Microsoft

Azure Security Center Deep Dive

Base-IT | Markus Nowak | Lead Architect Azure & Datacenter | Teamleitung

Agenda

- Cloud Security Considerations
- Using Azure Security Center to improve security posture
- New announcements and innovations

Cloud security is a shared responsibility

Shared responsibility model for cloud security

Microsoft's commitment	Joint responsibility
Secure foundation	**Microsoft provides built-in controls**
Physical assets	Virtual machines and networks
Datacenter operations	Apps and workloads
Cloud infrastructure	Data

Hybrid cloud requires new approach to security

Infrastructure increasingly distributed across public clouds and on-premises datacenter

Rapidly changing resources

Increasingly sophisticated attacks

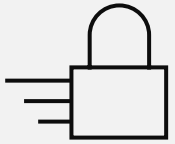
Security skills are in short supply

Improving security across hybrid cloud environments

Azure Security Center

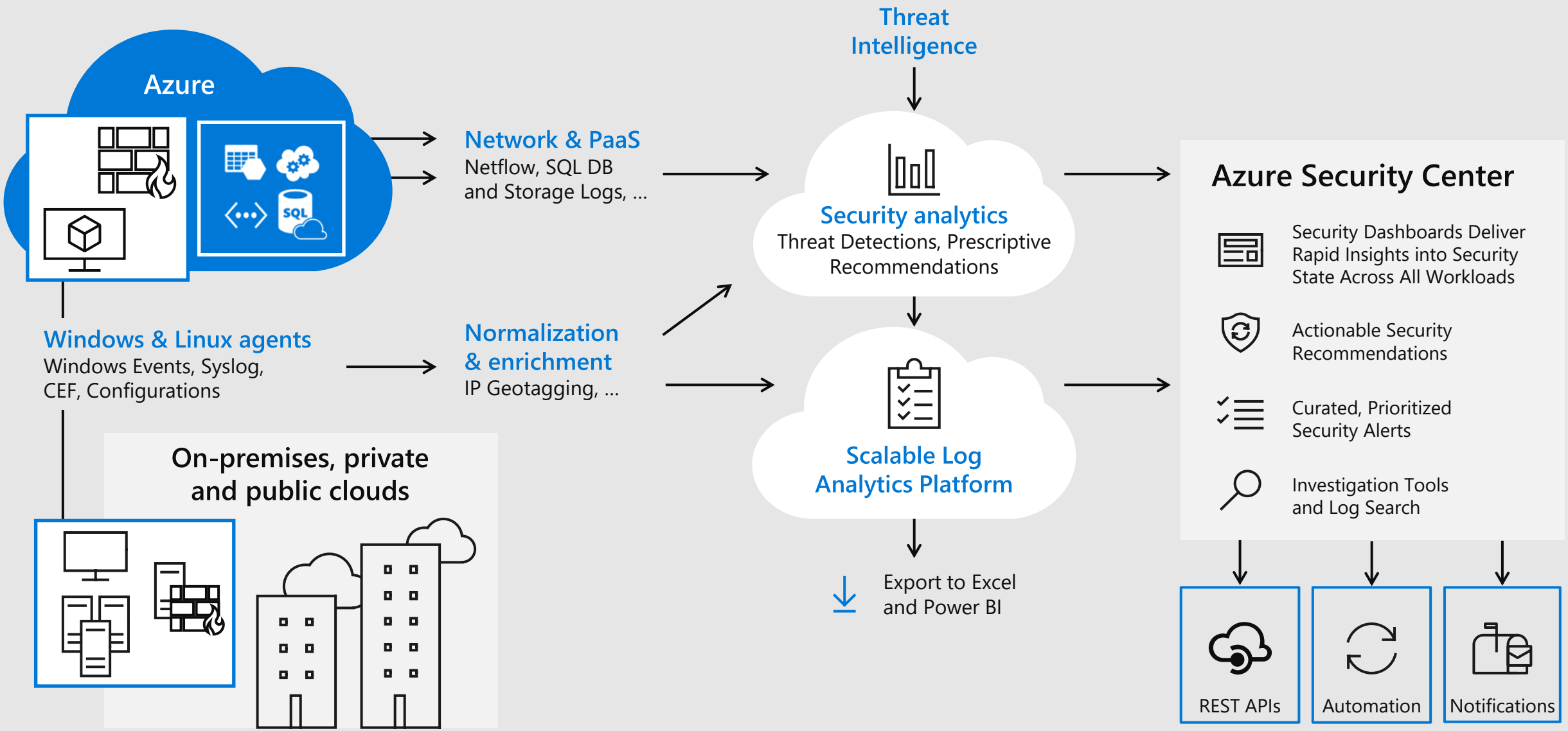
Strengthen security posture

Protect against threats



Get secure faster

Security Center Architecture



Strengthen security posture

Manage organizational security policy and compliance

Continuously assess security state

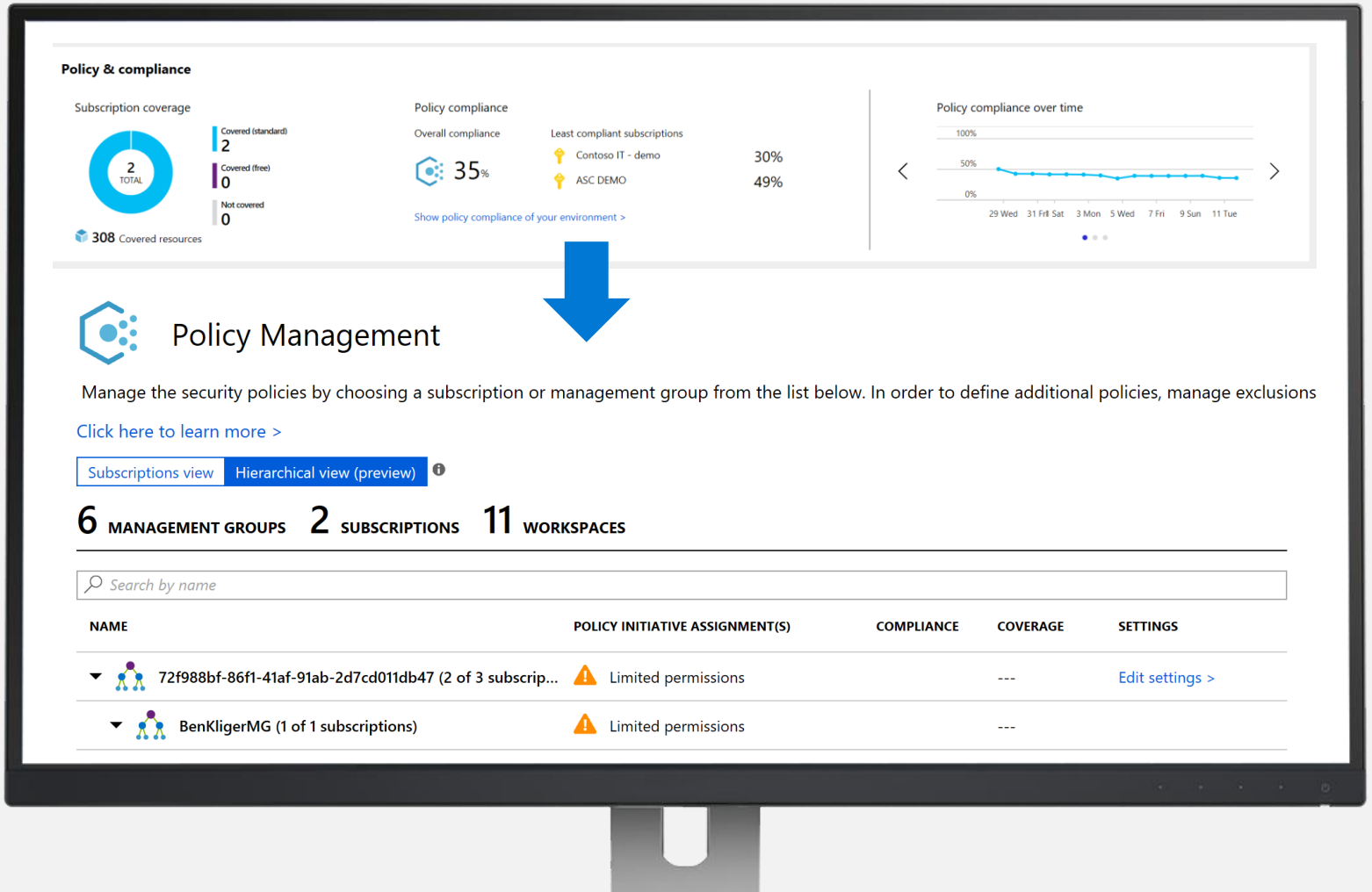
Optimize and improve security by configuring recommended controls

