NTT DATA
Trusted Global Innovator

Managed Cloud Security Posture Management & Cloud Workload Protection Powered by Microsoft Defender for Cloud

1/28/2022

Raul Neagoe

Multi-Cloud Cloud Requires a New Approach to Security

Infrastructure increasingly distributed across public clouds and on-premises datacenter

Rapidly changing resources

High complexity added when using Hybrid Cloud

Increasingly sophisticated attacks

Security skills are in short supply

Securing the Unknown

Increases in attack surface and vectors provide challenges

15+ TYPICAL ASSETS IN THE ATTACK SURFACE

11 CLOUD ATTACK VECTORS BY CLOUD SECURITY ALLIANCE*

3 RESULTS IN INCREASED RISK

* https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

General Predictions and Challenges in the Cloud

Predictions

Through 2023, **at least**

of cloud security failures
will be the customer's fault

Through 2024, workloads that leverage the programmability of cloud infrastructure to improve security protection will suffer at least

fewer security incidents than those in traditional data centers.

Source: Gartner

[1]Source: Ponemon Institute, Cost of a Breach Report
[2]Source: 451 Research

What Is CSPM and CWP ?

Continuously assess

- Know your security posture
- Identify and track security risks

Secure

- Harden cloud resources and services
- Check your compliance using security benchmarks

Defend

- Detect and resolve threats to resources, workloads and services

Through 2024, organizations implementing a CSPM & CWP offering and extending this into development will reduce cloud-related security incidents due to misconfiguration by 80%.

Source: Gartner

Cloud Security Posture Management (CSPM)

- **Enhanced visibility** to help you understand your current security situation.
- **Hardening guidance** to help you efficiently and effectively improve your security.
- **Enhanced automation:** Automatically fixing threats.

Cloud Workload Protection (CWP)

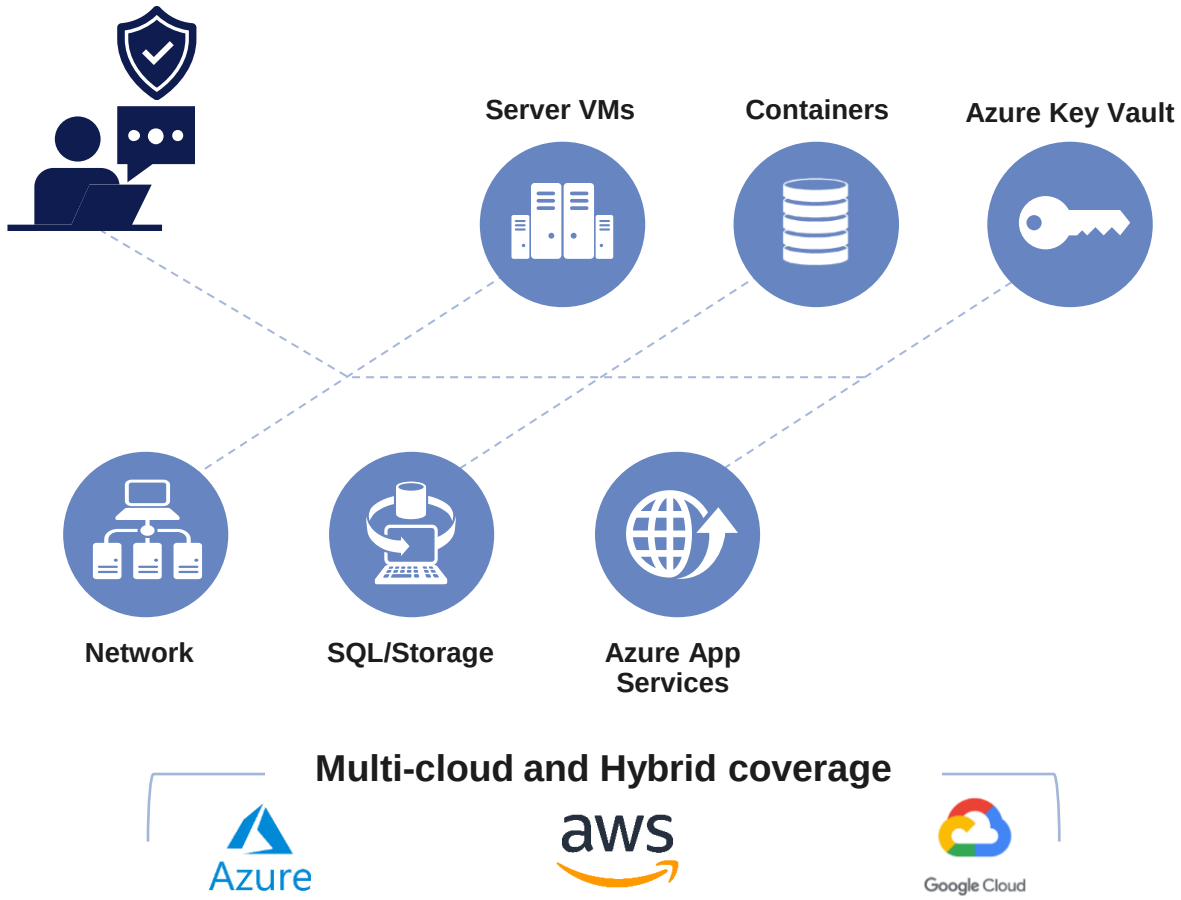
- Defender for Cloud offers security alerts that are powered by Microsoft Threat Intelligence. It also includes a range of advanced, intelligent, protections for your workloads**.**
- **Azure, hybrid, and multi-cloud protections**- Defend Azure, On-prem and AWS/GCP environments.

Multi-Cloud & Hybrid Protection With Microsoft Defender for Cloud

Security posture & compliance	Secure score	Asset management	Regulatory compliance
Protection (Defender for Servers, Containers)	Threat detection	Vulnerability Assessment	Hardening Recommendations
Automation & management at scale	Automation	SIEM integration	Export

Microsoft Defender for Cloud

Secure your critical cloud workloads running in Azure, AWS and Google Cloud

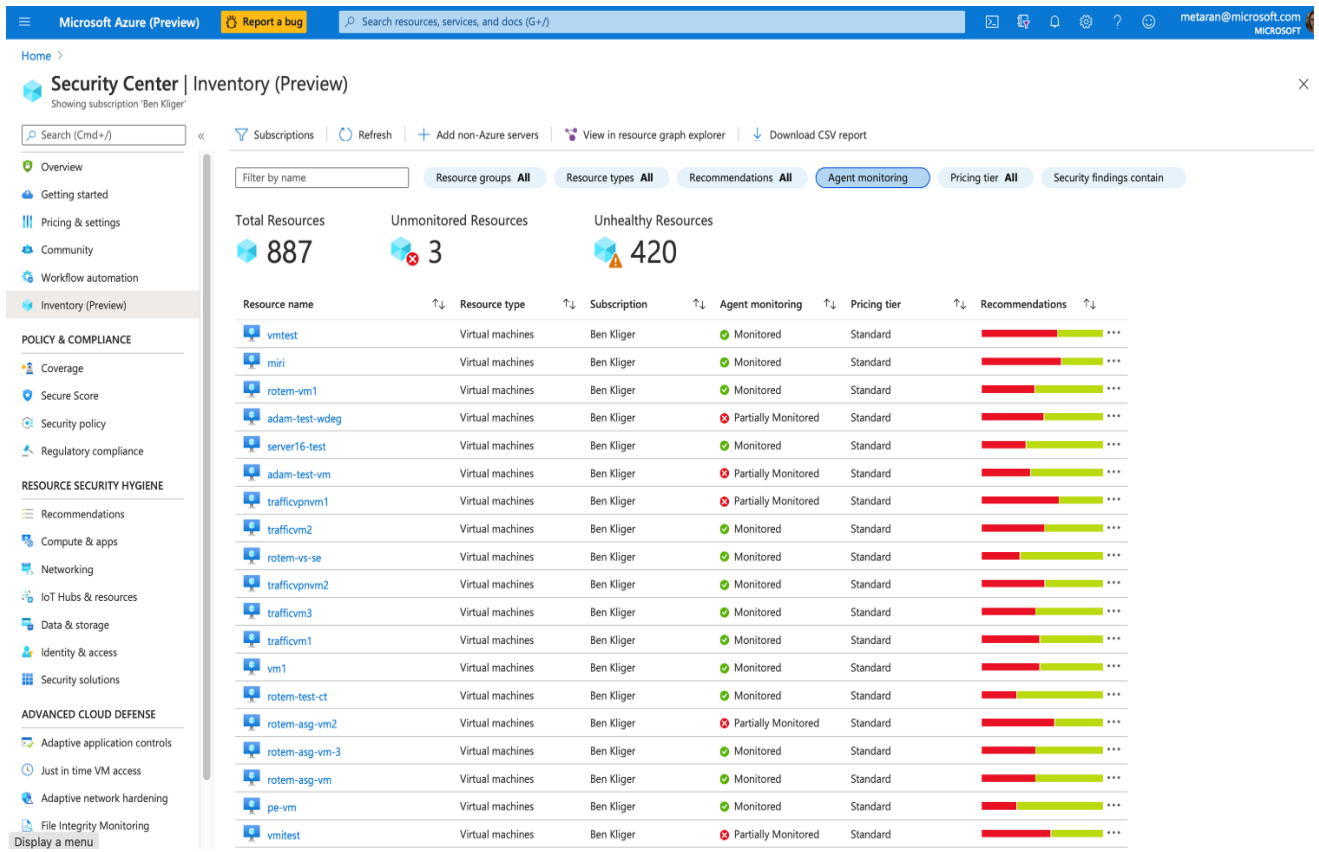


- Easy onboarding of AWS and GCP accounts and native support for Azure
- Get a bird's-eye view of your security posture and vulnerabilities across clouds with secure score
- Assess and implement best practices for compliance and security in the cloud
- Protect Amazon EKS clusters and AWS EC2 workloads
- Detect and block advanced malware and threats for Linux and Windows servers running in the cloud or on-premises

