

Continuous compliance in Azure

Sarah Young, Azure Security and Compliance Global Black Belt

April 2019

whoami?

Azure Security and Compliance Global Black Belt for Asia.

Worked in tech for the past 10 years.

Based in Melbourne (but I travel *lots*).

Prolific speaker at conferences and meetups.



What is continuous compliance?

Continuous compliance is the process by which a platform or application is constantly monitored for changes and compliance with organisational and/or regulatory standards.

“Compliance” may also refer to config drift and compliance to an organisation’s container/server/endpoint image.

An organisation may choose to either alert or block/remediate parts of the infrastructure if it deviates from agreed patterns.

How can Azure support continuous compliance activities?

Azure Security Center

Azure Policy

Azure Sentinel

Threat and Vulnerability Management (TVM) within Microsoft Defender
ATP

Adaptive network hardening

Azure Compliance Engineering



Standards

- ISO
- NIST
- FISMA
- FedRAMP
- HIPAA
- EU Data Directive
- Regional/National Standards



Customer Requirements



Azure Compliance

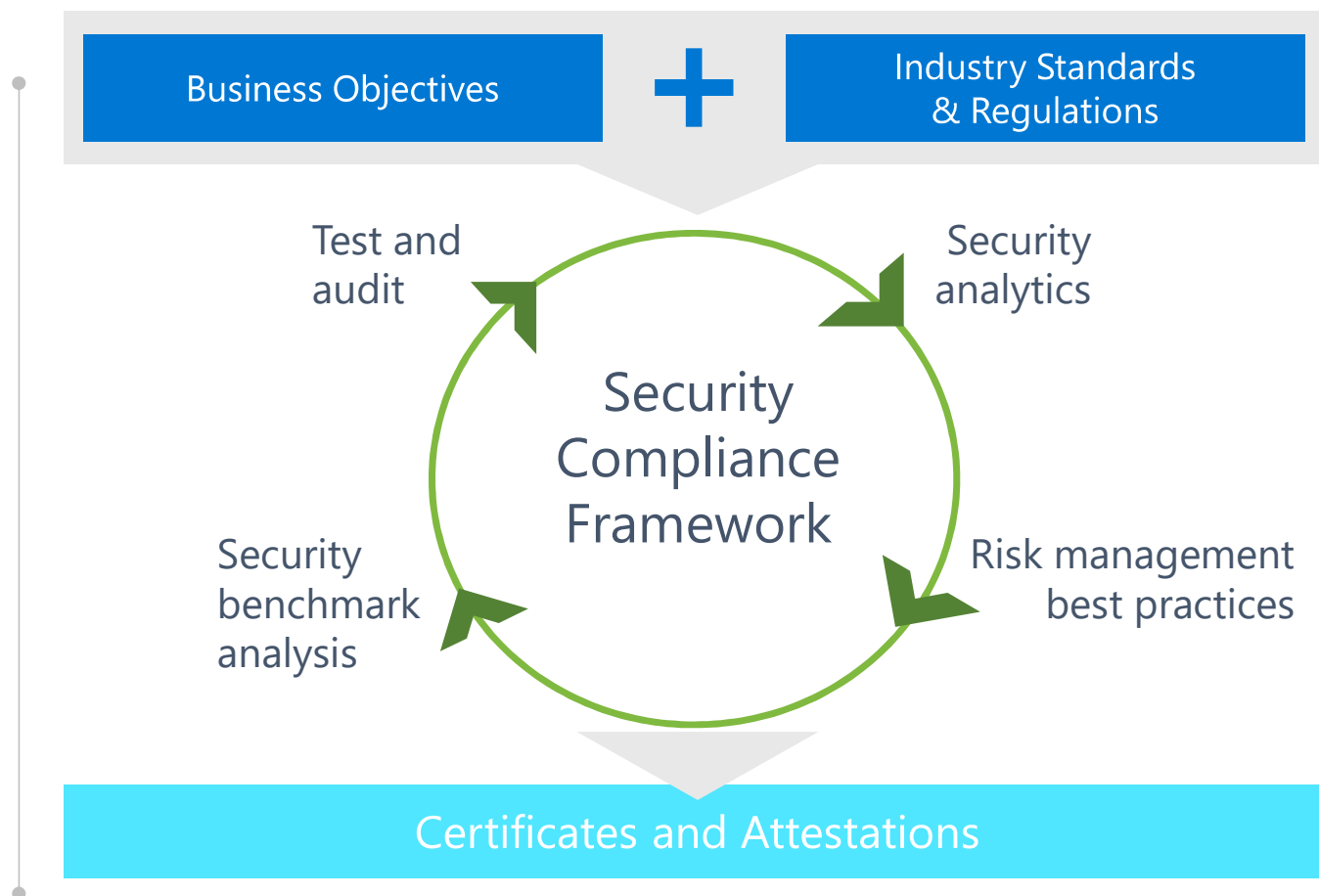


Certification

- ISO
- SOC I
- SOC II
- HIPAA BAA
- EU DPA
- Regional/National Certs

Continuous compliance approach

- Security goals set in context of business and industry requirements
- Security analytics & best practices deployed to detect and respond to threats
- Benchmarked to a high bar of certifications and accreditations to ensure compliance
- Continual monitoring, test and audit
- Ongoing update of certifications for new services

