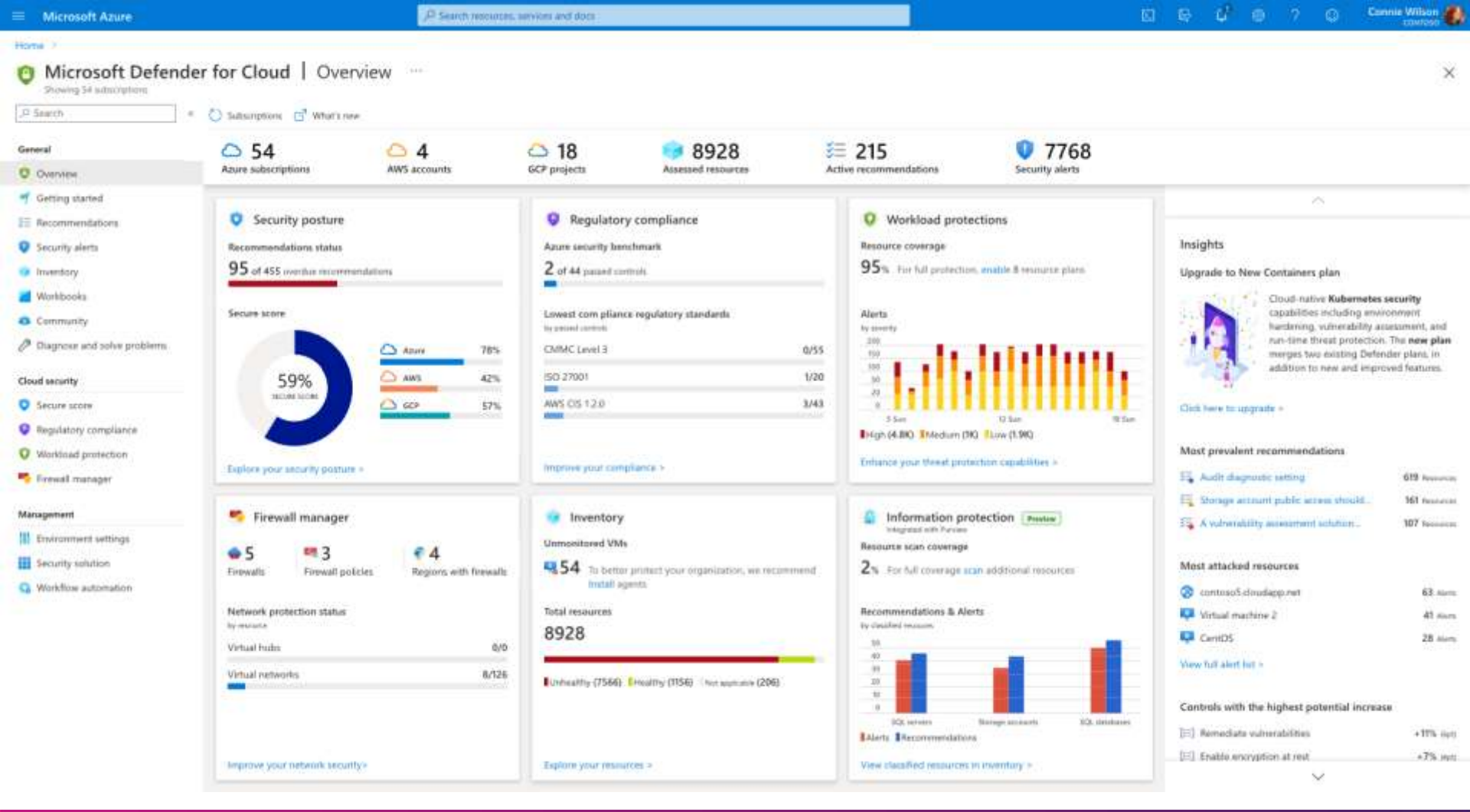
CSPM
Cloud Security Posture Management

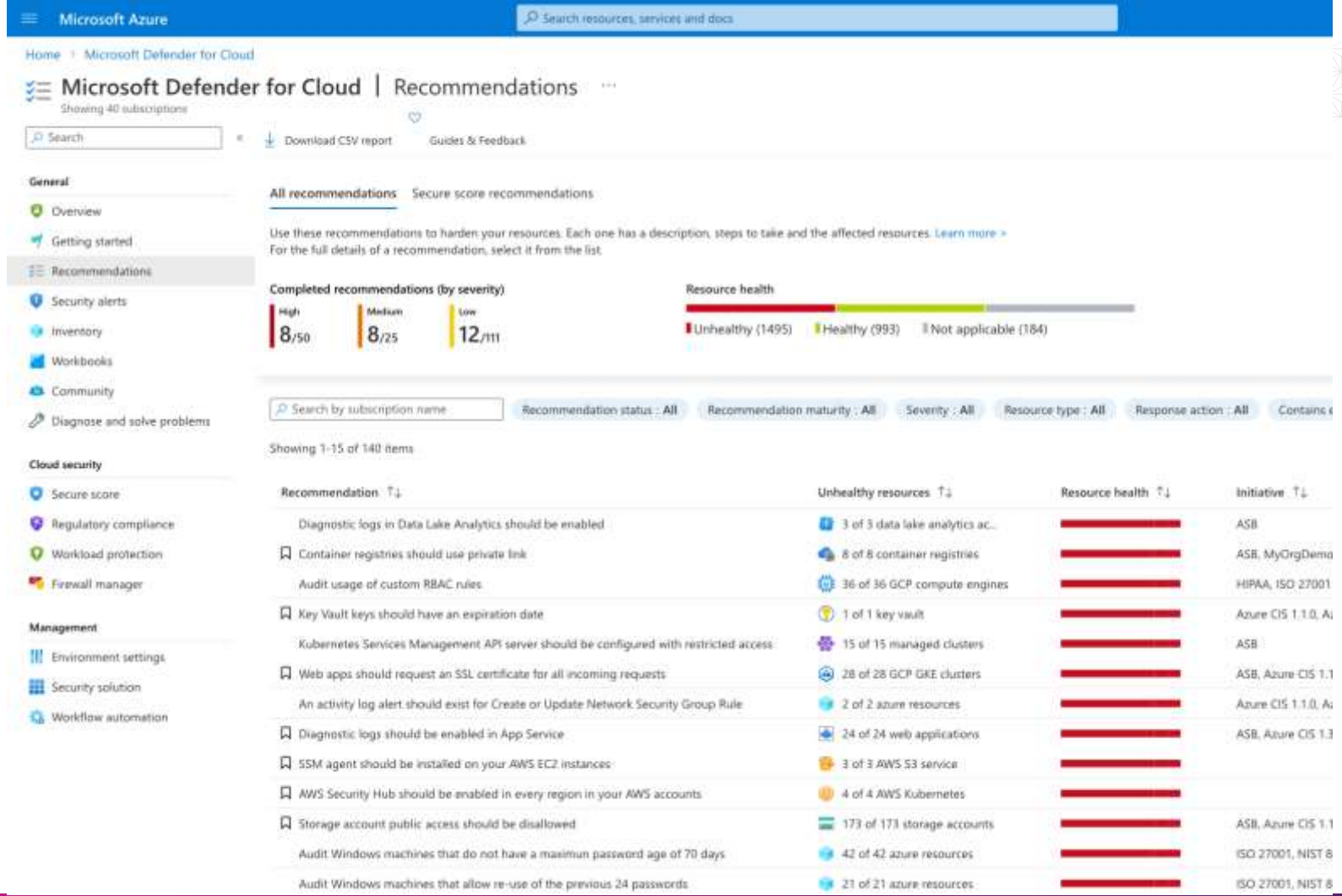
CWP
Cloud Workload Protection

Lykil eiginleikar Defender for Cloud

- Stjórnun öryggisstöðu
  - Meta og sjá fyrir sér heildaröryggisstöðu
- Secure Score
  - Mæla og bæta árangur í öryggismálum
- Fylgni á regluverki
  - Fylgjast með fylgni sérstakra krafa á regluverki
- Vörn gegn ógnum
  - Uppgötva og bregðast við ógnum í rauntíma

Cloud Security Posture Management (CSPM)


