

Azure Security Center Deep Dive

Mihály Kiléber

Senior Azure Engineer

Mihaly.Kileber@softlline.com




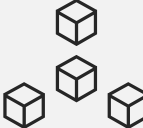

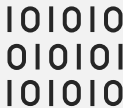


Agenda

- Cloud Security Considerations
- Using Azure Security Center to improve security posture
- Security Center Demo

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



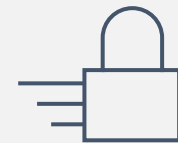
Azure Security Center



Strengthen security posture

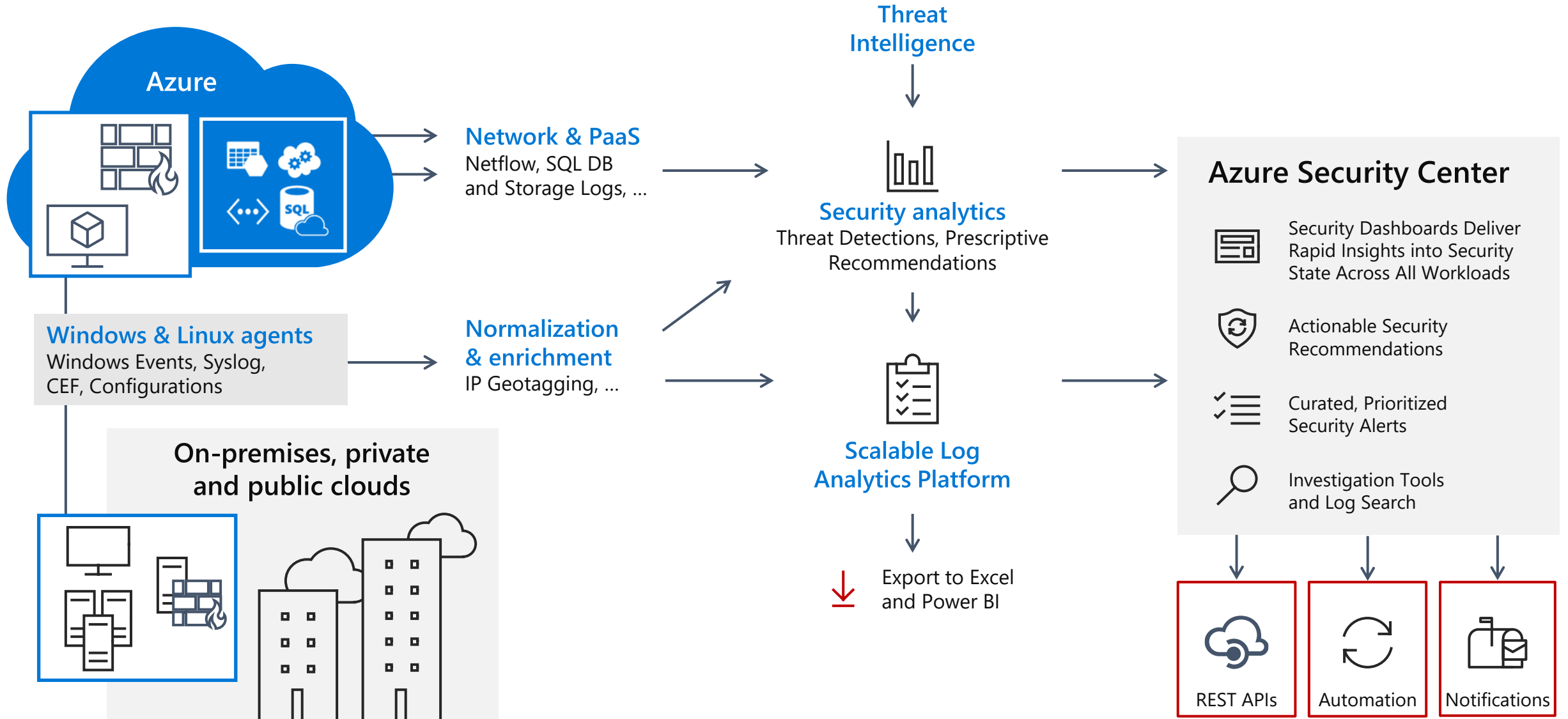


Protect against threats

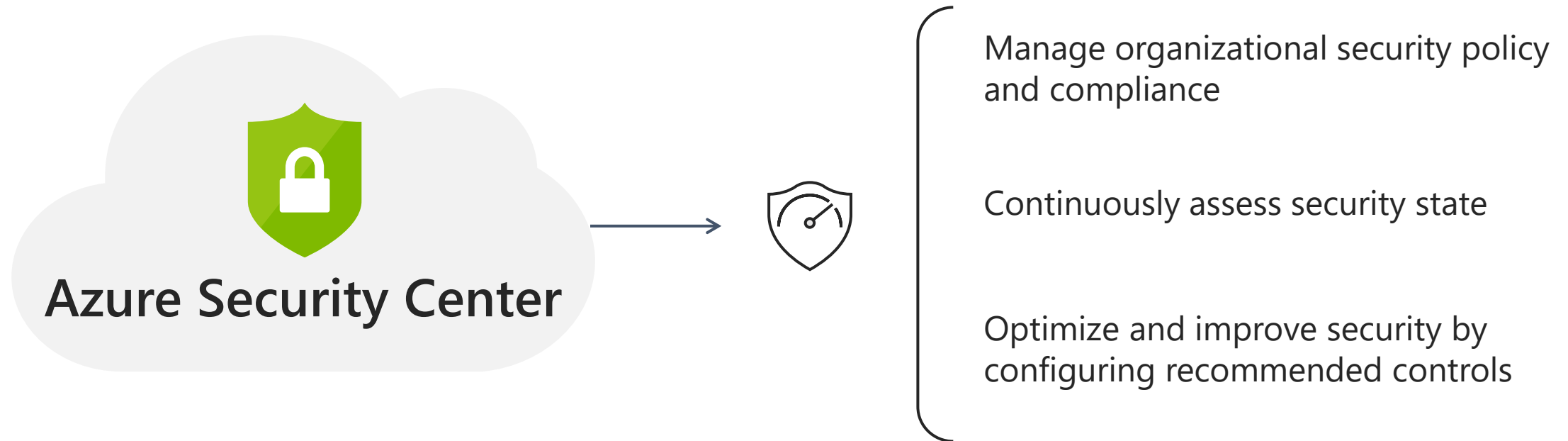


Get secure faster

Security Center Architecture