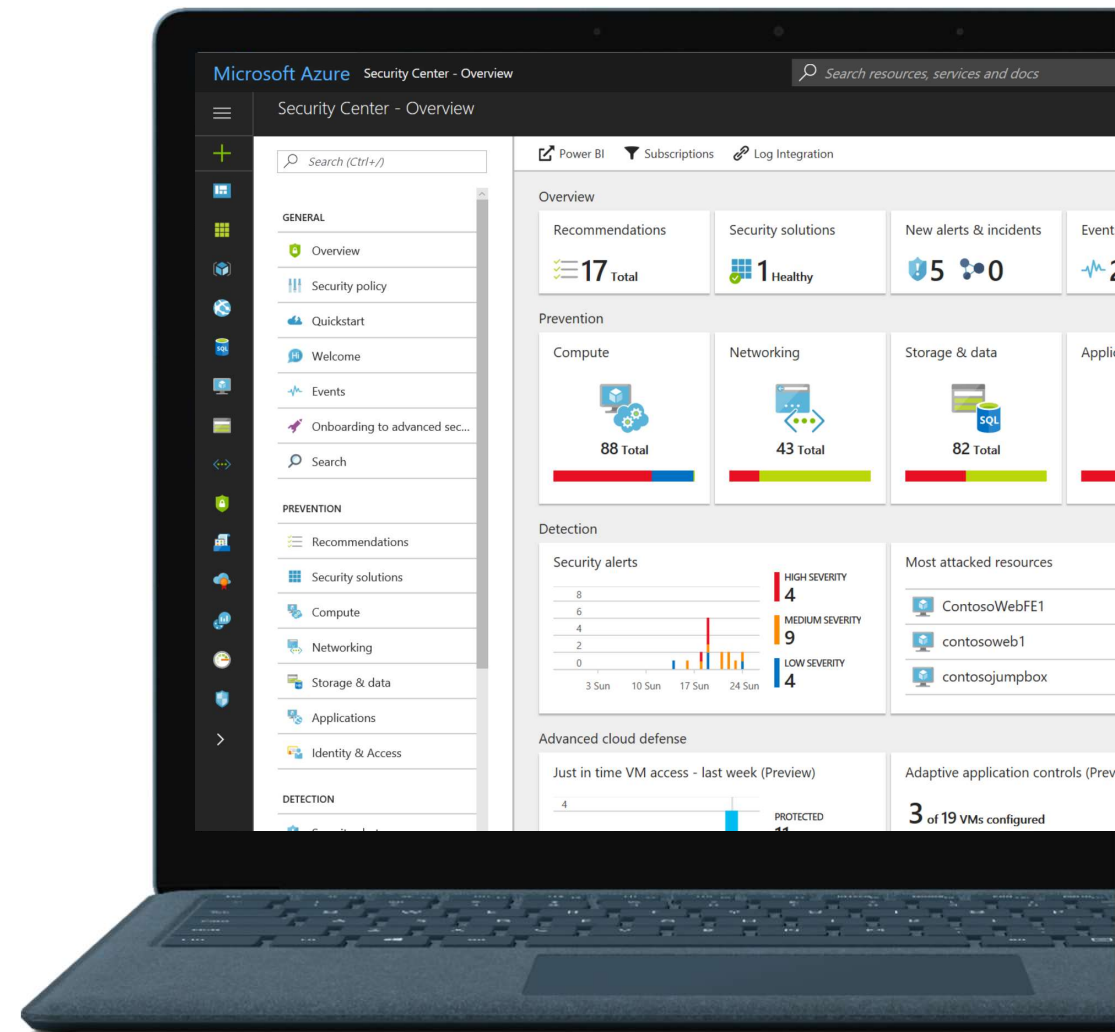


Azure Security Center

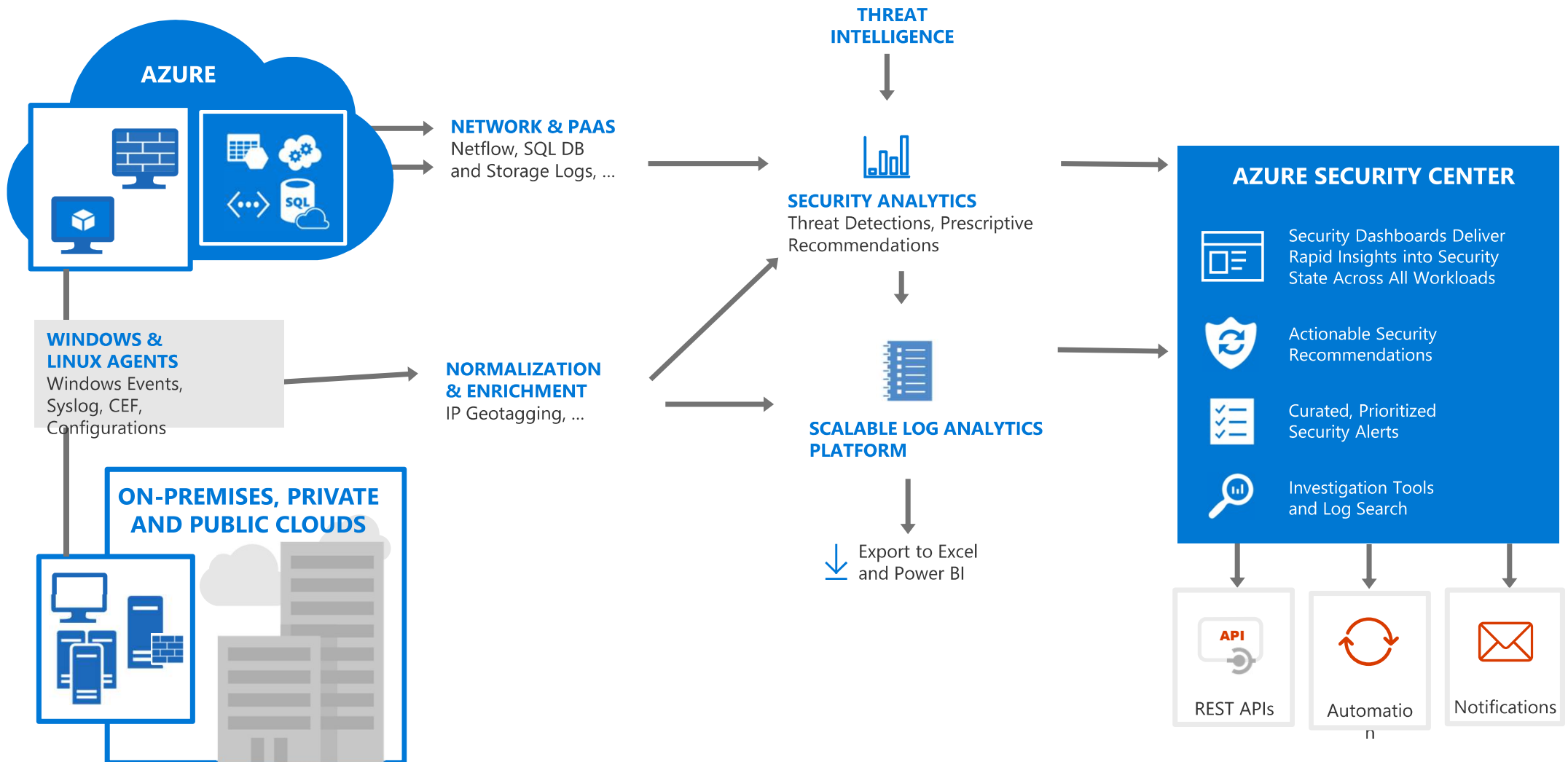