Microsoft Azure
Search resources, services and docs
Connie Wilson
contoso
Home
Microsoft Defender for Cloud | Overview
Showing 54 subscriptions
Search
Subscriptions
What's new
General
Overview
Getting started
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud security
Secure score
Regulatory compliance
Workload protection
Firewall manager
Management
Environment settings
Security solution
Workflow automation
54
Azure subscriptions
4
AWS accounts
18
GCP projects
8928
Assessed resources
215
Active recommendations
7768
Security alerts
Security posture
Recommendations status
95 of 455 overdue recommendations
Secure score
59%
SECURE SCORE
Azure 78%
AWS 42%
GCP 57%
Explore your security posture >
Regulatory compliance
Azure security benchmark
2 of 44 passed controls
Lowest compliance regulatory standards
CMMC Level 3 0/55
ISO 27001 1/20
AWS OS 1.2.0 3/43
Improve your compliance >
Workload protections
Resource coverage
95% For full protection, enable 8 resource plans
Alerts
High (4.8K) Medium (1K) Low (1.9K)
Enhance your threat protection capabilities >
Firewall manager
5
Firewalls
3
Firewall policies
4
Regions with firewalls
Network protection status
Virtual hubs 0/0
Virtual networks 8/126
Improve your network security >
Inventory
Unmonitored VMs
54 To better protect your organization, we recommend install agents.
Total resources
8928
Unhealthy (7566) Healthy (1156) Not applicable (206)
Explore your resources >
Information protection
Preview
Resource scan coverage
2% For full coverage scan additional resources
Recommendations & Alerts
SQL servers
Storage accounts
SQL databases
Alerts Recommendations
View classified resources in inventory >
Insights
Upgrade to New Containers plan
Cloud-native Kubernetes security capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The new plan merges two existing Defender plans, in addition to new and improved features.
Click here to upgrade >
Most prevalent recommendations
Audit diagnostic setting 619
Storage account public access should... 161
A vulnerability assessment solution... 107
Most attacked resources
contoso5.cloudapp.net 63
Virtual machine 2 41
CentOS 28
View full alert list >
Controls with the highest potential increase
Remediate vulnerabilities +11%
Enable encryption at rest +7%


Microsoft Azure
Search resources, services and docs
Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Recommendations
Showing 40 subscriptions
Search
Download CSV report
Guides & Feedback
General
Overview
Getting started
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud security
Secure score
Regulatory compliance
Workload protection
Firewall manager
Management
Environment settings
Security solution
Workflow automation
All recommendations
Secure score recommendations
Use these recommendations to harden your resources. Each one has a description, steps to take and the affected resources. Learn more >
For the full details of a recommendation, select it from the list.
Completed recommendations (by severity)
High 8/50
Medium 8/25
Low 12/111
Resource health
Unhealthy (1495)
Healthy (993)
Not applicable (184)
Search by subscription name
Recommendation status : All
Recommendation maturity : All
Severity : All
Resource type : All
Response action : All
Showing 1-15 of 140 items
Recommendation
Unhealthy resources
Resource health
Initiative
Diagnostic logs in Data Lake Analytics should be enabled
3 of 3 data lake analytics ac...
ASB
Container registries should use private link
8 of 8 container registries
ASB, MyOrgDemo
Audit usage of custom RBAC rules
36 of 36 GCP compute engines
HIPAA, ISO 27001
Key Vault keys should have an expiration date
1 of 1 key vault
Azure CIS 1.1.0, A
Kubernetes Services Management API server should be configured with restricted access
15 of 15 managed clusters
ASB
Web apps should request an SSL certificate for all incoming requests
28 of 28 GCP GKE clusters
ASB, Azure CIS 1.1
An activity log alert should exist for Create or Update Network Security Group Rule
2 of 2 azure resources
Azure CIS 1.1.0, A
Diagnostic logs should be enabled in App Service
24 of 24 web applications
ASB, Azure CIS 1.3
SSM agent should be installed on your AWS EC2 instances
3 of 3 AWS S3 service
AWS Security Hub should be enabled in every region in your AWS accounts
4 of 4 AWS Kubernetes
Storage account public access should be disallowed
173 of 173 storage accounts
ASB, Azure CIS 1.1
Audit Windows machines that do not have a maximun password age of 70 days
42 of 42 azure resources
ISO 27001, NIST 8
Audit Windows machines that allow re-use of the previous 24 passwords
21 of 21 azure resources
ISO 27001, NIST 8

