

Securing Cloud Infrastructure

Microsoft 365, Azure & AWS

Jan. 31, 2024



Agenda & Overview

- 01 Learning objectives
- 02 Compliance manager
- 03 Secure Score
- 04 Defender overview
- 05 Defender for cloud
- 06 AWS Security Hub overview
- 07 Deploy AWS Security Hub
- 08 Enable security standards
- 09 Operationalize findings

Presenters for today



Thomas Turner, Director

Thomas.Turner@rsmus.com

<https://www.linkedin.com/in/thturner/>

Advise, Build & Manage Azure & Microsoft 365 Solutions

- Commercial
- Government Community Cloud (GCC)
- Government Community Cloud Hight (GCC-H)



Ahmed ElShekh, Manager

Ahmed.Elshekh@rsmus.com

<https://www.linkedin.com/in/a-elshekh/>

Architect, Audit & Secure

- Azure & Microsoft 365
- AWS
- GCP & Google Workspace

RSM's Partnership with Microsoft



Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Information Protection and Governance
Threat Protection

Microsoft Solutions Partner
Modern Work

Specialist
Adoption and Change Management
Calling for Microsoft Teams
Teamwork Deployment
Modernize Endpoints

Microsoft Solutions Partner
Business Applications

Specialist
Small and Midsize Business Management
Supply Chain
Finance

Microsoft Solutions Partner
Data & AI
Azure

Specialist
Analytics
Infra and Database Migration
Migrate Enterprise Applications to Microsoft Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Specialist
Migrate Enterprise Applications to Microsoft Azure

Microsoft Solutions Partner
Infrastructure
Azure

Specialist
Infra and Database Migration
Azure Virtual Desktop

Recent Microsoft FY23 Awards



- ✓ Partner Of the Year Winner Defense and Intelligence
- ✓ Partner Of the Year Winner D365 Finance
- ✓ Partner Of the Year Finalists D365 Business Central
- ✓ Partner Of the Year US Finalists Government
- ✓ Partner Of the Year US Finalists Community Response
- ✓ Partner Of the Year WW Finalists Government
- ✓ Partner Of the Year WW Finalists Healthcare & Life Sciences
- ✓ Partner Of the Year WW Finalists Business Intelligence



Why is cloud security important?

- Cloud security incidents led to an average financial loss of \$3.4 million in 2020
- 88% of organizations using cloud services experienced a security incident in 2020
- Cloud security incidents can lead to huge financial losses
- Cloud security enhances your organization's ability to detect and respond to threats
- Frequent cloud security monitoring helps comply with regulations
- Cloud security monitoring helps identify weaknesses in security posture
- Your cloud security posture can be measured and improved over time

Learning Objectives

The goal is to provide an overview of dashboards leadership can use to measure the current and projected security & compliance posture of cloud-based information assets



Microsoft Security Capability Mapping

Access Control

Establish **Zero Trust** access model to modern and legacy assets using identity & network controls

Microsoft Entra

Identity Admin, Identity Architect, Identity Security

- **Entra ID (Formerly Azure AD)**
 - Multifactor Authentication
 - Conditional Access
 - Application Proxy
 - External Identities / B2B & B2C
 - Security Service Edge (SSE)
 - and more..
 - **Entra Permission Management**
 - **Windows Hello for Business**
 - **Microsoft 365 Defender**
 - Microsoft Defender for Identity
 - Microsoft Defender for Cloud Apps
 - **Microsoft 365 Lighthouse** *[multi-tenant]*
 - **Azure Lighthouse**
 - **Azure Bastion**
 - *Azure Administrative Model*
 - Portal, Management Groups, Subscriptions
 - Azure RBAC & ABAC
- Network Security*
- **Azure Firewall**
 - **Azure Firewall Manager**
 - **Azure DDoS**
 - **Azure Web Application Firewall**
 - *Azure Networking Design*
 - Virtual Network, NSG, ASG, VPN, etc.
 - PrivateLink / Private EndPoint

Endpoint / Device Admin

- **Microsoft Intune**
 - Configuration Management
- **Microsoft Defender for Endpoint**

Security Operations

Detect, Respond, and Recover from attacks; Hunt for hidden threats; share threat intelligence broadly

Incident preparation

Security Operations Analyst

- **Microsoft Defender XDR**
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Office 365
 - Microsoft Defender for Identity
 - Microsoft Defender for Cloud Apps
 - Microsoft Entra Identity Protection
- *Microsoft Defender for Cloud*
 - Microsoft Defender for DevOps
 - Microsoft Defender for Servers
 - Microsoft Defender for Storage
 - Microsoft Defender for SQL
 - Microsoft Defender for Containers
 - Microsoft Defender for App Service
 - Microsoft Defender for APIs *(preview)*
 - Microsoft Defender for Key Vault
 - Microsoft Defender for DNS
 - Microsoft Defender for open-source relational databases
 - Microsoft Defender for Azure Cosmos DB
- **Microsoft Security Copilot** *(preview)*
- **Microsoft Sentinel**
- **Microsoft Security Experts**
- *Microsoft Incident Response Detection and Response Team (DART)*

Microsoft Defender

Threat intelligence Analyst

- **Microsoft Defender Threat Intelligence (Defender TI)**
- **Microsoft Sentinel**

Security Governance

Protect sensitive data and systems. Continuously discover, classify & secure assets

Security architecture

- *Microsoft Cybersecurity Reference Architecture*
<https://aka.ms/MCRA>

Posture management, Policy and standards, Compliance management

- **Microsoft Defender for Cloud**
 - *Secure Score*
 - *Compliance Dashboard*
 - *Azure Security Benchmark*
- **Azure Blueprints**
- **Azure Policy**
- **Microsoft Defender External Attack Surface Management (MD-EASM)**
 - *Azure Administrative Model*
 - Portal, Management Groups, Subscriptions
 - Azure RBAC & ABAC
- **Microsoft Purview**
 - *Compliance manager*

Microsoft Purview

Data security

- **Microsoft Purview**
 - Information Protection
 - Data Loss Prevention
- **Microsoft 365 Defender**
 - Microsoft Defender for Cloud Apps

People security

- **Attack Simulator**
- **Insider Risk Management**

Privacy Manager

- **Microsoft Priva**



Continuously **Identify**, measure, and manage security posture to reduce risk & maintain compliance

Infrastructure and endpoint security, IT Ops, DevOps

- **Microsoft Defender for Cloud** *(including Azure Arc)*
- **Entra Permission Management**
- **Azure Blueprints**
- **Azure Policy**
- **Azure Firewall**
- **Azure Monitor**
- **Azure Web Application Firewall**
- **Azure DDoS**
- **Azure Backup and Site Recovery**
- *Azure Networking Design*
 - Virtual Network, NSG, ASG, VPN, etc.
 - PrivateLink / Private EndPoint
- **Azure Resource Locks**

OT and IoT Security

- **Microsoft Defender for IoT (& OT)**
- **Azure Sphere**



Innovation Security

Integrate Security into DevSecOps processes. Align security, development, and operations practices.

Application security and DevSecOps

- *(Same as Infrastructure Roles)*
- **GitHub Advanced Security**
- **Azure DevOps Security**



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles



Security Operations / SOC

Microsoft Security Experts
Defender Experts | Detection and Response Team (DART)

Managed Security Operations
Using Microsoft Security

Microsoft Defender XDR
Unified Threat Detection and Response across IT, OT, and IoT Assets
Incident Response | Automation | Threat Hunting | Threat Intelligence

Microsoft Security Copilot (Preview)

Microsoft Sentinel
Cloud Native SIEM, SOAR, and UEBA

Cloud Azure, AWS, GCP, On Prem & more	Endpoint Workstations, Server/VM, Containers, etc.	Office 365 Email, Teams, and more	Identity Cloud & On-Premises	SaaS Cloud Apps	Data SQL, DLP, & more	OT/IoT devices	Other Tools, Logs, & Data
---	--	---	--	---------------------------	---------------------------------	--------------------------	-------------------------------------

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)

Microsoft Entra Internet Access

Identity & Access

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

Endpoints & Devices

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)

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

Secure Score
Compliance Dashboard

Azure Firewall & Firewall Manager

Azure WAF

DDoS Protection

Azure Key Vault

Azure Bastion

Azure Lighthouse

Azure Backup

Security & Other Services

Extranet

Intranet

Azure Arc

Azure Stack

Azure Marketplace

Express Route

Private Link

Microsoft Entra Private Access & App Proxy
Beyond User VPN

NGFW, Edge DLP, IPS/IDS/NDR

aws, Cisco

PHP, .NET

Information Protection

Microsoft Purview
Information protection and governance across data lifecycle

Monitor | Discover | Classify | Protect

File Scanner
(on-premises and cloud)

Data Governance

Advanced eDiscovery

Compliance Manager

Microsoft Entra

Passwordless & MFA

- Hello for Business
- Authenticator App
- FIDO2 Keys

Entra ID Protection
Leaked cred protection
Behavioral Analytics

ID Governance

Microsoft Entra PIM

External Identities

Defender for Identity

Active Directory

Securing Privileged Access – aka.ms/SPA

Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep

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

Security Posture Management – Monitor and mitigate technical security risks using [Secure Score](#), [Compliance Score](#), [CSPM: Defender for Cloud](#), [Microsoft Defender External Attack Surface Management \(EASM\)](#) and [Vulnerability Management](#)

Windows 11 & 10 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 (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 (preview)

People Security

Attack Simulator

Insider Risk Management

Communication Compliance

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

Threat Intelligence – 65+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

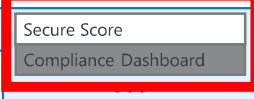
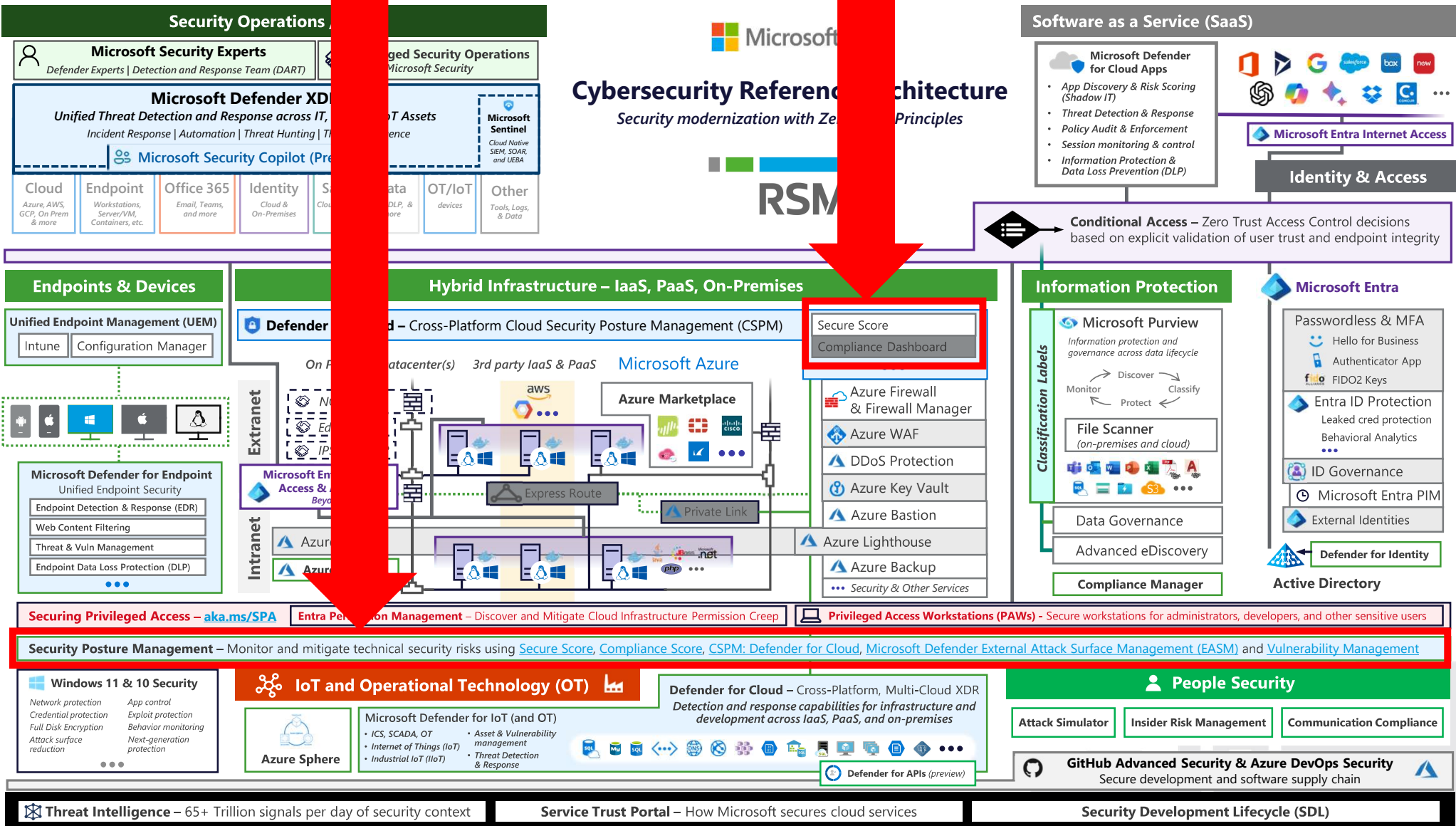
Security Development Lifecycle (SDL)

Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles



RSM



Securing Privileged Access – aka.ms/SPA | **Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep** | **Privileged Access Workstations (PAWs) – Secure workstations for administrators, developers, and other sensitive users**

Security Posture Management – Monitor and mitigate technical security risks using Secure Score, Compliance Score, CSPM: Defender for Cloud, Microsoft Defender External Attack Surface Management (EASM) and Vulnerability Management