Strengthen security posture

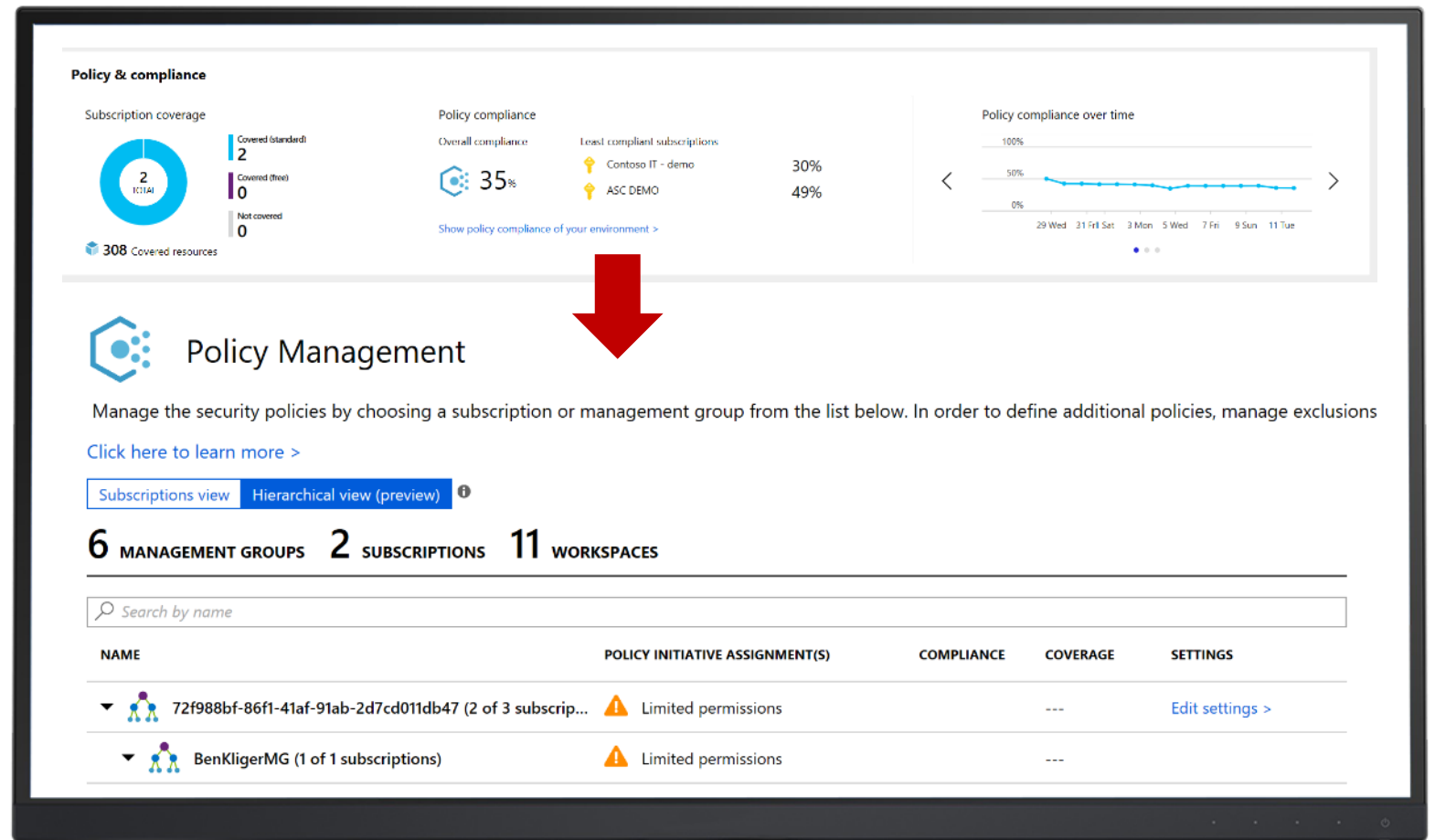


Manage organizational security policy and compliance

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

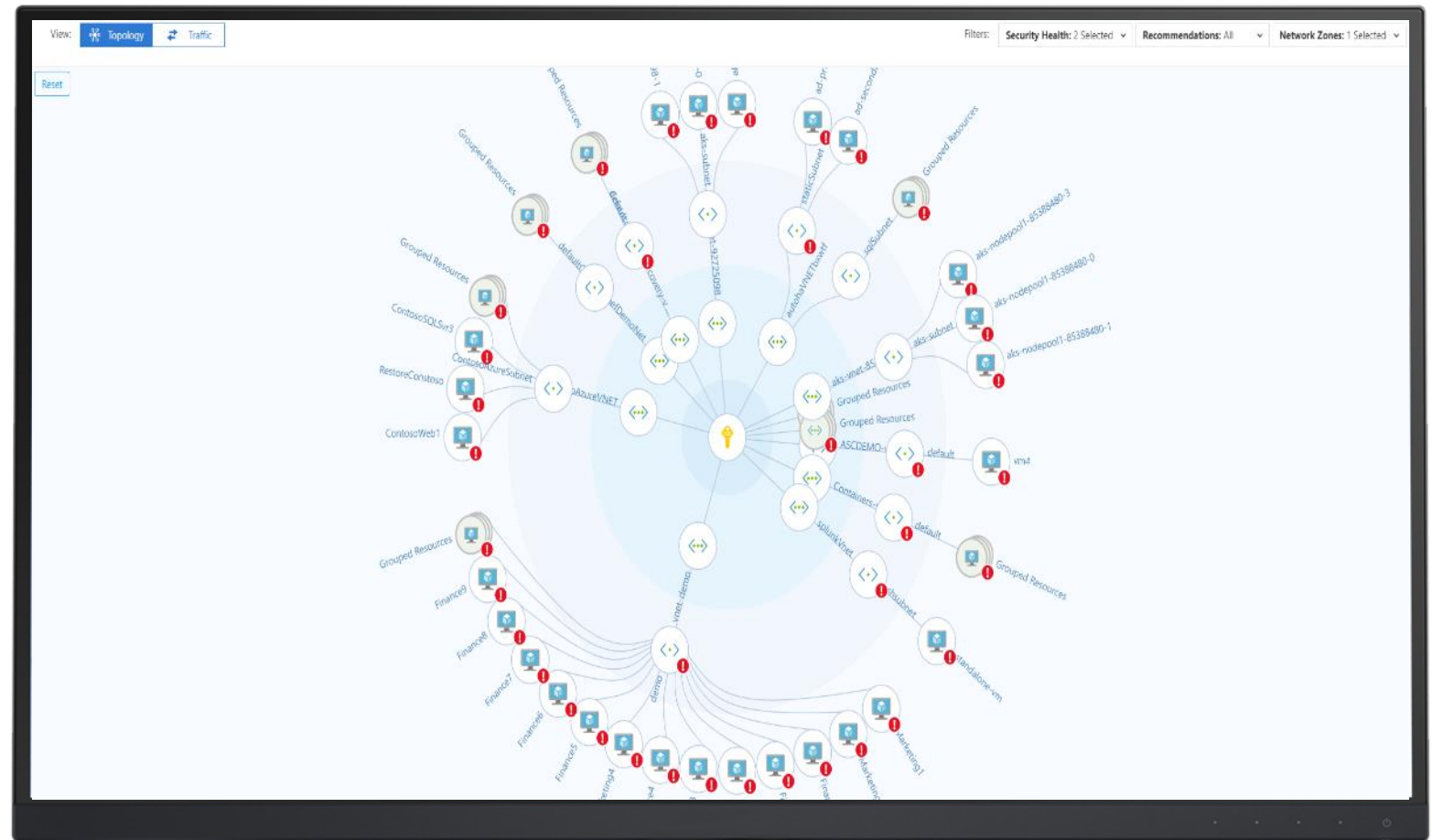


Continuously assess and optimize with Secure Score

Get insights on the security state across your infrastructure

Prioritized recommendations with a security score

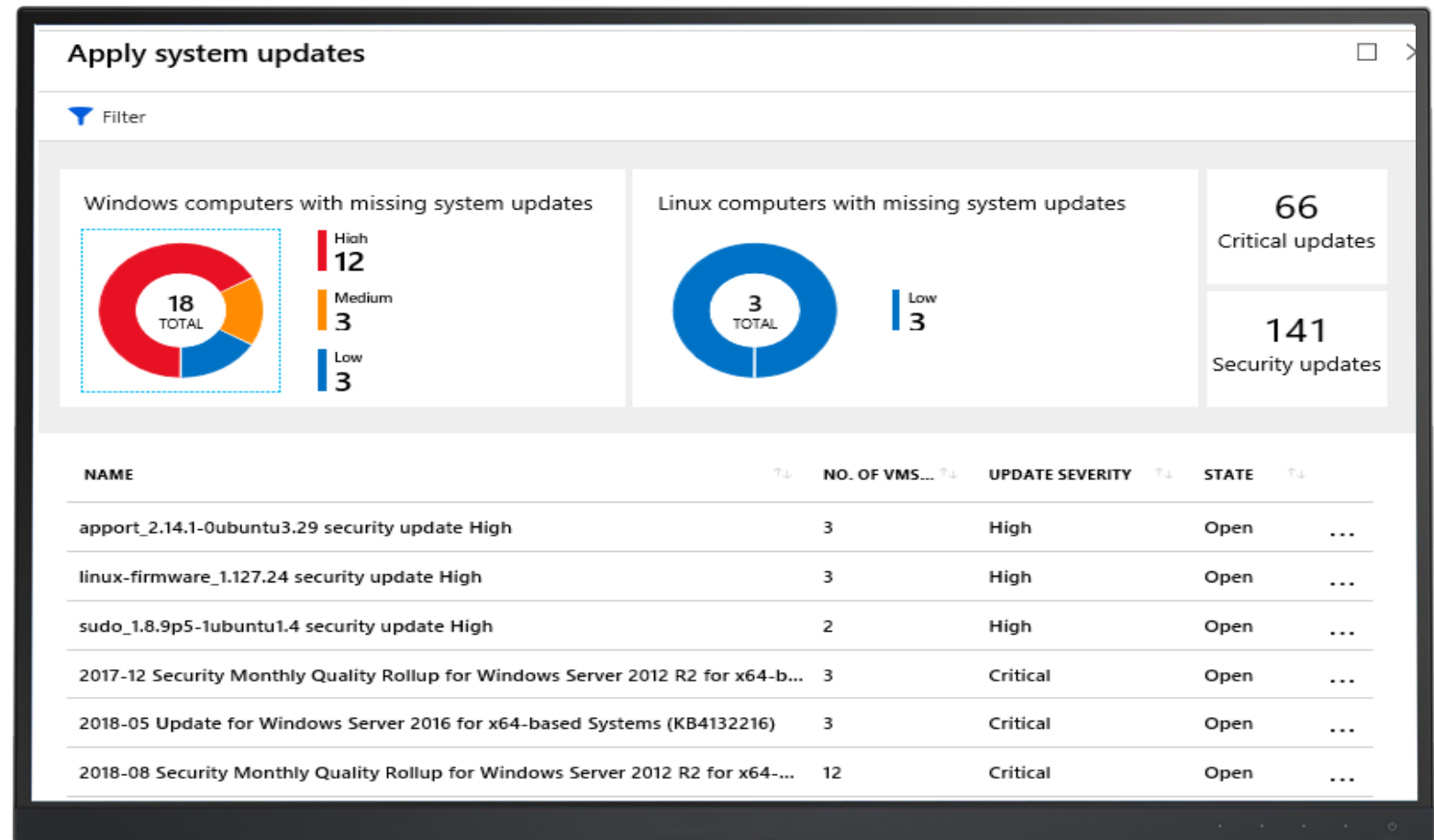
Understand the network topology and visualize configurations



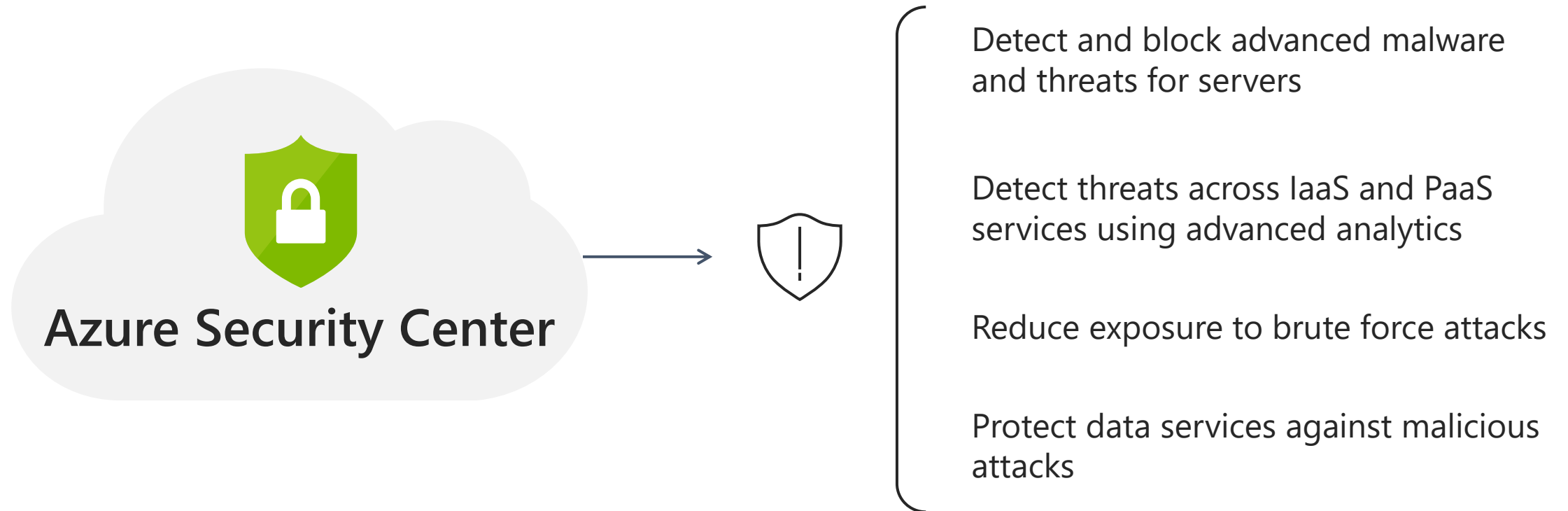
Optimize and improve security by configuring recommended controls