A Complete Security View From a Single Pane of Glass

Continuous detection, improvement & protection

- Detect threats across IaaS and PaaS services using advanced analytics
- Continuously monitor and protect all your cross-cloud resources
- Reduce exposure and protect data services against malicious attacks
- Reduce attack surface by applying proactive hygiene measures



Speed up compliance

- Manage security policies at an organizational level
- Easily set security policies for subscriptions or management groups
- Follow best practice recommendations
- Instantly understand your current policy compliance and review compliance overtime

Improved Automation

Apply quick fixes to recommendations

Automate responses with Logic Apps

Continuously export to Event Hub and Log Analytics

Autogenerate reports

With deep knowledge in Azure Automation our Cloud Security experts can help you gain:

- **Operational efficiencies**
- **Reduce attack surface**
- **Automate incident response triggers**
- **Support compliance efforts**

NTT DATA CSPM & CWP Advisory Engagement Overview

Zero Trust Assessment

- Conduct a Zero Trust assessment – review high-level environment architecture and security solutions currently in place
- Discuss business concerns and requirements
- **Output -** a Zero Trust evaluation report and top line objectives, concerns and requirements

Intro to Microsoft Defender for Cloud

- Review MS Defender for Cloud functionality and assess how these solutions can be used to protect your cloud environment
- Discuss specific ASC & Defender capabilities
- **Output -** Develop and deliver a prioritized list of objectives as they apply to ASC. Build an actionable roadmap

Secure Score & Compliance

- Interactive activity to discuss and run Secure Score for your environment, review findings and discuss opportunities to remediate issues and drive systemic improvements
- Discuss compliance requirements and assess Secure Score compliance findings
- **Output -** Develop a prioritized list of security improvement opportunities

Remediating Configuration Errors

- Determine what actions should be taken for common configuration and what can be set up for automatic remediation
- Determine the process for addressing uncommon security vulnerabilities
- **Output -** Create a mitigation plan and determine actions to remediate vulnerabilities

Security Posture Discovery & Policies

- Implement discovery and policies to identify shadow IT, unsanctioned activities, and subscriptions not leveraging recommended security policies
- Determine actions to take (or automate) to prevent unapproved activities
- **Output -** Develop critical CSPM policy and controls list

Amplifying CSPM

- Identify workflow automation opportunities and priorities
- Evaluate reporting requirements to determine dashboard and reporting needs
- **Output -** Develop integration strategy, outline workbook(s) configuration and workflow automation priorities

Threat Detection & Prevention

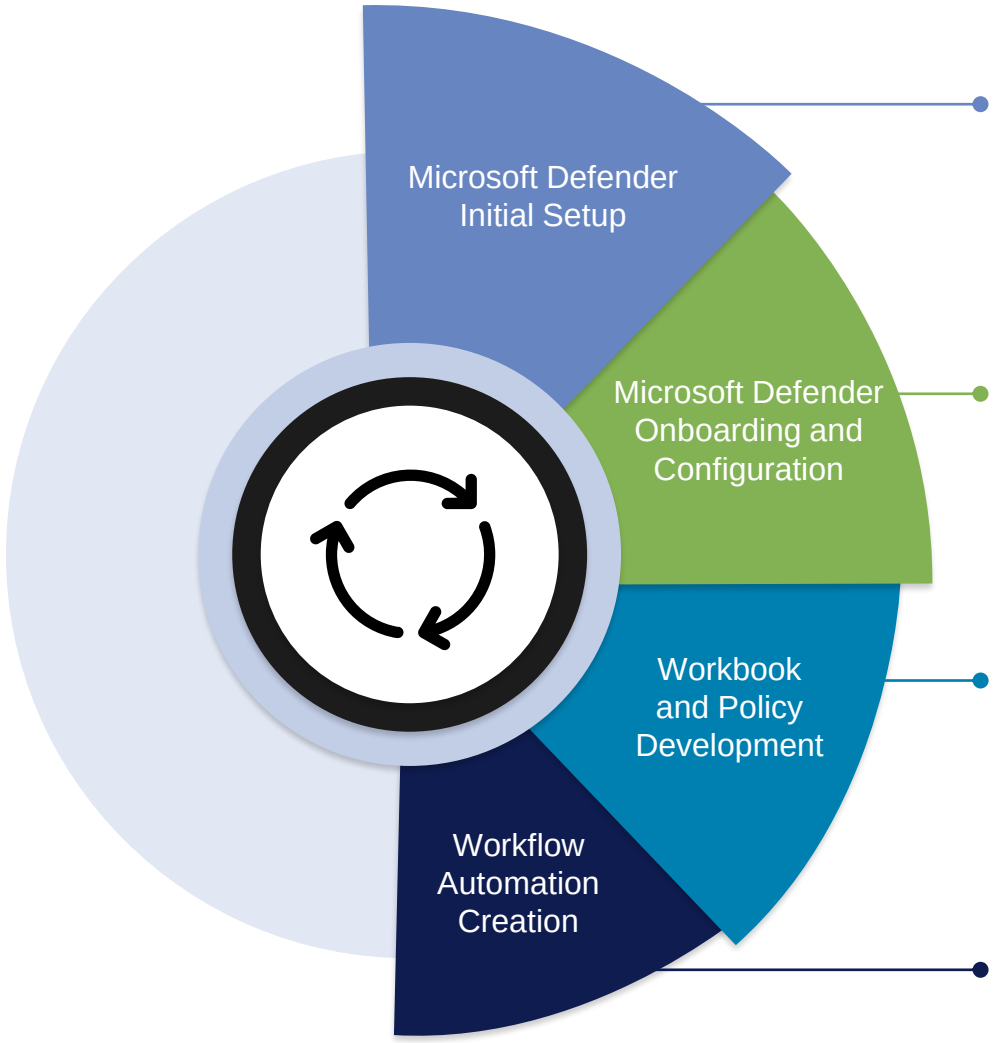
- Discuss the test plan process for enabling controls across the environment to determine the preferred approach ensuring productivity is not disrupted
- Integration with SIEM and X/MDR.

  (Example: Managed Sentinel)
- **Output -** agreed upon test plan approach and procedures

Design Decisions & Enabling Controls

- Summarize all gathered intel & established parameters, configuration details and data
- **Output -** A design guide, architectural diagram, and implementation plan combining your requirements and NTT DATA best-practices

Overview of the NTT DATA CSPM & CWP Implementation Phases



- Microsoft Defender will be enabled across the targeted subscription in the Management Group.
- An initial assessment of the Secure Score will be ran and assets will be reviewed to identify priority vulnerabilities.
- Alerts will be enabled at the preferred parameters and email notifications for designated stakeholders, in alignment with client preference or direction.
- Standard auto-responses to alerts may be configured during initial setup phase.
- The client will manage or provide direction on access levels for ASC.

- Microsoft Defender for Cloud will be deployed at the subscription level where the workloads to be protected reside to enable full functionality of the solution.
- Once the initial Microsoft Defender for Cloud solution is deployed, NTT DATA will enable automatic provisioning of the Log Analytics agent and applicable extensions for resources added to the Azure environment.

- Microsoft Defender embedded security policies will be enabled to assess vulnerabilities that create opportunities for threats and threat actors.
- Custom workbooks will be created to surface deeper insights on critical use cases the client wishes to assess at a more granular level, as determined during the advisory workshop engagement.

Note: Additional custom workbooks can be provided using our optional service

- NTT DATA will enable workflows to automatically remediate vulnerabilities the client determines are critical to their security objectives as defined during the advisory engagement.
- NTT DATA will work with the client's technical team to test the workflows to verify the remediation action aligns to the trigger. Any changes required as a result of testing will be updated in the CSPM design guide.
- The implementation engineer will need to be provided with Logic App Contributor access to create the automated workflows.

Note: Additional custom workflows can be provided using our optional service

Validate the controls and meet the objectives by enabling Controls Assess usage and performance patterns from the captured alerts established during the preceding phases.

Configure governance controls based on required modifications as indicated during the testing process.

NTT DATA CSPM & CWP Managed Services

Operational Support

- Security monitoring to help ensure defense integrity of the onboarded Cloud subscriptions, with analysis and validation support as sent by the SIEM or SOC team of impactful alerts.
- Daily vulnerability scan of protected resources, with analysis of findings and top concerns, and present to client stakeholders in alignment with determinations made during the advisory engagement.
- Weekly evaluation using Secure Score, analyze and validate recommendations and prioritize based on criticality.

On a monthly basis:

- Monthly report outlining operational metrics, security pattern trends and changes, improvements made, with impact or progress assessments.
- Identify cloud resources that need to be exempt from ASC recommendations, document accordingly.

Optimization Support

Continual improvement efforts to consistently improve your cloud security posture

On a monthly basis:

- Present top cloud security posture improvements for client consideration
- Review of policy and automation workflow effectiveness to validate the client's requirements are being met
- Validate remediation recommendations, assess impacts and present mitigation approach to the client.

On a quarterly basis:

- Identify 1-3 workflow automation opportunities to improve the security.
- Assess opportunities to develop new or refine policies if gaps exist in remediation recommendations.
- Validate the existing threat detection workbook effectiveness, optimize based on evolved security patterns and threat trends.

Audit Support

Support client-led audit preparations for compliance or security program-related efforts

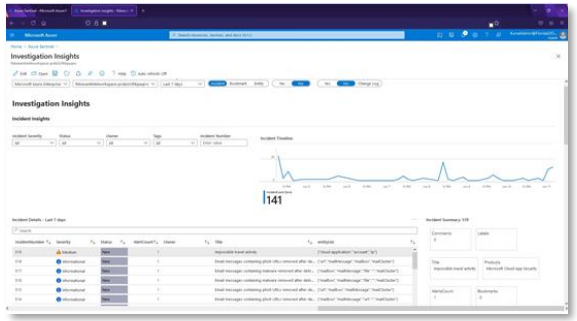
Audit assistance on up to a biannual basis.