Protection through best practices

Detect threats and attacks

Remediate issues



Architecture of Azure Security Center



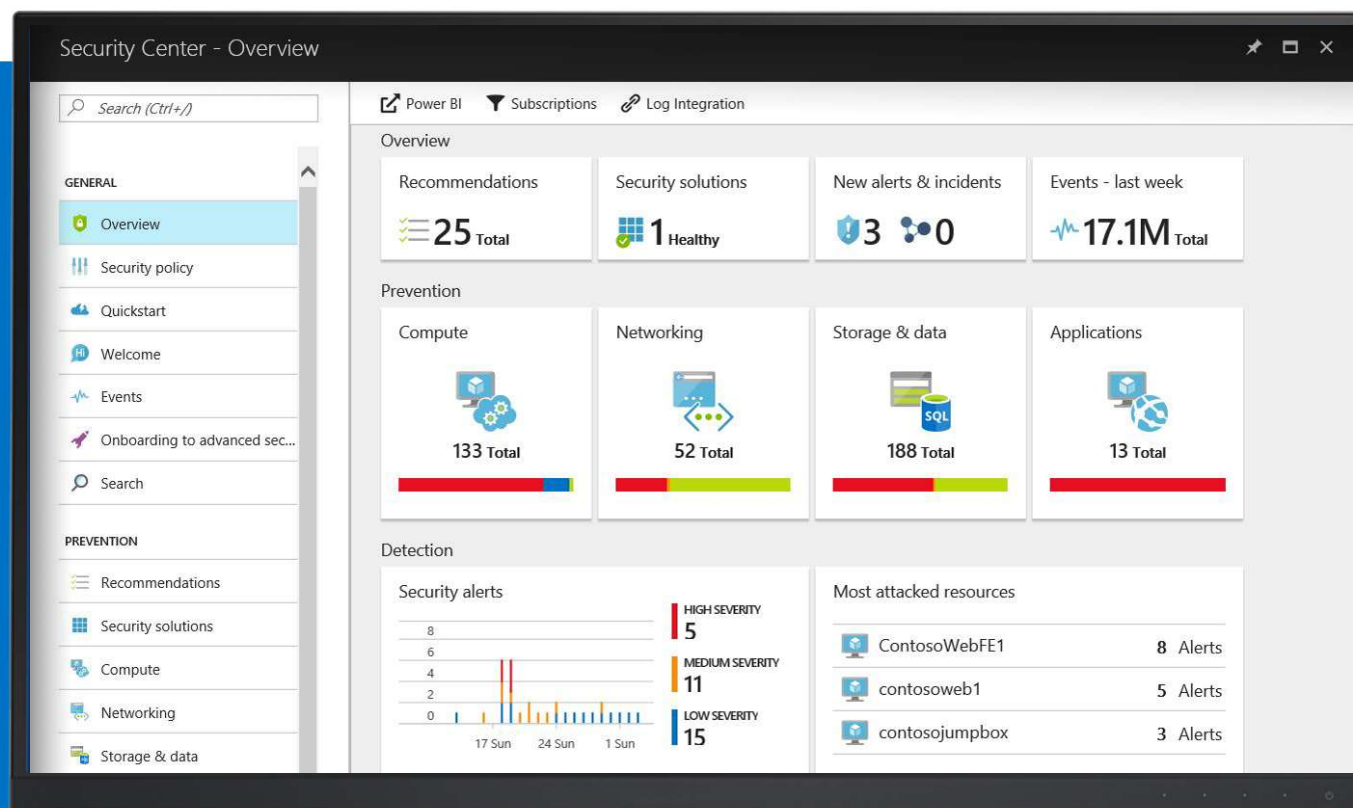
Understand security state across hybrid workloads