Apply a secure configuration standard with built-in recommendations

Reduce attack surface by applying proactive hygiene measures



Strengthen security posture



Detect and block advanced malware for Windows and Linux servers

Detect threats on servers with behavior analytics and machine learning

Get Windows server EDR (Endpoint Detection & Response) with the integration of Windows Defender ATP (Advanced Threat Protection)

Automate application whitelisting with a ML (Machine Learning) based solution

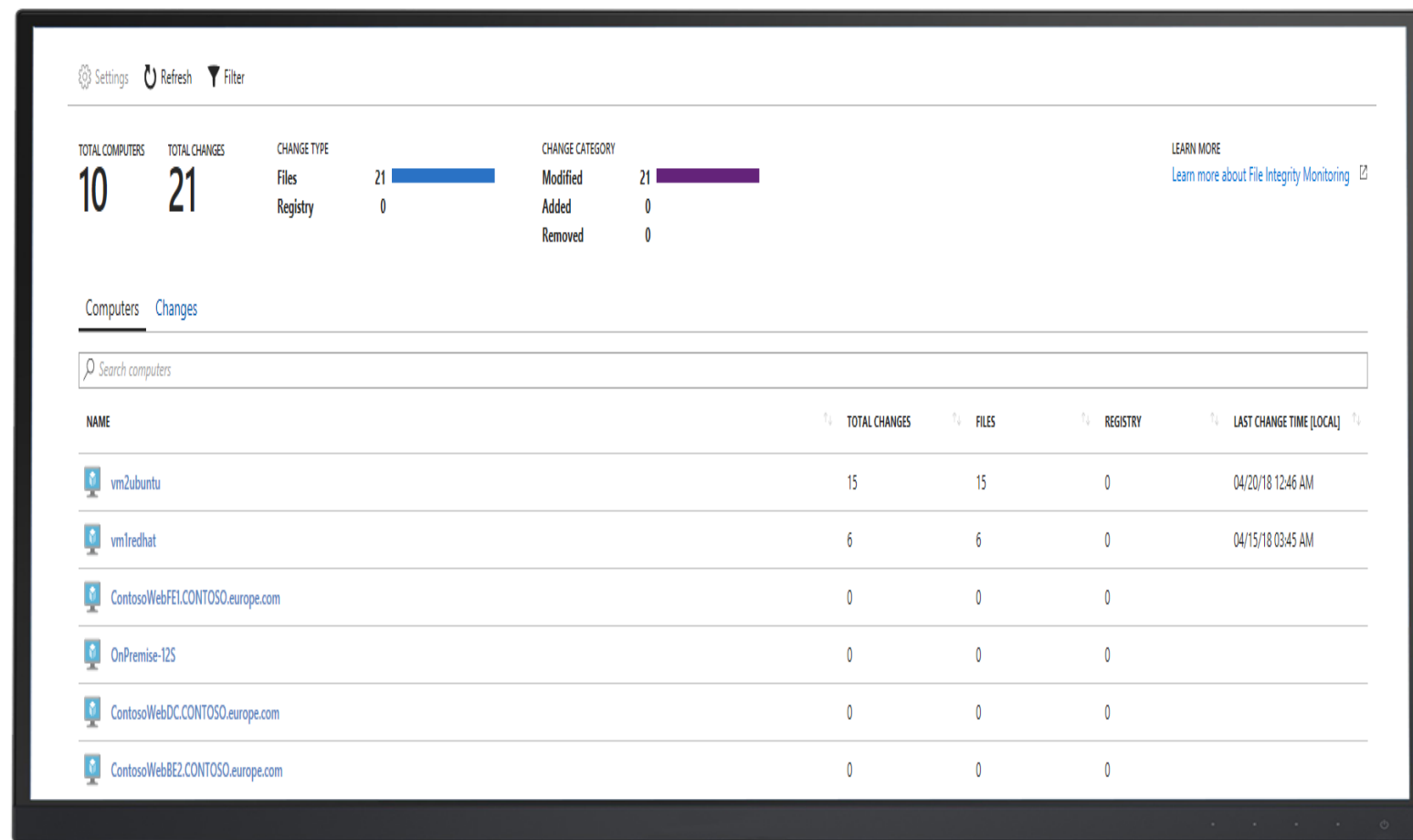


File integrity monitoring

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)