Microsoft Compliance Manager

Intuitive management

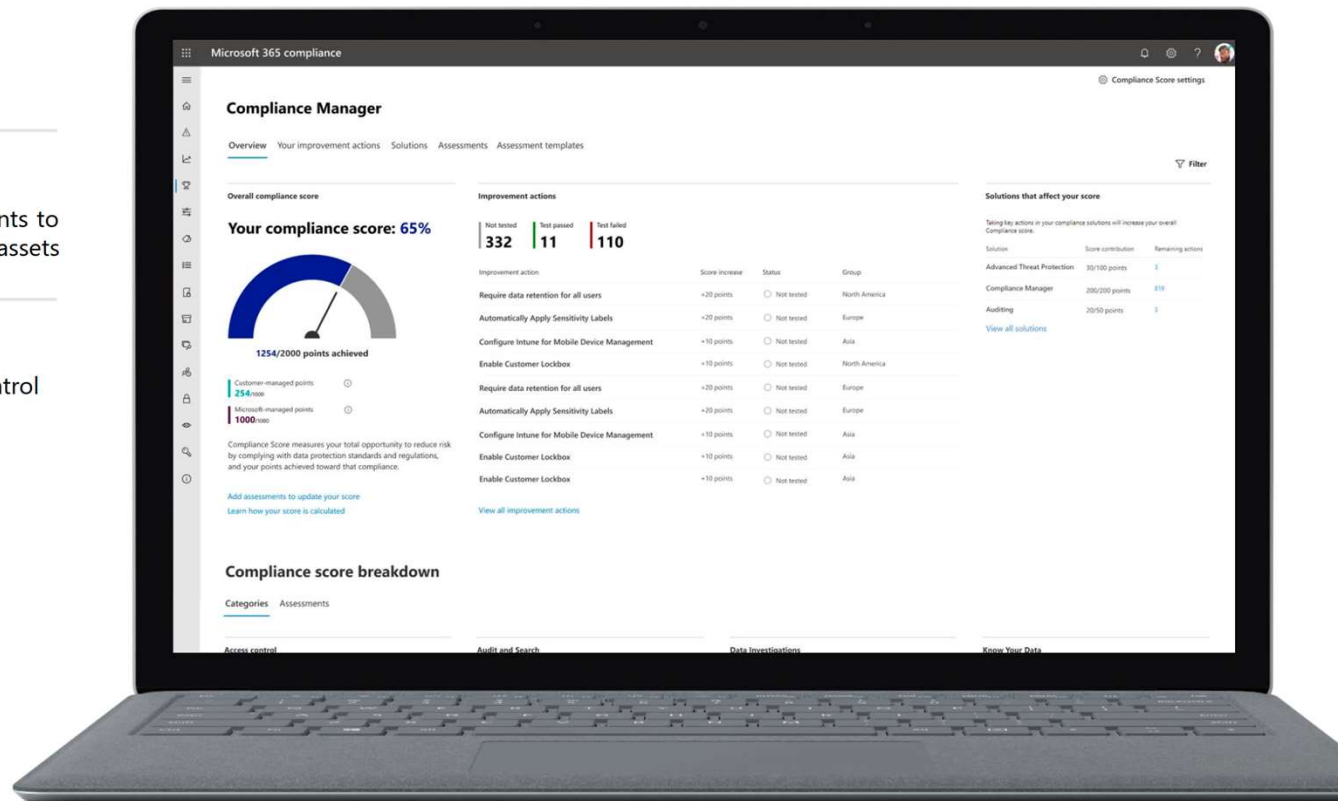
Intuitive end-to-end compliance management from easy onboarding to control implementation

Scalable assessments

Leverage out of the box assessments and custom assessments to meet your unique compliance requirements across all your assets

Built-in automation

Intelligent automation to reduce risk: compliance score, control mapping and continuous assessments



Supported Frameworks

Over 150+ out of the box assessment templates



Dashboard

Microsoft 365 compliance
? TT

Compliance Manager


Overview Improvement actions Solutions **Assessments** Assessment templates

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

[Compliance Manager settings](#)

Overall compliance score

Your compliance score: 69%



15629/22399 points achieved

Your points achieved ⓘ
432/₇₂₀₂

Microsoft managed points achieved ⓘ
15197/₇₅₁₉₇

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

Key improvement actions

	Not completed	Completed	Out of scope
	550	22	0

Improvement action	Impact	Test status	Group	Action type
Implement account lockout	+27 points	⊛ None	Default Group	Technical
Protect authenticators commensurate with use	+27 points	⊛ None	Default Group	Operational
Refresh authenticators	+27 points	⊛ None	Default Group	Operational
Protect wireless access	+27 points	⊛ None	Default Group	Operational
Protect passwords with encryption	+27 points	⊛ None	Default Group	Operational
Manage authenticator lifetime and reuse	+27 points	⊛ None	Default Group	Operational
Retain training records	+27 points	⊛ None	Default Group	Technical
Restrict access to private keys	+27 points	⊛ None	Default Group	Operational
Enforce rules of behavior and access agreements	+27 points	⊛ None	Default Group	Documentation

[View all improvement actions](#)

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
Audit	0/82 points	12
Azure	0/3 points	1
Azure Active Directory	0/514 points	32

[View all solutions](#)

Compliance score breakdown

Assessments

Microsoft 365 compliance
? TT

Compliance Manager

Compliance Manager settings

Overview Improvement actions Solutions Assessments Assessment templates

Use a template to help you create assessments for your organization. Templates contain the controls and action data needed to track compliance with regulations, standards, and policies. [Learn about working with templates](#)

Premium templates in use will be subject to new licensing terms in the near future. [Learn more](#)

Filter Filters

Certification: **Any** Product scope: **Any** Created by: **Any**

+ Create new template → Export all actions 180 items Search Group

Assessment template	Availability	Product scope	Certification	Created by	Last updated	Created
Included templates (4)						
EU GDPR	Included	Microsoft 365	EU GDPR	Microsoft	9/18/2020	9/18/2020
ISO/IEC 27001:2013	Included	Microsoft 365	ISO 27001	Microsoft	9/18/2020	9/18/2020
NIST 800-53	Included	Microsoft 365	NIST 800-53	Microsoft	9/18/2020	9/18/2020
Data Protection Baseline	Included	Microsoft 365	Data protection baseline	Microsoft	9/21/2020	9/21/2020
Premium templates (176)						
Massachusetts - 201 CMR 17.00: Sta...	Premium	Microsoft 365	201 CMR 17	Microsoft	9/18/2020	9/18/2020
Singapore - Outsourced Service Pr...	Premium	Microsoft 365	ABS-OSPAR	Microsoft	9/18/2020	9/18/2020
AICPA/CICA Generally Accepted Pri...	Premium	Microsoft 365	AICPA/CICA GAPP	Microsoft	9/18/2020	9/18/2020
Asia Pacific Economic Cooperation ...	Premium	Microsoft 365	APEC Privacy Framework	Microsoft	9/18/2020	9/18/2020
Australian Prudential Regulation A...	Premium	Microsoft 365	APRA CPS	Microsoft	9/18/2020	9/18/2020
Alabama - Policy 621: Data Breach ...	Premium	Microsoft 365	Alabama Data Breach Notificat...	Microsoft	9/18/2020	9/18/2020
Alaska - Chapter 48 - Personal Infor...	Premium	Microsoft 365	Alaska Personal Information Pr...	Microsoft	9/18/2020	9/18/2020

Disclaimer: Recommendations from Compliance Manager should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the [Online Services Terms](#). See also [Microsoft 365 licensing guidance](#)

Your Improvement Actions

Microsoft 365 compliance
? TT

Compliance Manager > Assessment templates > NYDFS

NYDFS

Created	Last updated	Created by	Certification	Product scope	Service scope	Achievable points
9/18/2020	9/18/2020	Microsoft	NYDFS	Microsoft 365	52 services	3117

About
 23 NYCRR Part 500 is a regulation issued by the New York Department of Financial Services (NYDFS) establishing cybersecurity requirements for financial services companies. [More info on the NYDFS Cybersecurity Regulation](#)
[More info on covered entities and exemptions](#)

[Create assessment](#) [Export to Excel](#)

Controls Your improvement actions Microsoft actions

Filter Filters

Control family: **Any** Action type: **Any** Solutions: **Any**

141 items Search Group

Improvement actions	Achievable points	Last updated	Solutions	Action type
Activate Azure Rights Management	27	9/21/2020	Azure Information Protection	Technical
Address coding vulnerabilities	9	9/21/2020	Compliance Manager	Operational
Adhere to retention periods defined	9	9/21/2020	Compliance Manager	Operational
Adopt biometric authentication mechanisms	9	9/18/2020	Compliance Manager	Operational
Alert personnel of information spillage	1	9/21/2020	Compliance Manager	Operational
Apply Sensitivity Labels to Protect Sensitive or Critical Da...	27	9/21/2020	Information protection	Technical
Assess risk in third party relationships	9	9/21/2020	Compliance Manager	Operational
Audit privileged functions	1	9/21/2020	Audit	Operational
Audit user account status	1	9/21/2020	Audit	Operational

Services In-scope

Microsoft 365 compliance
⚙️ ? 🏠

Compliance Manager > Assessment templates > NYDFS

NYDFS

Created	Last updated	Created by	Certification	Product scope	Service scope	Achievable points
9/18/2020	9/18/2020	Microsoft	NYDFS	Microsoft 365	52 services	3117

About
 23 NYCRR Part 500 is a regulation issued by the New York Department of Financial Services (NYDFS) establishing cybersecurity requirements for financial services companies. [More info on the NYDFS Cybersecurity Regulation](#)
[More info on covered entities and exemptions](#)

[Create assessment](#) [Export to Excel](#)

Controls | Your improvement actions | Microsoft actions

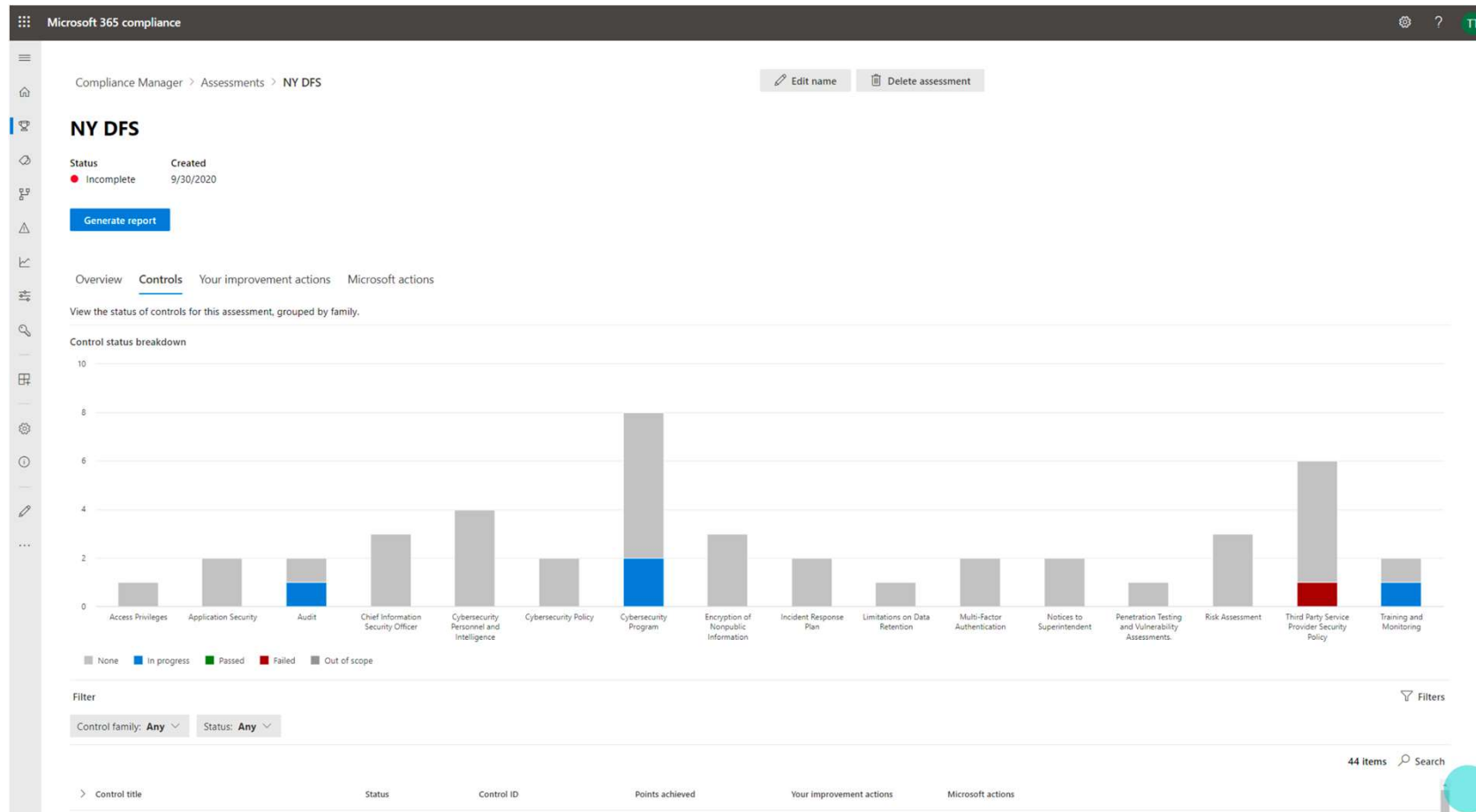
Filter
 Control family: **Any**

Control title	Control ID	Achievable points	Improvement actions	Microsoft actions
> Access Privileges (1)				
> Application Security (2)				
> Audit (2)				
> Chief Information Security Officer (3)				
> Cybersecurity Personnel and Intelligence (4)				
> Cybersecurity Policy (2)				
> Cybersecurity Program (8)				
> Encryption of Nonpublic Information (3)				

In-scope services

- Azure Active Directory
- Azure Information Protection
- Exchange Online
- Exchange Online Protection
- Flow
- Kaizala
- Microsoft Analytics
- Microsoft Booking
- Microsoft Dynamics 365
- Microsoft Graph
- Microsoft Intune
- Microsoft Planner
- Microsoft PowerApps
- Microsoft StaffHub
- Microsoft Stream
- Microsoft Teams
- Microsoft To-Do for Web
- MyAnalytics
- Microsoft 365 Cloud App Security
- Office 365 Groups
- Office 365 Video
- OneDrive for Business
- Power Apps
- Power BI
- SharePoint Online
- Skype for Business
- Sway
- Yammer
- Security Workload Environment
- Office Service Infrastructure
- Suite User Experience
- Outlook Mobile
- Domain Name Services
- Aria (Bing)
- Object Store (Bing)
- Forms
- Planner
- Siphon (Bing)
- Delve
- QAS (incl TEE) (Bing)
- Speller (Bing)
- My Analytics
- ORAS
- IP
- WAC
- People Card
- Falcon/MSB
- OXO/Intelligent Services
- Search Content Service

Controls Breakdown



Control Overview

Microsoft 365 compliance
⚙️ ? IT

Compliance Manager > Assessments > NY DFS > Limit Access Privilege > Use role-based privileged account management for M365 accounts

Use role-based privileged account management for M365 accounts

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
0/27	● Not Implemented	Not Implemented	● Not assessed	None	None	Default Group

Edit status

At a glance

This action is part of following standards and regulatory requirements

- Data Protection Baseline ▼
- Data Protection Baseline ▼
- Data Protection Baseline ▼
- Data Protection Baseline ▼
- Data Protection Baseline ▼
- Data Protection Baseline ▼
- NYDFS ▼
- RBI Cyber Security Framework ▼
- SWIFT ▼
- SWIFT ▼
- SWIFT ▼

Implementation

How to implement

Microsoft recommends that your organization manage Microsoft 365 privileged user accounts using role-based access controls that organize Microsoft 365 admin privileges into separate roles. Microsoft 365 comes with a set of admin roles that you can assign to users in your organization. Each **admin role** maps to common business functions and gives people in your organization permissions to do specific tasks in the Microsoft 365 admin center. Your organization should consider creating and maintaining Access Control policies and standard operating procedures that include details on role assignments, including the requirements for each role and the process to assign and monitor the use of each role. Select **Launch Now** to access the Microsoft 365 admin center where you can manage admin roles and provide users permissions to view data and complete tasks in Microsoft 365 admin centers.