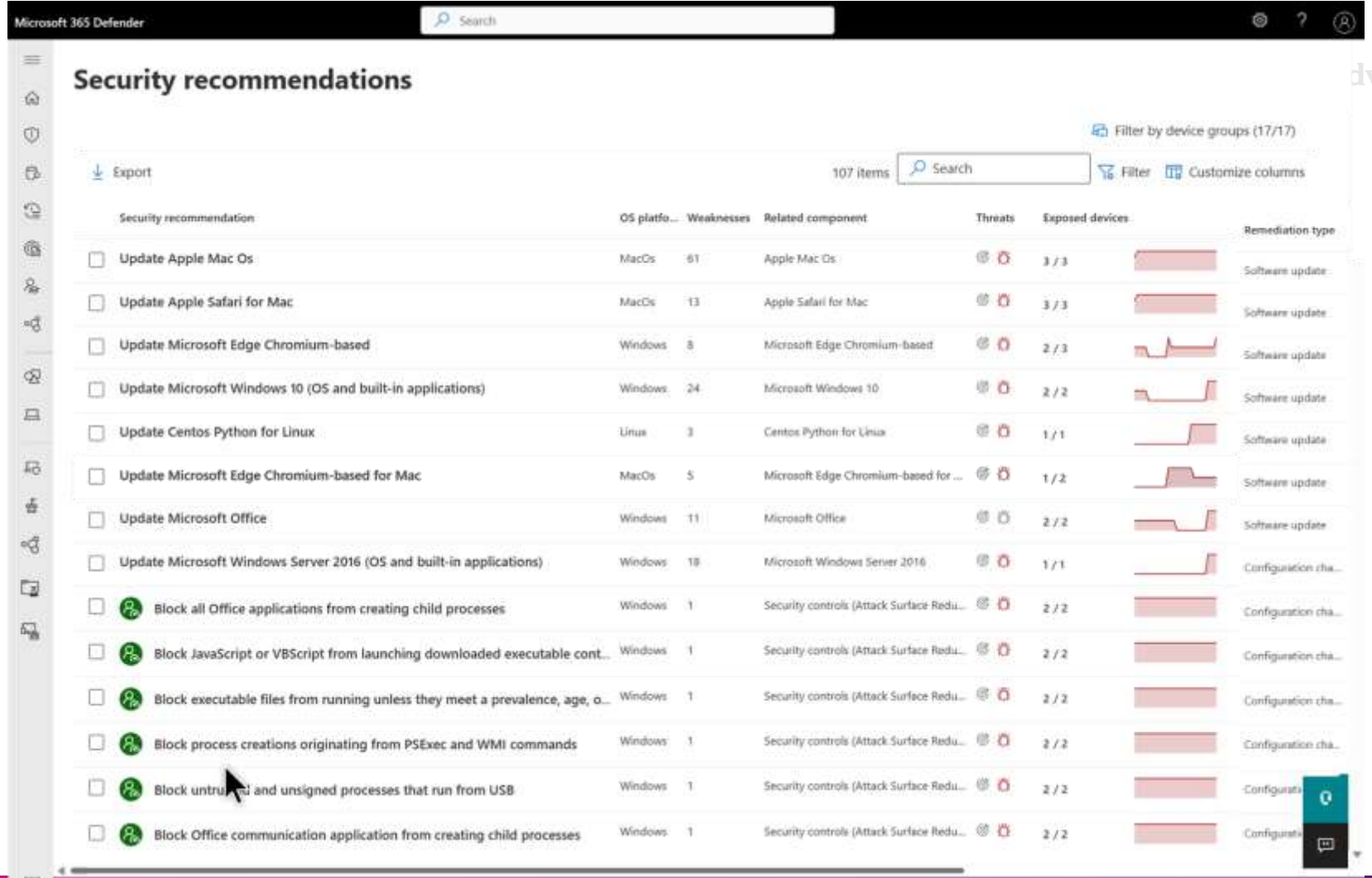
Microsoft Defender Vulnerability Management

Dragðu úr áhættu með stöðugri greiningu á veikleikum, áhættumiðaðri forgangsröðun og úrbótum.