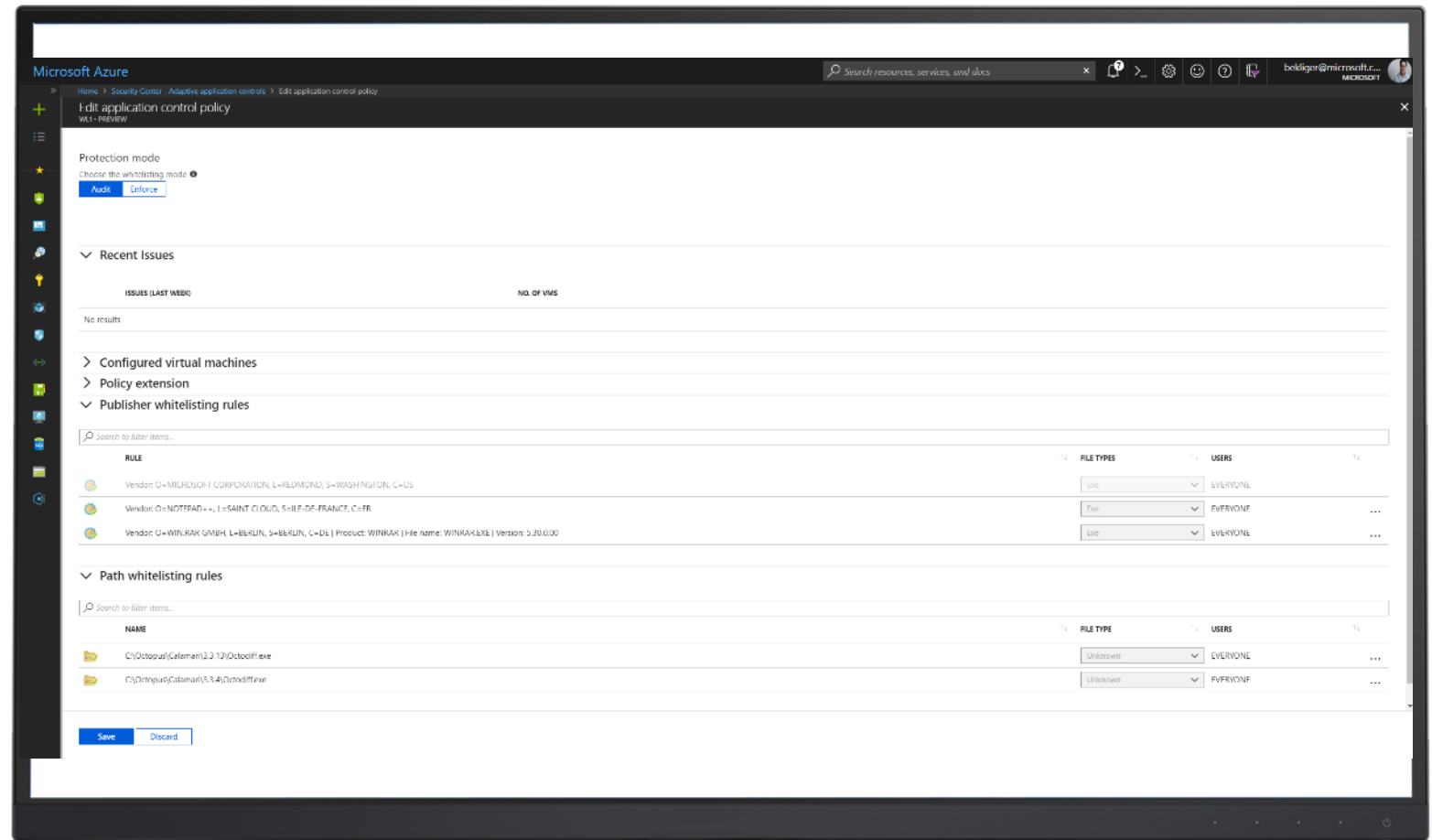


Adaptive application controls

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

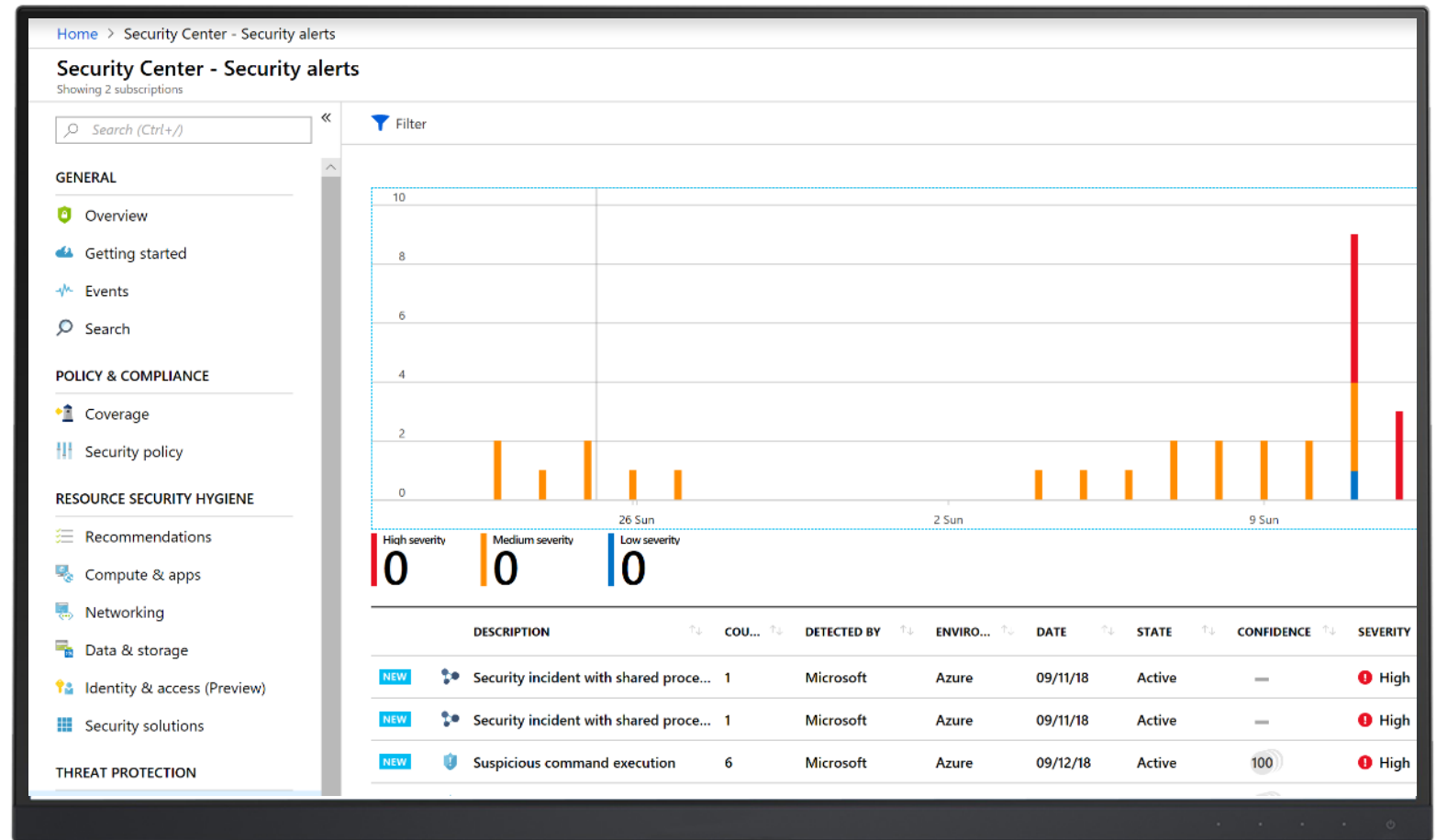


Detect threats across services

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

Get Azure UEBA (User and Entity Behavior Analytics) with the integration of Microsoft Cloud App Security

Investigate and respond to an attack with ASC (Azure Security Center) Fusion kill chain analysis



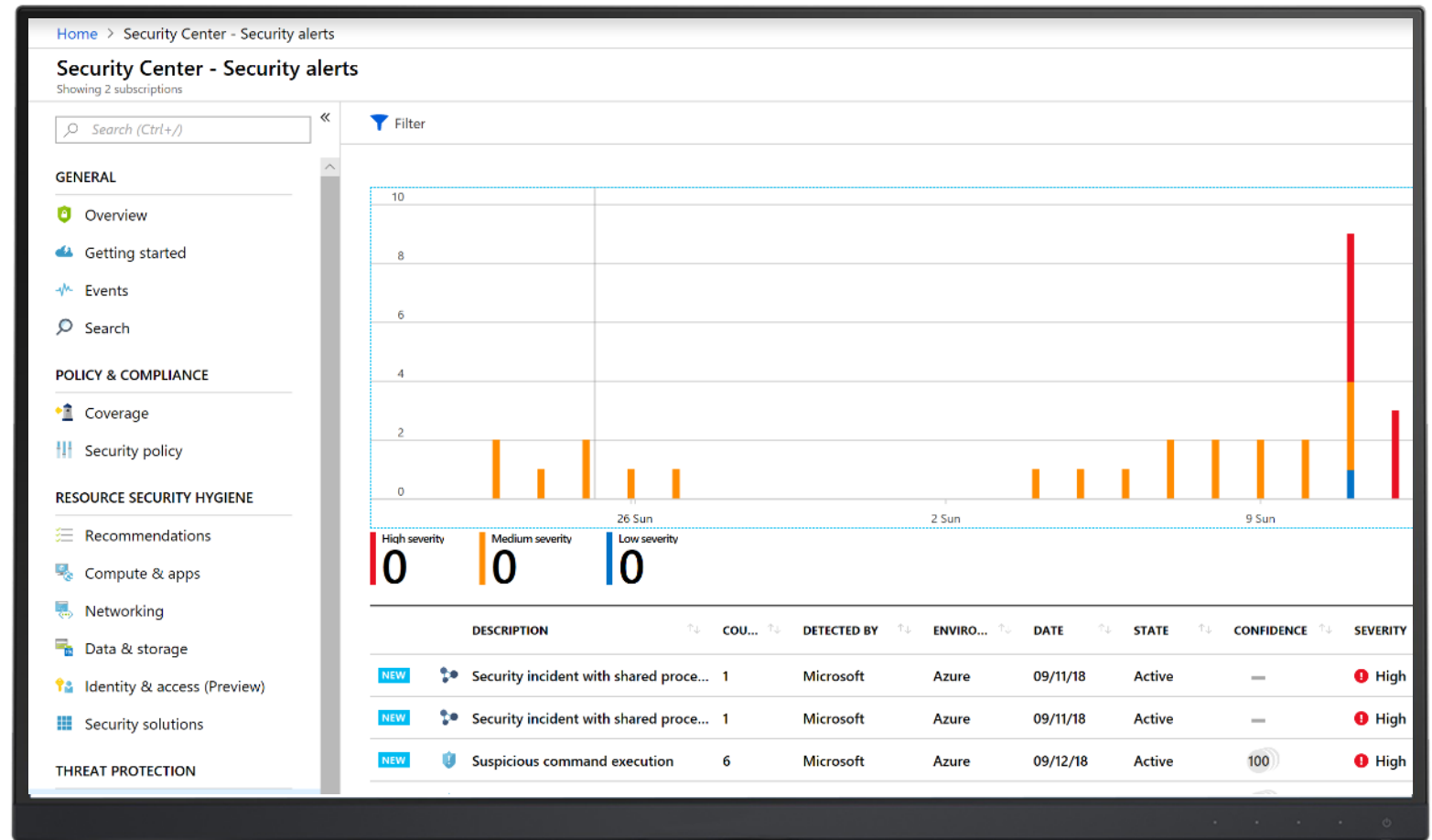
Detect threats across services using advanced analytics

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 (Endpoint Detection & Response) - integrated solution with Windows Defender ATP (Advanced Threat Protection)



Windows Server EDR with Windows Defender ATP

Leveraging Windows Defender ATP support for Windows Server

Next-gen post breach detection sensors

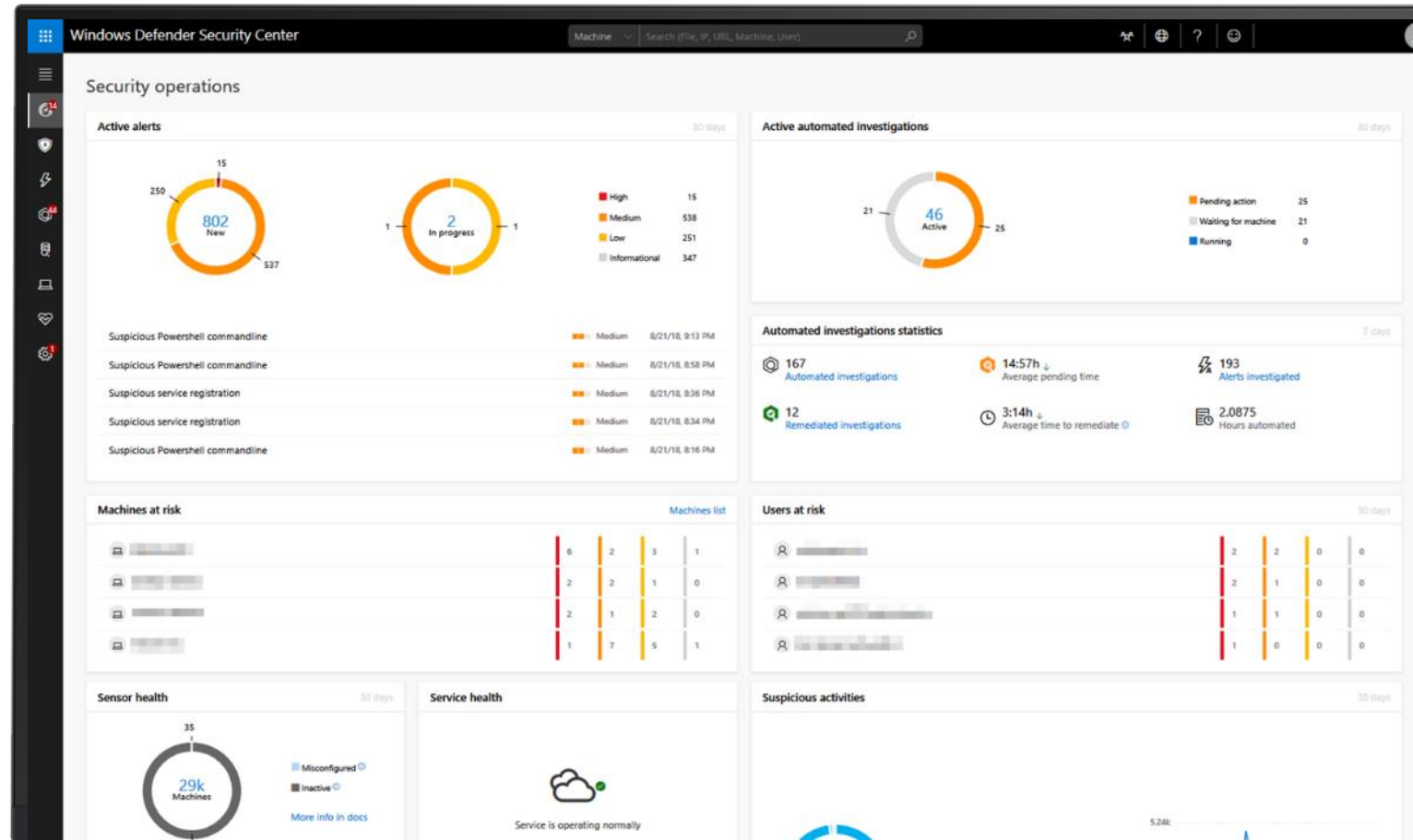
Windows Defender ATP sensor for Windows Servers that collect a vast array of behavioral signals to enable advanced attack detection & investigation.