Manage organizational security policy and compliance

Review coverage for Azure Security Center across different subscriptions

Easily set centralized security policies across multiple subscriptions

Track and review policy compliance and governance over time

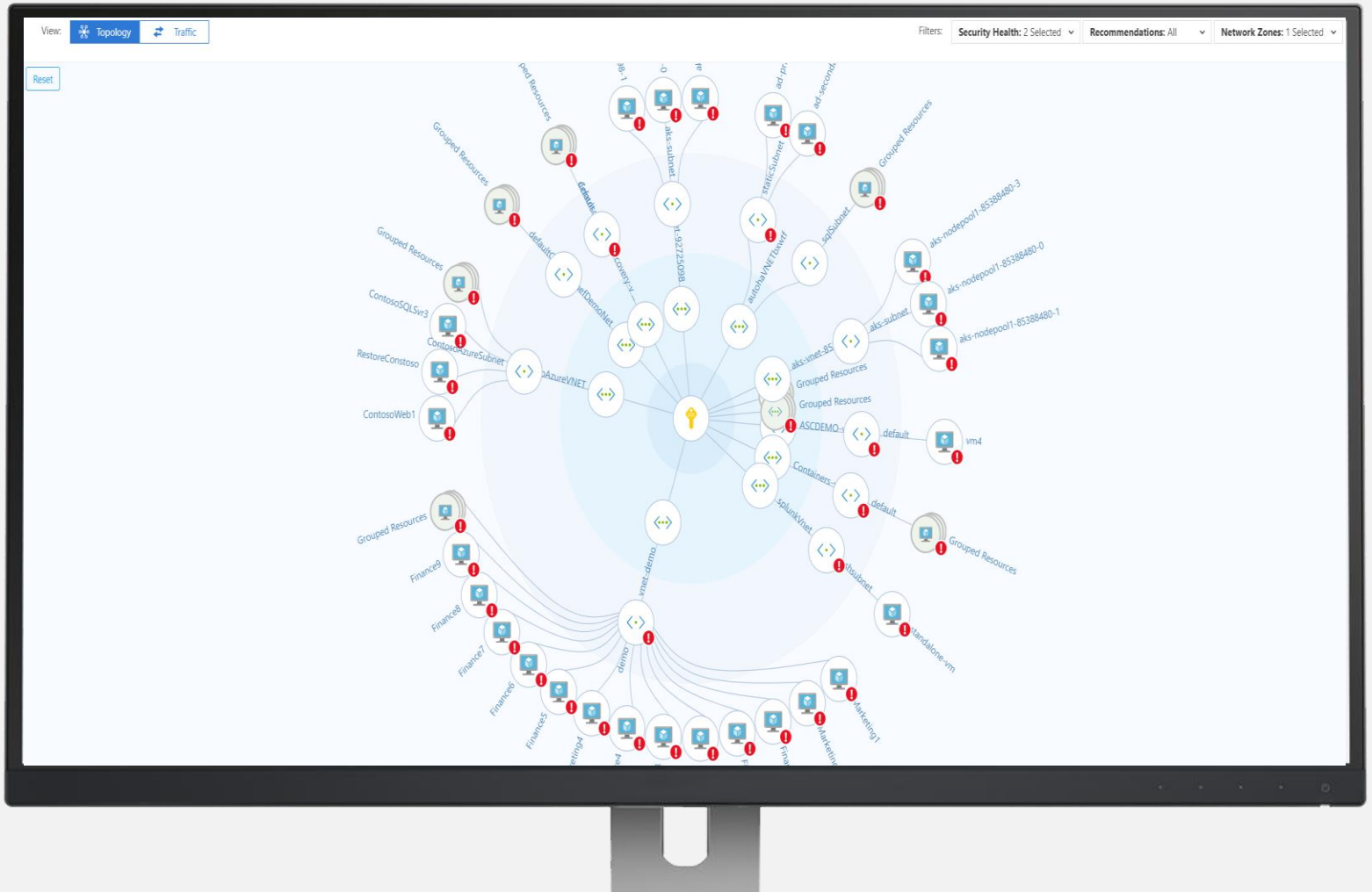


Continuously assess and optimize with Secure Score

Get insights on the security state across your infrastructure

Prioritized recommendations with a security score

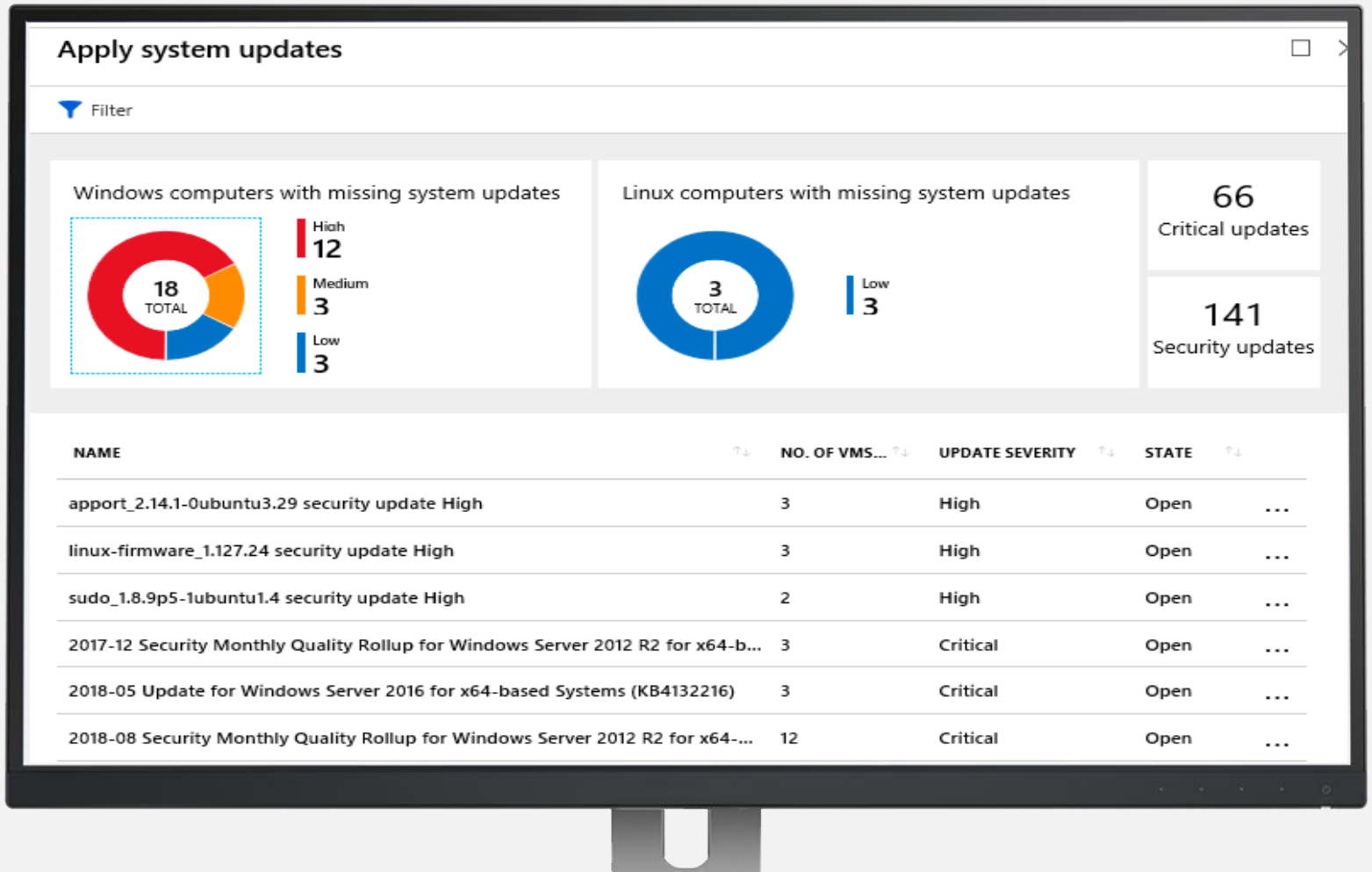
Understand the network topology and visualize configurations



Optimize and improve security by configuring recommended controls

Apply a secure configuration standard with built-in recommendations

Reduce attack surface by applying proactive hygiene measures



Protect against threats

- Detect and block advanced malware and threats for servers
- Detect threats across IaaS and PaaS services using advanced analytics
- Reduce exposure to brute force attacks
- Protect data services against malicious attacks

Detect and block advanced malware for Windows and Linux servers

Detect threats on servers with behavior analytics and machine learning

Get Windows server EDR with the integration of Windows Defender ATP

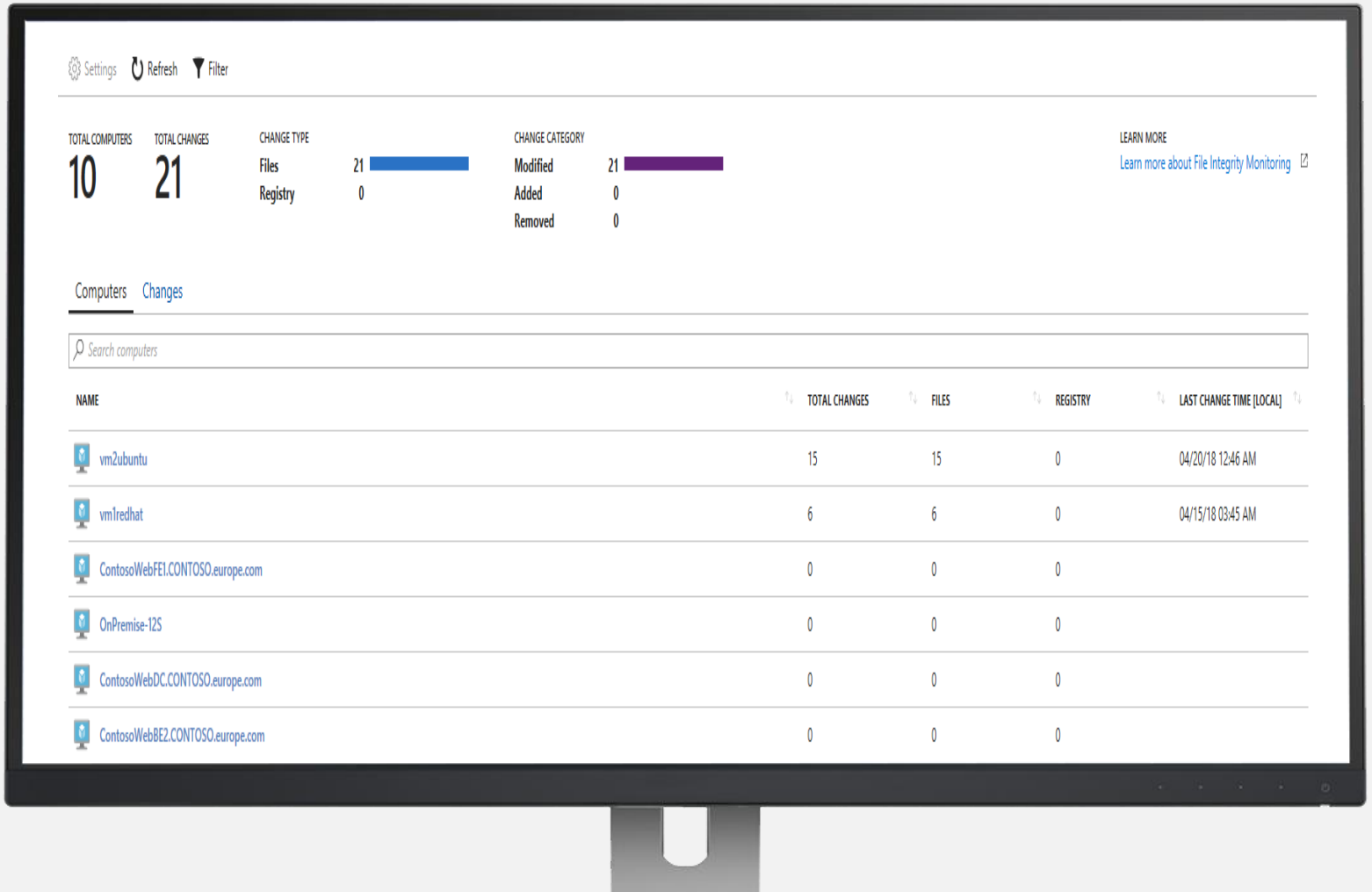
Automate application whitelisting with a ML based solution

File integrity monitoring

Examines files and registries of the operating system, application software, and others for changes that might indicate an attack

Validates the integrity of Windows files, Windows registry, and Linux files.