Launch now

Learn more Administrator role permissions in Azure Active Directory Assign admin roles in Office 365 for business About Office 365 Admin Roles Understanding Role Based Access Control

Notes and documentation

Uploaded documents

[Manage documents](#)

Implementation notes

[Edit implementation notes](#)

Test notes

[Edit test notes](#)

Additional notes

[Edit additional notes](#)

Control Updated

Microsoft 365 compliance

Compliance Manager > Assessments > NY DFS > Limit Access Privilege > Use role-based privileged account management for M365 accounts

Changes saved successfully.

Use role-based privileged account management for M365 accounts

Points achieved 27/27	Implementation status ✔ Implemented	Implementation date 9/30/2020	Test status ✔ Passed	Test date 9/30/2020	Assigned to TT Test Tenant	Group Default Group
---------------------------------	--	----------------------------------	-------------------------	------------------------	--------------------------------------	------------------------

Edit status

At a glance

This action is part of following standards and regulatory requirements

Data Protection Baseline	▼
Data Protection Baseline	▼
Data Protection Baseline	▼
Data Protection Baseline	▼
Data Protection Baseline	▼
Data Protection Baseline	▼

Implementation

How to implement

Microsoft recommends that your organization manage Microsoft 365 privileged user accounts using role-based access controls that organize Microsoft 365 admin privileges into separate roles. Microsoft 365 comes with a set of admin roles that you can assign to users in your organization. Each **admin role** maps to common business functions and gives people in your organization permissions to do specific tasks in the Microsoft 365 admin center. Your organization should consider creating and maintaining Access Control policies and standard operating procedures that include details on role assignments, including the requirements for each role and the process to assign and monitor the use of each role. Select **Launch Now** to access the Microsoft 365 admin center where you can manage admin roles and provide users permissions to view data and complete tasks in Microsoft 365 admin centers.

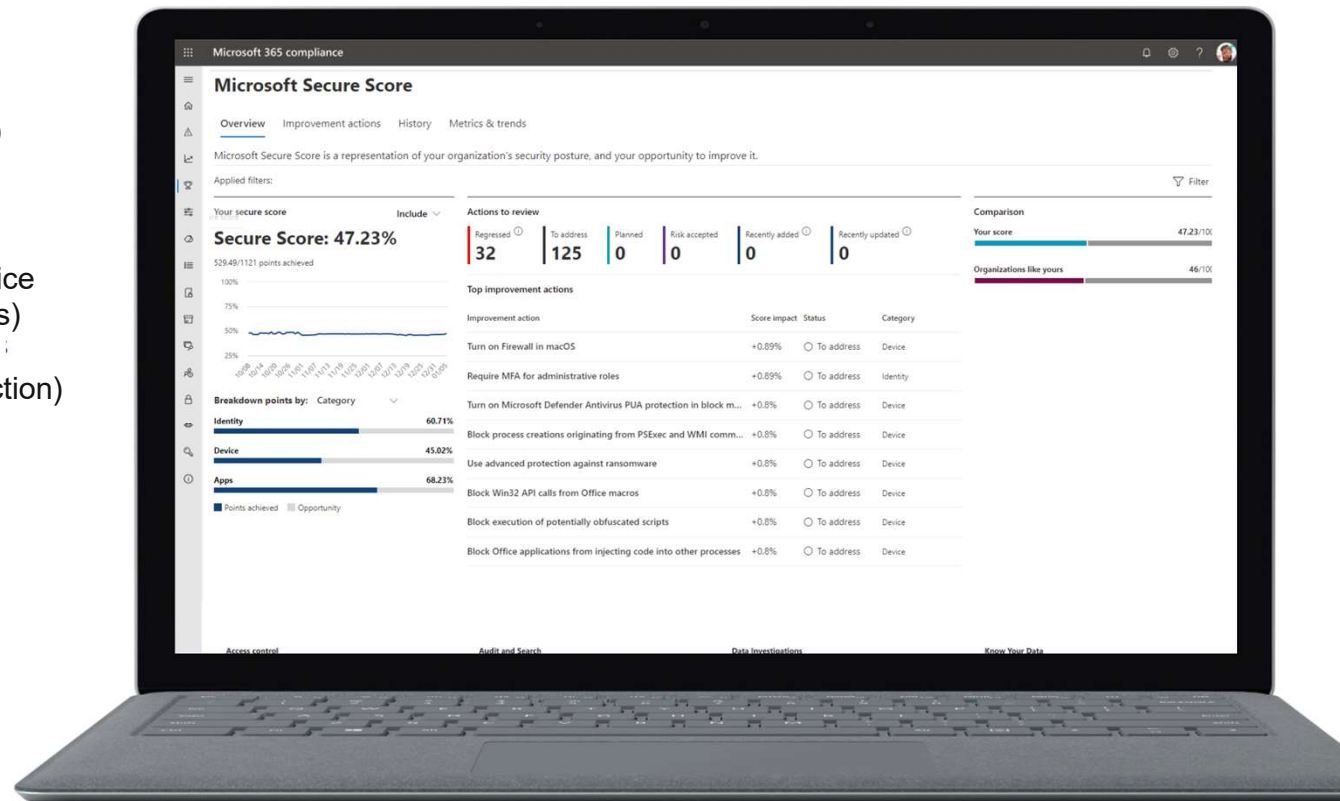
[Launch now](#)

Learn more [Administrator role permissions in Azure Active Directory](#) [Assign admin roles in Office 365 for business](#) [About Office 365 Admin Roles](#) [Understanding Role Based Access Control](#)

Microsoft Secure Score

Microsoft Best Practices

- **Identity** (Microsoft Entra accounts & roles)
- **Device** (Microsoft Defender for Endpoint)
- **Apps** (email and cloud apps, including Office 365 and Microsoft Defender for Cloud Apps)
- **Data** (through Microsoft Information Protection)



Dashboard Overview

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Filter

Your secure score

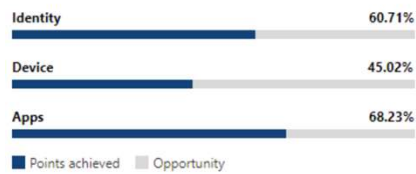
Include

Secure Score: 47.23%

529.49/1121 points achieved



Breakdown points by: Category



Actions to review



Top improvement actions

Improvement action	Score impact	Status	Category
Turn on Firewall in macOS	+0.89%	To address	Device
Require MFA for administrative roles	+0.89%	To address	Identity
Turn on Microsoft Defender Antivirus PUA protection in block m...	+0.8%	To address	Device
Block process creations originating from PSEXEC and WMI comm...	+0.8%	To address	Device
Use advanced protection against ransomware	+0.8%	To address	Device
Block Win32 API calls from Office macros	+0.8%	To address	Device
Block execution of potentially obfuscated scripts	+0.8%	To address	Device
Block Office applications from injecting code into other processes	+0.8%	To address	Device

[View all](#)

Comparison



History

Resources

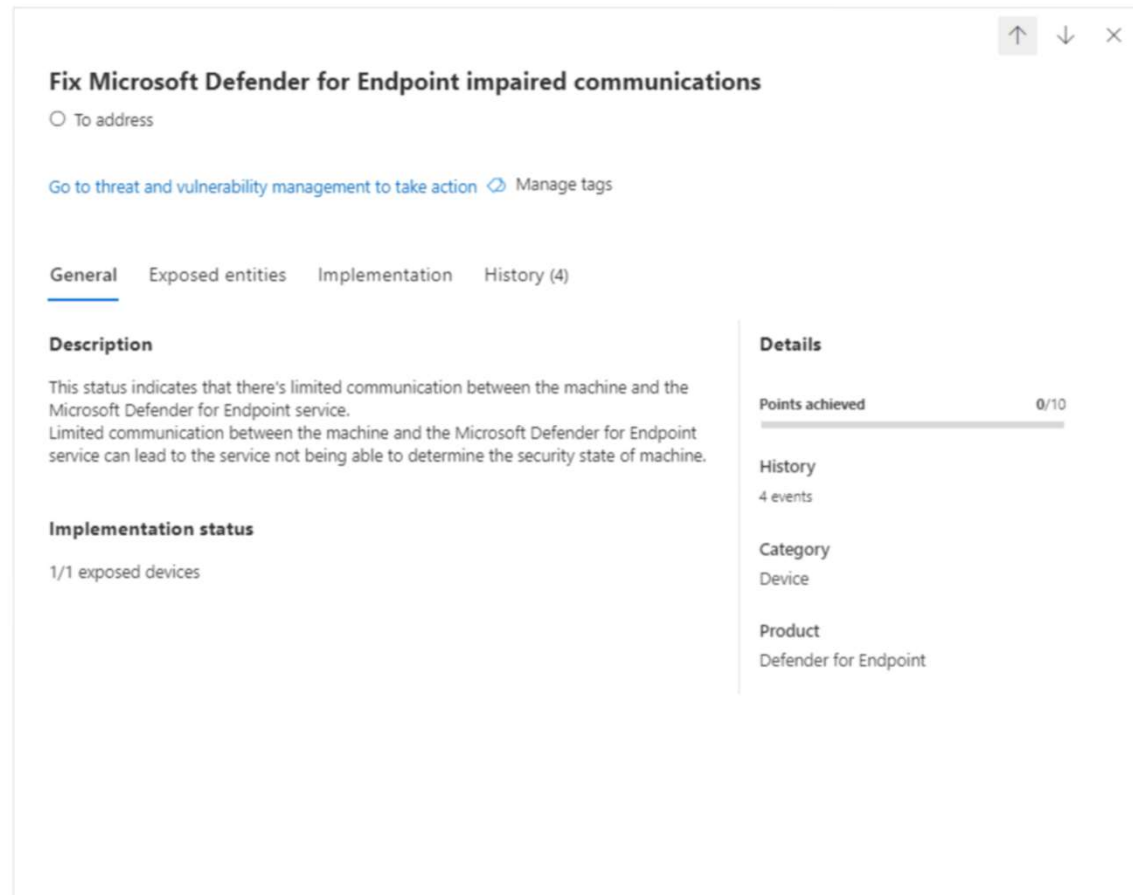
Messages from Microsoft

Improvement Actions

Ranking

Ranking is based on the number of points left to achieve, implementation difficulty, user impact and complexity.

The highest ranked recommended actions have a large number of points remaining with low difficulty, user impact and complexity.



The screenshot shows a window titled "Fix Microsoft Defender for Endpoint impaired communications". It includes a "To address" field, a link to "Go to threat and vulnerability management to take action", and a "Manage tags" link. The interface has tabs for "General", "Exposed entities", "Implementation", and "History (4)". The "General" tab is active, showing a "Description" section with text about limited communication between the machine and the Microsoft Defender for Endpoint service. Below the description is the "Implementation status" section, which shows "1/1 exposed devices". On the right side, there is a "Details" panel with a "Points achieved" progress bar at 0/10, a "History" section with "4 events", a "Category" section with "Device", and a "Product" section with "Defender for Endpoint".

Tracking History

Date/Time	Activity	Resulting points	Category	Attributed to
Jun 25, 2020 5:00 PM	9 points regressed for Use advanced protection against ransomware	0/9	Device	System
Jun 25, 2020 5:00 PM	8 points regressed for Set User Account Control (UAC) to automatically deny elevation requests	0/8	Device	System
Jun 18, 2020 8:50 AM	██████████ marked Require MFA for administrative roles as planned	2/10	Identity	██████████
Jun 17, 2020 2:11 PM	██████████ marked Require MFA for administrative roles as third party	10/10	Identity	██████████

History > Use advanced protection against ransomware

Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyber attacks and malicious software. This [ASR rule](#) scans executable files entering the system to determine whether they're trustworthy.

This security control is only applicable for machines with Windows 10, version 1803 or later. This provides an extra layer of protection against files that closely resemble ransomware, by blocking them from running, unless they're in a trusted list or exclusion list.

Points achieved
0/9

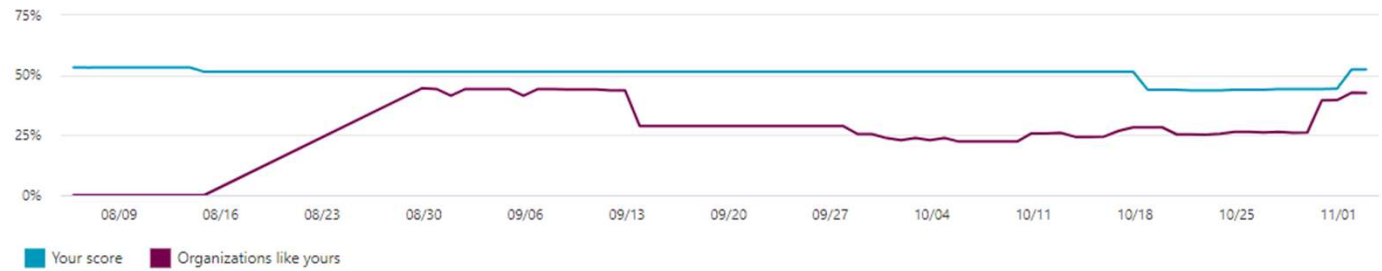
History
[10 events](#)

- [Manage](#)
- [Share](#)
- [Save and close](#)
- [Cancel](#)

Trends & Other Orgs

Comparison trend

How your organization's Secure Score compares to others' over time.



Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

Secure Score: 26.39%

20.06/76 points achieved

Breakdown points by: Category

- Identity: 16.18%
- Apps: 55%

■ Points achieved ■ Opportunity

Actions to review

0 Regressed |
 14 To address |
 0 Planned |
 0 Risk accepted |
 0 Recently added

0 Recently updated

Top improvement actions

Improvement action	Score impact	Status	Category
Require MFA for administrative roles	+13.16%	To address	Identity
Ensure all users can complete multi-factor authenti...	+11.84%	To address	Identity
Enable policy to block legacy authentication	+10.53%	To address	Identity
Turn on user risk policy	+9.21%	To address	Identity
Turn on sign-in risk policy	+9.21%	To address	Identity
Do not allow users to grant consent to unmanaged...	+5.26%	To address	Identity
Create an app discovery policy to identify new and...	+3.95%	To address	Apps

Comparison

Your score: 26.39/100

Organizations like yours: 46.57/100

History

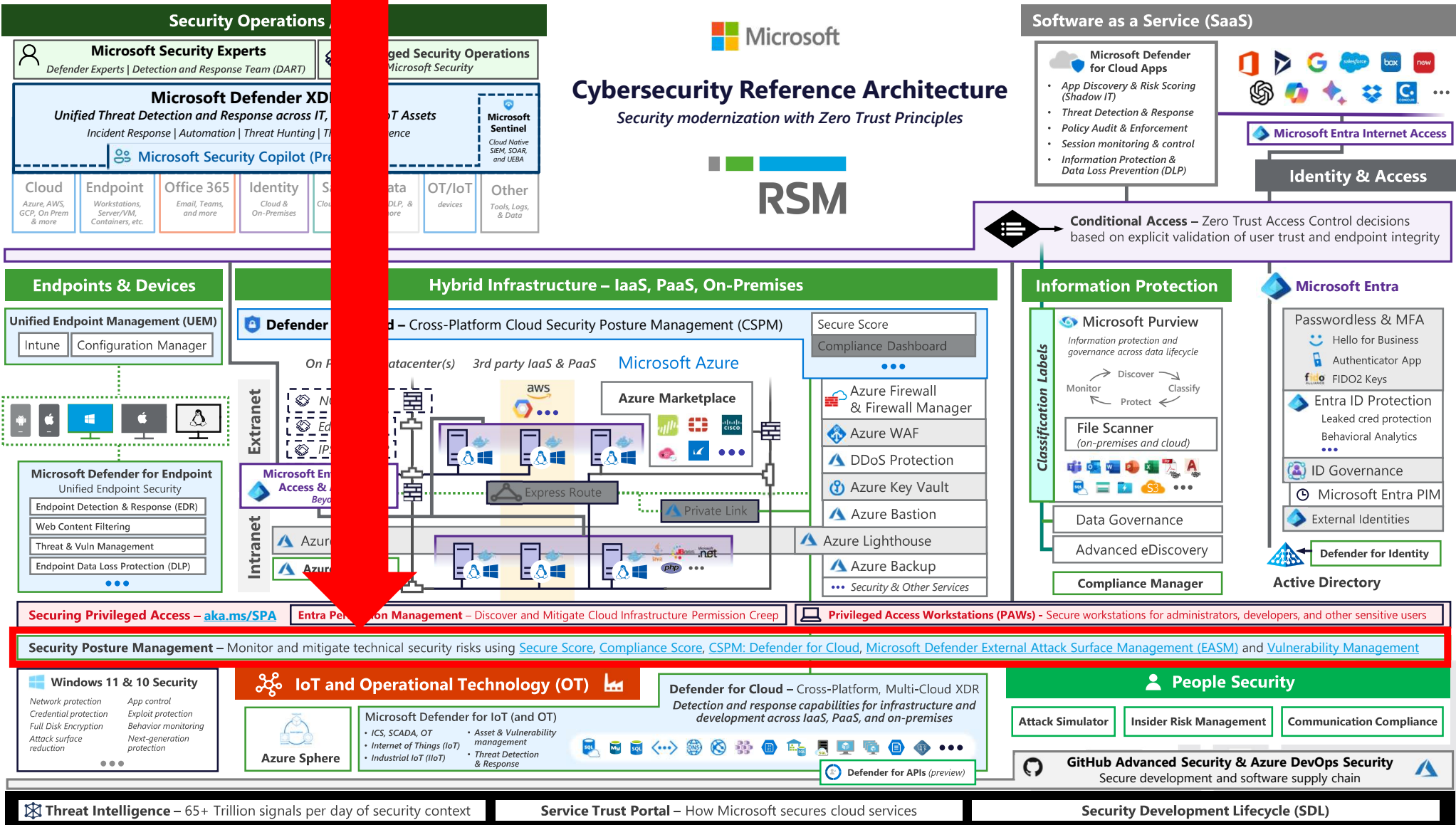
- Nov 8, 2021 4:00 PM: +1.00 points score change because Remove TLS 1.0/1.1 and 3DES ...
- Nov 8, 2021 4:00 PM: +0.00 points score change because Use limited administrative roles ...
- Nov 8, 2021 4:00 PM: -0.00 points score change because Turn on user risk policy has be...
- Nov 8, 2021 4:00 PM: +1.00 points score change because Designate more than one glob...
- Nov 8, 2021 4:00 PM: -0.00 points score change because Enable policy to block legacy a...

[View history](#)



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles



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)



Microsoft Entra Internet Access

Identity & Access

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

Endpoints & Devices

Unified Endpoint Management (UEM)

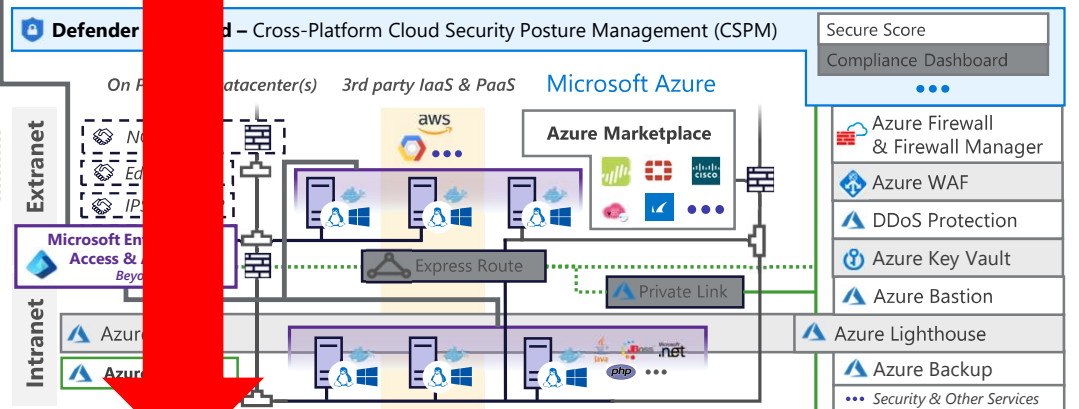
- Intune
- Configuration Manager



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



Information Protection

Microsoft Purview
Information protection and governance across data lifecycle

Classification Labels

Monitor → Discover → Classify → Protect

- File Scanner (on-premises and cloud)
- Data Governance
- Advanced eDiscovery
- Compliance Manager

Microsoft Entra

Passwordless & MFA

- Hello for Business
- Authenticator App
- FIDO2 Keys
- Entra ID Protection
- Leaked cred protection
- Behavioral Analytics
- ID Governance
- Microsoft Entra PIM
- External Identities

Defender for Identity

Active Directory

Securing Privileged Access – aka.ms/SPA | **Entra Permission Management** – Discover and Mitigate Cloud Infrastructure Permission Creep | **Privileged Access Workstations (PAWs)** – Secure workstations for administrators, developers, and other sensitive users

Security Posture Management – Monitor and mitigate technical security risks using [Secure Score](#), [Compliance Score](#), [CSPM: Defender for Cloud](#), [Microsoft Defender External Attack Surface Management \(EASM\)](#) and [Vulnerability Management](#)

Windows 11 & 10 Security

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

IoT and Operational Technology (OT)

Azure Sphere

Microsoft Defender for IoT (and OT)

- ICS, SCADA, OT
- Internet of Things (IIoT)
- 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 (preview)

People Security

- Attack Simulator
- Insider Risk Management
- Communication Compliance

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

Threat Intelligence – 65+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Microsoft Defender for Cloud

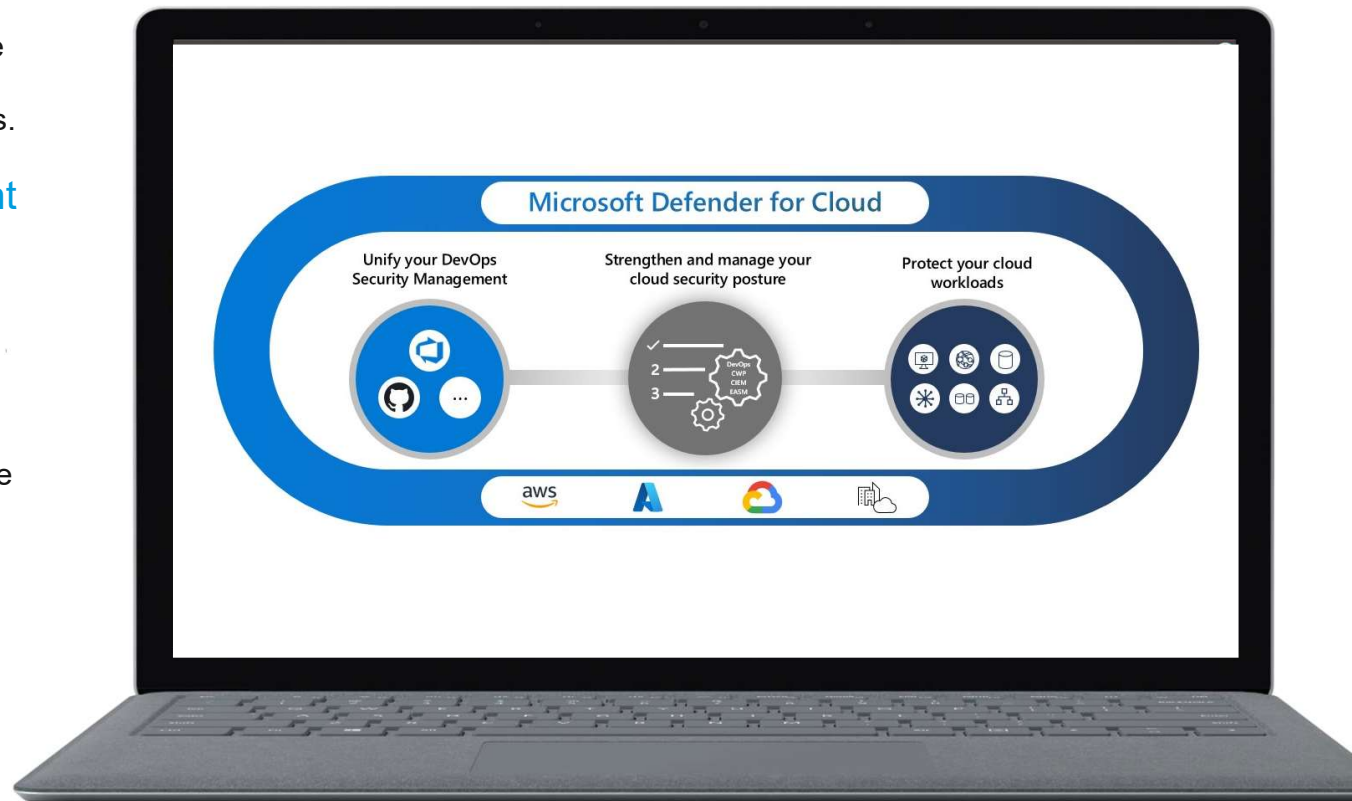
Secure Score

Summarize your security posture based on the security recommendations. As you remediate recommendations, your secure score improves.

Cloud Security Posture Management

Get advanced tools to identify weaknesses in your security posture, including:

- Governance to drive actions to improve your security posture
- Regulatory compliance to verify compliance with security standards
- Cloud security explorer to build a comprehensive view of your environment



Cross-cloud and cross-platform

Industry Partnerships

NIST / CIS / The Open Group / Others Microsoft Intelligent Security Association Solution Integration and MDR/MSSP Partners CERTs / ISACs / Others Law Enforcement ...



Microsoft Security, Compliance, and Identity Capabilities

Threat Intelligence – 65+ Trillion signals per day of security context

Access Control
Identity and Network

Modern Security Operations
Rapid Resolution with XDR, SIEM, SOAR, UEBA and more

Asset Protection
Information Protection and App Security / DevSecOps

Technical Governance
Risk Visibility, Scoring, and Policy Enforcement

People Security – User Education/Empowerment and Insider Threats

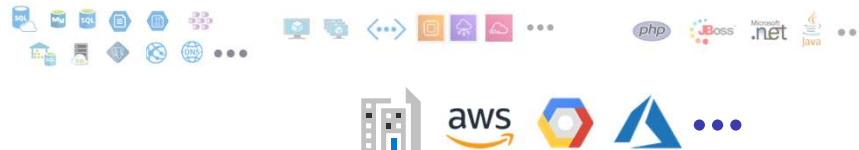
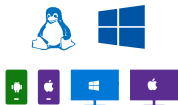


Endpoints & Devices

Software as a Service (SaaS)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

IoT Devices



Operational Technology (OT)

Security Operations [Center] (SOC) – Reduce attacker time/opportunity to impact business

Dashboard Overview

Microsoft Azure
Search resources, services, and docs (G+)

Home >

Microsoft Defender for Cloud | Overview

Showing subscription 'ContosoHotels'

Search (Ctrl+/) Subscriptions What's new

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Workflow automation

1

Azure subscriptions

2

AWS accounts

1

GCP projects

2536

Assessed resources

280

Active recommendations

1280

Security alerts

Security posture

135/161 Unassigned recommendation

13/28 Overdue recommendations

Secure score

37%

SECURE SCORE

Azure	40%
AWS	33%
GCP	34%

[Explore your security posture >](#)

Regulatory compliance

Azure Security Benchmark **16** of 43 passed controls

Lowest compliance regulatory standards by passed controls

ISO 27001:2013	0/17
CMMC Level 3	0/55
Canada Federal PBMM	1/14

[Improve your compliance >](#)

OMI vulnerabilities detected (CVE-2022-29149):

The OMI elevation of privilege vulnerability (CVE-2022-29149) can allow attackers that abuse this vulnerability to execute arbitrary code and potentially take full control of a running host or container.

Microsoft supports auto-update for the OMI vulnerability. Please refer to the following link to activate it: [Auto update](#)

[Read guidance >](#)

Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities include environment hardening, vulnerability assessment, and threat protection. The **new plan** merges two existing D plans, in addition to new and improved features.

[Click here to upgrade >](#)

2 machines and 0 container images are vulnerable to Log4j v2

All three log4j vulnerabilities (CVE-44228, CVE-2021-45046) can be remotely exploited, allowing an attacker to exploit the vulnerabilities to execute arbitrary code and potentially take full control of a running host or container.

[View machines](#) | [Read guidance](#)

Workload protections

Resource coverage

99% For full protection, enable 2 resource plans

Alerts by severity

High

49

Med...

Firewall Manager

1

Firewalls

2

Firewall policies

1

Regions with firewalls

Network protection status by resource

Virtual hubs 0/0

High Level Cloud Posture Overview

Microsoft Azure
Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud | Overview >

Security posture

Secure score over time | Governance report (preview) | Guides & Feedback

All environments

Secure score

37%
SECURE SCORE

- Azure 40%
- AWS 33%
- GCP 34%

Environment

4 Total

Subscriptions 1 | Accounts 2 | Projects 1

858/1174 Unhealthy resources

239 Recommendations

62 Attack paths

Governance (preview)

13/28

Overdue recommendations

135/161

Unassigned recommendations

See your score over time

Track the progress of your score with this workb changed recently, scores for individual subscript useful metrics.