Such entitlements include:

- Export CSPM data upon request
- Detailed data usage reports
- Off-band reporting per client-directed requirements

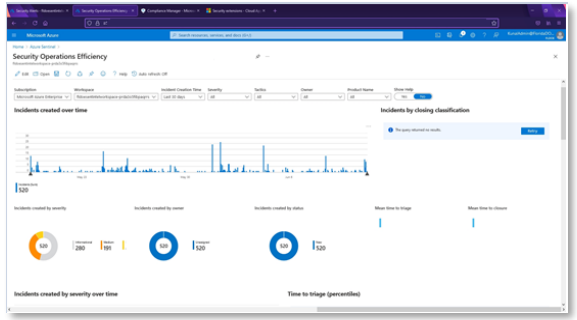
Amplifying Managed CSPM & CWP: NTT DATA's Add-On Value

Workbooks



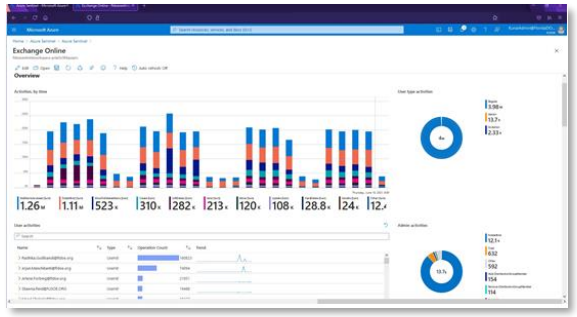
Investigation Insights

Help analysts gain insight into incident, bookmark and entity data.



Security Operations Efficiency

Security operations center managers can view overall efficiency metrics and measures regarding the performance of their team.



Mail Exchange Online

Gain insights into Microsoft Exchange online by tracing and analyzing all Exchange operations and user activities. Ex: monitor permission changes, and mailbox creations to discover suspicious trends among them.

Automation Scripts

Examples

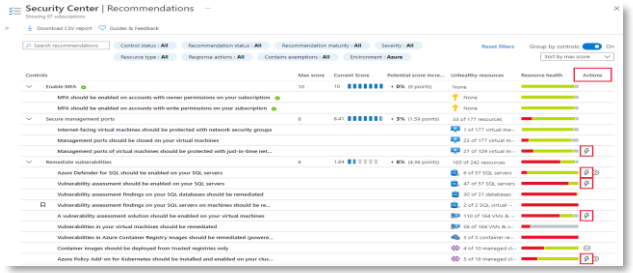
Alert/Report Scripts	Remediation Scripts	Workflow Automations
JIT custom role	Restrict access to storage accounts with firewall and virtual network configurations	Notify-security issues
Security alerts in Azure activity log	Enable transparent data encryption on SQL databases	Post-sec-teams message
Read Azure storage transaction metrics	Remove external accounts	Remove-malware blob
		Run-MDE-antivirus

Custom Security Recommendations		Custom Secure Score
Require Linux VM to use SSH key authentication	Sensitive information types scanning should be enabled	Secure Score reduction alerts

Remediate and Prevent Configurations Drifts With Microsoft Defender for Cloud

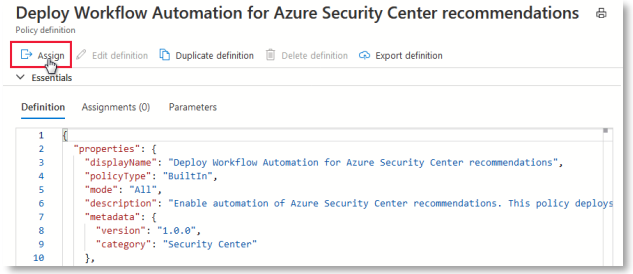
Security Recommendations

- Recommendations against regulatory and compliance standards
- Custom security initiatives and policies
- Continuous audit of assets/configurations with logging



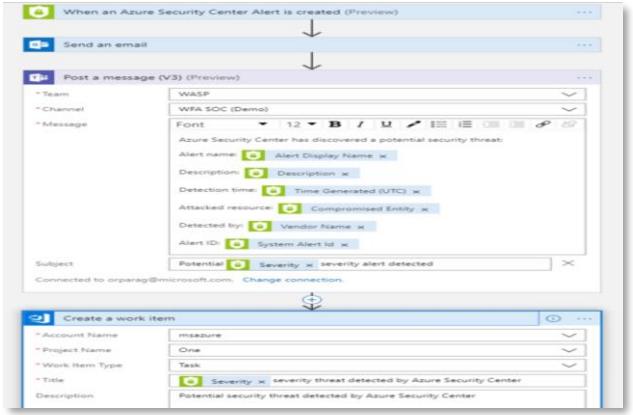
Automate response to misconfigurations and drift configurations

- Automation for remediations and violations
- Automation responses and alerts to configurations
- Automated versioning of configurations



Prevent drift configurations

- Prevent misconfigurations of new resources to specific recommendations by denying, enforcing rules, policies and blueprints
- 500+ workbooks/playbooks/blueprints

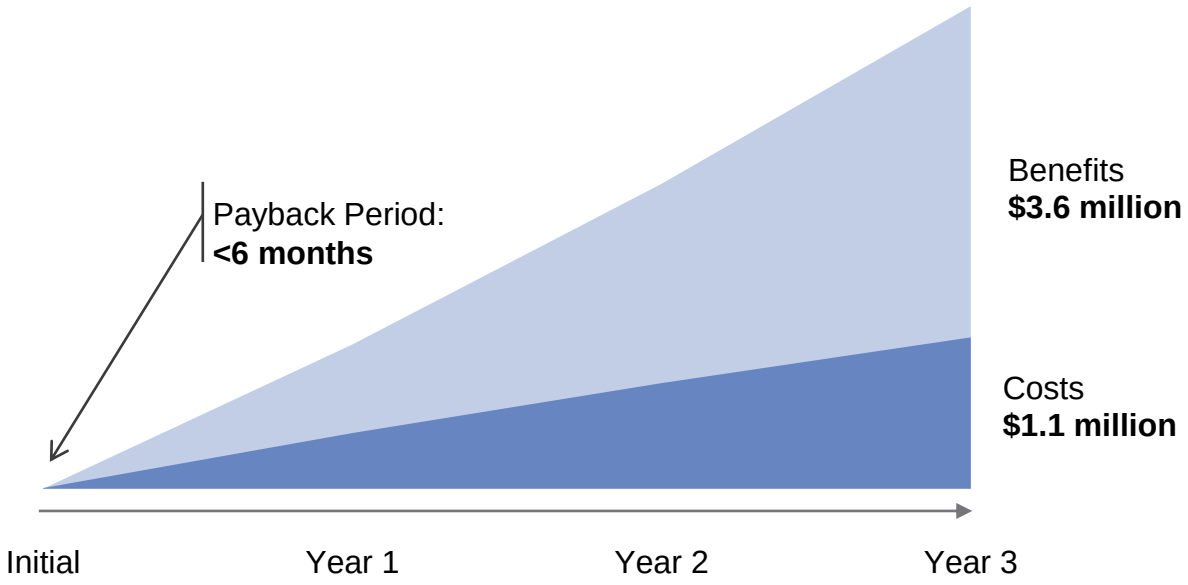


The Total Economic Impact™ of Microsoft Defender for Cloud

(former Azure Security Center)

Financial Summary

ROI	Benefits PV	NPV	Payback
219%	3.56M	$2.44M	<6 months



Security Center cost savings and business benefits

25%
reduction in risk of a security breach

50%
reduction in time to threat mitigation

30%
reduction in security policy and compliance management time

$216K
annual reduction in security tool spend

Read the full study

What Makes Us So Different

Strength of the NTT Group

6.1+ trillion logs analyzed annually
14 SOCs and 7 R&D centers
6.2B attacks defended annually
150+ million identities managed

Flexibility of Our Delivery and Pricing Model

Broad range of leveraged and dedicated delivery models
Maximize clients existing toolsets and investments

Our People

5,000+ security and cloud engineers
1,000+ DevOps (build & release) engineers
1,500+ cloud certifications
Over 3,000 public cloud certifications

Vertical Expertise

Deep vertical expertise
Consulting
Digital Transformation services that are complemented by deep security expertise

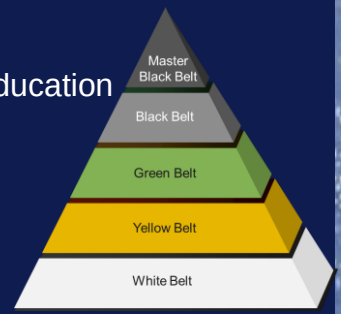
Innovation

$4B Annual R&D
Focus on Internal IP

NTT partnerships with universities , research labs and incubator programs

Learning obsessed culture

Employees complete continual education courses
Learning focus on emerging technologies: Cloud Security ,AI, automation.