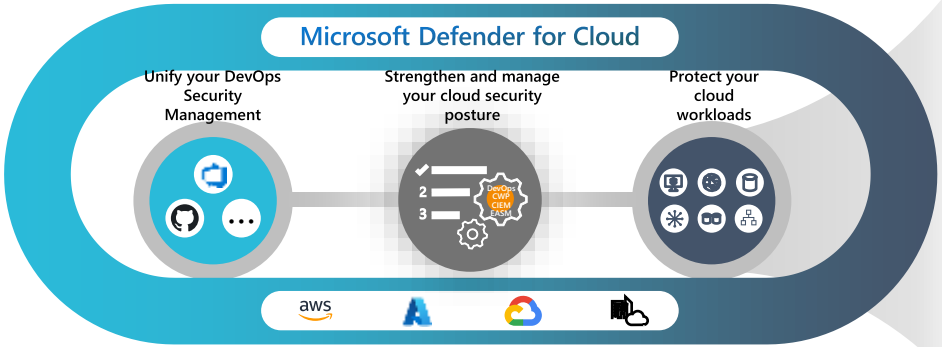
Stöðug greining og vöktun

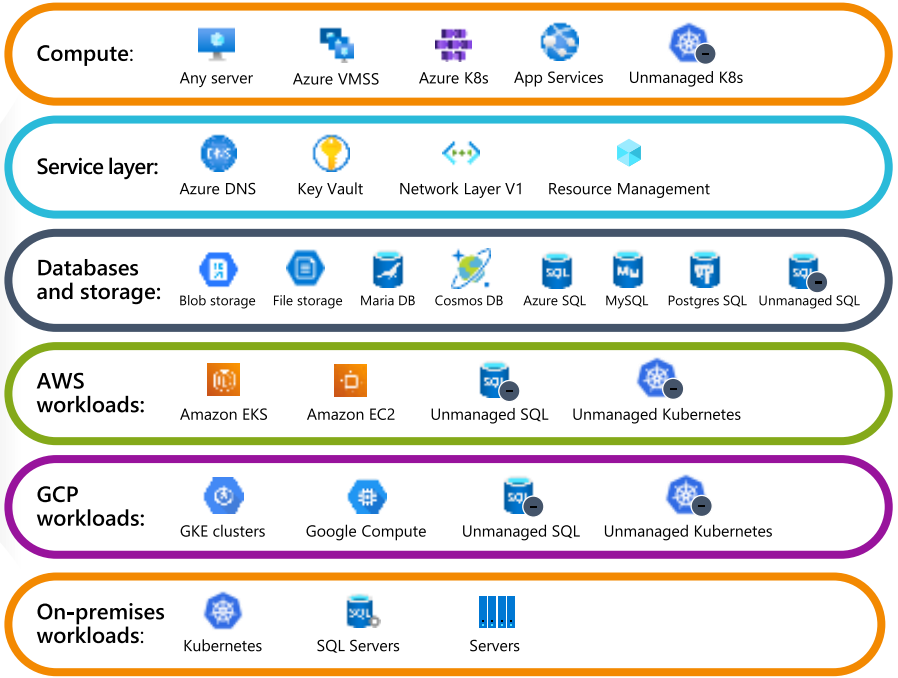
Áhættumiðuð greind forgangsröðun

Úrbætur og mælingar


Microsoft 365 Defender
Search
Security recommendations
Filter by device groups (17/17)
Export
107 items
Search
Filter
Customize columns
Security recommendation
OS platfo...
Weaknesses
Related component
Threats
Exposed devices
Remediation type
Update Apple Mac Os
MacOs
61
Apple Mac Os
3 / 3
Software update
Update Apple Safari for Mac
MacOs
13
Apple Safari for Mac
3 / 3
Software update
Update Microsoft Edge Chromium-based
Windows
8
Microsoft Edge Chromium-based
2 / 3
Software update
Update Microsoft Windows 10 (OS and built-in applications)
Windows
24
Microsoft Windows 10
2 / 2
Software update
Update Centos Python for Linux
Linux
3
Centos Python for Linux
1 / 1
Software update
Update Microsoft Edge Chromium-based for Mac
MacOs
5
Microsoft Edge Chromium-based for ...
1 / 2
Software update
Update Microsoft Office
Windows
11
Microsoft Office
2 / 2
Software update
Update Microsoft Windows Server 2016 (OS and built-in applications)
Windows
18
Microsoft Windows Server 2016
1 / 1
Configuration cha...
Block all Office applications from creating child processes
Windows
1
Security controls (Attack Surface Redu...
2 / 2
Configuration cha...
Block JavaScript or VBScript from launching downloaded executable cont...
Windows
1
Security controls (Attack Surface Redu...
2 / 2
Configuration cha...
Block executable files from running unless they meet a prevalence, age, o...
Windows
1
Security controls (Attack Surface Redu...
2 / 2
Configuration cha...
Block process creations originating from PSExec and WMI commands
Windows
1
Security controls (Attack Surface Redu...
2 / 2
Configuration cha...
Block untrusted and unsigned processes that run from USB
Windows
1
Security controls (Attack Surface Redu...
2 / 2
Block Office communication application from creating child processes
Windows
1
Security controls (Attack Surface Redu...
2 / 2

Cloud workload protection (CWP)