Built-in Azure, no setup required

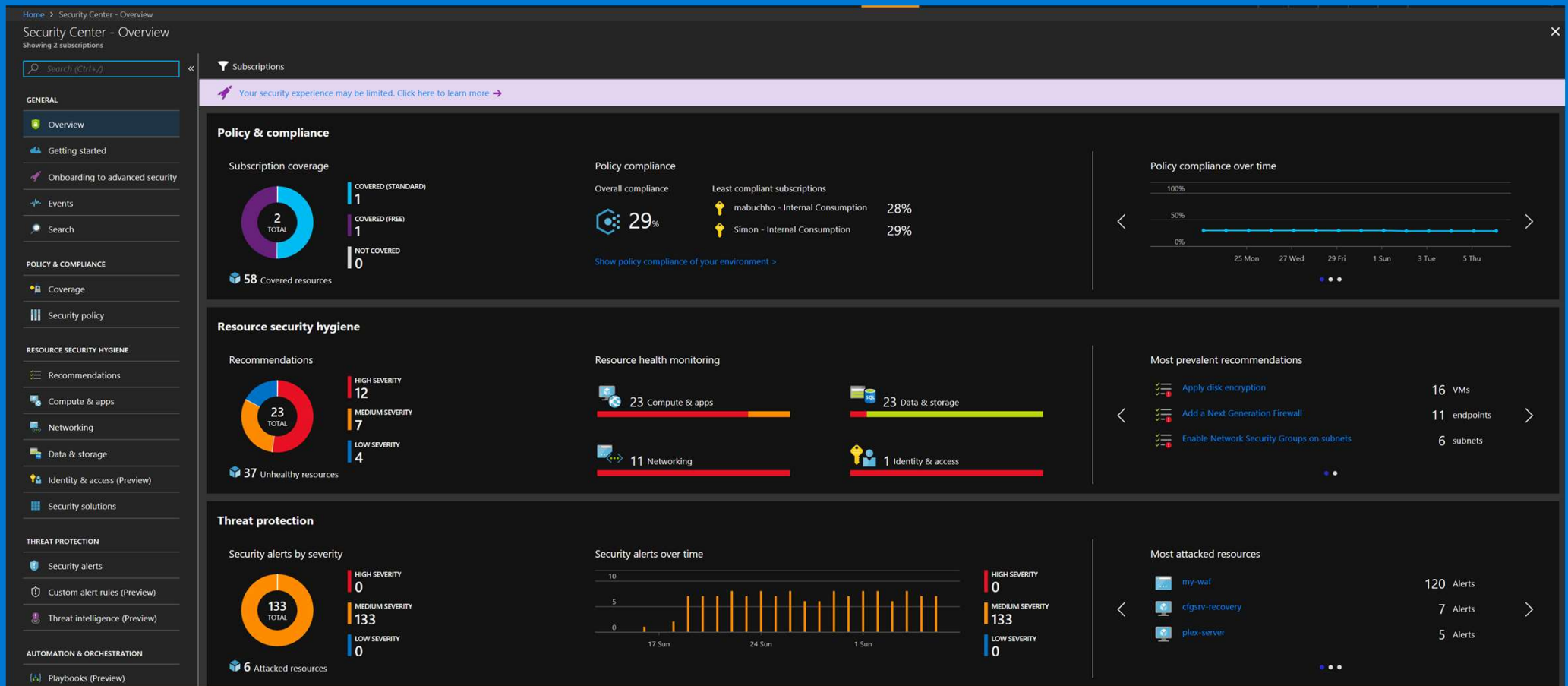
- Automatically discover and monitor security of Azure resources