[Learn more >](#)

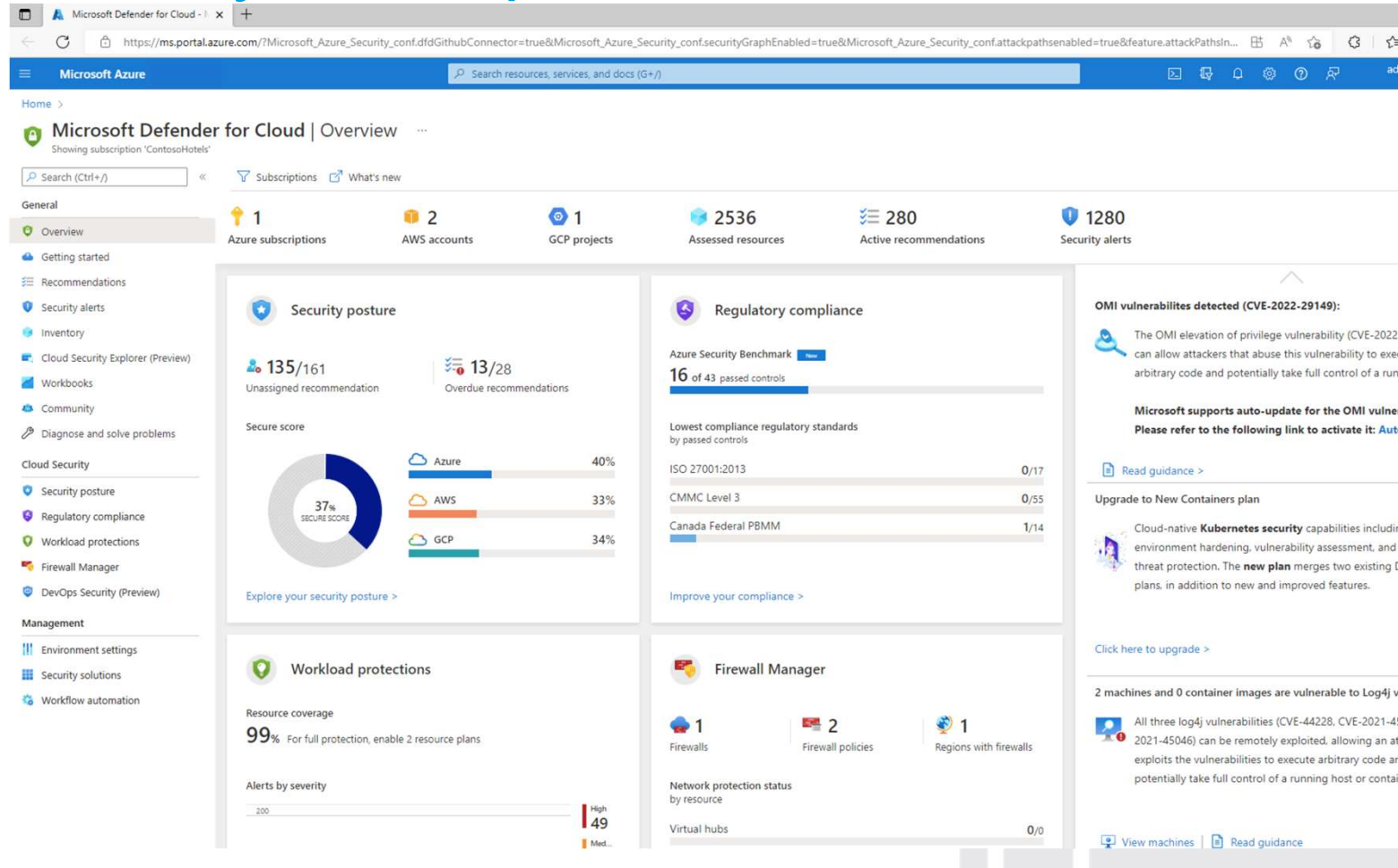
Environment | Owner (preview)

Search by name | Environment == All

Name ↑↓	Secure score ↑↓	Unhealthy resources ↑↓	Attack paths ↑↓	Recommendations
ContosoHotels Azure subscription	40%	347 of 423	62	View recommendations >
123456789012 (AWSNinjaConnector) AWS account	36%	266 of 413	0	View recommendations >
345678901234 (GCPNinjaConnector) GCP project	34%	123 of 147	0	View recommendations >
567890123456 (containerVA-demo) AWS account	20%	122 of 163	0	View recommendations >

< Previous | Page 1 of 1 | Next >

Security & Compliance Posture Overview



The screenshot displays the Microsoft Defender for Cloud Overview page for the subscription 'ContosoHotels'. The dashboard provides a comprehensive view of the organization's security and compliance posture across various cloud services.

General Summary:

- 1 Azure subscription
- 2 AWS accounts
- 1 GCP project
- 2536 Assessed resources
- 280 Active recommendations
- 1280 Security alerts

Security posture: Shows 135/161 unassigned recommendations and 13/28 overdue recommendations. The overall secure score is 37%.

Cloud Provider	Secure Score
Azure	40%
AWS	33%
GCP	34%

Regulatory compliance: The Azure Security Benchmark shows 16 of 43 passed controls. Compliance is tracked against standards such as ISO 27001:2013 (0/17), CMMC Level 3 (0/55), and Canada Federal PBMM (1/14).

Workload protections: Resource coverage is at 99%. Alerts by severity are categorized as High (49) and Medium (Med...).

Firewall Manager: Shows 1 Firewall, 2 Firewall policies, and 1 Region with firewalls. Network protection status by resource shows 0/0 for Virtual hubs.

OMI vulnerabilities detected (CVE-2022-29149): A vulnerability in OMI elevation of privilege (CVE-2022-29149) is noted, which can allow attackers to execute arbitrary code. Microsoft supports auto-update for this vulnerability, with a link to activate it.

Upgrade to New Containers plan: Information regarding the upgrade to the new plan, which includes enhanced Kubernetes security capabilities.

Log4j vulnerabilities: 2 machines and 0 container images are vulnerable to Log4j. All three log4j vulnerabilities (CVE-44228, CVE-2021-45201, CVE-2021-45046) are noted as being remotely exploitable.

Recommendations

Microsoft Azure | Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Recommendations

Showing subscription 'ContosoHotels'

Search Refresh Download CSV report Open query Governance report (preview) Guides & Feedback

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Workflow automation

Secure score recommendations All recommendations

Secure score 34% Active recommendations 158/231

Search recommendations Recommendation status == None Severity == None Resource type == None Recommendation maturity == None Add filter More (2) Show my it

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources
Enable MFA	10	0.00	+18%	Overdue	3 of 3 resources
Secure management ports	8	3.92	+6%	Overdue	27 of 177 resources
Remediate vulnerabilities	6	2.27	+5%	Overdue	74 of 207 resources
Apply system updates	6	3.31	+5%	Overdue	24 of 184 resources
Encrypt data in transit	4	1.60	+4%	On time	81 of 180 resources
Manage access and permissions	4	2.20	+4%	Overdue	77 of 792 resources
Enable encryption at rest	4	0.70	+7%	Overdue	124 of 275 resources
Remediate security configurations	4	1.74	+4%	Overdue	58 of 225 resources
Restrict unauthorized network access	4	1.54	+6%	Overdue	164 of 553 resources
Apply adaptive application control	3	1.18	+2%	Overdue	43 of 174 resources
Enable endpoint protection	2	0.82	+1%	Overdue	42 of 180 resources
Protect applications against DDoS attacks	2	0.92	+2%	Unassigned	11 of 86 resources
Enable auditing and logging	1	0.19	+2%	Unassigned	309 of 426 resources

< Previous Page 1 of 1 Next >

Quick Hit Findings

Microsoft Azure | Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Cloud Security Explorer (Preview)

Showing subscription 'ContosoHotels'

Search | Guides & Feedback | Share query link

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)**
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Workflow automation

What would you like to search?

Select resource types

Start creating a query

Use the Cloud Security Explorer query builder to easily run graph-based queries and proactively hunt for security risks in your cloud environment. [Learn more](#)

Scope: All | Search

Query templates

<p>Internet exposed VM</p> <p>Returns all internet exposed virtual machines</p> <p>Open query ></p>	<p>Internet exposed VMs with high severity vulnerabilities</p> <p>Returns all internet exposed virtual machines that have high severity vulnerabilities</p> <p>Open query ></p>	<p>VMs vulnerable to a specific vulnerability</p> <p>Returns all internet exposed virtual machines vulnerable to Log4Shell vulnerabilities</p> <p>Open query ></p>	<p>Internet exposed SQL servers with managed identity</p> <p>Returns all internet exposed SQL servers with managed identity assigned</p> <p>Open query ></p>	<p>User accounts without MFA with permissions to Storage Accounts</p> <p>Returns all user accounts that have MFA disabled, and have permissions on a storage account</p> <p>Open query ></p>
<p>Azure Kubernetes pods running images with high severity vulnerabilities</p> <p>Returns all Kubernetes pods running an image with vulnerability severity high or above</p>	<p>Key Vault keys and secrets without any expiration period</p> <p>Returns all Azure key vaults where expiration is not set for secrets or keys</p>	<p>User accounts with permission to vulnerable VMs</p> <p>Returns all user accounts with permission to VMs that have high severity vulnerabilities</p>	<p>Internet exposed SQL Servers tagged as production</p> <p>Returns all SQL Servers which tagged as production and exposed to the internet</p>	<p>External users with permissions to SQL VMs allow code execution on the host</p> <p>Returns all the users with permissions to a SQL VM that can run the host</p>

Drill Down View

Microsoft Azure | Search resources, services, and docs (G+/)

Home > Microsoft Defender for Cloud | Cloud Security Explorer (Preview) >

Resource health

9 Active recommendations | 14 Active alerts

Resource information

Subscription: ContosoHotels | Resource Group: soc-purview

Environment: Azure | Location: eastus

Status: Ready

Security value

Microsoft Defender for Azure SQL database servers: On

Data sensitivity labels: Secret

Data classifications: Person's Name (19), Credit Card Number (9), EU Debit Card Number (5)

See more (14)

Purview account: purviewninjacatalog

Recommendations Alt

Search [More \(2\)](#)

Severity ↑↓	Description	Status ↑↓
High	Microsoft Defender for SQL should be enabled for unprotected Azure SQL servers	Healthy
High	SQL servers should have vulnerability assessment configured	Unhealthy
High	SQL servers should have an Azure Active Directory administrator provisioned	Healthy
Medium	Public network access on Azure SQL Database should be disabled Preview	Unhealthy
Medium	Private endpoint connections on Azure SQL Database should be enabled Preview	Unhealthy
Low	Audit resource location matches resource group location	Unhealthy
Low	SQL Auditing settings should have Action-Groups configured to capture critical activities	Healthy
Low	SQL servers should use customer-managed keys to encrypt data at rest	Unhealthy
Low	Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports	Unhealthy
Low	Virtual network firewall rule on Azure SQL Database should be enabled to allow traffic from the specified subnet	Unhealthy
Low	Azure SQL Database should be running TLS version 1.2 or newer	Unhealthy
Low	Auditing on SQL server should be enabled	Healthy
Low	SQL Server should use a virtual network service endpoint	Unhealthy
Low	Audit retention for SQL servers should be set to at least 90 days Preview	Healthy

< Previous | Page 1 of 1 | Next >

Compliance Posture Overview

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud | Overview >

Regulatory Compliance

[Download report](#)
[Manage compliance policies](#)
[Open query](#)
[Compliance over time workbook](#)
[Audit reports](#)

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

[Microsoft Cloud Security Benchmark](#)
[PCI DSS 3.2.1](#)
[TSP](#)
[HIPAA HITRUST](#)
[NIST SP 800 53 R4](#)
[NIST SP 800 171 R2](#)
[UKO and UK NHS](#)
[Canada Federal PBMM](#)
[SWIFT CSP CSCF v2020](#)
[Azure CIS 1.1.0](#)
[GCP CIS 1.1.0 \(Classic\)](#)
[AWS CIS 1.2.0 \(Classic\)](#)

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control, if they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any pa are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to the subscription ContosoHotels

Expand all compliance controls

NS. Network Security

- NS-1. Establish network segmentation boundaries [Control details](#) MS C
- NS-2. Secure cloud services with network controls [Control details](#) MS C
- NS-3. Deploy firewall at the edge of enterprise network [Control details](#) MS C
- NS-4. Deploy intrusion detection/intrusion prevention systems (IDS/IPS) [Control details](#) MS C
- NS-5. Deploy DDOS protection [Control details](#) MS C
- NS-6. Deploy web application firewall [Control details](#) MS C

Customer responsibility	Resource type	Failed resources	Resource compliance status
Storage accounts should restrict network access using virtual network n	Storage accounts	72 of 72	<div style="width: 100%; height: 10px; background-color: red;"></div>
Storage account should use a private link connection	Storage accounts	71 of 72	<div style="width: 100%; height: 10px; background-color: red;"></div>
Access to storage accounts with firewall and virtual network configurations should be restricted	Storage accounts	69 of 72	<div style="width: 100%; height: 10px; background-color: red;"></div>
Storage account public access should be disallowed Quick Fix	Storage accounts	58 of 72	<div style="width: 100%; height: 10px; background-color: red;"></div>
Private endpoint should be configured for Key Vault	Key vaults	22 of 23	<div style="width: 100%; height: 10px; background-color: red;"></div>

1 2 3 4

Compliance Posture Overview

Microsoft Azure | Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Security posture

Showing subscription 'ContosoHotels'

Search (Ctrl+/) | Secure score over time | Governance report (preview) | Guides & Feedback

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture**
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Workflow automation

All environments

Secure score: 37% SECURE SCORE

- Azure 40%
- AWS 33%
- GCP 34%

Environment: 4 Total

- Subscriptions 1
- Accounts 2
- Projects 1

Governance (preview): 13/28 Overdue recommendations

859/1176 Unhealthy resources | 239 Recommendations | 62 Attack paths

135/161 Unassigned recommendations

Environment: Owner (preview)

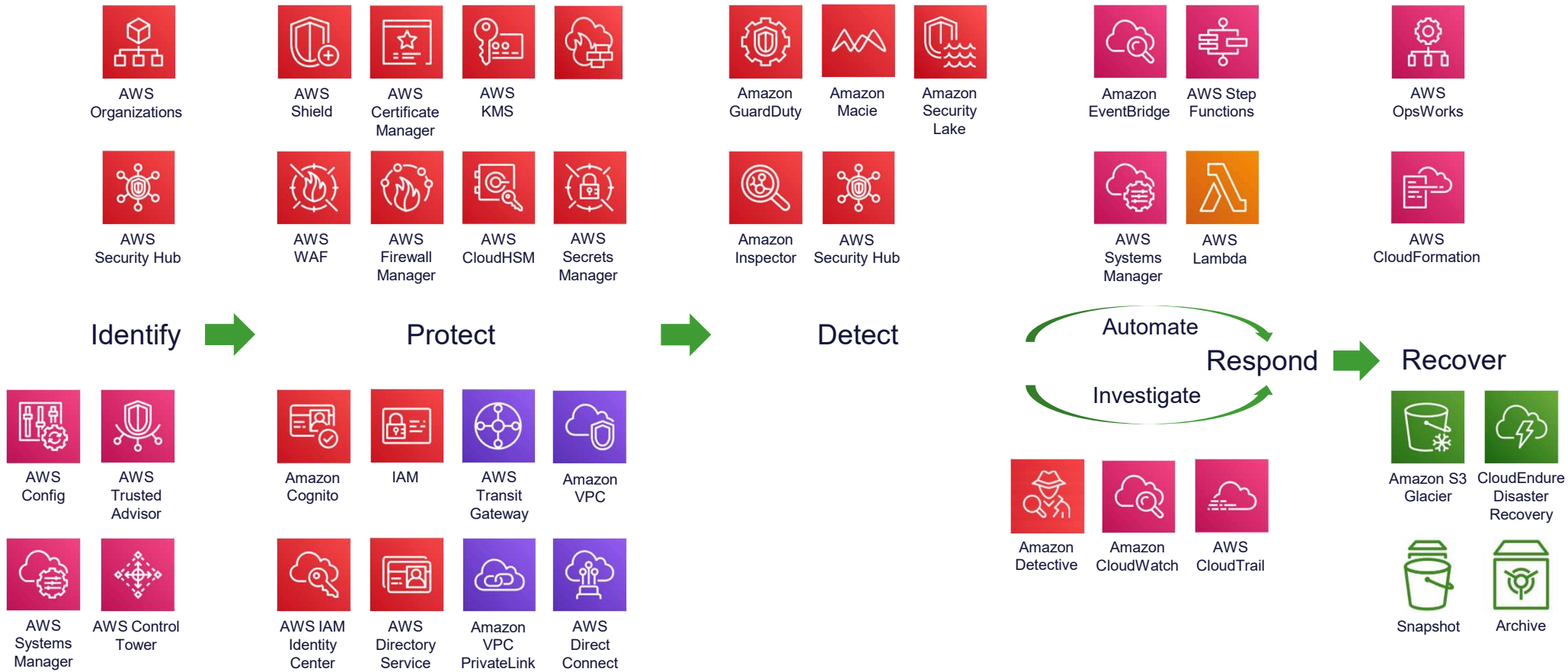
Search by name | Environment == All

Name ↑↓	Secure score ↑↓	Unhealthy resources ↑↓	Attack paths ↑↓	Recommendations
CyberSecSOC Azure subscription	40%	347 of 423	62	View recommendations >
424151343163 (AWSNinjaConnector) AWS account	36%	267 of 415	0	View recommendations >
177044279360 (GCPNinjaConnector) GCP project	34%	123 of 147	0	View recommendations >
571346966349 (containerVA-demo) AWS account	20%	122 of 163	0	View recommendations >