Select the files that you want to be monitored by enabling File Integration Monitoring (FIM)

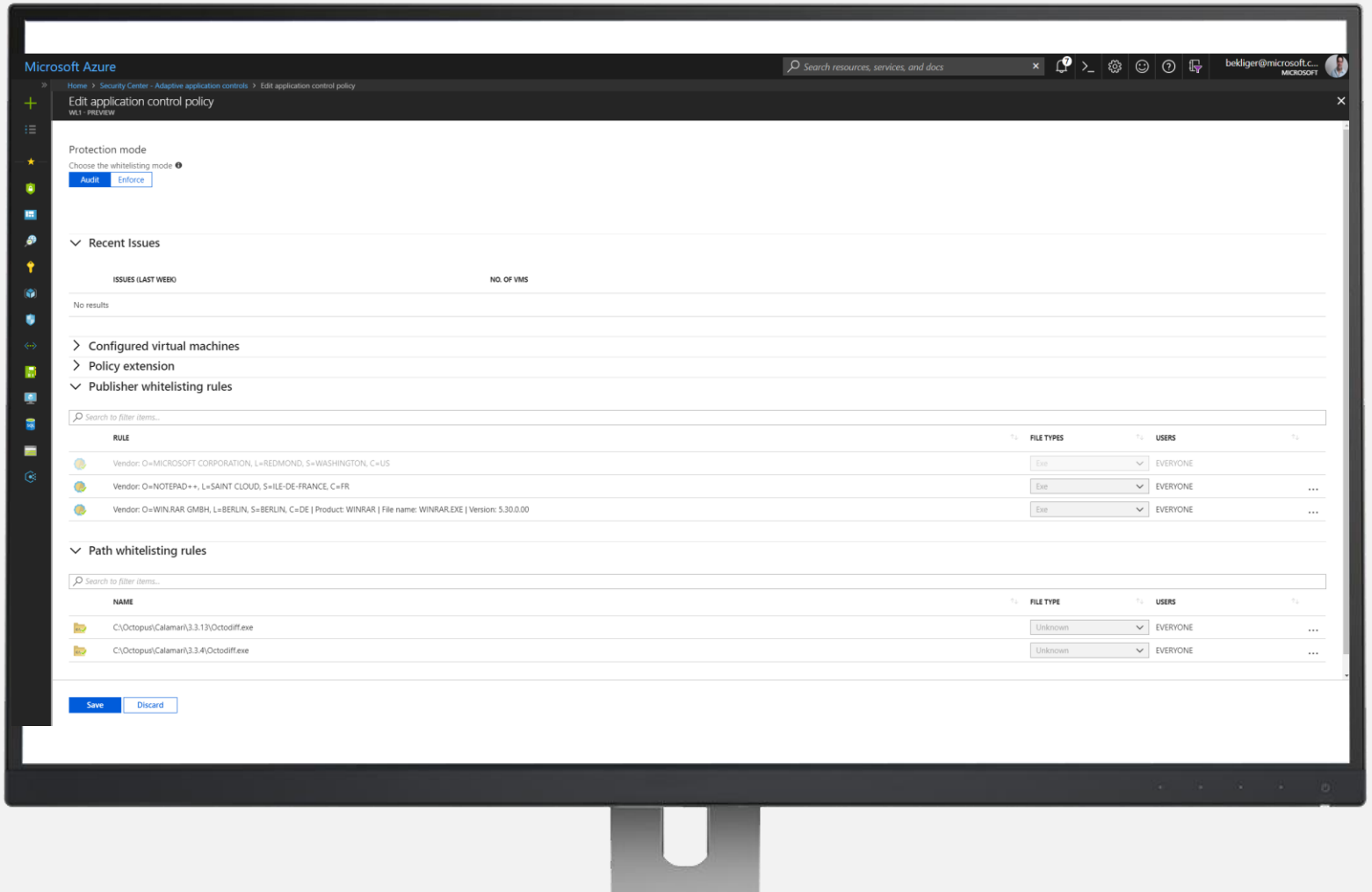


Adaptive application controls

Control which applications can run on your VMs located in Azure with Adaptive Application Controls to help harden your VMs against malware

Adaptive whitelisting learns application patterns

Simplify management with recommended whitelists

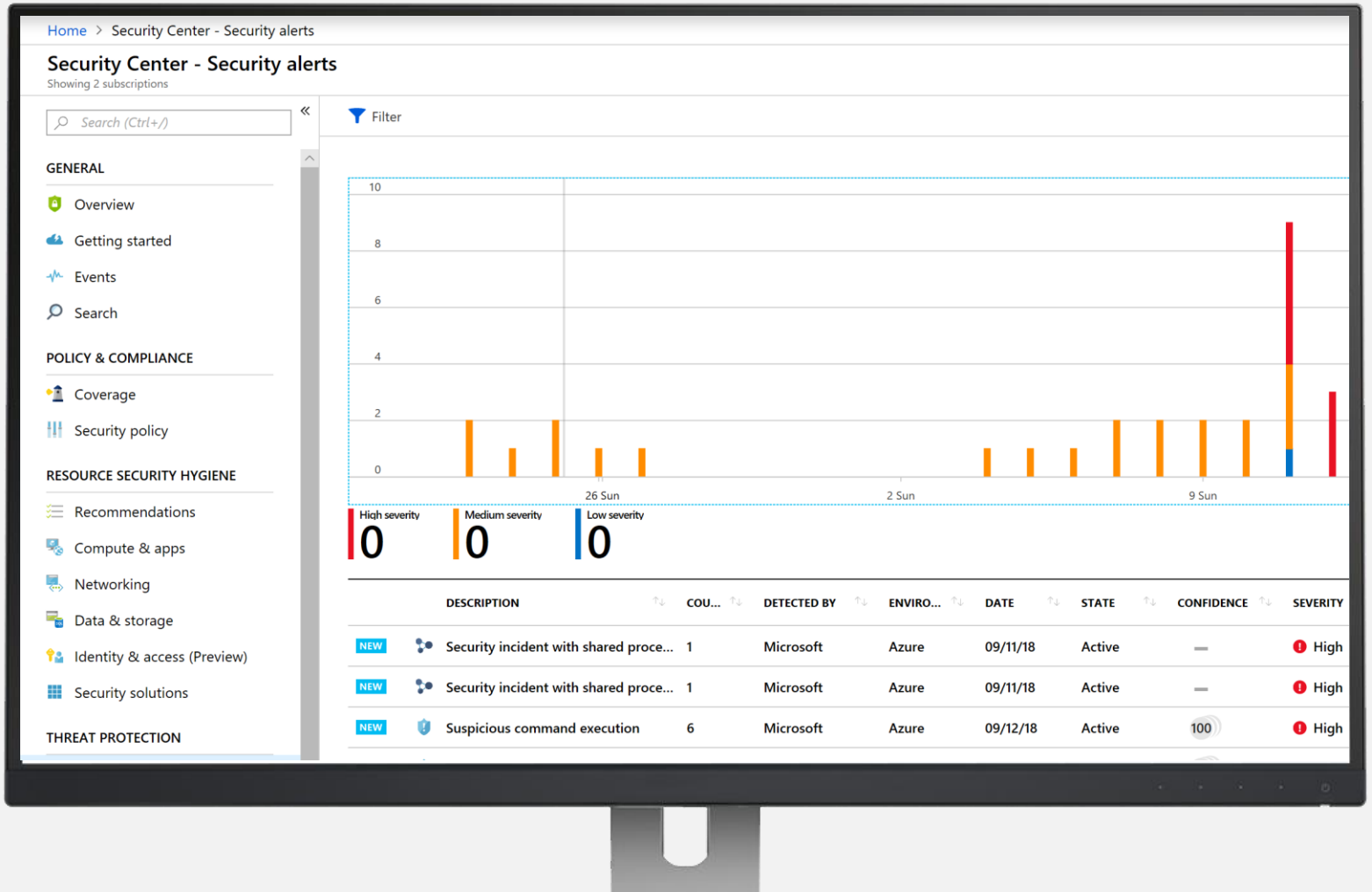


Detect threats across services

Detect threats targeting Azure services such as Azure App Services, Azure SQL, Storage services and more