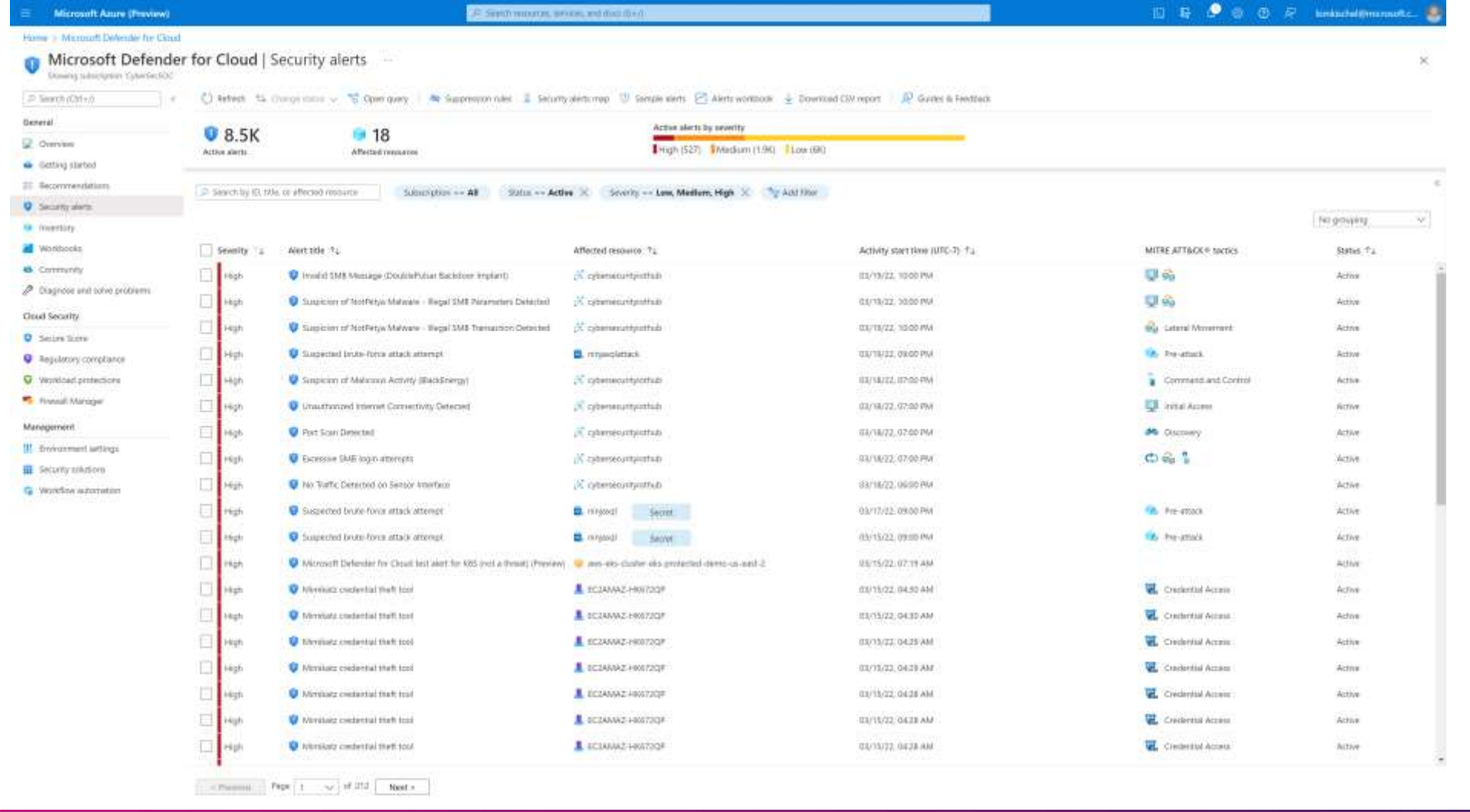




Cloud workload protection (CWP)

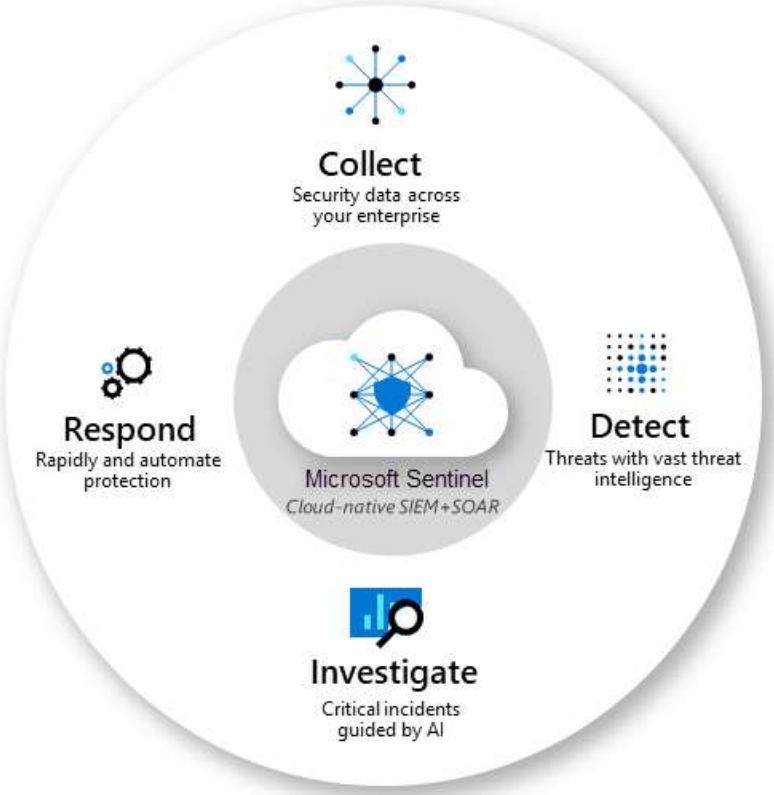
- Verndaðu netþjóna, geymsluauðlindir, gagnagrunna og containera
- Innsýn í innviðaþjónustur, öryggis tilkynningar, and öryggisatvik atvik
- Yfirlit yfir Defender svítuna
-
  - Defender for Servers
  - Defender for App Service
  - Defender for Storage
  - Defender for Databases
  - Defender for Containers
  - Defender for Key Vault
  - Defender for Resource Manager
  - Defender for DNS
  - Defender for API