Page 1 of 1

AWS Security

AWS foundational and layered security services



Security and Compliance Challenges



Backlog of
Compliance
requirements



Complexity



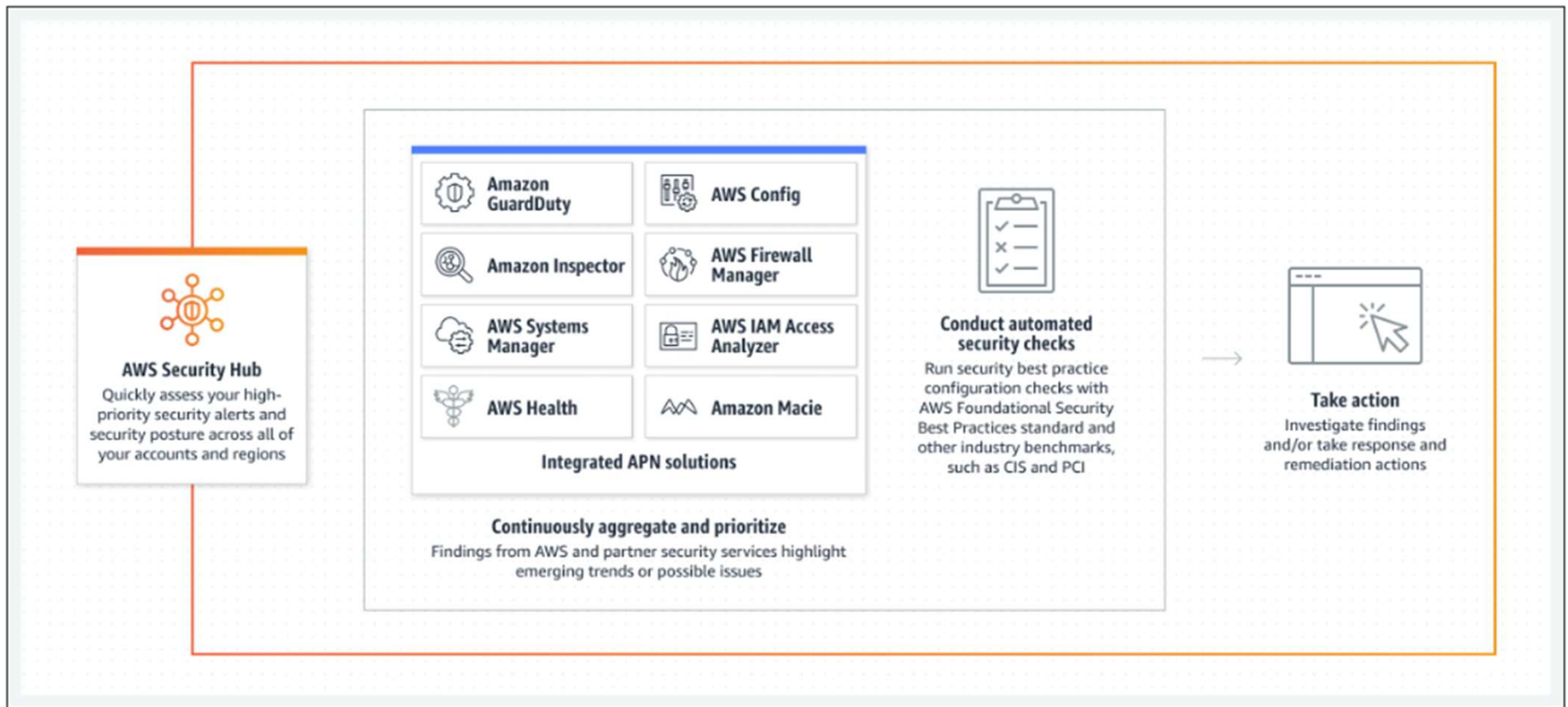
Signal to Noise
Ratio



Lack of an
Integrated View

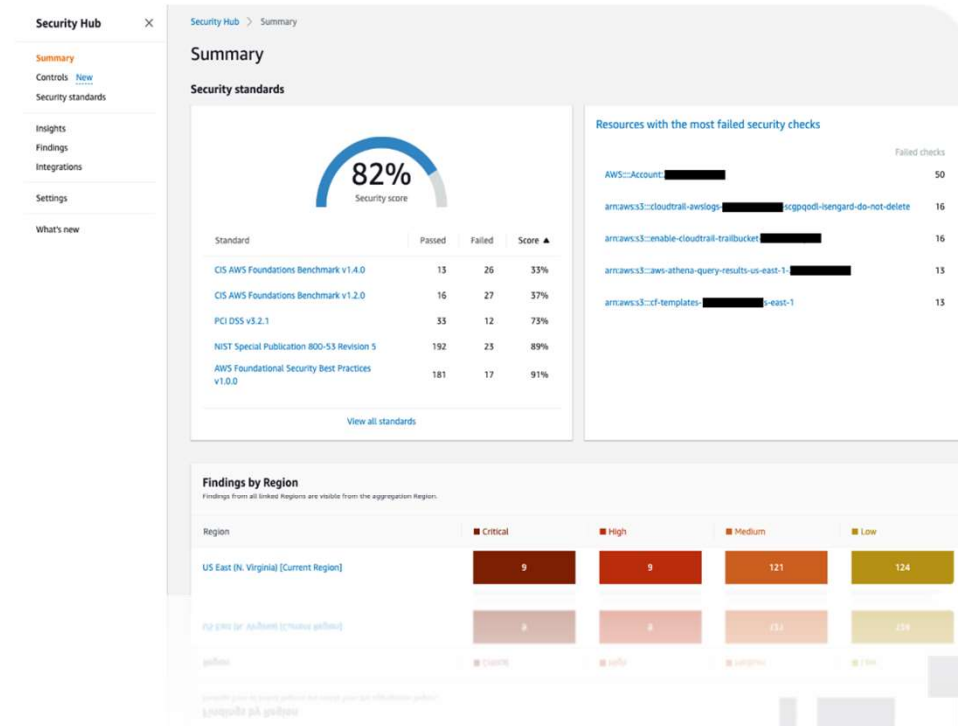


AWS Security Hub overview



Use Case Overview

- 1. View, Triage and Take Action**
 Single pane of glass of security and compliance events across accounts
- 2. Consolidate and Route**
 Easily route events in normalized format to SIEM, log management tool or to take action
- 3. Visibility**
 Visibility on security and compliance posture of accounts



Deploy AWS Security Hub

Turn Security Hub on in all regions and accounts

- Continuously monitor all regions across your AWS accounts for unauthorized behavior or misconfigurations, even in regions that you don't use heavily.
- This aligns to AWS Config and AWS CloudTrail best practices

<https://aws.amazon.com/blogs/mt/aws-config-best-practices/>

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html>

Designate a Management Account for Security Hub

Gain extensive visibility into your security and compliance status across multiple AWS accounts.

Considerations

- Align internally on where and by whom findings will be viewed, notified, and resolved.
- The manager-member relationship is independent from GuardDuty, Amazon Inspector, or Amazon Macie.
- It is operationally efficient to use the same AWS Account as the security management account across all AWS security services.

Process

Invite other AWS accounts to enable AWS Security Hub and become associated with your AWS account.

- Permission is granted to the management account to manage the findings of the member account. Security Hub supports up to 5000 member accounts per management account per Region.

Enable Config in all regions and accounts

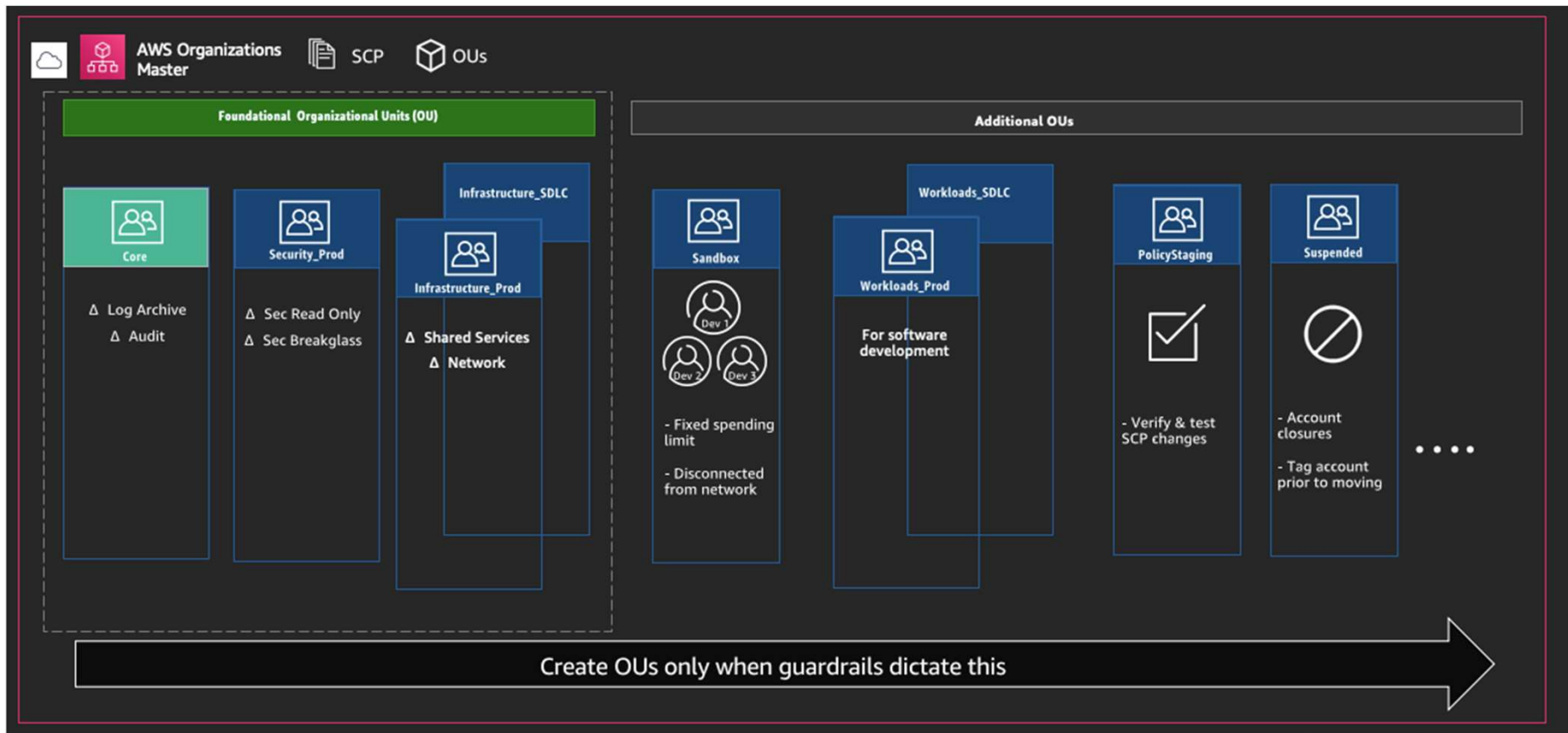
When you enable Security Hub in any region, the AWS CIS standard checks and AWS Foundational Security Best Practices are enabled by default.

Security Hub uses service-linked AWS Config rules to perform most of the security standards' checks.

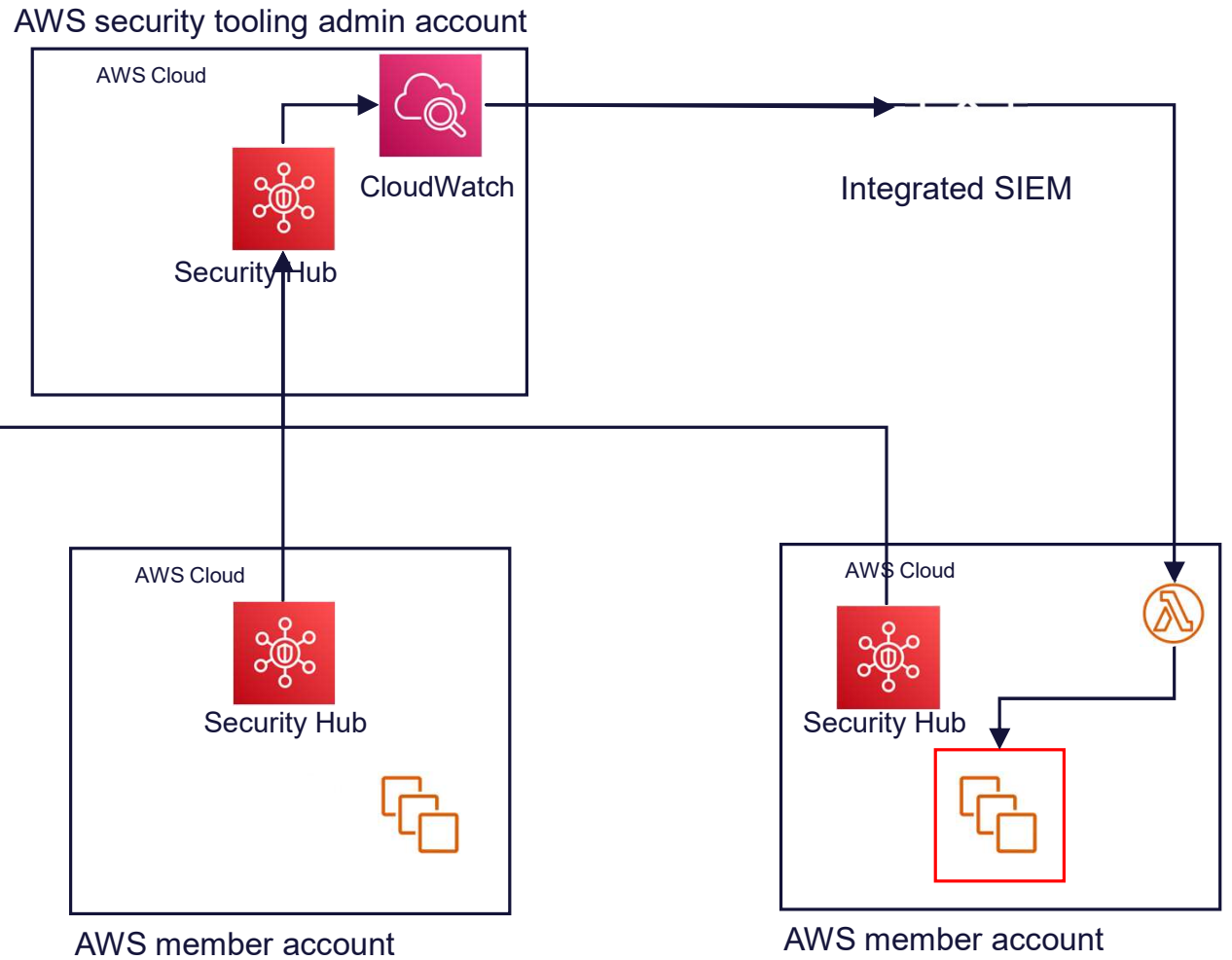
You have read-only access to these rules.