Get Azure UEBA with the integration of Microsoft Cloud App Security

Investigate and respond to an attack with ASC Fusion kill chain analysis



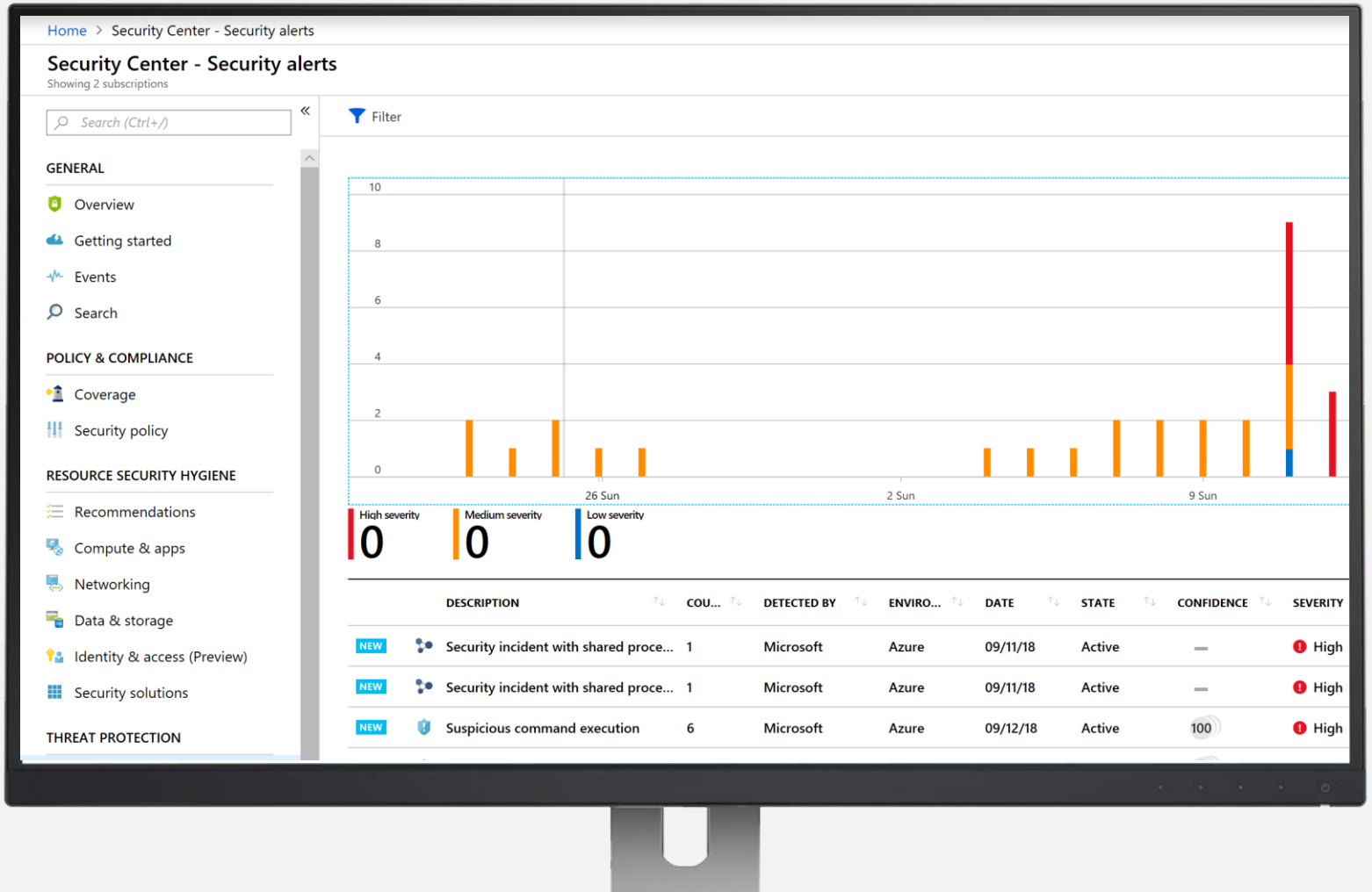
Detect threats across services using advanced analytics

Threat intelligence- looks for known malicious actors using Microsoft global threat intelligence

Advanced analytics- use anomaly detection and behavioral analytics to detect malicious behaviors

Fusion- automatically correlating events and alerts from across the kill chain to map an attack campaign

Windows server EDR- integrated solution with Windows Defender ATP



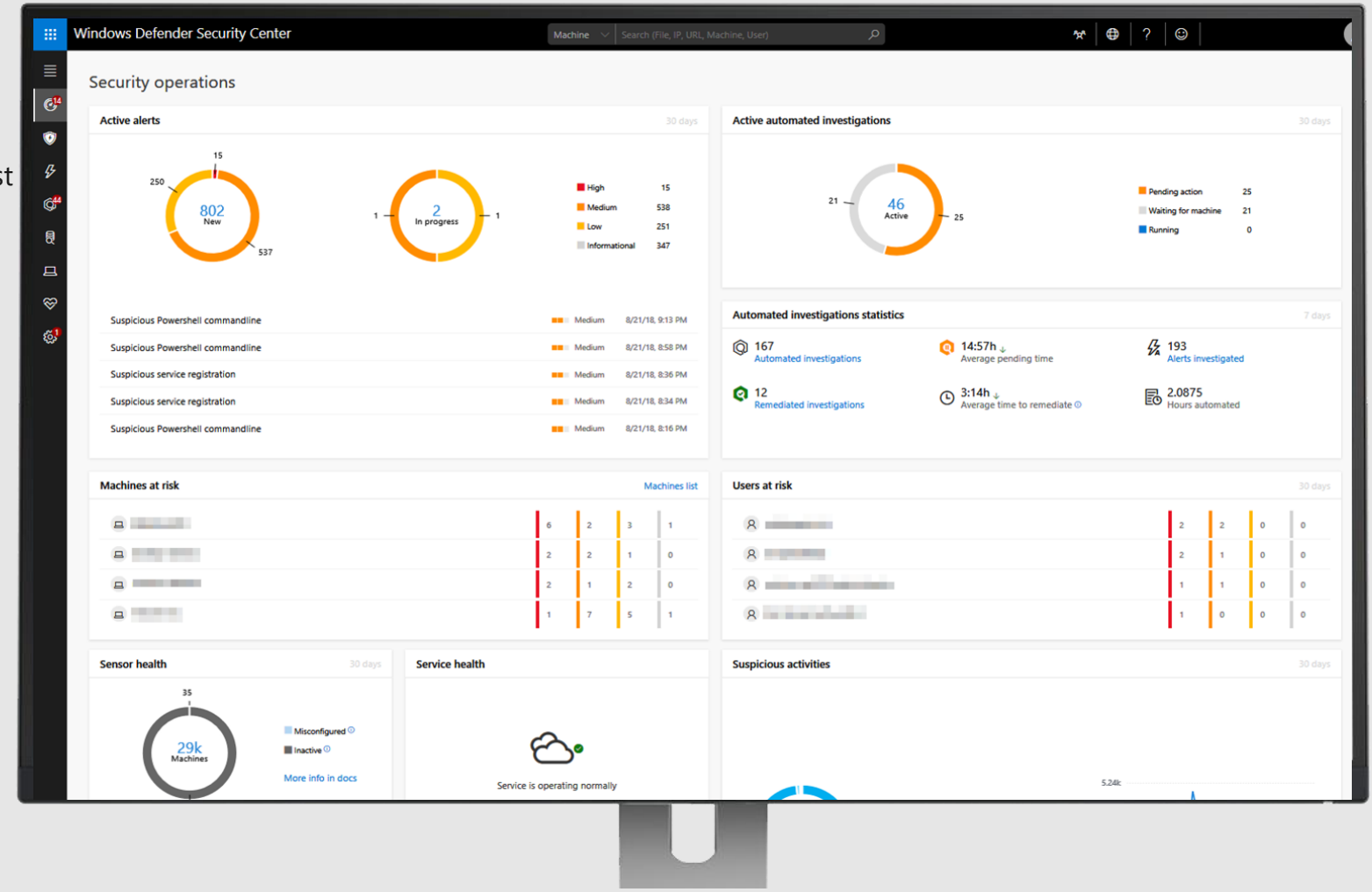
Windows Server EDR with Windows Defender ATP

Leveraging Windows Defender ATP support for Windows Server

Next-gen post breach detection sensors
Windows Defender ATP sensor for Windows Servers that collect a vast array of behavioral signals to enable advanced attack detection & investigation.

Behavior-based, cloud-powered breach detection
Signature-less, intelligent, behavioral, machine learning and past attack detections.
Actionable, correlated alerts for known and unknown adversaries.

Unique threat intelligence knowledge base
Unparalleled threat optics provide detailed actor profiles
1st and 3rd party threat intelligence data.



WINDOWS Defender ATP Alerts in ASC

Automatic onboarding through ASC

Windows Defender ATP sensor is automatically enabled on Windows Servers that are onboarded to ASC

Integrated alerts

Windows Defender ATP alerts are available in the ASC console

Detailed machine investigation

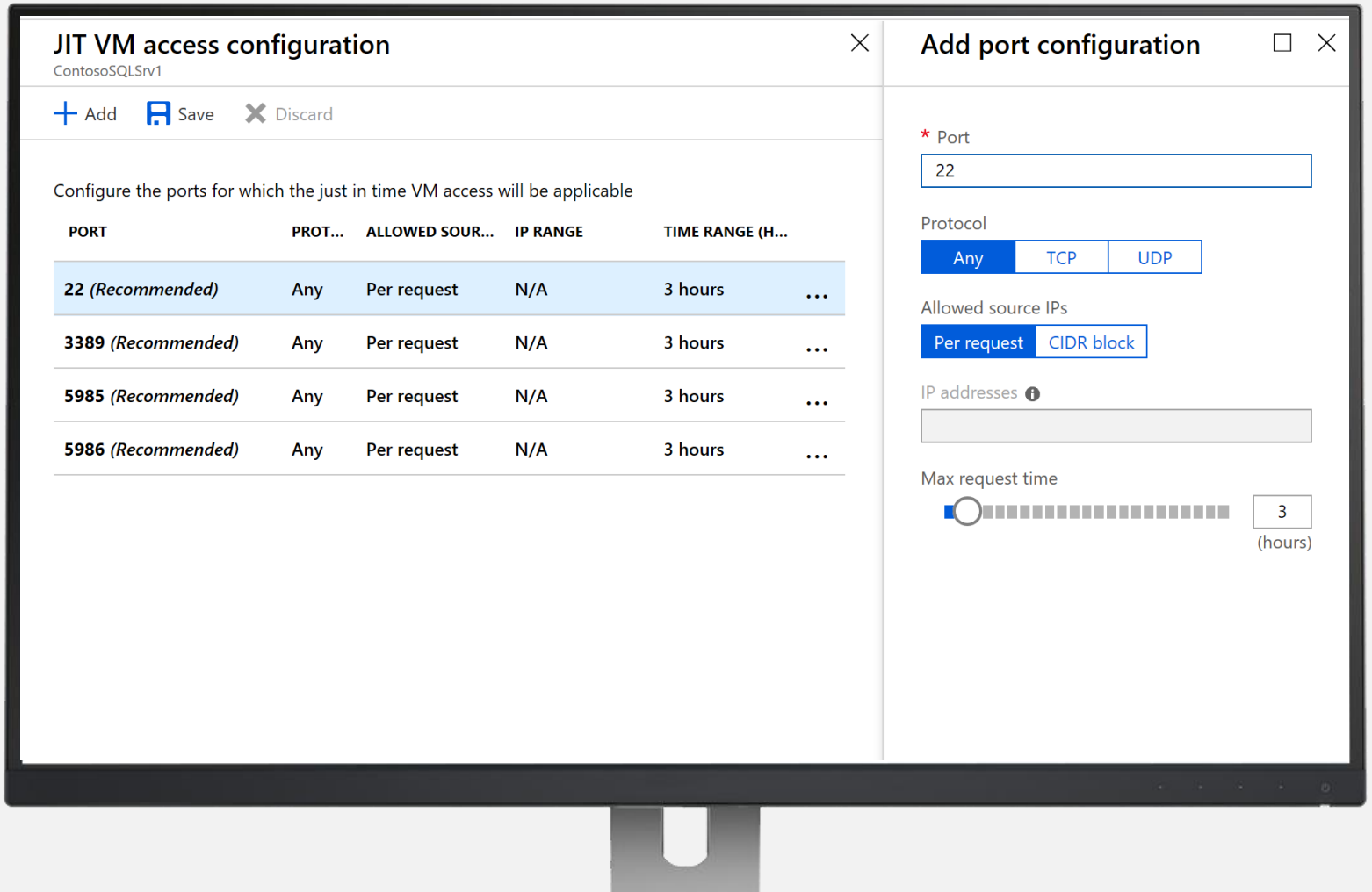
ASC customers can access Windows Defender ATP console to perform detailed investigation to uncover scope of breach

DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Security incident detected	1	Microsoft	Azure	09/07/17	Active	High
Security incident detected	1	Microsoft	Azure	09/01/17	Active	High
Security incident detected	1	Microsoft	Azure	08/26/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	09/10/17	Active	High
Modified system binary discovered in dump...	1	Microsoft	Azure	09/07/17	Active	High
Successful RDP brute force attack	1	Microsoft	Azure	09/06/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	09/04/17	Active	High
Suspicious process executed	1	Microsoft	Azure	09/03/17	Active	High

Limit exposure to brute force attacks

Reduce access to VM ports only when it is needed with Just-in-Time VM Access

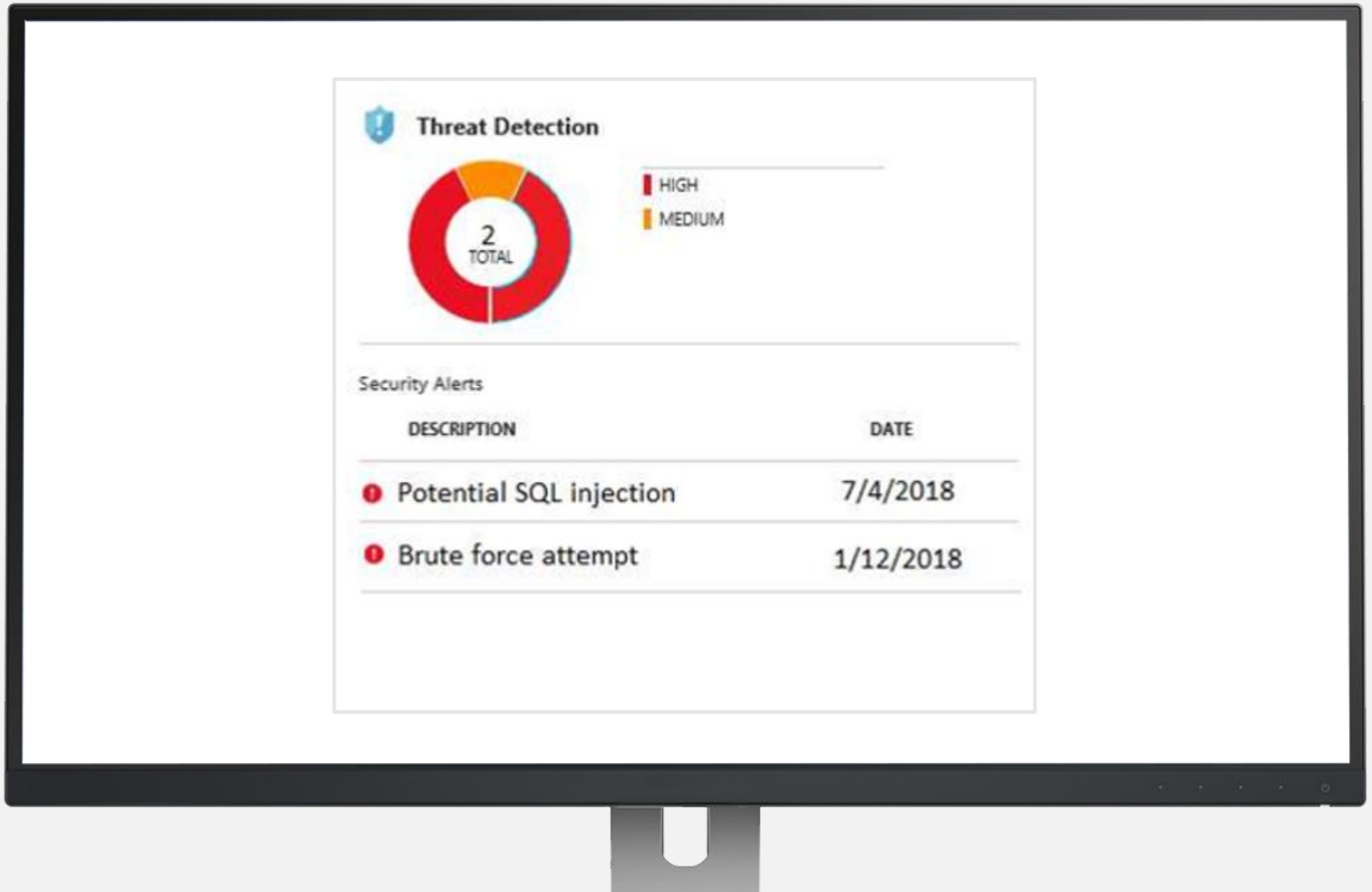
Access automatically granted
for selected ports, and for limited time, approved users and source IPs



Protect data services

Assess potential vulnerabilities across Azure SQL and Storage services

Classify and audit access to sensitive data in Azure SQL



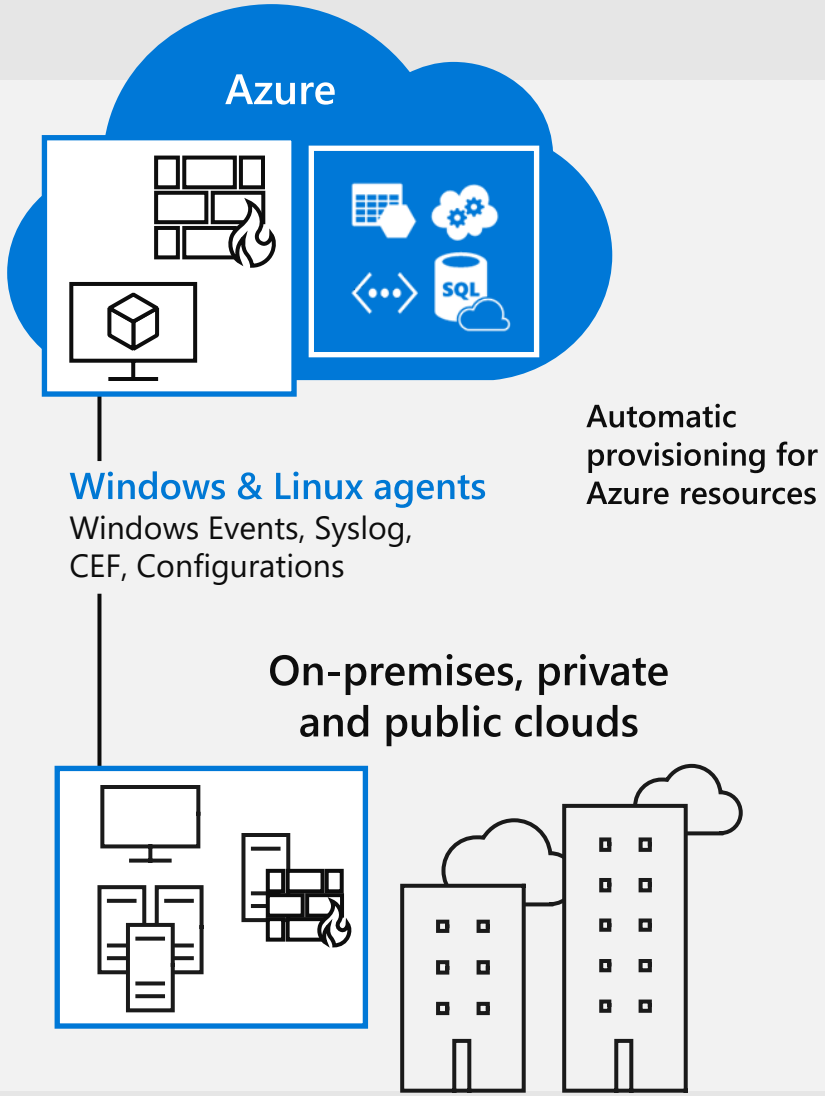
Get secure faster

Automatically discover and onboard Azure resources

Extend to server workloads running in other clouds and on-premises datacenter

Integrate with existing workflows and tools (SIEM, NG Firewall..)