Microsoft Azure
Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Workload protections
Showing 54 subscriptions
Search
Subscriptions
What's new
General
Overview
Getting started
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud security
Secure score
Regulatory compliance
Workload protections
Firewall manager
Management
Environment settings
Security solution
Workflow automation
Defender for Cloud coverage
665
TOTAL
Fully covered (89.5%)
Agent not installed (3.8%) Install
Not covered (6.8%) Upgrade all
216/225
Servers
Upgrade
51/51
App service
21/30
Containers
Upgrade
40/40
Key vaults
27/27
Azure SQL database servers
195/209
Storage
Upgrade
12/12
Resource manager subscriptions
12/12
DNS subscriptions
Security alerts
High severity
4.8K
Medium severity
1K
Low severity
1.9K
Advance protection
VM vulnerability assessment
127 Unprotected
Just-in-time VM Access
70 Unprotected
Adaptive application control
44 Unprotected
Container image scanning
6 Unprotected
SQL vulnerability assessment
9 Unprotected
File integrity monitoring
Network map
IoT security
Insights
Upgrade to New Containers plan
Cloud-native Kubernetes security capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The new plan merges two existing Defender plans, in addition to new and improved features.
Click here to upgrade >
Most prevalent recommendations
Audit diagnostic setting 619
Storage account public access should... 161
A vulnerability assessment solution... 107
Most attacked resources
contoso5.cloudapp.net 83
Virtual machine 2 41
CentOS 28
View full alert list >
Controls with the highest potential increase
Remediate vulnerabilities +11%
Enable encryption at rest +7%
Remediate security configurations +6%
View controls >


Microsoft Azure (Preview)
Home > Microsoft Defender for Cloud
Microsoft Defender for Cloud | Security alerts
Showing subscription 'CyberSecSOC'
Refresh
Change status
Open query
Suppression rules
Security alerts map
Sample alerts
Alerts workbook
Download CSV report
Guides & Feedback
General
Overview
Getting started
Recommendations
Security alerts
Inventory
Workbooks
Community
Diagnose and solve problems
Cloud Security
Secure Score
Regulatory compliance
Workload protections
Firewall Manager
Management
Environment settings
Security solutions
Workflow automation
8.5K
Active alerts
18
Affected resources
Active alerts by severity
High (527)
Medium (1.9K)
Low (6K)
Search by ID, title, or affected resource
Subscription == All
Status == Active
Severity == Low, Medium, High
Add Filter
No grouping
Severity
Alert title
Affected resource
Activity start time (UTC-7)
MITRE ATT&CK® tactics
Status
High
Invalid SMB Message (DoublePulsar Backdoor Implant)
cybersecurityiothub
03/19/22, 10:00 PM
Active
High
Suspicion of NotPetya Malware - Illegal SMB Parameters Detected
cybersecurityiothub
03/19/22, 10:00 PM
Active
High
Suspicion of NotPetya Malware - Illegal SMB Transaction Detected
cybersecurityiothub
03/19/22, 10:00 PM
Lateral Movement
Active
High
Suspected brute-force attack attempt
rsnjavaattack
03/19/22, 09:00 PM
Pre-attack
Active
High
Suspicion of Malicious Activity (BlackEnergy)
cybersecurityiothub
03/18/22, 07:00 PM
Command and Control
Active
High
Unauthorized Internet Connectivity Detected
cybersecurityiothub
03/18/22, 07:00 PM
Initial Access
Active
High
Port Scan Detected
cybersecurityiothub
03/18/22, 07:00 PM
Discovery
Active
High
Excessive SMB login attempts
cybersecurityiothub
03/18/22, 07:00 PM
Active
High
No Traffic Detected on Sensor Interface
cybersecurityiothub
03/18/22, 06:00 PM
Active
High
Suspected brute-force attack attempt
rsnjavajl
Secret
03/17/22, 09:00 PM
Pre-attack
Active
High
Suspected brute-force attack attempt
rsnjavajl
Secret
03/15/22, 09:00 PM
Pre-attack
Active
High
Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)
aws-eks-cluster-eks-protected-demo-us-east-2
03/15/22, 07:19 AM
Active
High
Mimikatz credential theft tool
EC2AMAZ-H6672QF
03/15/22, 04:30 AM
Credential Access
Active
High
Mimikatz credential theft tool
EC2AMAZ-H6672QF
03/15/22, 04:30 AM
Credential Access
Active
High
Mimikatz credential theft tool
EC2AMAZ-H6672QF
03/15/22, 04:29 AM
Credential Access
Active
High
Mimikatz credential theft tool
EC2AMAZ-H6672QF
03/15/22, 04:29 AM
Credential Access
Active
High
Mimikatz credential theft tool
EC2AMAZ-H6672QF
03/15/22, 04:28 AM
Credential Access
Active
High
Mimikatz credential theft tool
EC2AMAZ-H6672QF
03/15/22, 04:28 AM
Credential Access
Active
High
Mimikatz credential theft tool
EC2AMAZ-H6672QF
03/15/22, 04:28 AM
Credential Access
Active
Previous
Page 1 of 213
Next