- You cannot edit or delete these rules if you are subscribed to AWS service that these rules are linked to.
- You are not charged by AWS Config for these service-linked rules. You are only charged via Security Hub's pricing model.

AWS Control Tower/Multi-Account Framework Example

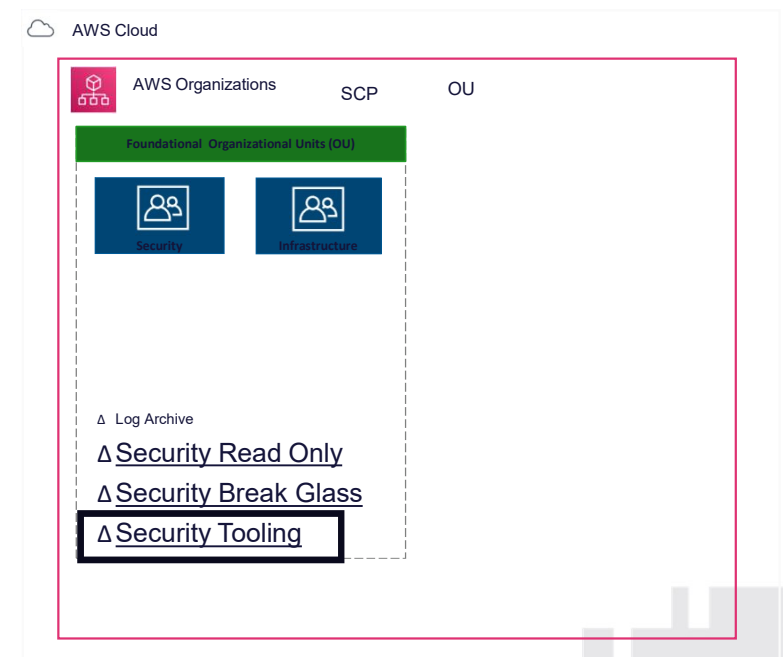
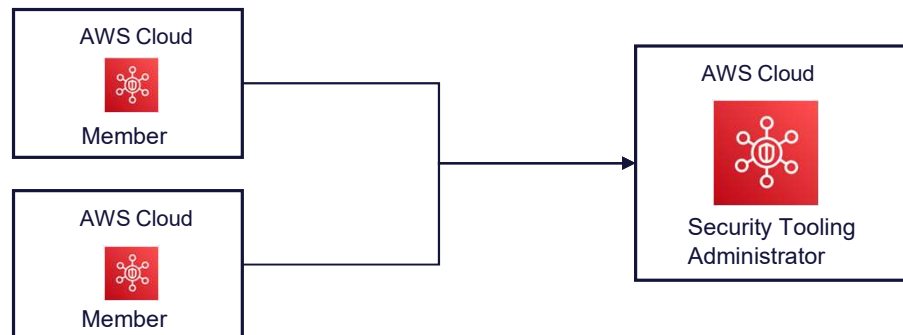


Architecture with multi-account strategy

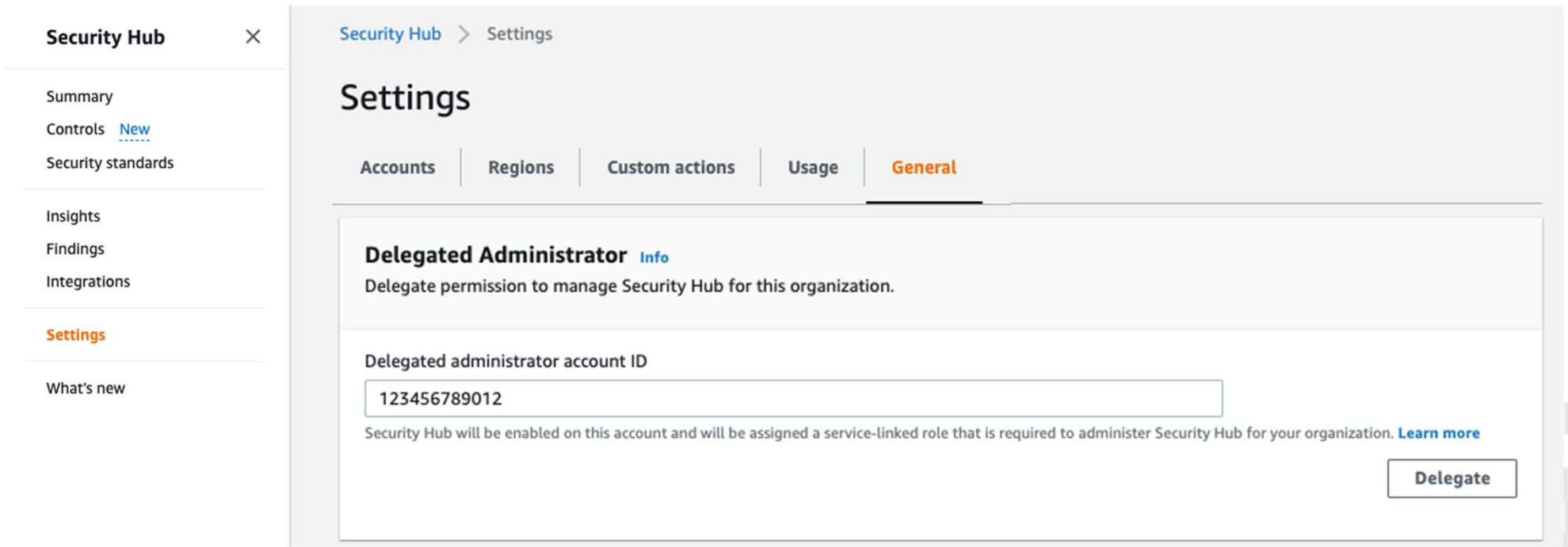


Enable Security Hub in all Accounts in Your Organization

1. From the Organization Manager account setup, the Security Tooling account as a Security Hub “Delegated Administrator”
2. Log into the Security Tooling AWS Account and navigate to Security Hub
3. Enable Security Hub for all accounts in your AWS Organization
4. Enable the “auto-enable” setting



1. Make your Security Tooling Account a “Delegated Administrator”



The screenshot displays the AWS Security Hub console interface. On the left is a navigation sidebar with the following items: Security Hub (with a close icon), Summary, Controls (with a 'New' link), Security standards, Insights, Findings, Integrations, Settings (highlighted in orange), and What's new. The main content area is titled 'Settings' and includes a breadcrumb 'Security Hub > Settings'. Below the title are five tabs: Accounts, Regions, Custom actions, Usage, and General (which is selected and highlighted in orange). The 'Delegated Administrator' section is visible, featuring a title 'Delegated Administrator' with an 'Info' link, a description 'Delegate permission to manage Security Hub for this organization.', and a field for 'Delegated administrator account ID' containing the value '123456789012'. Below the field is explanatory text: 'Security Hub will be enabled on this account and will be assigned a service-linked role that is required to administer Security Hub for your organization. [Learn more](#)'. A 'Delegate' button is located at the bottom right of the section.

2. In the Security Tooling Account Navigate to Security Hub -> Settings -> Accounts

Security Hub ×

Summary

Controls [New](#)

Security standards

Insights

Findings

Integrations

Settings

What's new

i **Enable Security Hub for your organization in this region** Enable

This will enable Security Hub in this Region for all of the accounts in your organization (see AWS Organizations). Security Hub will also be enabled automatically for accounts that are added to your organization in the future. After you enable Security Hub for your organization, you can enable and disable individual accounts from Settings: Accounts.

Security Hub > Settings

Settings

Accounts
Regions
Custom actions
Usage
General

Accounts

Info ↻

Via AWS Organizations (Active/All) 0/3
By invitation (Active/All) 0/0
Active/All 0/3

+ Add accounts
Auto-enable is OFF
Export CSV
Actions ▼

<input type="checkbox"/>	Account ID ▼	Name ▼	Type ▼	Status ▼	Last action ▼
<input type="checkbox"/>	...	Log archive	Via AWS Organizations	Not a member	4 months ago
<input type="checkbox"/>	...	Forensics	Via AWS Organizations	Not a member	4 months ago

3. Enable Security Hub for all Accounts in Your AWS Org

Security Hub ×

- Summary
- Controls [New](#)
- Security standards
- Insights
- Findings
- Integrations
- Settings**
- What's new

Enable Security Hub for your organization in this region
This will enable Security Hub in this Region for all of the accounts in your organization (see AWS Organizations). Security Hub will also be enabled automatically for accounts that are added to your organization in the future. After you enable Security Hub for your organization, you can enable and disable individual accounts from Settings: Accounts. **Enable**

Security Hub > Settings

Settings

Accounts | Regions | Custom actions | Usage | General

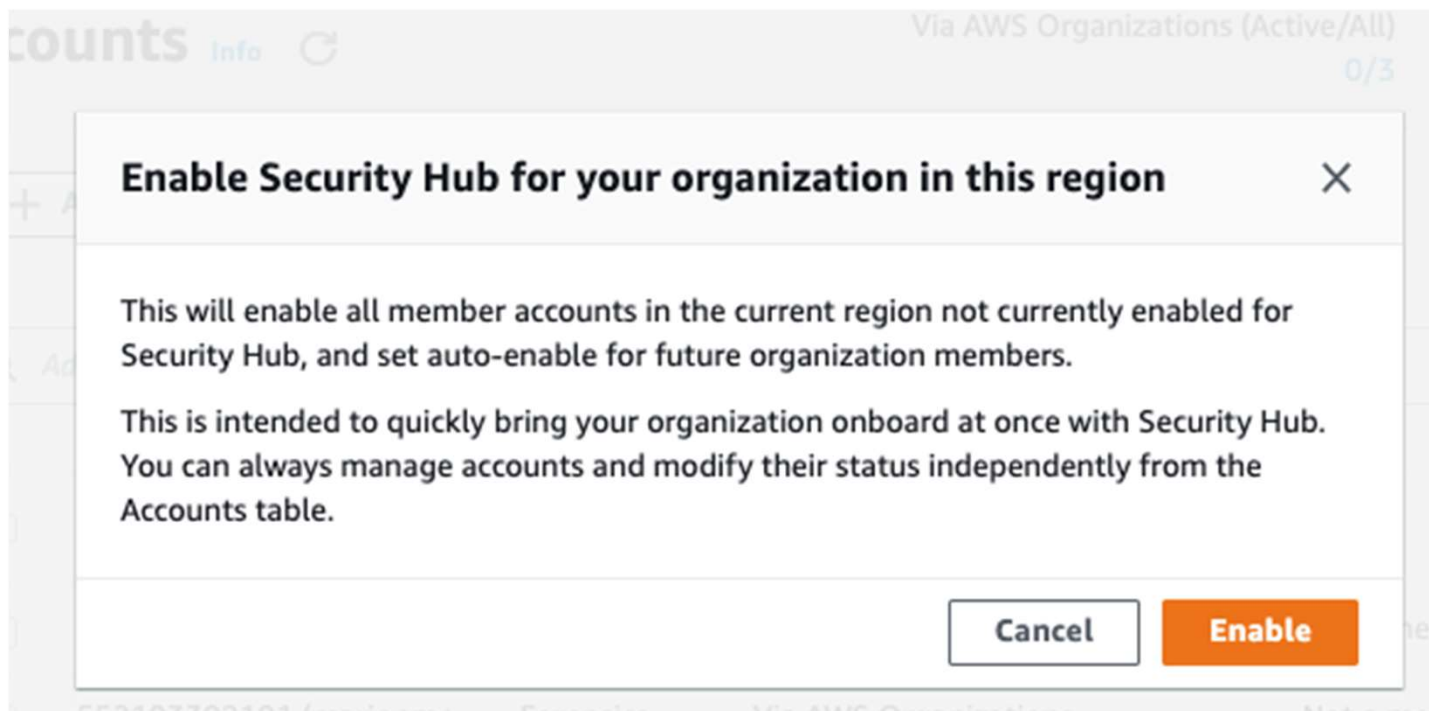
Accounts [Info](#) [Refresh](#)

Via AWS Organizations (Active/All) 0/3 | By invitation (Active/All) 0/0 | Active/All 0/3

| Auto-enable is OFF | |

<input type="checkbox"/>	Account ID	Name	Type	Status	Last action
<input type="checkbox"/>	...	Log archive	Via AWS Organizations	Not a member	4 months ago
<input type="checkbox"/>	...	Forensics	Via AWS Organizations	Not a member	4 months ago

4. Enable the “Auto-enable” Setting, All New Accounts Will Have Security Hub Enabled



Enable Security Standards

Enable Security Hub Security Standards

With Security Hub, you can run automated, continuous account level configuration and compliance checks based on industry standards and best practices.

Current Security standards include:

- AWS Foundational Security Best Practices v1.0.0
- CIS AWS Foundations Benchmark v1.2.0
- CIS AWS Foundations Benchmark v1.4.0
- NIST Special Publication 800-53 Revision 5
- PCI DSS v3.2.1

Security Hub Security Standards

AWS Foundational Security Best Practices v1.0.0

- Curated set of controls defined by AWS security experts.
- Set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices.

CIS AWS Foundations Benchmark v1.2.0/v.1.4.0

- Checks for compliance readiness against a subset of Center for Internet Security requirements

PCI DSS v3.2.1

- An information security standard for entities that store, process, and/or transmit cardholder data.
- Automatically checks for your compliance readiness against a subset of PCI DSS requirements.