Automatic onboarding & extending to hybrid cloud



Seamless Azure integration

Automatically discovers and monitors security of Azure resources

Extensive log collection

Protect servers running on other clouds and on-premise

Using PowerShell for Security Center tasks

 Onboarding assets (subscriptions) to ASC	Subscription RP registration Setting pricing tier Configure data collection (auto provisioning, WS to report to) Security contact configuration Security policy assignment
 Organizational security policy management	Security policy assignment/removal Security policy configuration Get compliance and recommendation data Get connected security solutions
 Threat monitoring	Get alerts
 Advanced prevention capabilities	Get JIT policy Apply/Remove JIT

Programmable capabilities

Each officially published API is automatically assigned with a PS counterpart

Composite/iterative operations can further be achieved with Powershell scripts

MG level APIs are not supported yet

ARM Templates

As ASC REST APIs become official, the ability to define a subscription level ARM template becomes possible – applying the ASC settings and setting default policies as part of automating the subscription creation process – thus having ASC configured on a subscription as its provisioned

Existing APIs

PUT+GET: Pricing, Workspace setting, Auto-provisioning, Security contact, JIT (also initiate JIT access request), Alerts, Tasks (Only the resource IDs to which recommendations exist and the task state)

GET: Compliance, Security solutions (discovered + external)

Missing APIs

PUT+GET: Recommendations (actual recommendation data), Security event tier settings, Baseline customization (might be redundant), Adaptive Application Controls, FIM

GET: Resource Health, Coverage

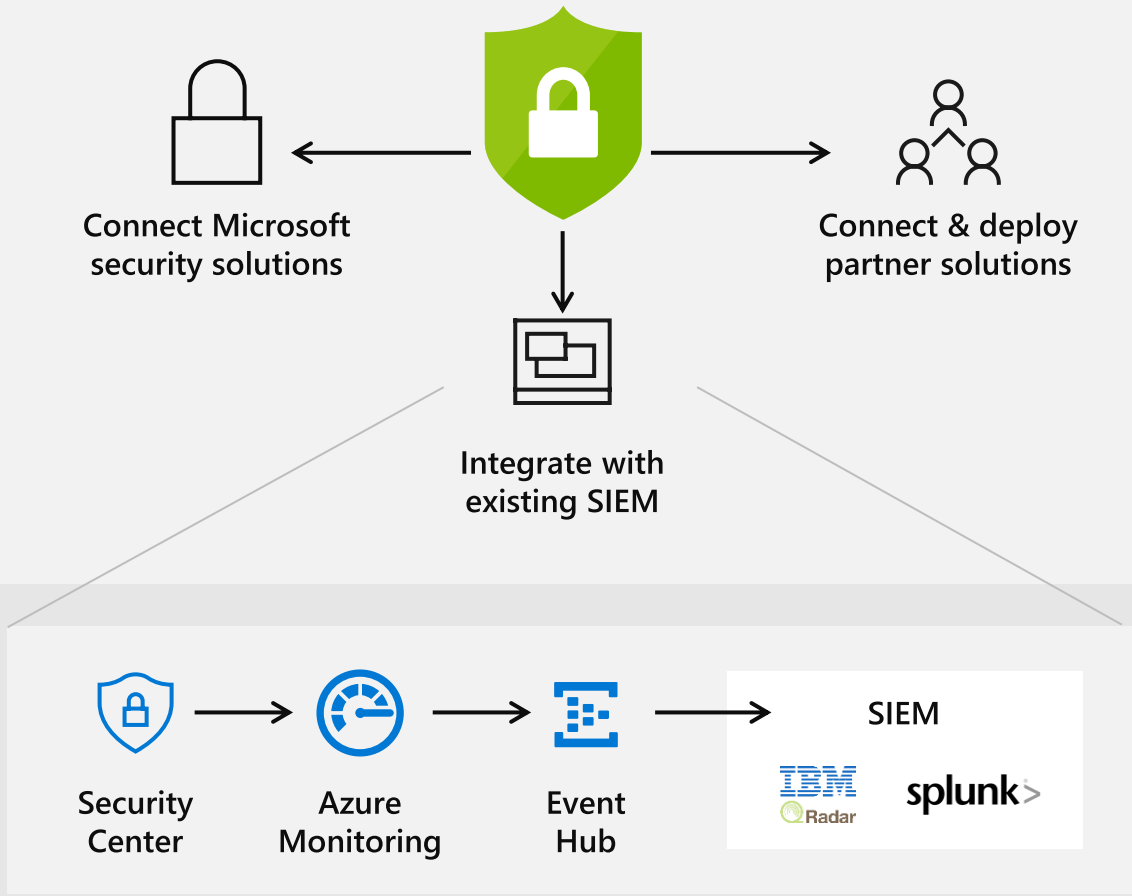
PUT: Connect security solutions/Add data sources, Run playbooks

Integrating with existing workflows and tools

Respond quickly to threats with automated workflows

Automation support with REST APIs and PowerShell cmdlts

Consolidate SOC insights by integrating with existing SIEM solution



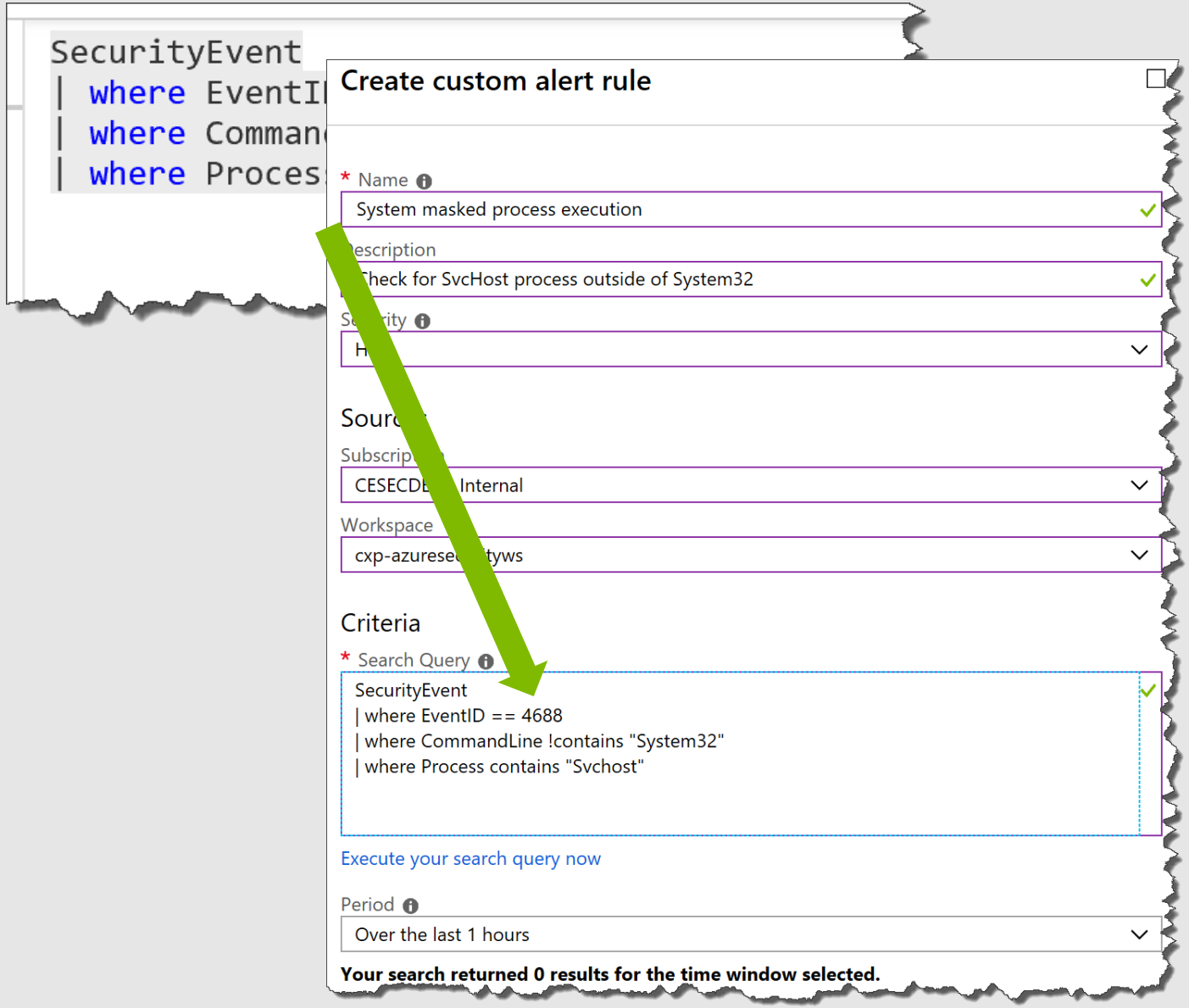
What is a custom alert?

A ‘Breadth’ check for indicators of compromise

1. Log Analytics query over Security Center-collected data

2. Save query as a Security Center Custom Alert

3. Build automation workflows when the alert fires

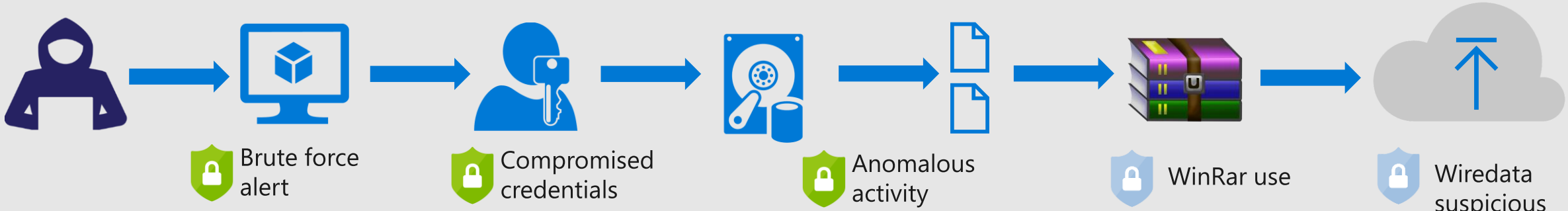


Custom alert example

Data ex-filtration example: *"Alert me when compression software is used in suspicious ways"*

Attack approaches:

1. Masking commands used with WinRAR
2. Spoofing System file names with other executables




```
SecurityEvent
| where
| search
| projec
```

```
SecurityEvent
| where TimeGenerated >= ago(2d)
| where ProcessName contains "svchost.exe"
| where SubjectUserSid != "S-1-5-18"
| where S
| where S
| where N
| where N
```