Our partnerships

Gold Microsoft Partner
Azure Expert MSP

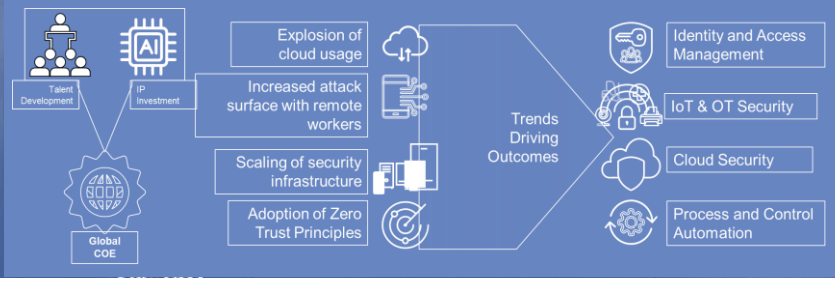
aws partner network
ADVANCED CONSULTING PARTNER

Premier Partner
Google Cloud

14 Microsoft Gold Competencies

Strategic Alliance and Collaboration Agreement Between NTT and Microsoft

Center of Excellence

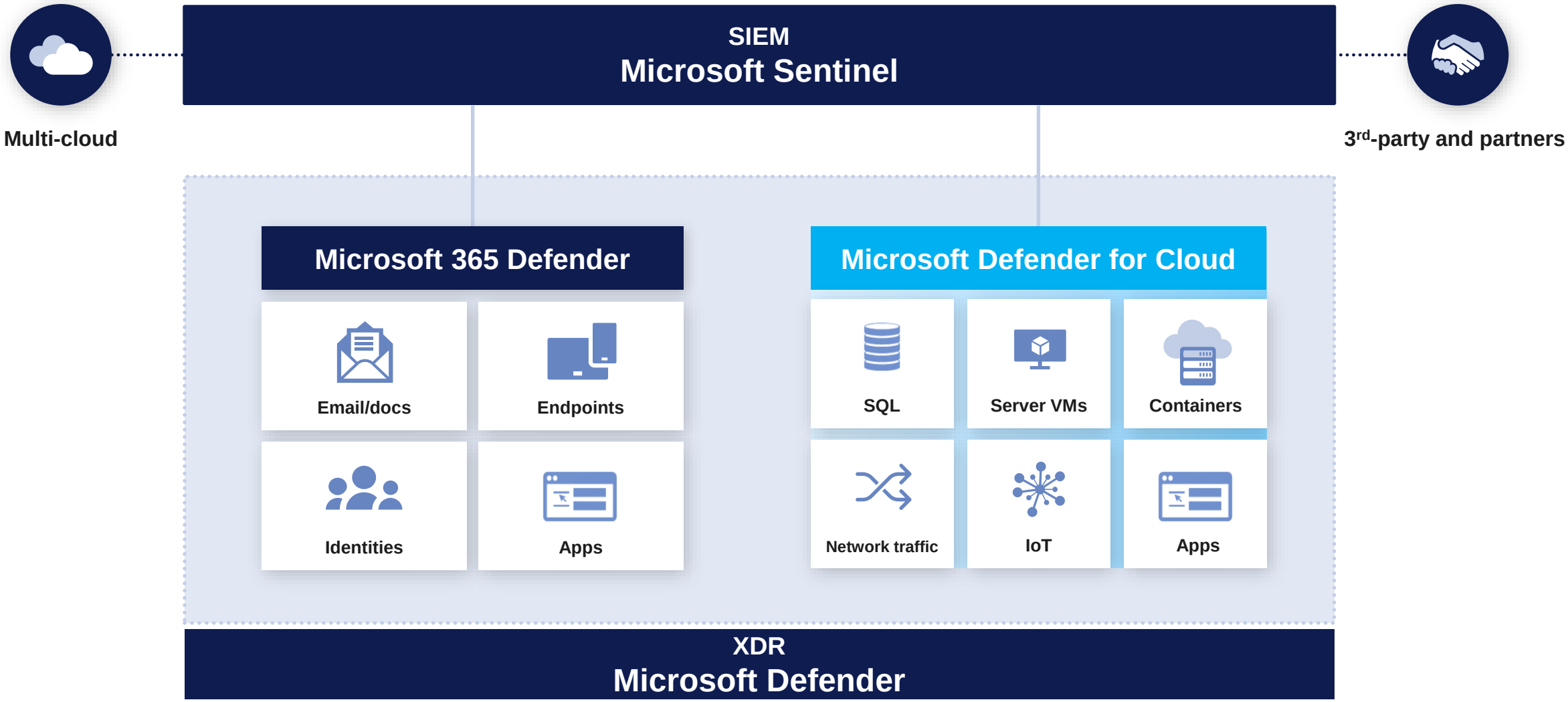


Technical Slide Deck

1. Overview & Architecture
2. Cloud Security Posture Management
3. Cloud Workload Protection

1. Overview and Architecture

Integrated Threat Protection for Your Enterprise



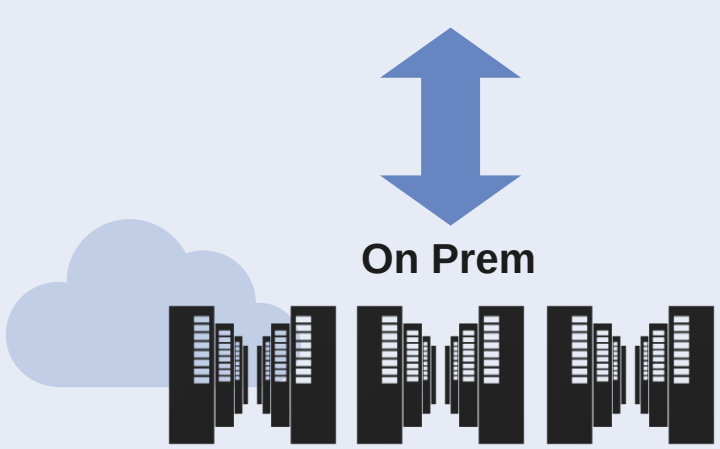
Cloud Security Posture Management

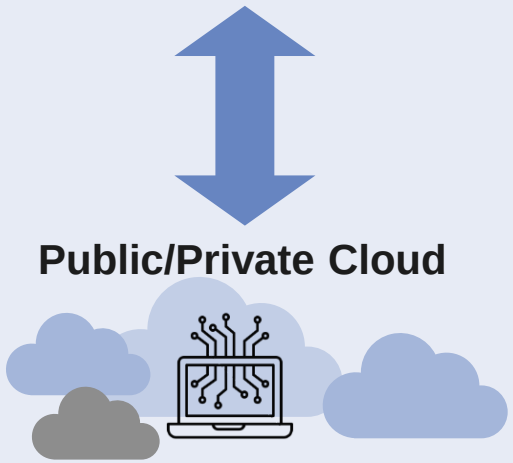
Alerts → SIEM

- Secure Score
- Unified Pane of Glass
- Continuous assessment

Cloud Workload Protection

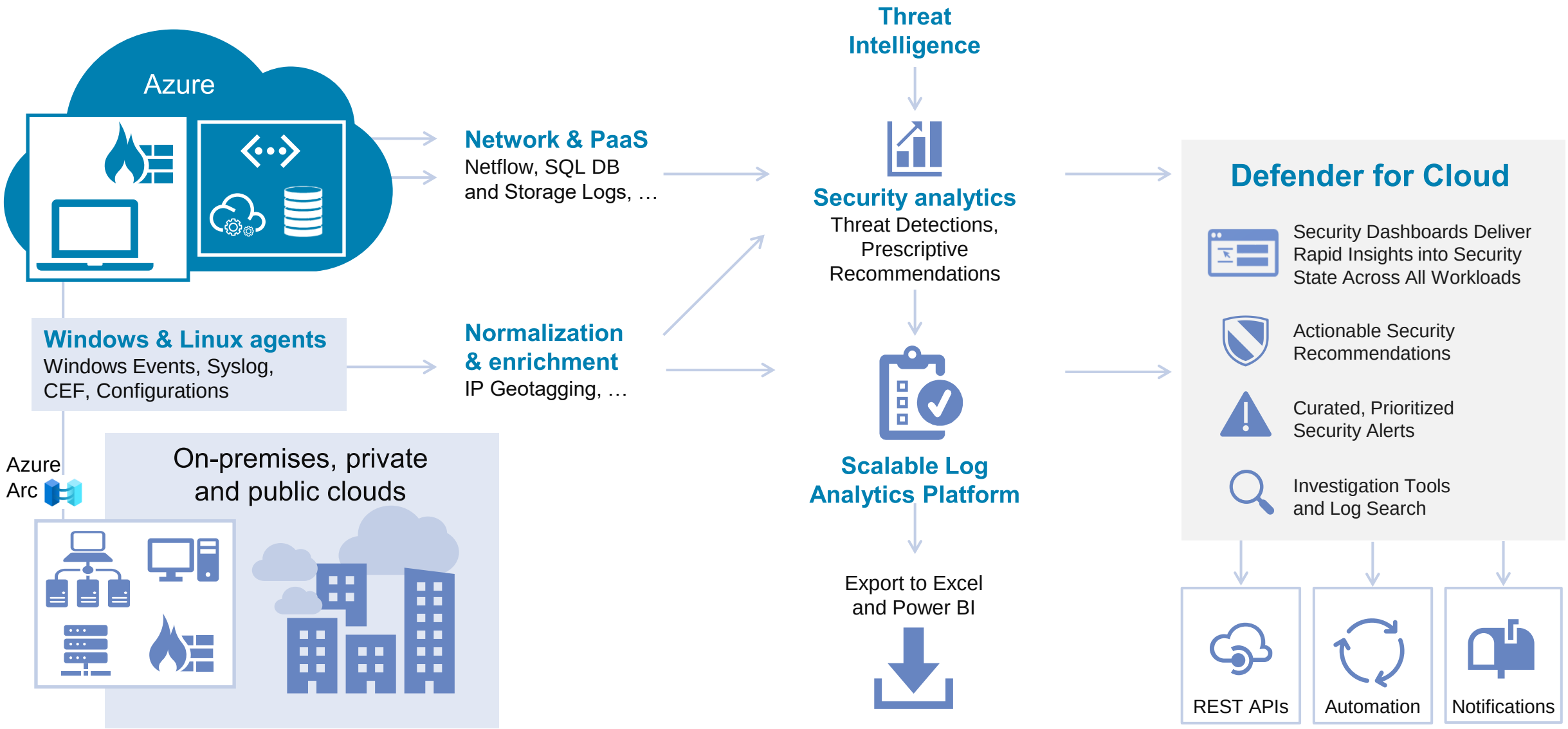
Microsoft Defender for Servers	Microsoft Defender for App Services	Microsoft Defender for Storage
Microsoft Defender for SQL	Microsoft Defender for Containers	Microsoft Defender for DNS
Microsoft Defender for Key Vault	Microsoft Defender for Resource Manager	Microsoft Defender for Open-Source Relational DB