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

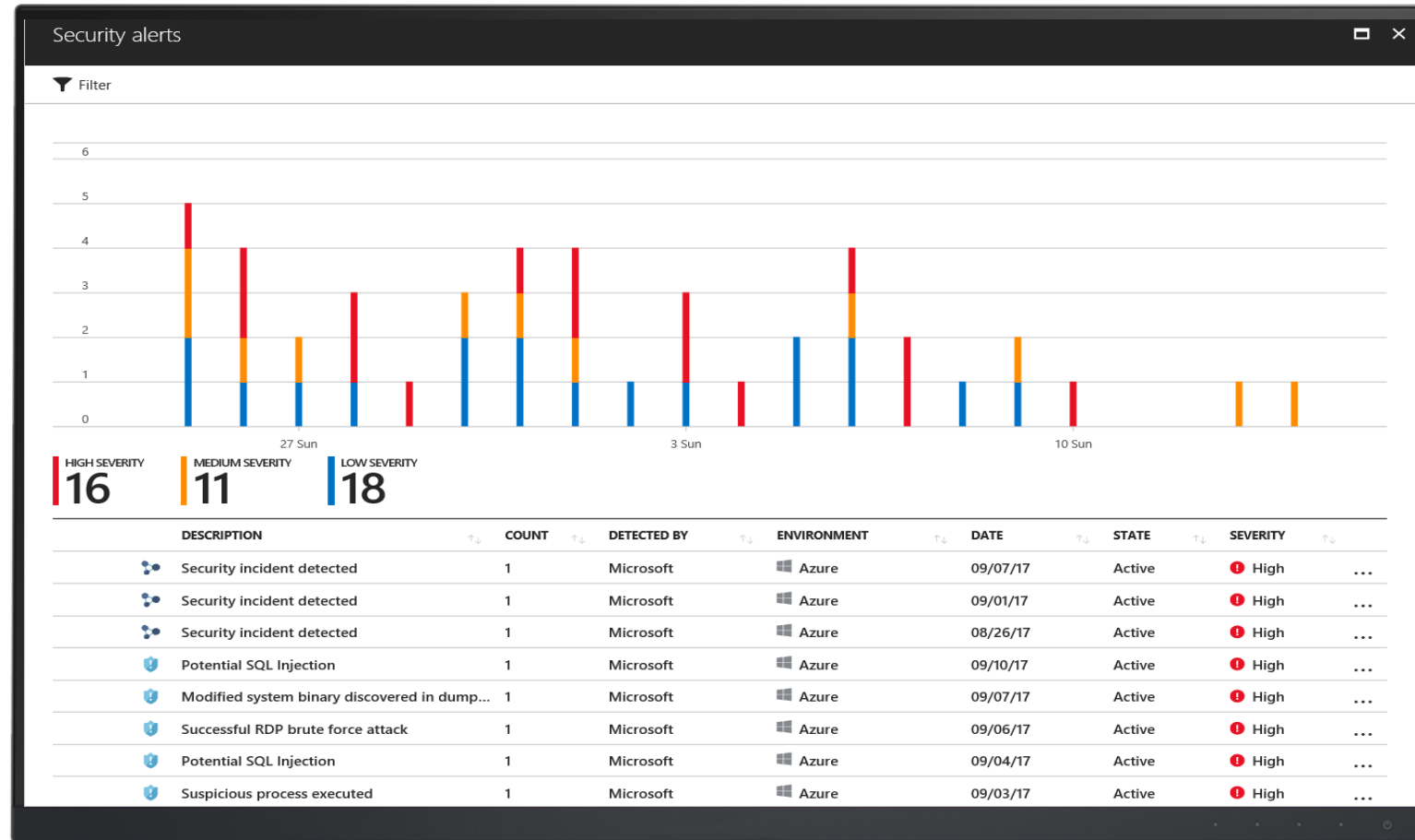
Windows Defender ATP sensor is automatically enabled on Windows Servers that are onboarded to ASC

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



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

The screenshot displays the 'JIT VM access configuration' window for 'ContosoSQLSrv1'. It features a table of existing configurations and a sidebar for adding new ones.

JIT VM access configuration
ContosoSQLSrv1

+ Add Save Discard

Configure the ports for which the just in time VM access will be applicable

PORT	PROT...	ALLOWED SOUR...	IP RANGE	TIME RANGE (H...	
22 (Recommended)	Any	Per request	N/A	3 hours	...
3389 (Recommended)	Any	Per request	N/A	3 hours	...
5985 (Recommended)	Any	Per request	N/A	3 hours	...
5986 (Recommended)	Any	Per request	N/A	3 hours	...

Add port configuration

* Port
22

Protocol
Any TCP UDP

Allowed source IPs
Per request CIDR block

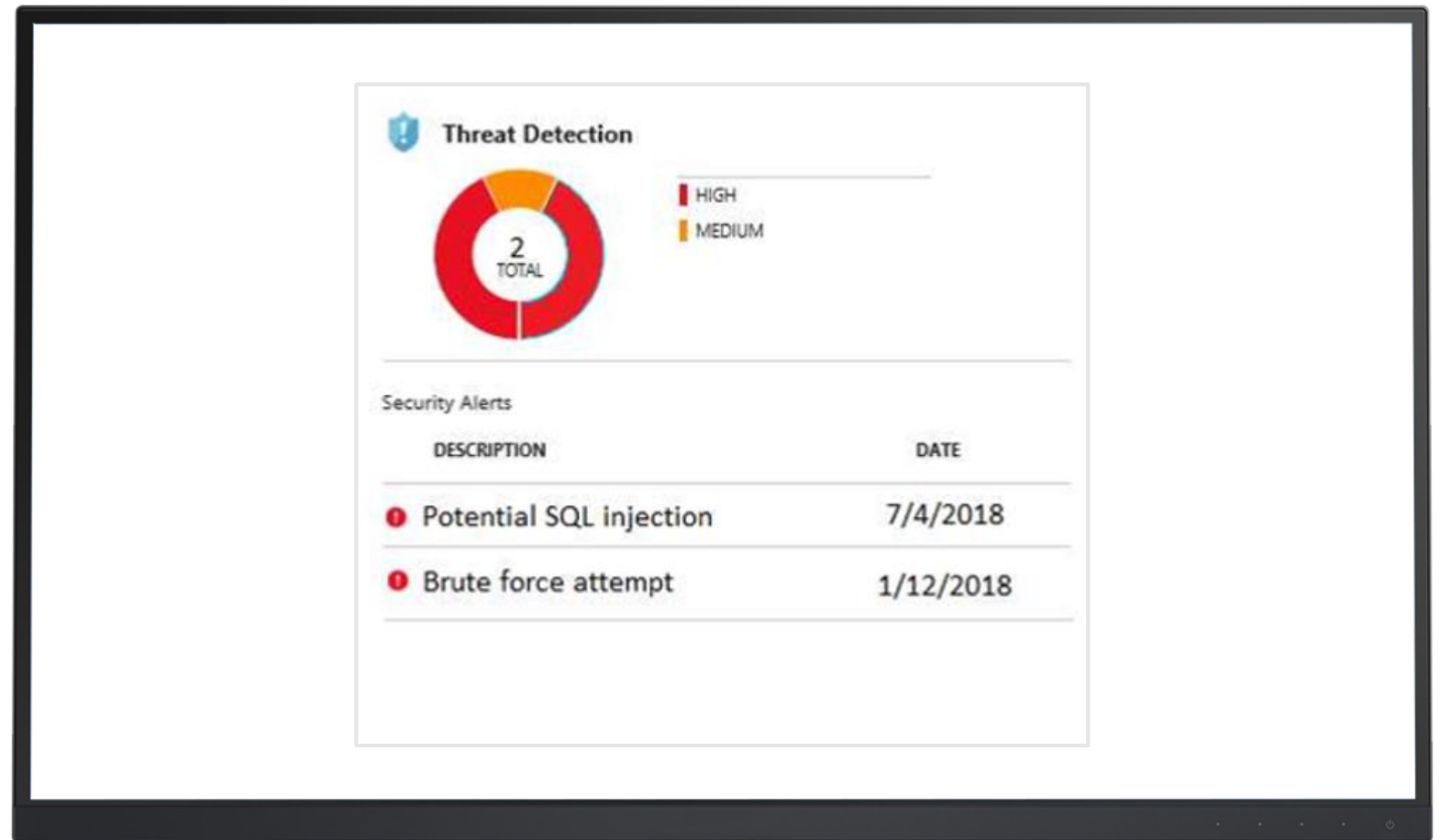
IP addresses ⓘ
[Empty text box]