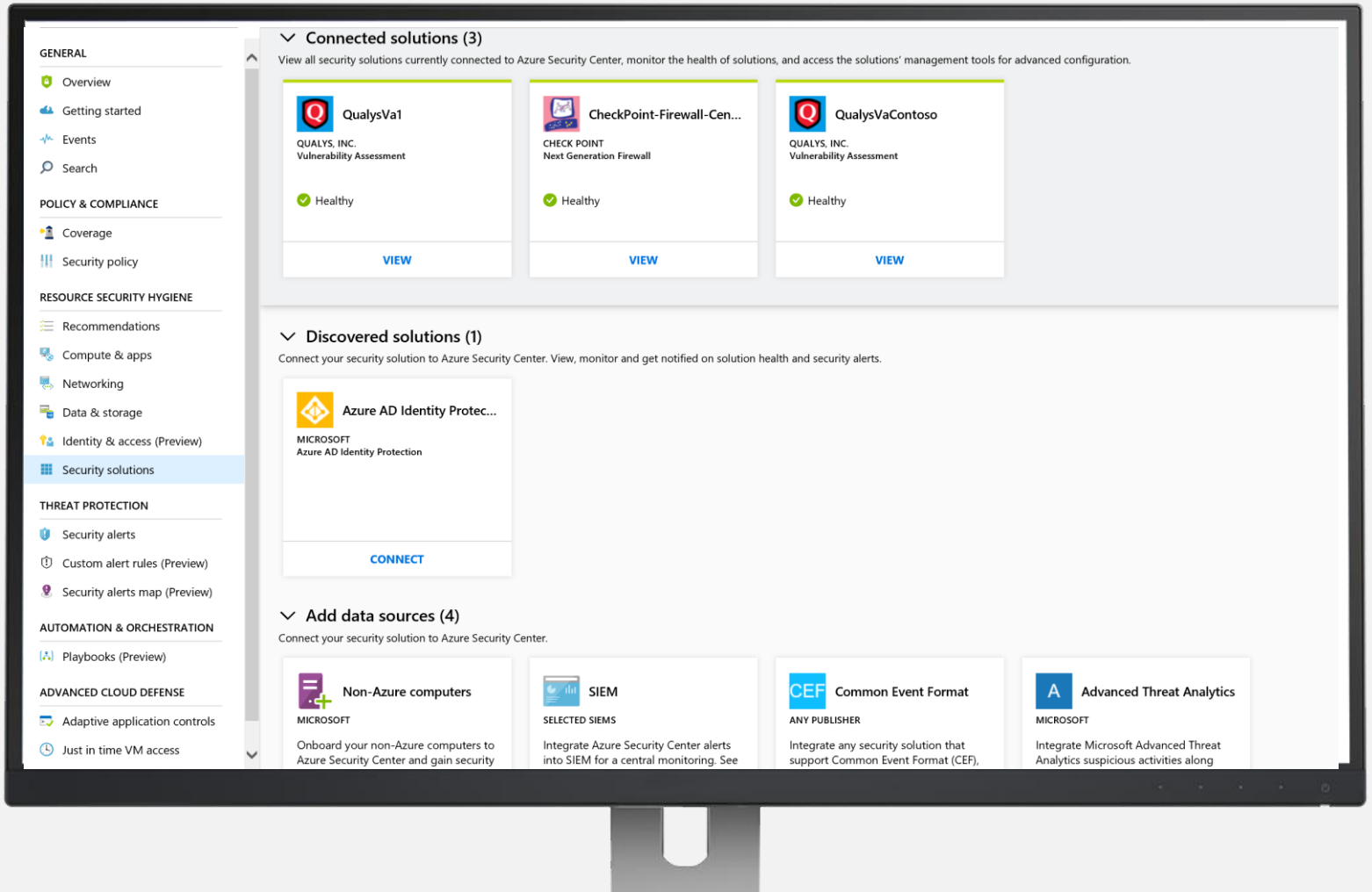
```
WireData
| where Direction == "Outbound"
| where ProcessName contains "powershell.exe"
| summarize sum(SentBytes) by Computer, ProcessName
```