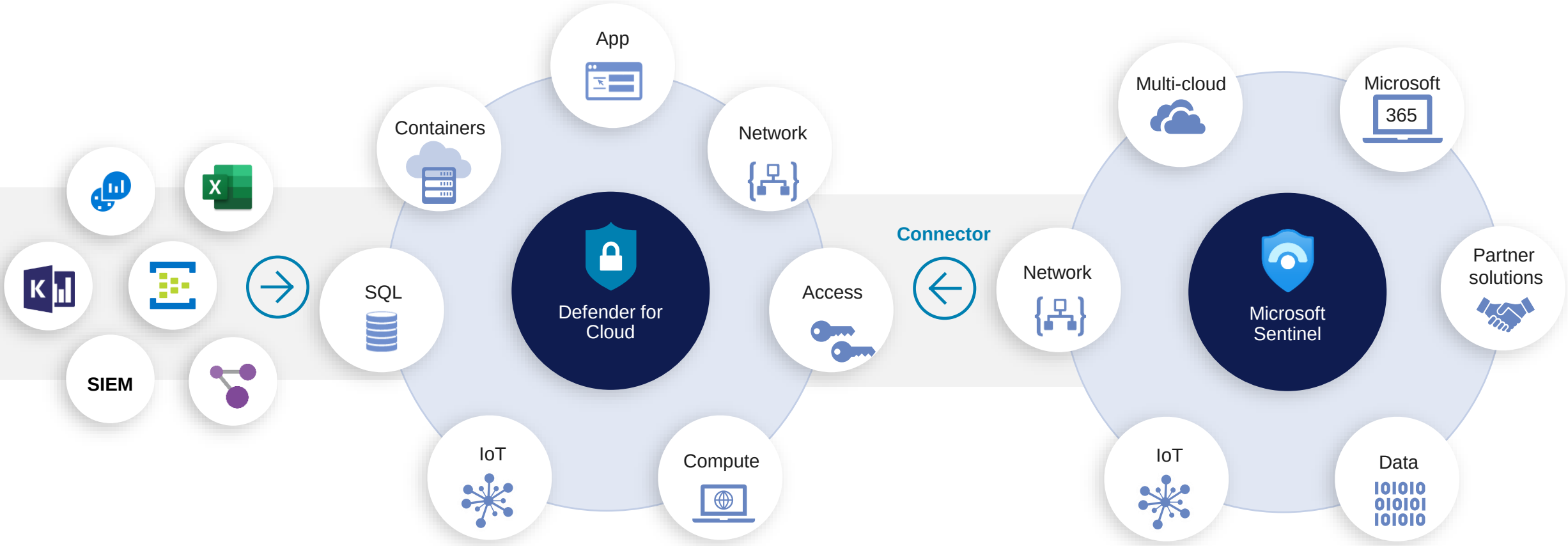


Defender for Cloud is a unified infrastructure security management system that strengthens the security posture of your data and provides advanced threat detection across your workloads in the cloud.

Defender for Cloud Architecture



Threat Protection for Cloud at Scale



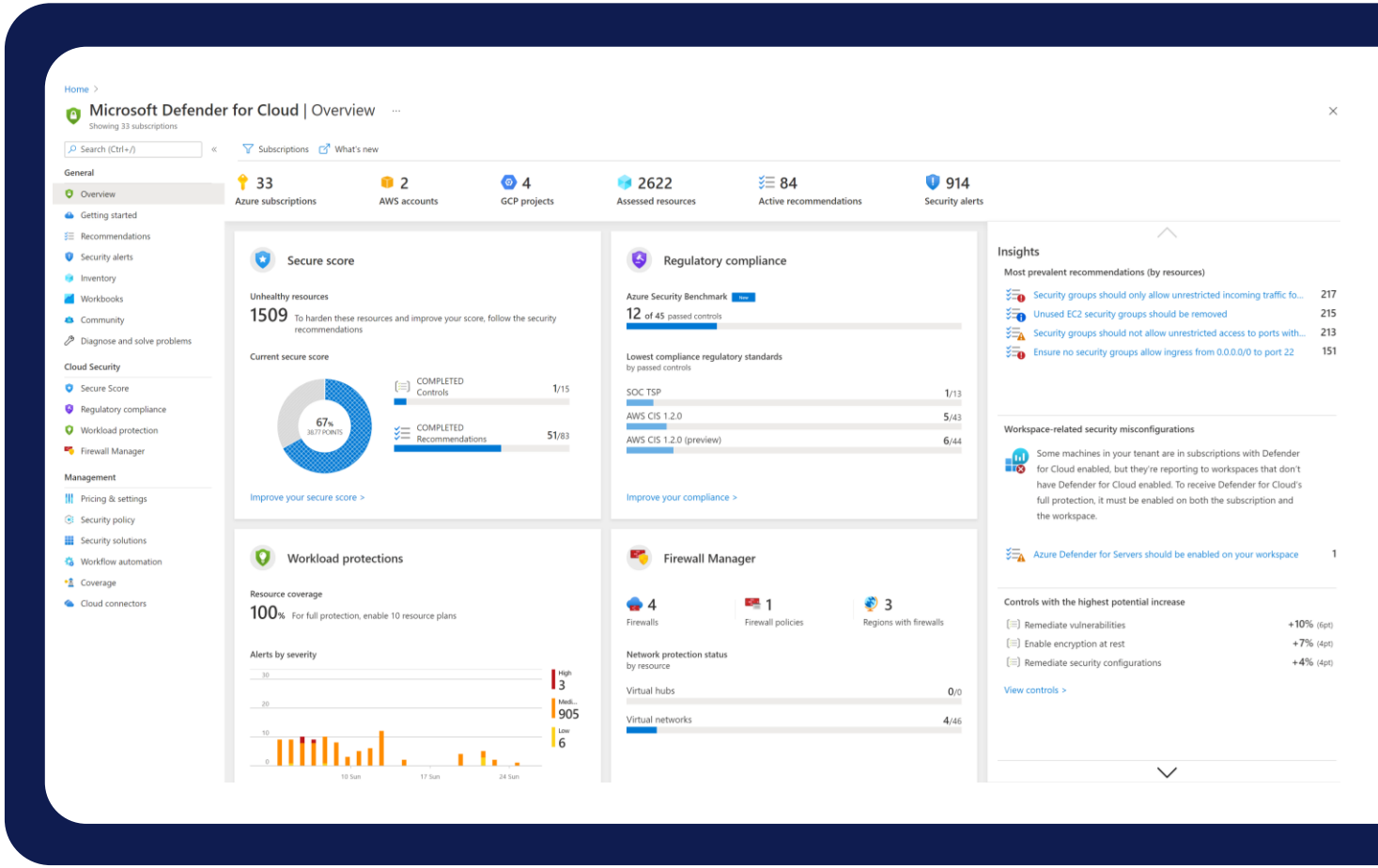
Microsoft Defender
Cloud Workload Protection

Microsoft Sentinel
Cloud Native SIEM

2. Cloud Security Posture Management

The Security Dashboard

- Unified resource view
- All your cloud resources in one place: Azure, AWS, on premises and other clouds
- Focused views for security posture, compliance, and workload protection
- Clear & simple view
- Identify all your security related stats at a glance
- Emphasis on visibility & clear KPIs



Security Posture Management With Secure Score

Gain instant insight into the security state of your cloud workloads

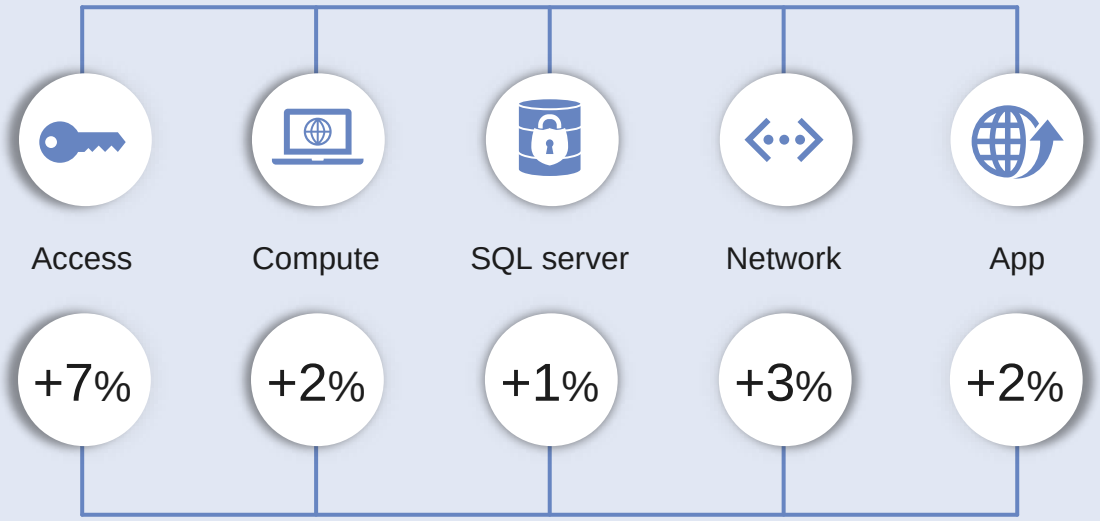
Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes

Speed up regulatory compliance

Granular control of Secure Score

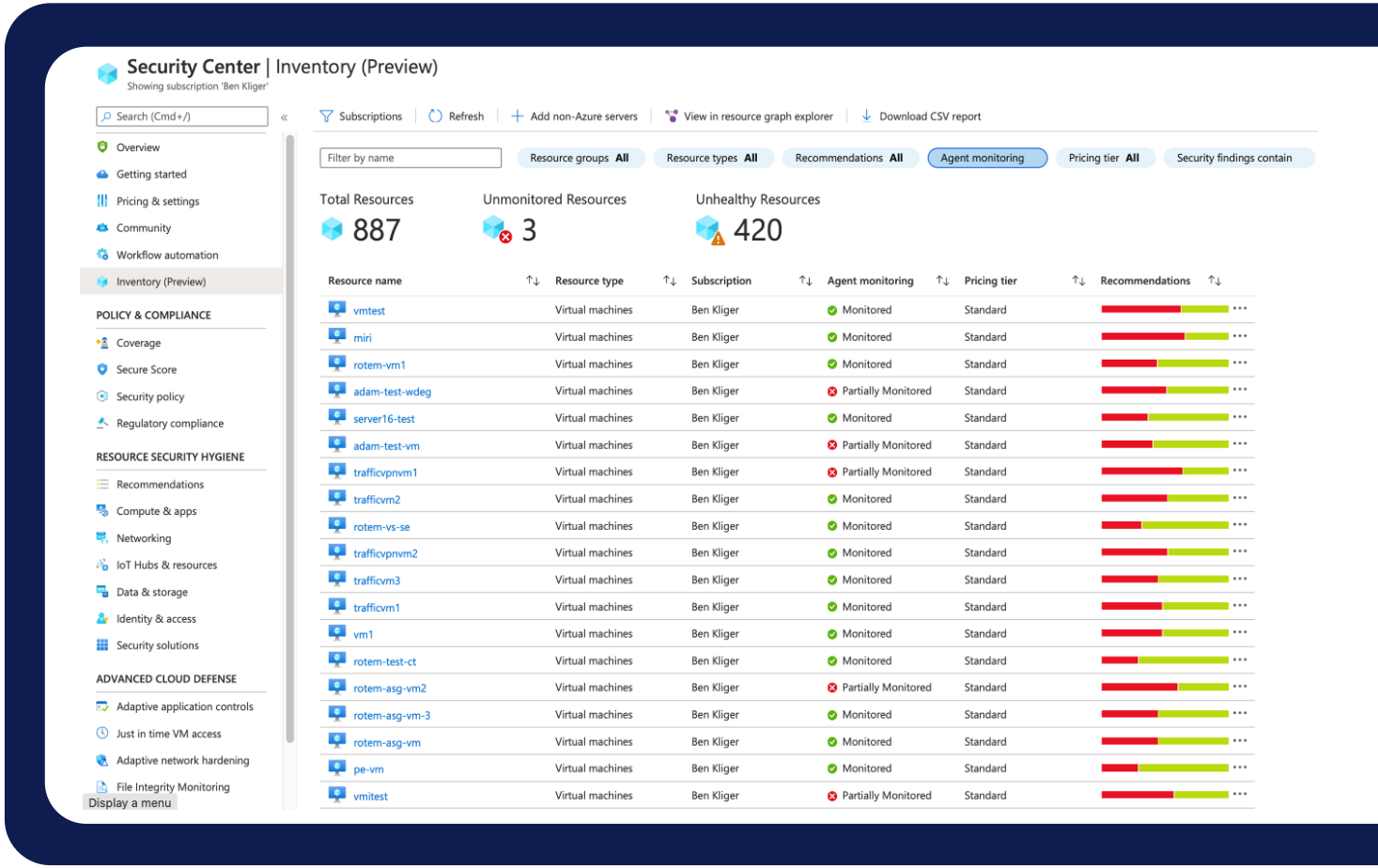
Evaluated Categories



Secure Score Impact

Inventory View – Improved Visibility Across the Entire Estate

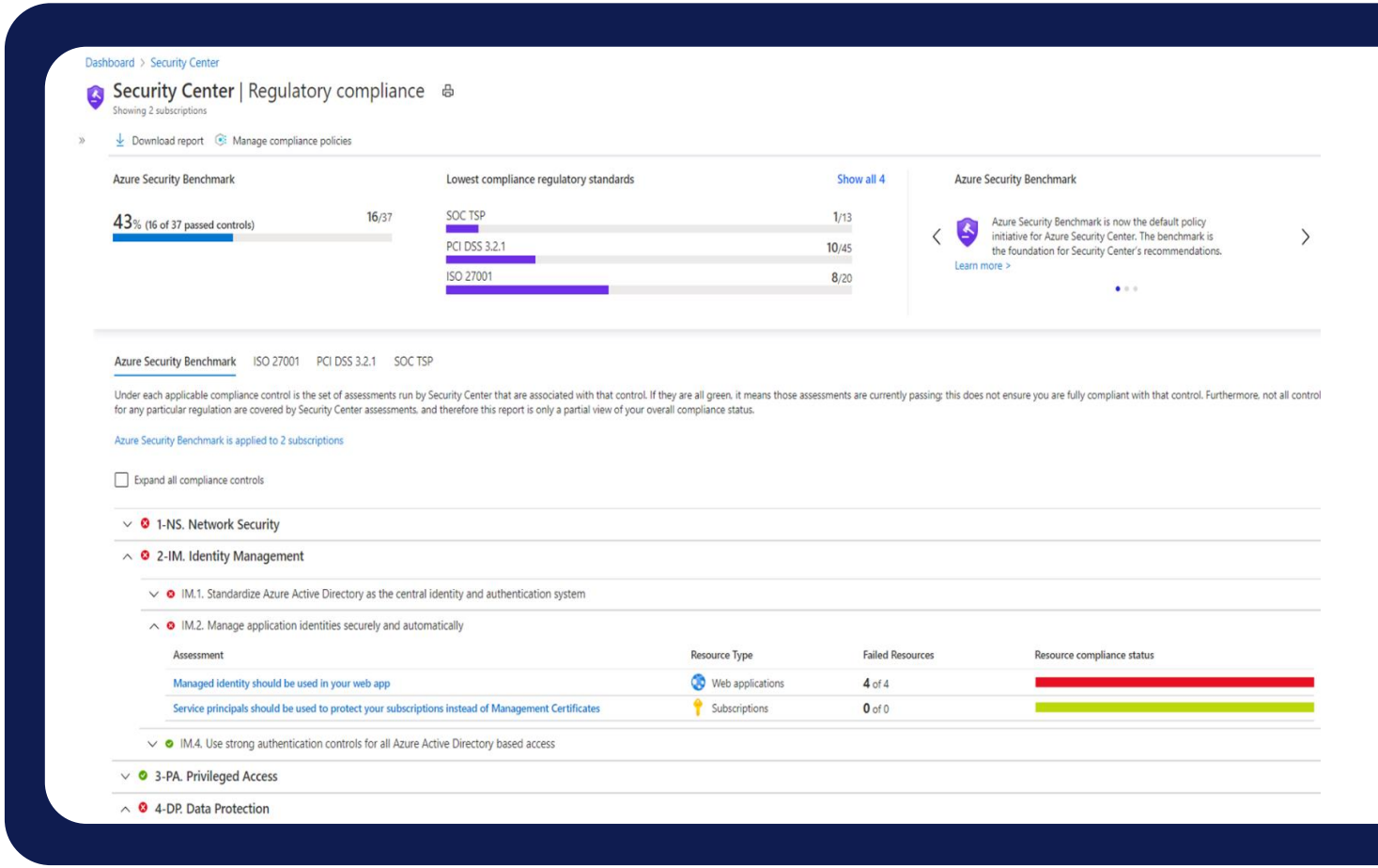
- Single view of all monitored resources
- Easy filtering, sorting and cross-referencing experience
- Continue exploration in Azure Resource Graph & export to CSV
- Management of resources



Google Cloud aws Azure

Compliance Management and Assessment

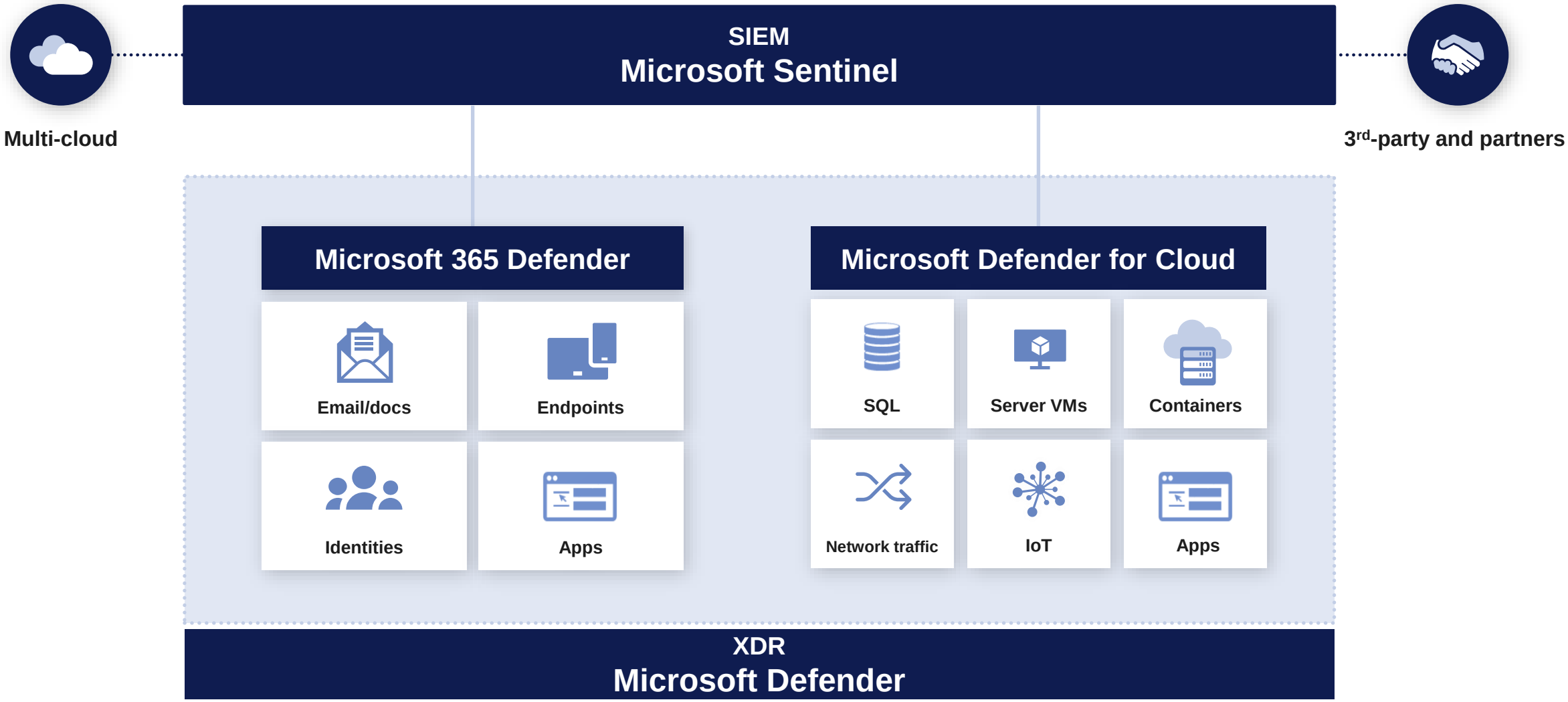
- Demonstrate compliance status, based on continuous assessments of Azure resources
- Monitor AWS and GCP resources with multi-cloud support
- Azure Security Benchmark monitoring enabled by default, fully aligned with Secure Score
- Support common industry standards, as well as custom initiatives based on Azure Policy
- Overview of compliance status and report download