Max request time
[Slider bar] 3 (hours)

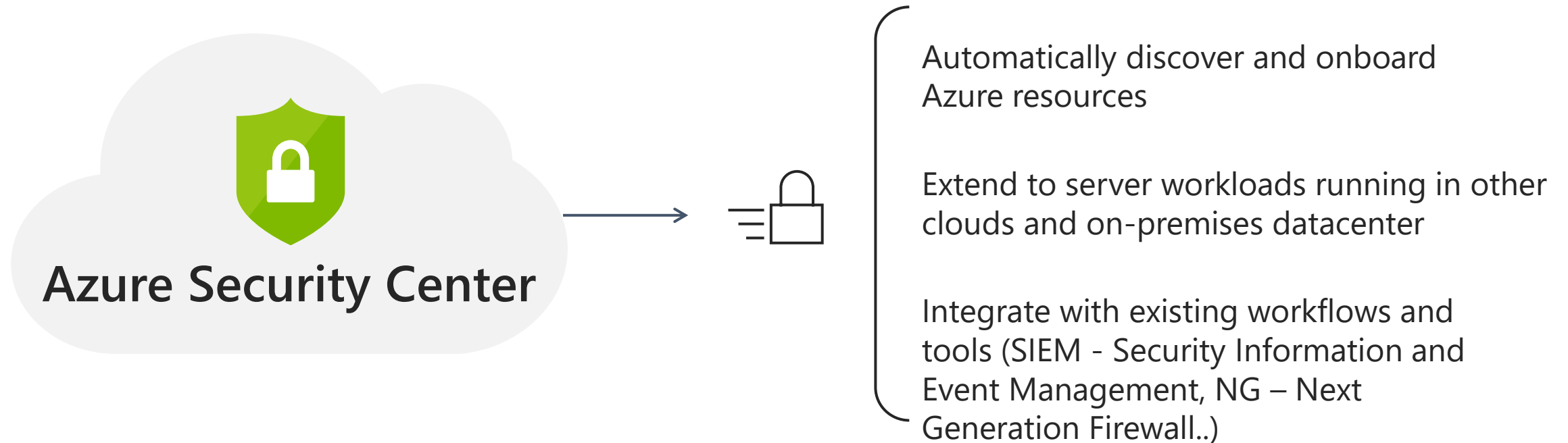
Protect data services

Assess potential vulnerabilities across Azure SQL and Storage services

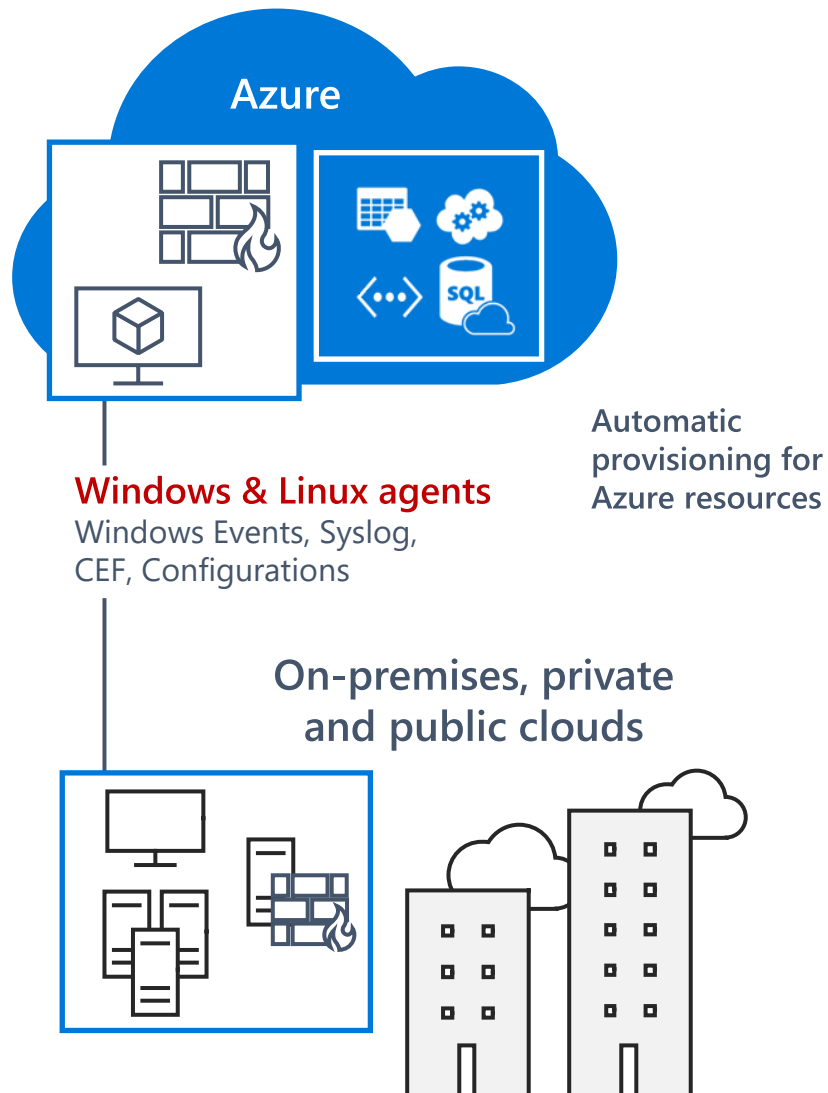
Classify and audit access to sensitive data in Azure SQL



Get secure faster



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

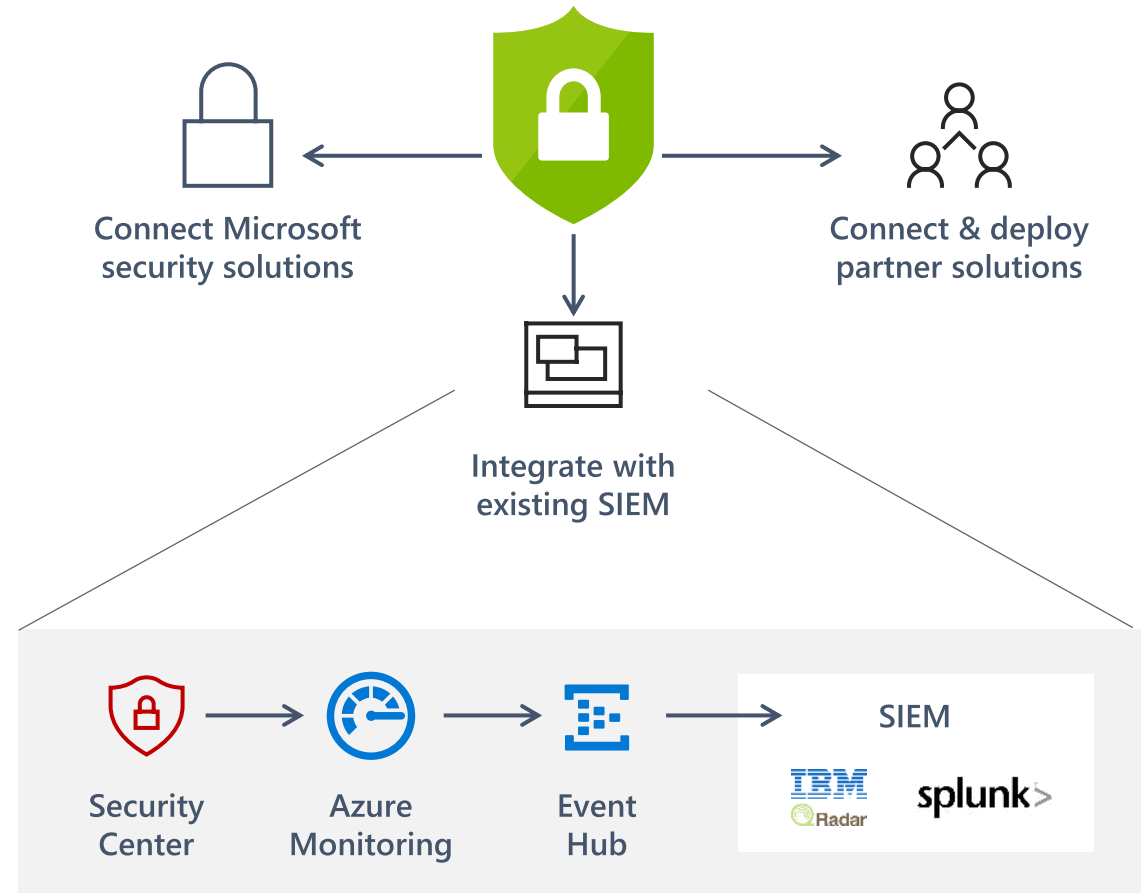
PUT: Connect security solutions/Add data sources, Run playbooks