Integrating with security partners

Recommends and streamlines provisioning of partner solutions

Integrates signals for centralized alerting and advanced detection

Enables monitoring and basic management

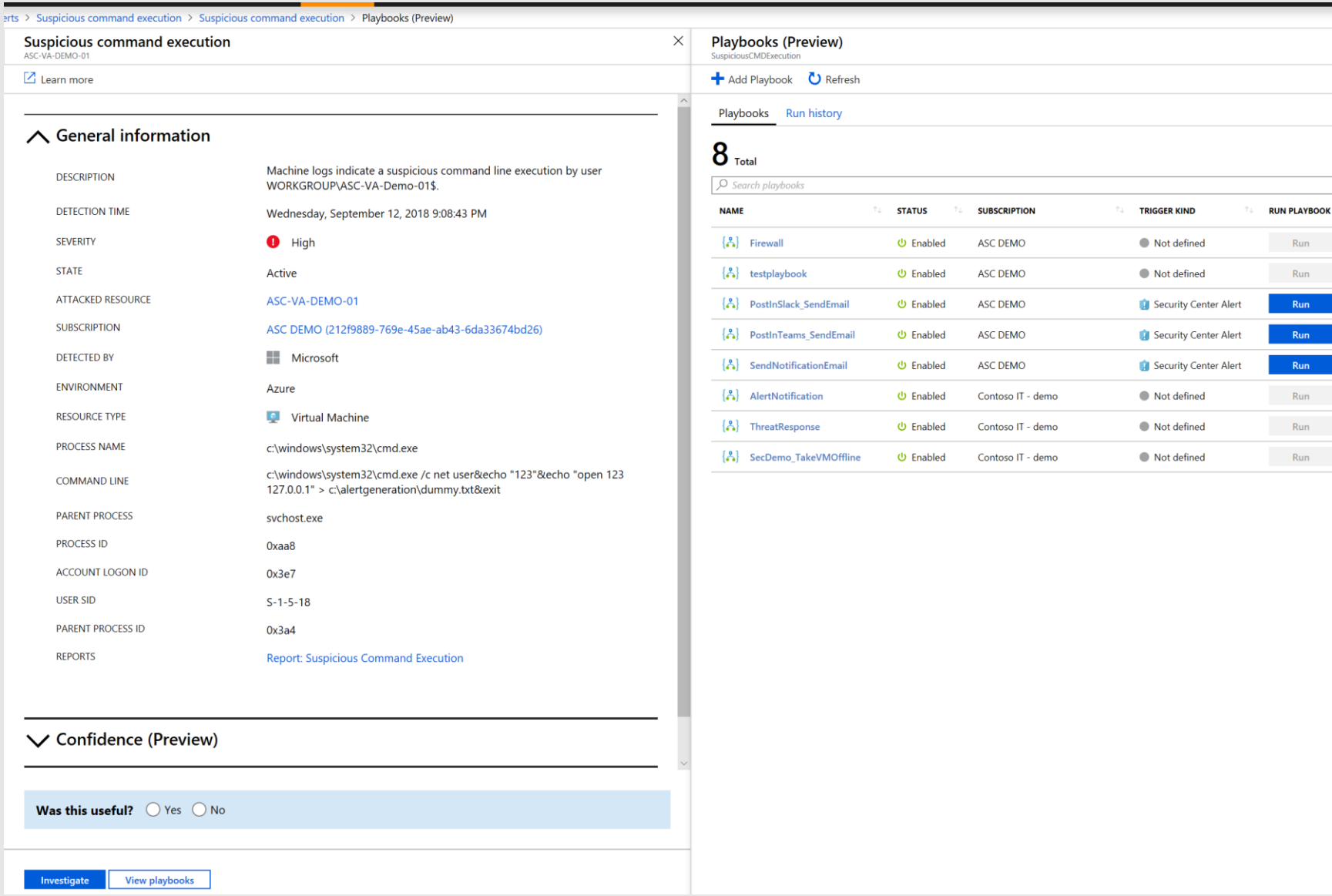


Automating Response

2 Options:

Logic Apps

Interactive

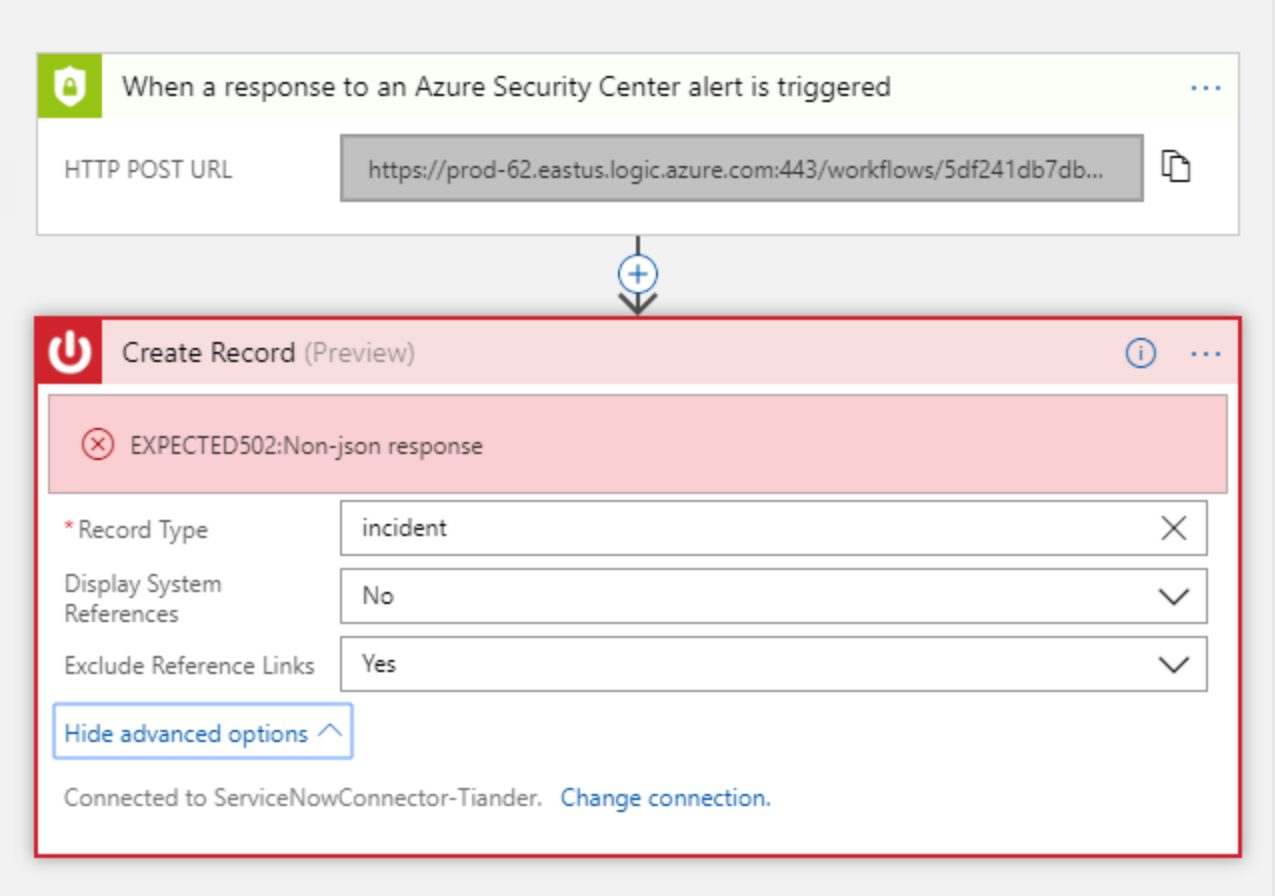


Automating Response

2 Options:

Logic Apps

Interactive



Automating Response

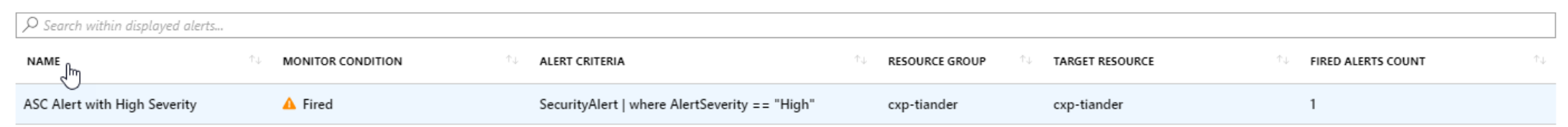
2 Options

Logic Apps

Interactive

Azure Monitor Alerts

Automatic



Automating Response

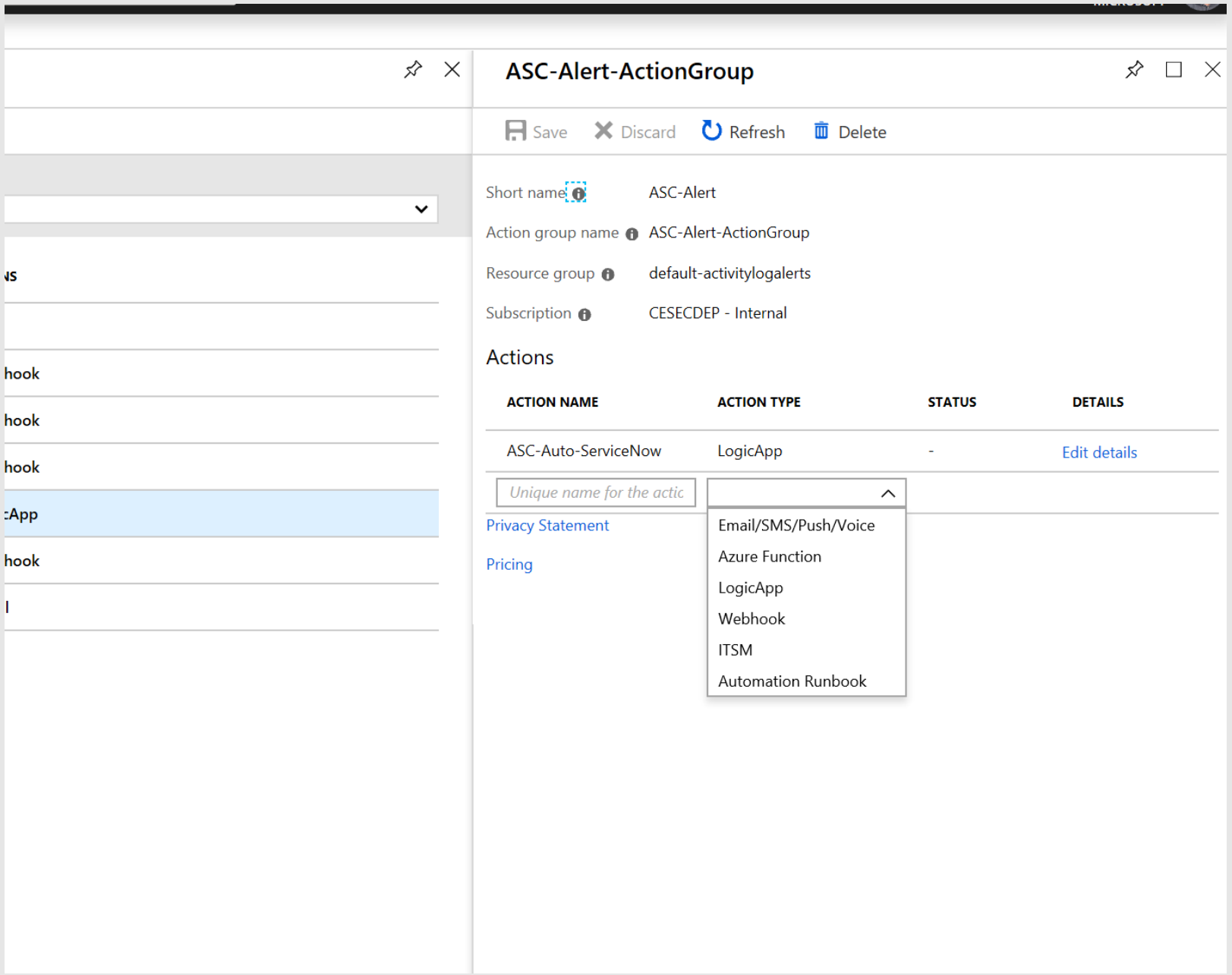
2 Options

Logic Apps

Interactive

Azure Monitor Alerts

Automatic



Automating Response

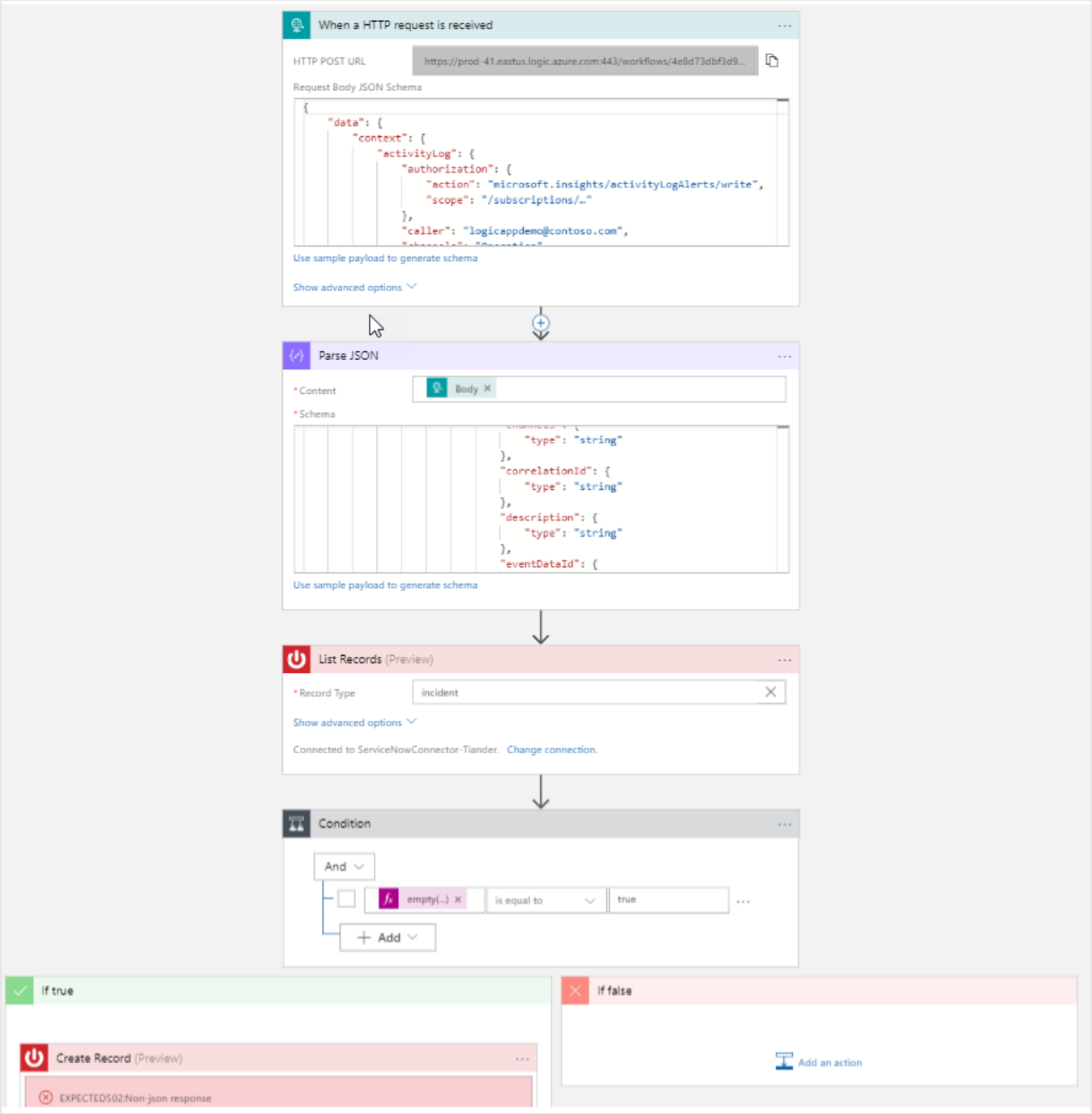
2 Options

Logic Apps

Interactive

Azure Monitor Alerts

Automatic



Take actions today

01

Use Security Center to manage security for Azure resources

02

Get advanced threat protection with Security Center standard

03

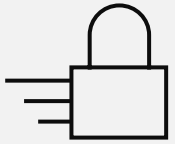
Onboard on-premises and other cloud workloads

To learn more, visit
azure.microsoft.com/en-us/services/security-center/

Azure Security Center

Strengthen security posture

Protect against threats



Get secure faster

Microsoft

Thanks!