Microsoft Sentinel

- SIEM og SOAR skýjalausn
- Safna, greina, rannsaka og bregðast við öryggisgögnum fljótt
- Samþætting við Defender for Cloud og Microsoft 365 Defender og margar aðrar lausnir



SIEM –Security Information and Event Management
SOAR – Security Orchestration, Automation, and Response

Vertu á undan árásaraðilunum

Microsoft Sentinel

Sýnileiki yfir allt fyrirtækið þitt

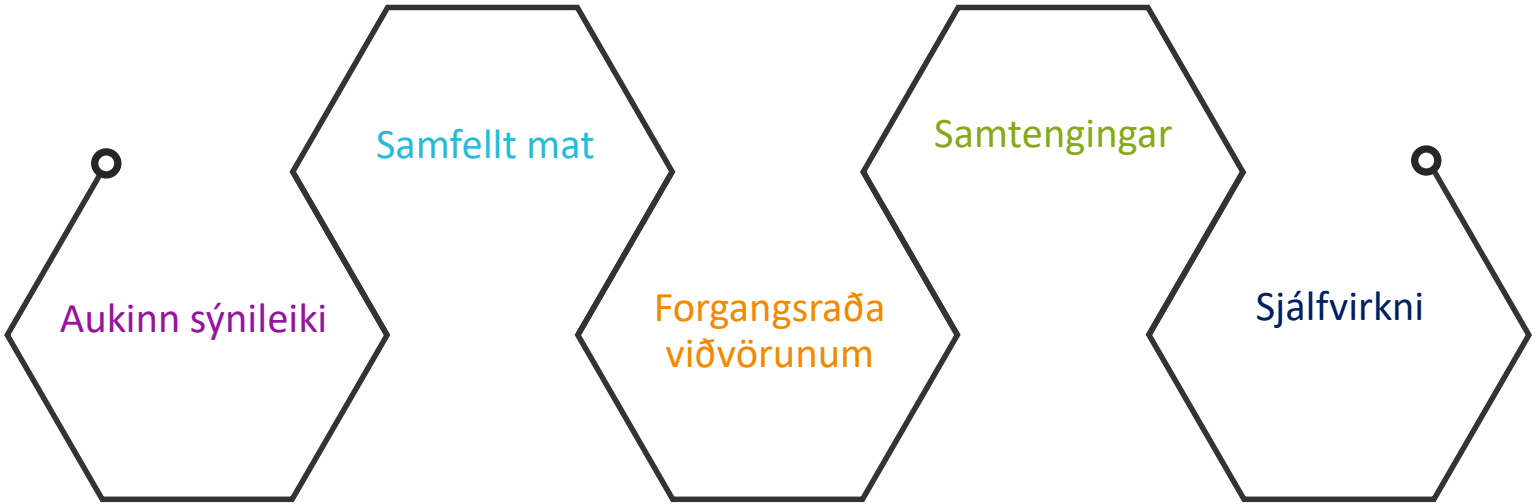
Microsoft 365 Defender

Tryggðu öryggi notenda þinna

Microsoft Defender for

Tryggðu innviði þína

Virði Defender for Cloud og Microsoft Sentinel



Niðurstaða og tillögur

- Defender for Cloud: Sameinað öryggi í rauntíma fyrir innviði þín
- Microsoft Sentinel: Öflug SIEM / SOAR samþætting til að vakta öryggi

- Tillögur
  - ARC virkja on-prem netþjóna þína
  - Nota Defender svítuna á öllum innviðum þínum
  - Fara yfir Secure Score og meðfylgjandi tillögur
  - Nota Azure Sentinel til að bera kennsl á og bregðast við öryggisatvikum