Integrating with existing workflows and tools

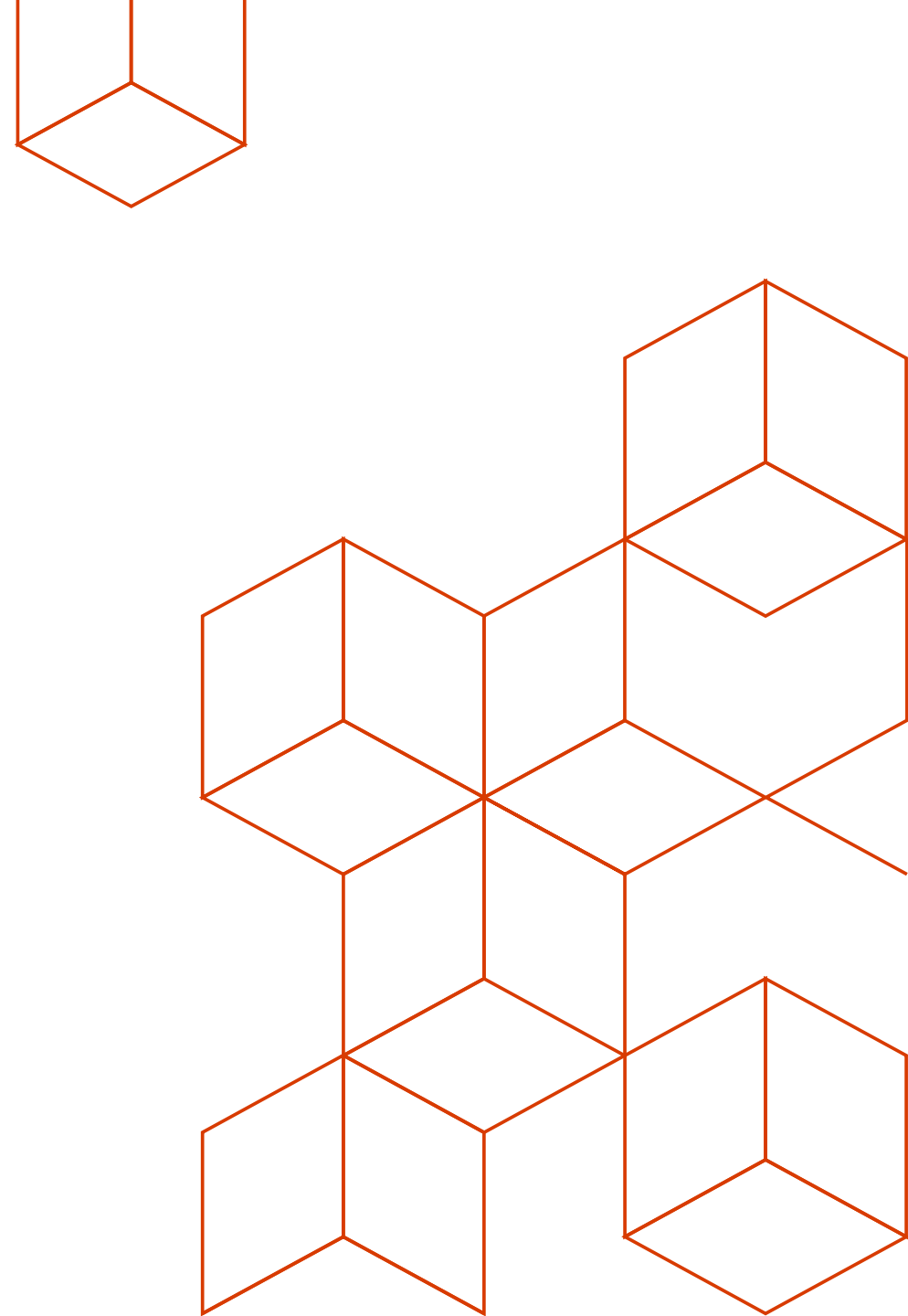
Respond quickly to threats with automated workflows

Automation support with REST APIs and PowerShell cmdlets

Consolidate SOC (Security Operations Center) insights by integrating with existing SIEM (Security Information and Event Management) solution



EXAMPLE



What is a custom alert?

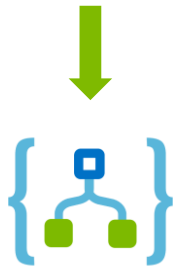
A 'Breadth' check for indicators of compromise



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

SecurityEvent

```
| where EventID == 4688  
| where CommandLine !contains "System32"  
| where Process contains "Svchost"
```

Create custom alert rule

* Name ⓘ
System masked process execution ✓

Description
Check for SvcHost process outside of System32 ✓

Severity ⓘ
High ✓

Sources

Subscription
CESE - Internal ✓

Workspace
cxp-azure-securityws ✓

Criteria

* Search Query ⓘ
SecurityEvent
| where EventID == 4688
| where CommandLine !contains "System32"
| where Process contains "Svchost" ✓

[Execute your search query now](#)

Period ⓘ
Over the last 1 hours ✓

Your search returned 0 results for the time window selected.

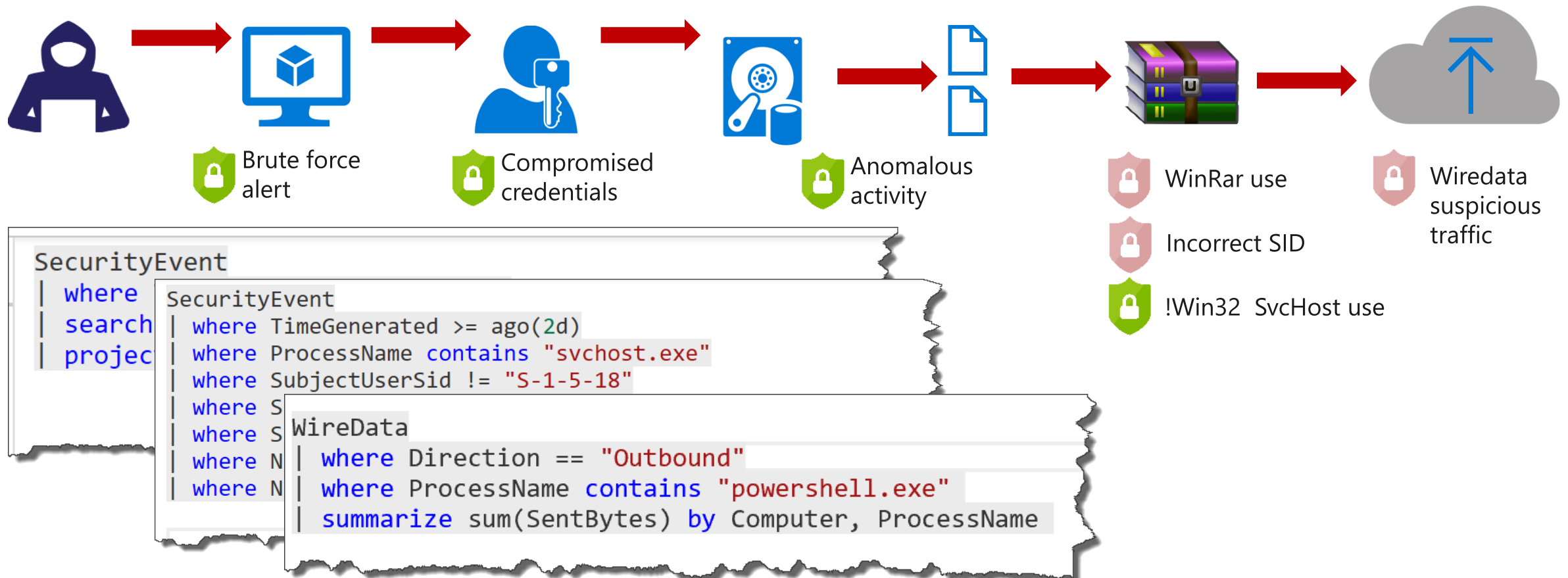
Custom alert example

Attack approaches:

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

Data ex-filtration example:

"Alert me when compression software is used in suspicious ways"