Google Cloud aws Azure

3. Cloud Workload Protection

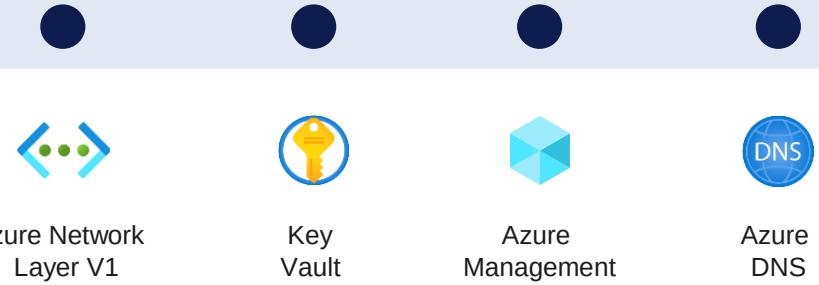
Integrated Threat Protection for Your Enterprise



Threat Protection for Cloud and Hybrid Workloads

Threat protection for common cloud resources

Threat protection for Azure service layer



Microsoft Defender for Servers

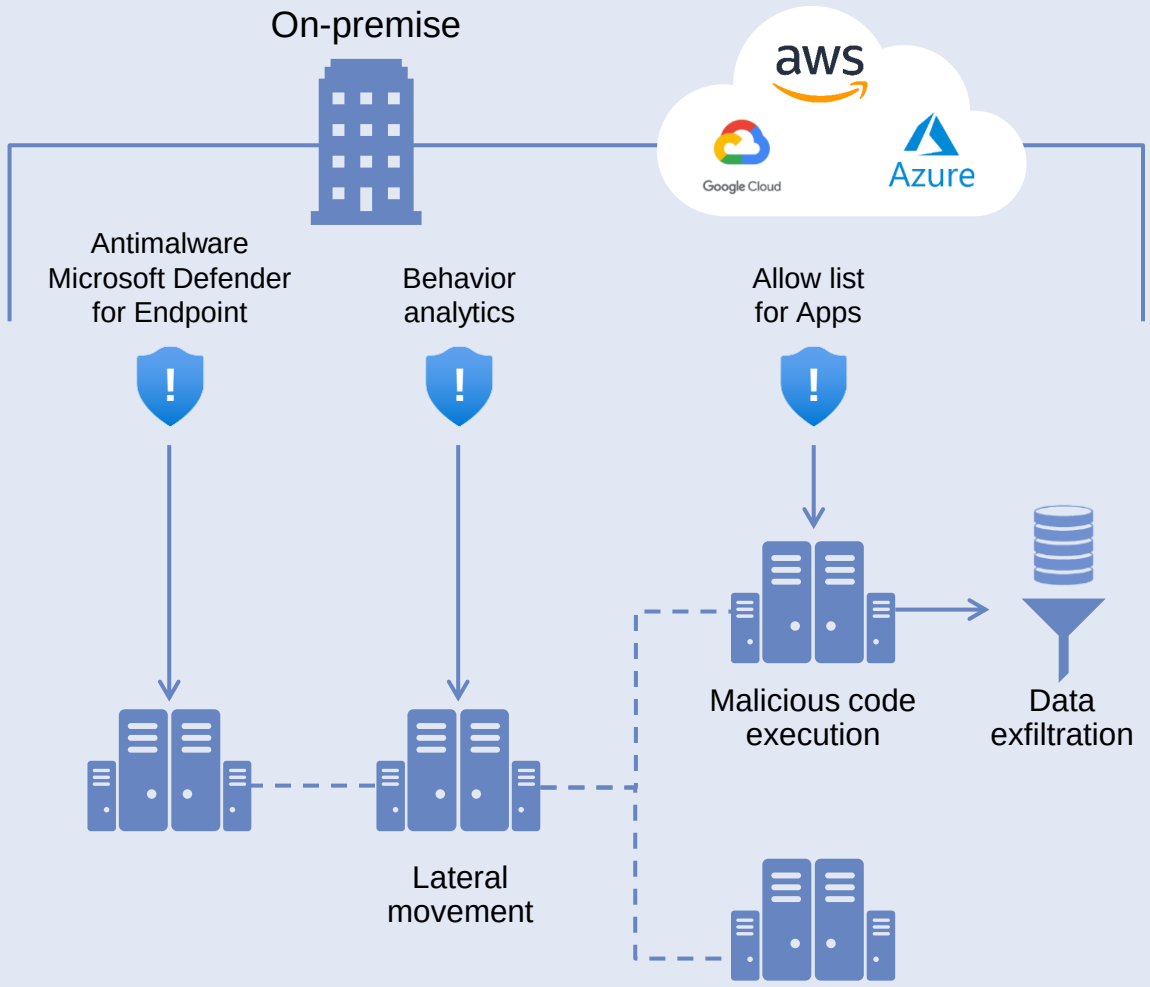
Protect Linux and Windows servers from threats

Reduce open network ports

- Use Just-in-Time VM to control access to commonly attacked management ports
- Limit open ports with adaptive network hardening

Block malware with adaptive application controls

Protect Windows servers and clients with the integration of Microsoft Defender for Endpoint and protect Linux servers



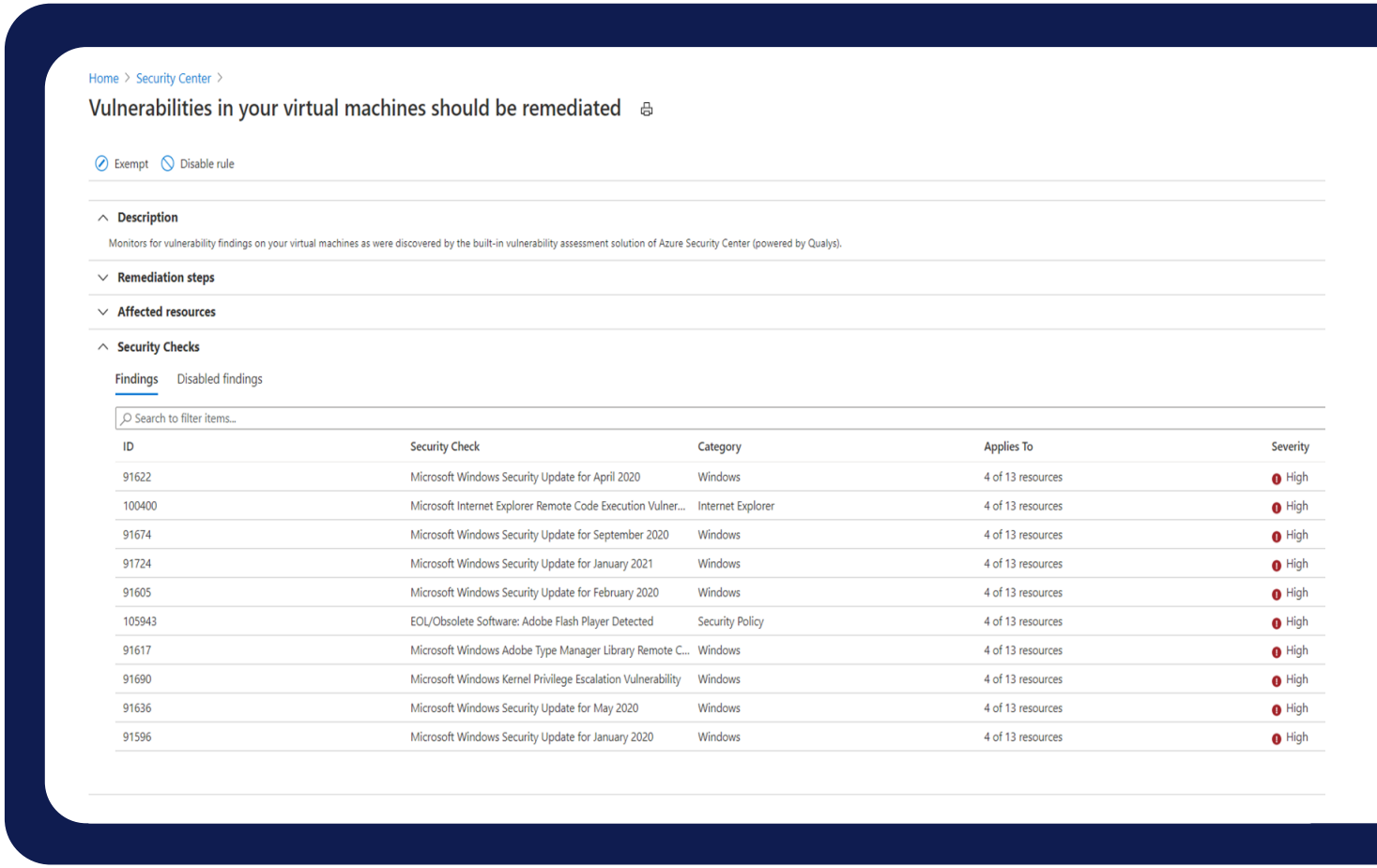
Turn on Built-in Vulnerability Assessment for VMs: Available as Part of Microsoft Defender for Servers

Automated deployment of the vulnerability scanner

Continuously scans installed applications to find vulnerabilities for Linux & Windows VMs