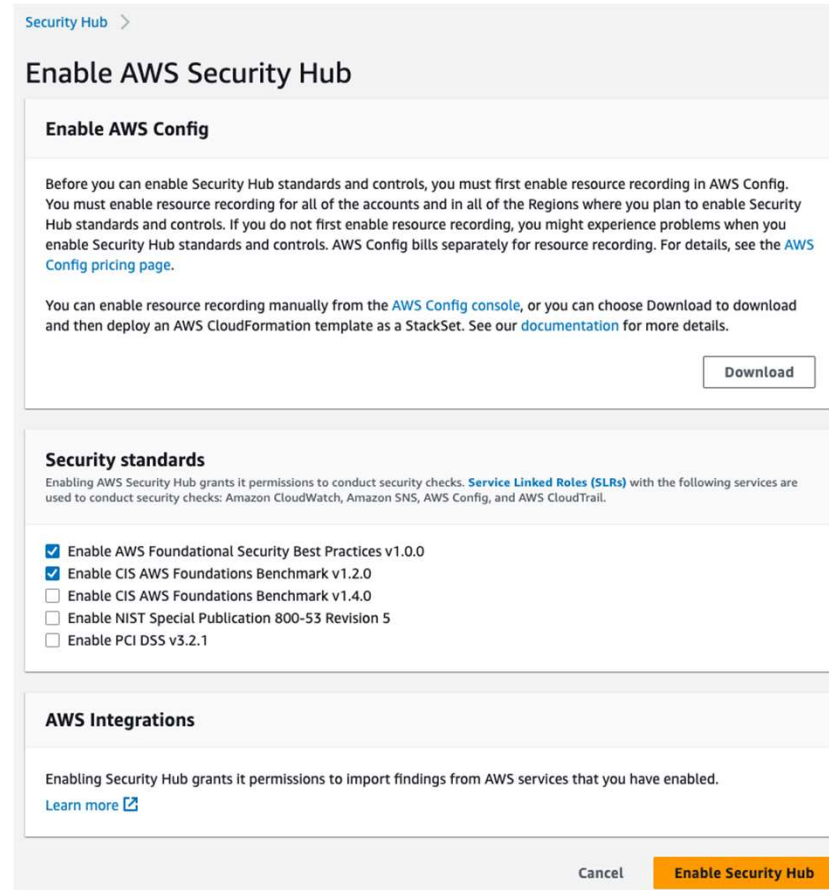
NIST Special Publication 800-53 Revision 5

- provides a catalogue of security and privacy controls for information systems and organizations.
- automatically checks for your compliance readiness against a subset of NIST 800-53 R5 requirements.

Default Security Hub Security Standards

By default, when you enable Security Hub, the AWS Foundational Best Practices and the CIS Foundations Benchmark are enabled, but the PCI standard is not enabled.

We recommend enabling the PCI standard in AWS accounts where it applies.



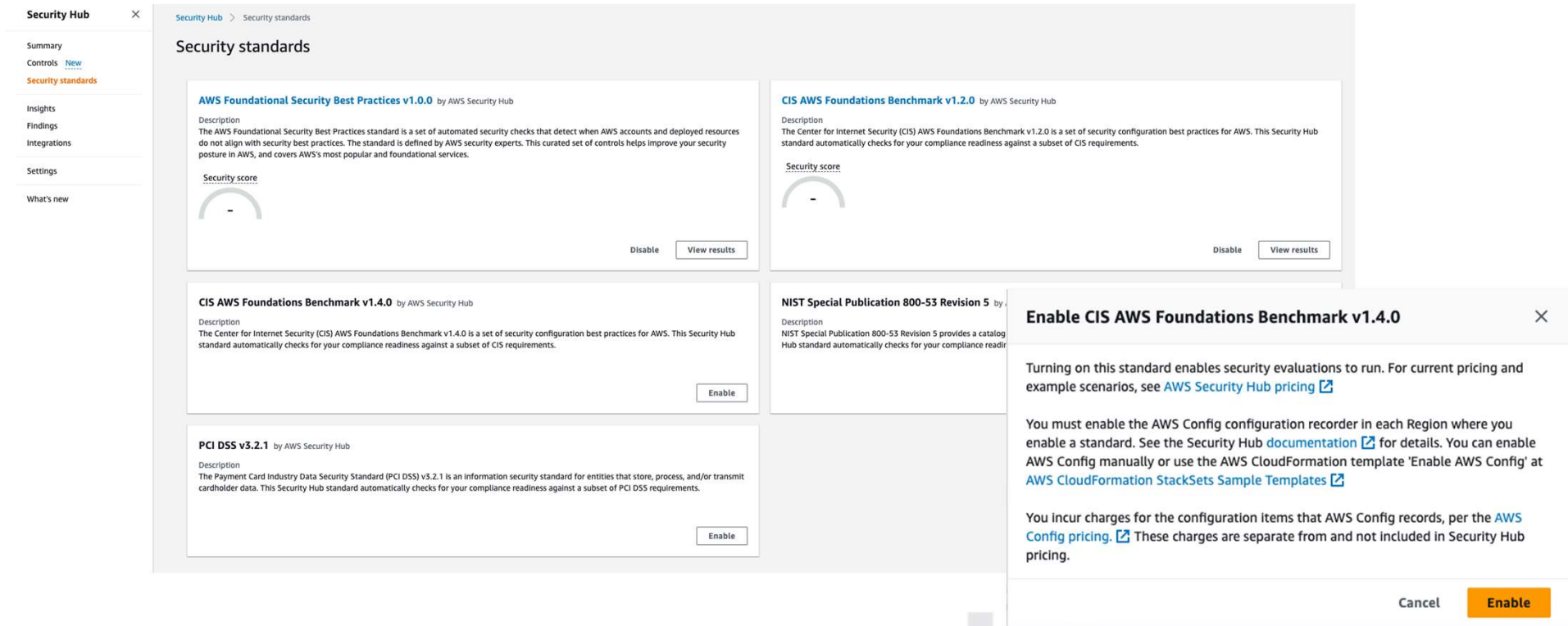
The screenshot shows the 'Enable AWS Security Hub' page in the AWS console. It is divided into three main sections:

- Enable AWS Config:** This section explains that enabling Security Hub standards requires resource recording in AWS Config. It includes a 'Download' button for a manual setup guide.
- Security standards:** This section lists the default standards that will be enabled:
 - Enable AWS Foundational Security Best Practices v1.0.0
 - Enable CIS AWS Foundations Benchmark v1.2.0
 - Enable CIS AWS Foundations Benchmark v1.4.0
 - Enable NIST Special Publication 800-53 Revision 5
 - Enable PCI DSS v3.2.1
- AWS Integrations:** This section notes that enabling Security Hub grants permissions to import findings from other AWS services and includes a 'Learn more' link.

At the bottom right of the console, there are 'Cancel' and 'Enable Security Hub' buttons.

Enabling New Security Hub Security Standards

New security standards can be enabled by clicking enable on the standard in the Security standards portion of Security Hub



The screenshot displays the AWS Security Hub console interface. On the left is a navigation sidebar with options: Summary, Controls (with a 'New' indicator), Security standards (highlighted in orange), Insights, Findings, Integrations, Settings, and What's new. The main content area is titled 'Security standards' and lists several standards:

- AWS Foundational Security Best Practices v1.0.0** by AWS Security Hub: Includes a description and a 'Security score' gauge showing a dash (-). Buttons for 'Disable' and 'View results' are present.
- CIS AWS Foundations Benchmark v1.2.0** by AWS Security Hub: Includes a description and a 'Security score' gauge showing a dash (-). Buttons for 'Disable' and 'View results' are present.
- CIS AWS Foundations Benchmark v1.4.0** by AWS Security Hub: Includes a description and an 'Enable' button.
- NIST Special Publication 800-53 Revision 5** by AWS Security Hub: Includes a description and an 'Enable' button.
- PCI DSS v3.2.1** by AWS Security Hub: Includes a description and an 'Enable' button.

An overlay dialog box is open for the 'CIS AWS Foundations Benchmark v1.4.0' standard. The dialog title is 'Enable CIS AWS Foundations Benchmark v1.4.0'. The content includes:

- A closing 'X' button in the top right.
- Text: 'Turning on this standard enables security evaluations to run. For current pricing and example scenarios, see [AWS Security Hub pricing](#)'
- Text: 'You must enable the AWS Config configuration recorder in each Region where you enable a standard. See the Security Hub [documentation](#) for details. You can enable AWS Config manually or use the AWS CloudFormation template 'Enable AWS Config' at [AWS CloudFormation StackSets Sample Templates](#)'
- Text: 'You incur charges for the configuration items that AWS Config records, per the [AWS Config pricing](#). These charges are separate from and not included in Security Hub pricing.'
- Buttons for 'Cancel' and 'Enable' at the bottom right.

Operationalize Security Findings

Consolidate your findings

When you turn on consolidated control findings, Security Hub generates a single finding per security check, even when a control is shared across multiple standards.

Security Hub ×

Summary

Controls New

Security standards

Insights

Findings

Integrations

Settings


What's new

Security Hub > Controls

Controls

Overview


Security score




82%

200 of 244 controls passed

236 of 888 checks failed



27% failed



Consolidate your findings

When you turn on consolidated control findings, Security Hub generates a single finding per security check, even when a control is shared across multiple standards.

Configure control settings
Not right now

Failed	Unknown	Passed	Disabled	No data	All enabled	All
44	0	200	0	7	244	251

RSM | 57

Operationalize Security Findings – Good - Better - Best

- **Good:**
 - Create custom insight to track security initiative over time
- **Better:**
 - Automate Security Finding alerting
 - Blog: <https://aws.amazon.com/blogs/security/how-to-set-up-a-recurring-security-hub-summary-email/>
- **Best**
 - Fully automate Security Finding response and remediation
 - Blog: <https://aws.amazon.com/blogs/security/automated-response-and-remediation-with-aws-security-hub/>

Take Action on CRITICAL and HIGH Findings

- Filter Findings on Severity label and Status
- Filters are case sensitive
- Review and Remediate

Findings

A finding is a security issue or a failed security check.

Severity label EQUALS CRITICAL X
Workflow status EQUALS NEW X
Workflow status EQUALS NOTIFIED X
Record state EQUALS ACTIVE X
Add filters

<input type="checkbox"/>	Severity	Workflow status	Company	Product	Title	Resource ID
<input type="checkbox"/>	● CRITICAL	NEW	AWS	Security Hub	1.1 Avoid the use of the "root" account	AWS:::Account: [redacted]

1.1 Avoid the use of the "root" account

Finding ID: [arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0/1.1/finding/e022f8b1-f7e3-407b-ad91-dd3c90b377e7](#)

● CRITICAL
 The "root" account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.

Workflow status

RECORD STATE

ACTIVE

Set by the finding provider

AWS account ID

[redacted]

Severity (normalized)

90

Severity (original)

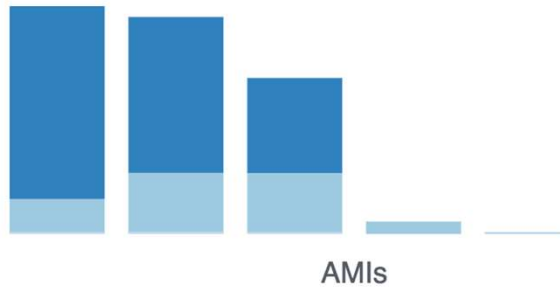
90

Status

FAILED

Insights help identify resources to prioritize

Top AMIs by finding severity



Insight: 5. AMIs that are generating the most findings

Actions ▼ Create insight

Insight results show an aggregated view of findings, typically by resource ID. To view the underlying findings of an insight result, click on the linked text below, or select a result(s) to take an action. You can also modify and save the insight definition

Record state EQUALS ACTIVE Group By: ResourceAwsEc2InstanceImageId Add filter

<input type="checkbox"/>	EC2 instance image ID	Count
<input type="checkbox"/>	ami-f2d3638a	4051
<input type="checkbox"/>	ami-d1c5d1e1	3729
<input type="checkbox"/>	ami-5d967725	2640
<input type="checkbox"/>	ami-f6f16b9f	753
<input type="checkbox"/>	ami-2a8f2f43	502
<input type="checkbox"/>	ami-31814f58	502

Create Customized Insights with AWS Security Hub

Create Insights with the context from your environment


Insights are created using the 'Group By' filter

Add filters before using Group By to focus Insight

- Example: Status EQUALS FAILED

Useful Insights

- ResourceType – Groups findings by AWS resource
- AWS account ID – Groups findings by AWS Account in multi account setup.



The screenshot shows the AWS Security Hub Findings console. At the top, there are buttons for 'Actions', 'Change workflow status', and 'Create insight'. Below this, a search bar contains two filters: 'Status EQUALS FAILED' and 'Group by: ResourceType'. A 'Create insight' dialog box is open, showing a text input field for 'Insight name' and buttons for 'Cancel' and 'Create insight'.

Leverage available remediation instructions

Each Security Hub finding from a Security or Compliance Standard has an associated Remediation

The screenshot displays the AWS Security Hub console interface. At the top, a finding titled "[Config.1] AWS Config should be enabled" is shown with a status of "Failed" and a severity of "MEDIUM". A red box highlights the "Remediation instructions" link, which points to "Config.1 remediation". Below this, a table lists findings, with the same finding highlighted. A second red box highlights the "Remediation" section in the details pane, which includes a link to "For directions on how to fix this issue, please consult the AWS Security Hub Foundational Security Best Practices documentation."

Remediation

To configure AWS Config settings

1. Open the AWS Config console at <https://console.aws.amazon.com/config/>.
2. Choose the Region to configure AWS Config in.
3. If you have not used AWS Config before, choose **Get started**.
4. On the **Settings** page, do the following:
 - a. Under **Resource types to record**, choose **Record all resources supported in this region and include global resources (e.g. AWS IAM resources)**.
 - b. Under **Amazon S3 bucket**, specify the bucket to use or create a bucket and optionally include a prefix.
 - c. Under **Amazon SNS topic**, choose an Amazon SNS topic from your account or create one. For more information about Amazon SNS, see the [Amazon Simple Notification Service Getting Started Guide](#).
 - d. Under **AWS Config role**, either choose **Create AWS Config service-linked role** or **Choose a role from your account** and then choose the role to use.
5. Choose **Next**.
6. On the **AWS Config rules** page, choose **Skip**.
7. Choose **Confirm**.

AWS Security Finding Format (ASFF) in Security Hub

- Security Hub processes all findings using standard ASFF format
- Eliminates the need for time-consuming data conversion
- Correlates findings across products
- Security Hub uses this to prioritize the most important findings
- Can be used to create custom findings for ingestion in Security Hub

<https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format.html>

So... What's Next?

Next Steps

- Check your dashboards.
 - <https://compliance.microsoft.com>
 - <https://security.microsoft.com>
 - https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade
- Review the recommendations for security & compliance gaps
- Reach out if you have questions or concerns

Microsoft incentives



RSM is part of an exclusive group of Microsoft partners that can utilize Microsoft's incentive programs to assist in funding client projects and engagements.

Threat Protection

The Threat Protection Engagement is designed to create intent for purchasing and/or deploying advanced Microsoft Security products, including Microsoft Sentinel and Microsoft 365 Defender.

Data Security

The Data Security Engagement is designed to create intent for deploying and adopting Microsoft Purview solutions.

Microsoft Sentinel

The Microsoft Sentinel Engagement is designed to demonstrate how Microsoft Sentinel helps organizations use intelligent security analytics and threat intelligence to detect and quickly stop active threats.

Cybersecurity Assessment

The Cybersecurity Assessment is designed to evaluate a customer's cybersecurity posture and reduce their risk exposure by using advanced Microsoft Security products: Microsoft Defender Vulnerability Management, Secure Score, Microsoft Purview for Information Protection Content Explorer and Insider Risk.

Contact our team to see if your organization is eligible for funding.



Thank you





THE POWER OF BEING UNDERSTOOD ASSURANCE | TAX | CONSULTING

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2023 RSM US LLP. All Rights Reserved.