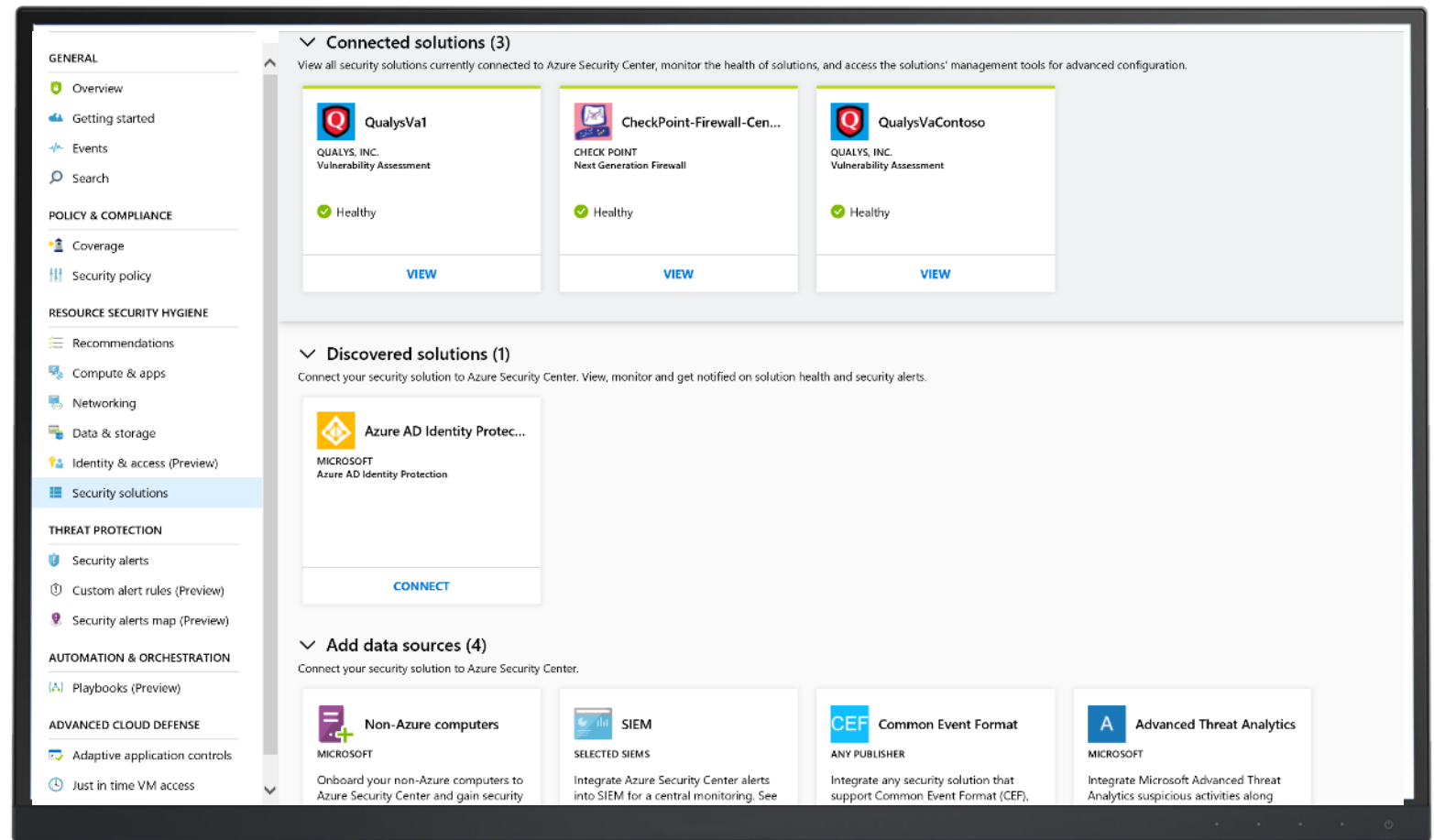


Integrating with security partners

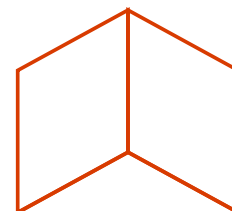
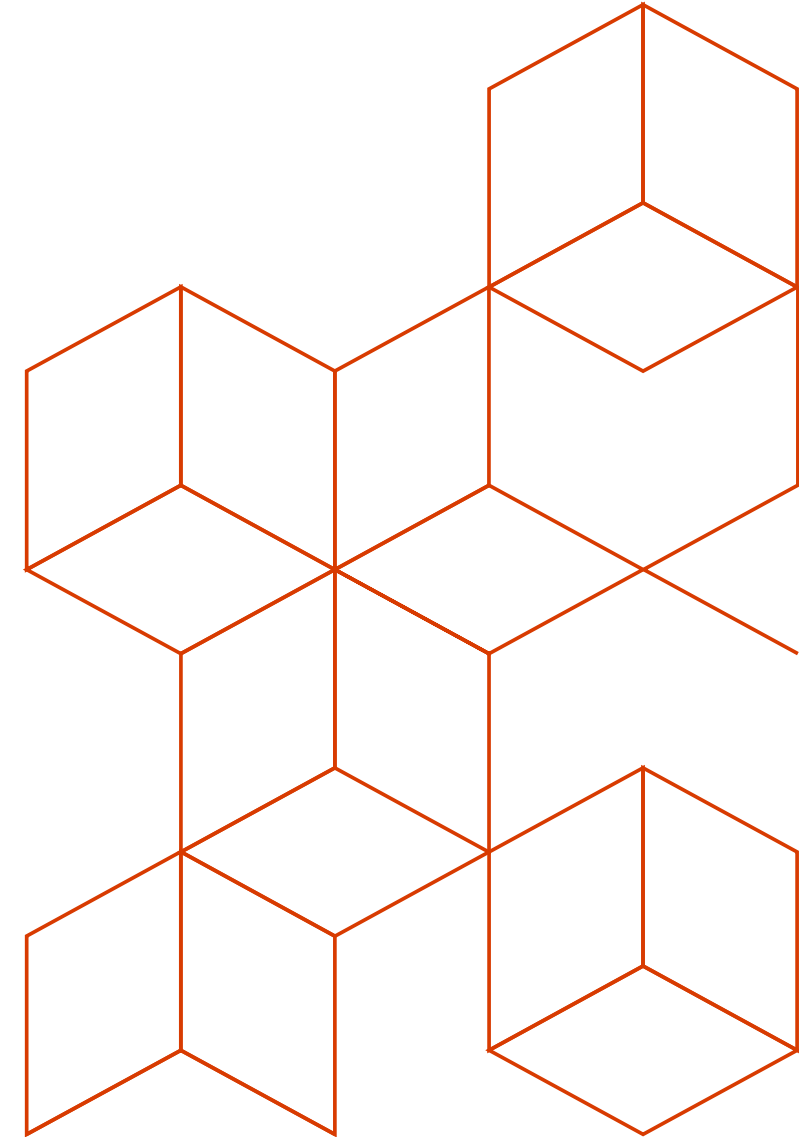
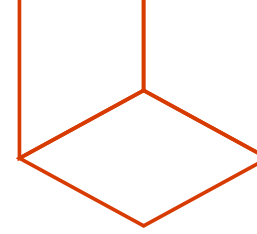
Recommends and streamlines provisioning of partner solutions

Integrates signals for centralized alerting and advanced detection

Enables monitoring and basic management



EXAMPLE



Automating Response

2 Options: Logic Apps Interactive

Suspicious command execution

ASC-VA-DEMO-01

Learn more

General information

DESCRIPTION

Machine logs indicate a suspicious command line execution by user WORKGROUP\ASC-VA-Demo-01\$.

DETECTION TIME

Wednesday, September 12, 2018 9:08:43 PM

SEVERITY

High

STATE

Active

ATTACKED RESOURCE

ASC-VA-DEMO-01

SUBSCRIPTION

ASC DEMO (212f9889-769e-45ae-ab43-6da33674bd26)

DETECTED BY

Microsoft

ENVIRONMENT

Azure

RESOURCE TYPE

Virtual Machine

PROCESS NAME

c:\windows\system32\cmd.exe

COMMAND LINE

c:\windows\system32\cmd.exe /c net user&echo "123"&echo "open 123 127.0.0.1" > c:\alertgeneration\dummy.txt&exit

PARENT PROCESS

svchost.exe

PROCESS ID

0xaa8

ACCOUNT LOGON ID

0x3e7

USER SID

S-1-5-18

PARENT PROCESS ID

0x3a4

REPORTS

Report: Suspicious Command Execution

Confidence (Preview)

Was this useful? ☐ Yes ☐ No

Investigate

View playbooks

Playbooks (Preview)

SuspiciousCMDExecution

Add Playbook

Refresh

Playbooks

Run history

8 Total

Search playbooks

NAME	STATUS	SUBSCRIPTION	TRIGGER KIND	RUN PLAYBOOK
Firewall	Enabled	ASC DEMO	Not defined	Run
testplaybook	Enabled	ASC DEMO	Not defined	Run
PostInSlack_SendEmail	Enabled	ASC DEMO	Security Center Alert	Run
PostInTeams_SendEmail	Enabled	ASC DEMO	Security Center Alert	Run
SendNotificationEmail	Enabled	ASC DEMO	Security Center Alert	Run
AlertNotification	Enabled	Contoso IT - demo	Not defined	Run
ThreatResponse	Enabled	Contoso IT - demo	Not defined	Run
SecDemo_TakeVMOOffline	Enabled	Contoso IT - demo	Not defined	Run

Automating Response

2 Options:
Logic Apps
Interactive

The screenshot displays a Logic App workflow. The first step is a trigger: "When a response to an Azure Security Center alert is triggered". This is followed by an action: "HTTP POST URL" with the address "https://prod-62.eastus.logic.azure.com:443/workflows/5df241db7db...". An arrow points down to a second action: "Create Record (Preview)". This action is highlighted with a red border and contains a red error message: "EXPECTED502:Non-json response". Below the error, there are three configuration fields: "Record Type" set to "incident", "Display System References" set to "No", and "Exclude Reference Links" set to "Yes". At the bottom of the action panel, there is a button labeled "Hide advanced options ^" and a status message: "Connected to ServiceNowConnector-Tiander. Change connection."

Automating Response

2 Options

Logic Apps

Interactive

Azure Monitor Alerts

Automatic

🔍 Search within displayed alerts...						
NAME	↑↓ MONITOR CONDITION	↑↓ ALERT CRITERIA	↑↓ RESOURCE GROUP	↑↓ TARGET RESOURCE	↑↓ FIRED ALERTS COUNT	↑↓
ASC Alert with High Severity	🚨 Fired	SecurityAlert where AlertSeverity == "High"	cxp-tiander	cxp-tiander	1	

Automating Response

2 Options

Logic Apps

Interactive

Azure Monitor Alerts

Automatic

The screenshot displays the 'Alert Action Group' configuration page in the Azure portal. The title bar shows 'ASC-Alert-ActionGroup' with standard window controls. Below the title bar are buttons for 'Save', 'Discard', 'Refresh', and 'Delete'. The configuration details on the right include:

- Short name: ASC-Alert
- Action group name: ASC-Alert-ActionGroup
- Resource group: default-activitylogalerts
- Subscription: CESECDEP - Internal

The 'Actions' section contains a table with the following data:

ACTION NAME	ACTION TYPE	STATUS	DETAILS
ASC-Auto-ServiceNow	LogicApp	-	Edit details

Below the table, there is a text input field with the placeholder 'Unique name for the action', a 'Privacy Statement' link, and a 'Pricing' link. A dropdown menu is open, showing the following options: Email/SMS/Push/Voice, Azure Function, LogicApp, Webhook, ITSM, and Automation Runbook.

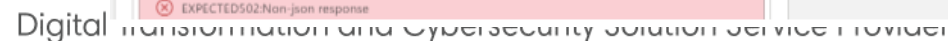
2 Options

Logic Apps

Interactive

Azure Monitor Alerts

Automatic



Resources

Resource	Link	Comment
Securing Azure reference	http://aka.ms/myasis	Definitive reference guide
Azure security best practices	https://azure.microsoft.com/resources/security-best-practices-for-azure-solutions/	In-depth guidance for securing specific Azure workloads
Creating compliant workloads	https://servicetrust.microsoft.com/ViewPage/BlueprintOverview	FedRAMP, NIST SP800, FFIEC, and more
Getting started with Security Center	https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started	
Security playbook	ASCPlaybooks	Simulate & hunt threats, WAF playbooks & more
Azure templates for attack simulation	https://ASCPlaybooksSQLi https://ASCPlaybooksVAttack https://ASCPlaybooksXSS https://ASCPlaybooksDDos	SQL injection, Virus, cross-site scripting, and DDoS playbooks Credit: Avyan consulting
Security Center and Powershell samples	https://github.com/tianderturpijn/ASC	Common operations and ARM template

DEMO

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/

Questions?



GO GLOBAL



GO CLOUD



GO INNOVATIVE