Visibility to the vulnerability findings in Security Center portal and APIs

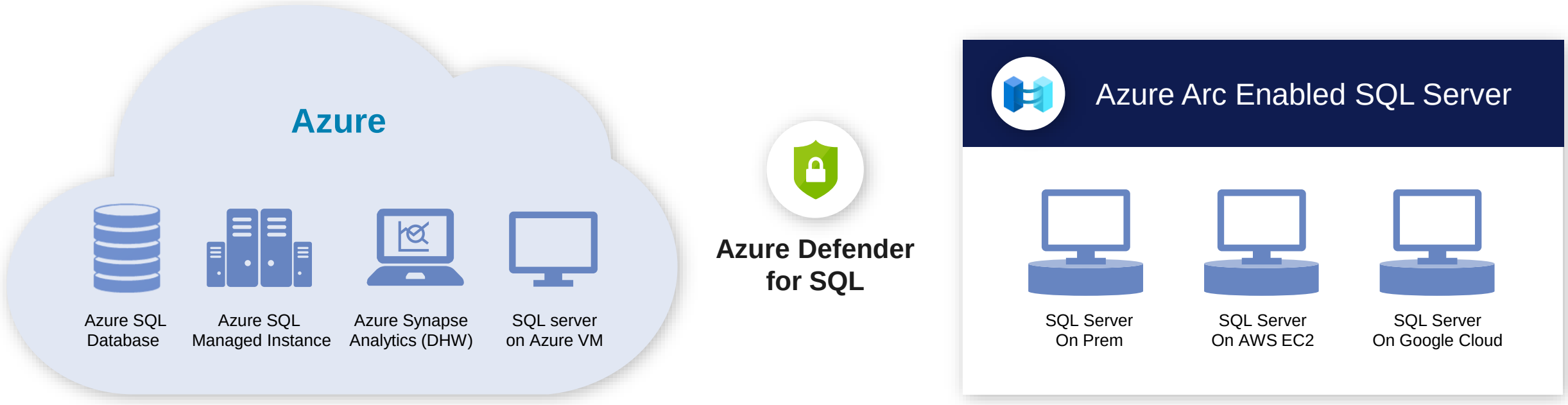
Powered by Qualys



Google Cloud aws Azure

Microsoft Defender for SQL

Protect SQL Server anywhere: in Azure, on premises or in other clouds

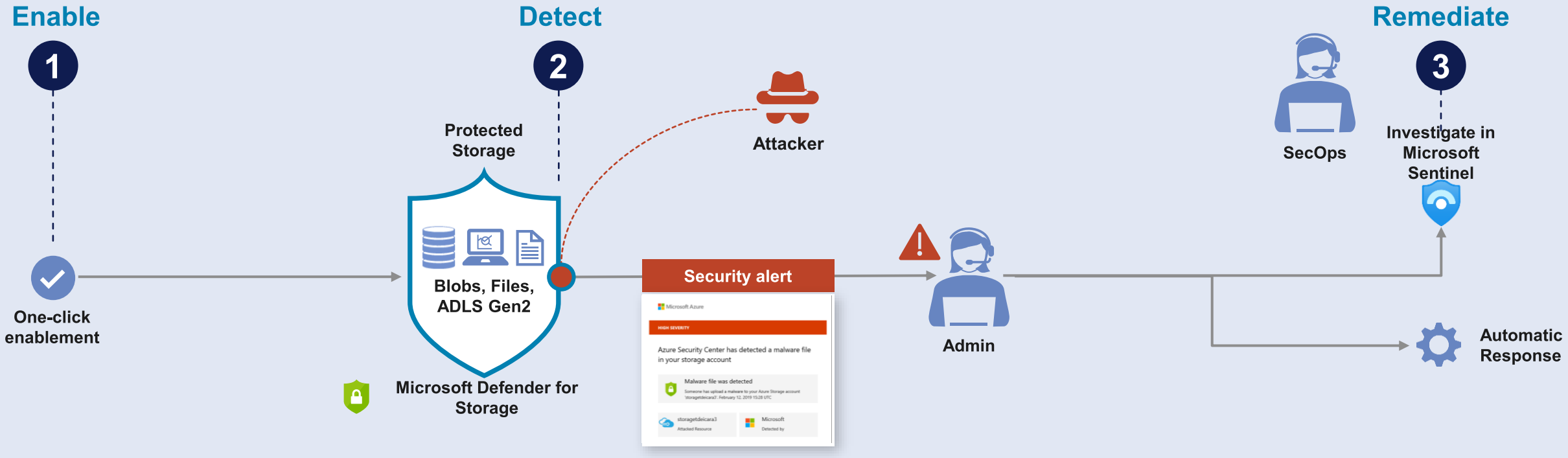


Advanced Threat Protection: detect unusual and harmful attempts to breach SQL servers across hybrid estate

Vulnerability Assessment: discover and remediate security misconfigurations in SQL servers across hybrid estate

Microsoft Defender for Storage

Protect blobs containers, file shares and data lakes in Azure



Azure Native Security

Built-in within Azure with 1-click enablement. Protect Azure Blob, Azure Files and Data Lakes

Rich Detection Suite

Covering top Storage threats powered by Microsoft Threat Intelligence

Response at Scale

Reduce frictions preventing and responding to top threats

Centralized & Integrated

Centralize security across all data assets managed by Azure and built-in integration with Azure Sentinel & Azure Purview

Microsoft Defender for Containers

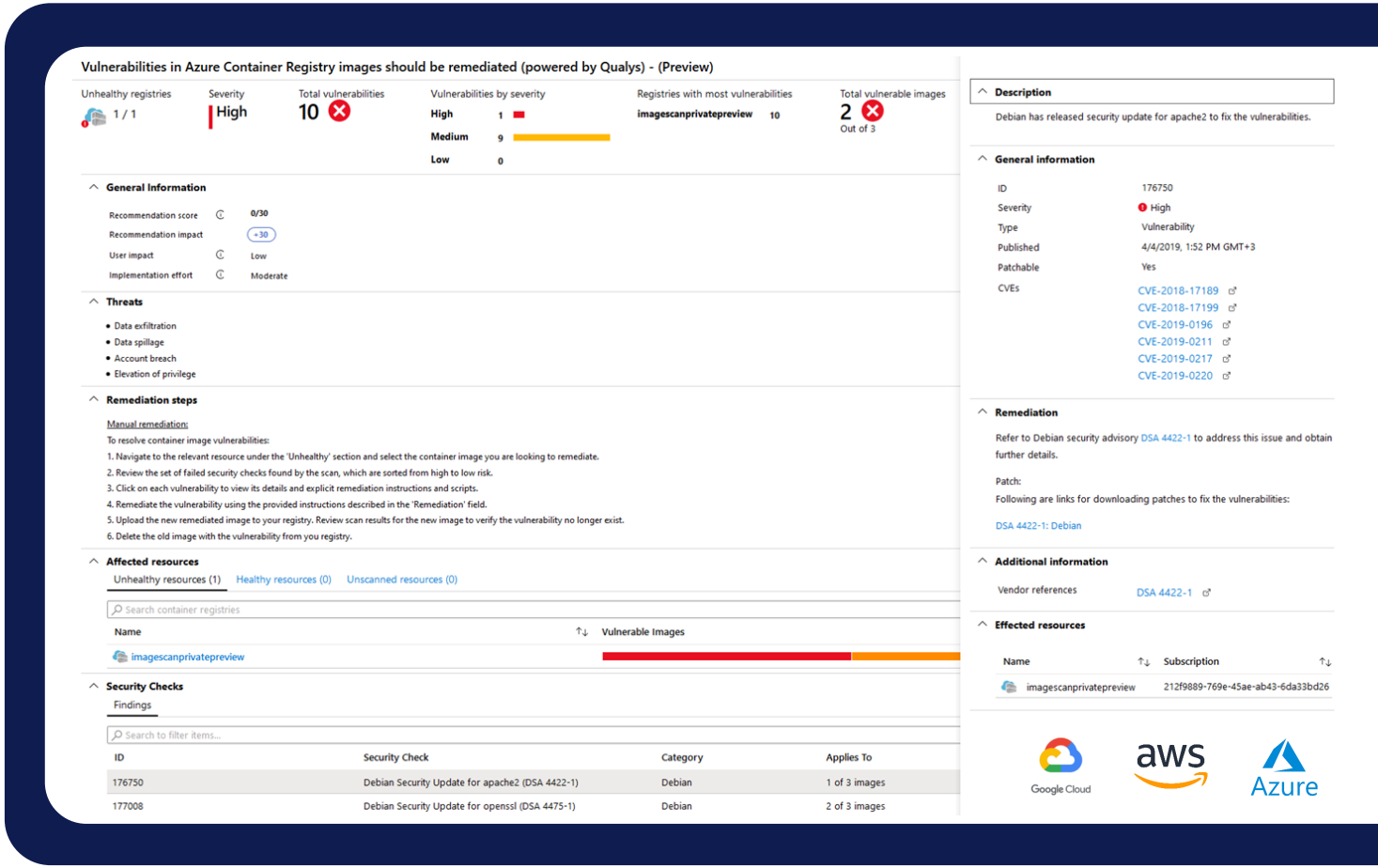
Seamless deployment and configuration

Image scan in ship

Discover ACR registries, scan all pushed images, and get visibility to vulnerable images

Image scan in runtime

Continuous scanning of recently pulled images



Microsoft Defender for Containers

AKS cluster and nodes hygiene

Harden and audit AKS clusters according to Azure security benchmarks and follow the Docker CIS benchmark on container nodes

Runtime threat detection

Detect suspicious behavior in Kubernetes workloads via a unique agentless approach leveraging Kubernetes audit log, in addition to Kubernetes workers dedicated detections

Admission control policy management

Mandate/audit security best practices on Kubernetes workloads

Kubernetes Attack Matrix

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral Movement	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data destruction
Compromised images in registry	Bash / CMD inside container	Writable hostPath mount	Cluster-admin biding	Delete K8S events	Mount service principle	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal network	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

Breadth Threat Protection With Microsoft Defender

Protect ANY Workload in Azure

Microsoft Defender for Resource Manager

Automatically monitors all resource management operations performed in your organization

Detects suspicious Azure Resource Management activities and sends alerts

Microsoft Defender for DNS

Continuously monitors all DNS queries from your Azure resources

Sends alerts when suspicious activity is detected

Microsoft Defender for Key Vault

Detect unusual and potentially harmful attempts to exploit Azure Key Vault

Automation Example

NTT DATA

Trusted Global Innovator