Gain insights for hybrid resources

- Easily onboard resources running in other clouds and on-premises



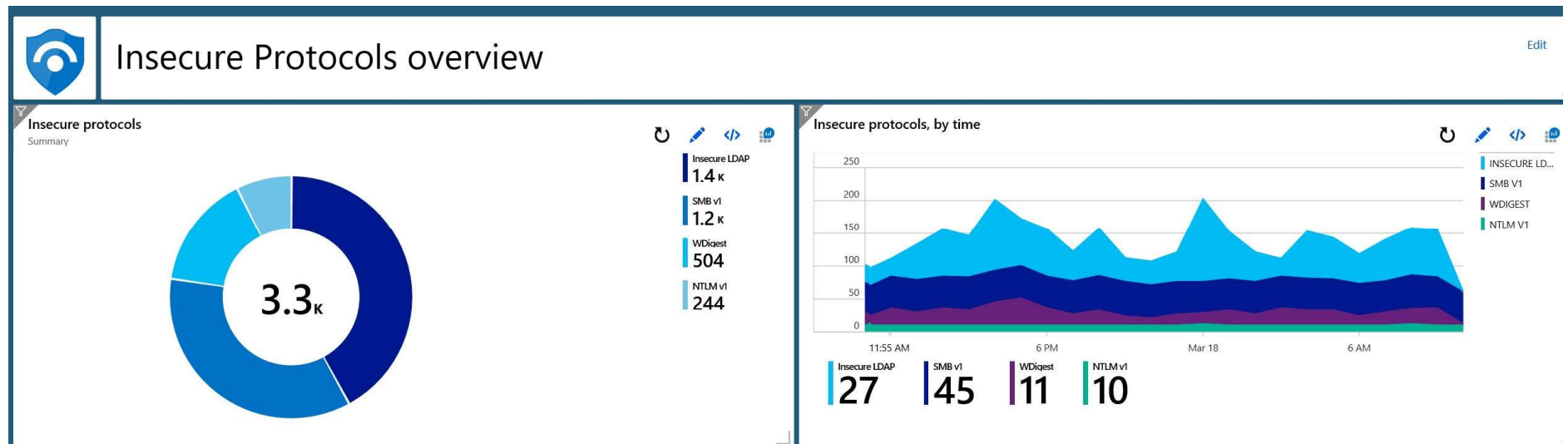
Demo in Azure Portal



Azure Sentinel insecure protocols dashboard

The Azure Sentinel IP dashboard allows you to gain insights into insecure protocol traffic by collecting and analysing security events from Microsoft products.

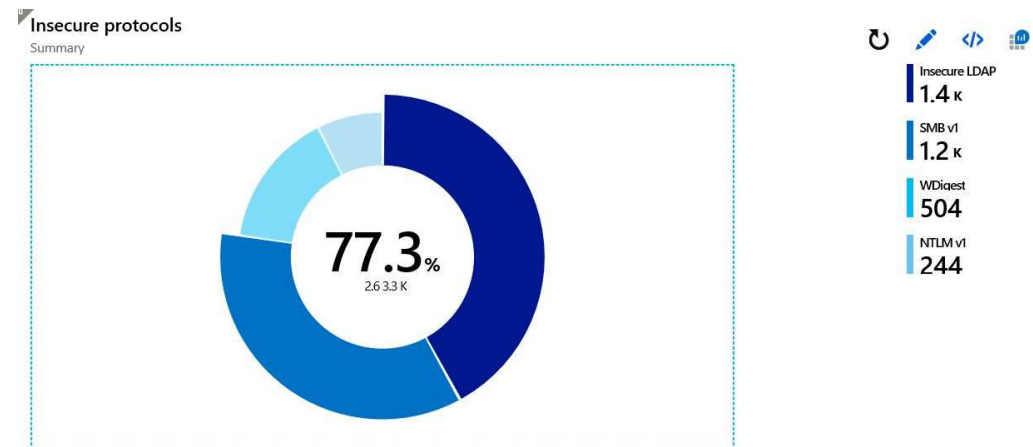
You can view analytics and quickly identify use of weak authentication as well as sources of legacy protocol traffic, like NTLM and SMBv1. You will also have the ability to monitor use of weak ciphers.



Azure Sentinel insecure protocols dashboard

The IP dashboard consist of detections for the following insecure protocols and procedures:

- NTLMv1
- SMBv1
- wDigest
- Unsigned LDAP Binds
- Weak ciphers being used in the Kerberos stack



<https://blogs.technet.microsoft.com/jonsh/azure-sentinel-insecure-protocols-dashboard-setup/>

Threat and Vulnerability Management (TVM) within Microsoft Defender ATP

Empower security teams to discover, prioritise, and remediate known vulnerabilities and misconfigurations

Customers can speed up mitigations by leveraging the integrated remediation processes in ATP to bridge the gap between security and IT teams.

Real-time detection insights correlated with endpoint vulnerabilities.

Built-in remediation processes through integration with Microsoft Intune and Microsoft System Center Configuration Manager.

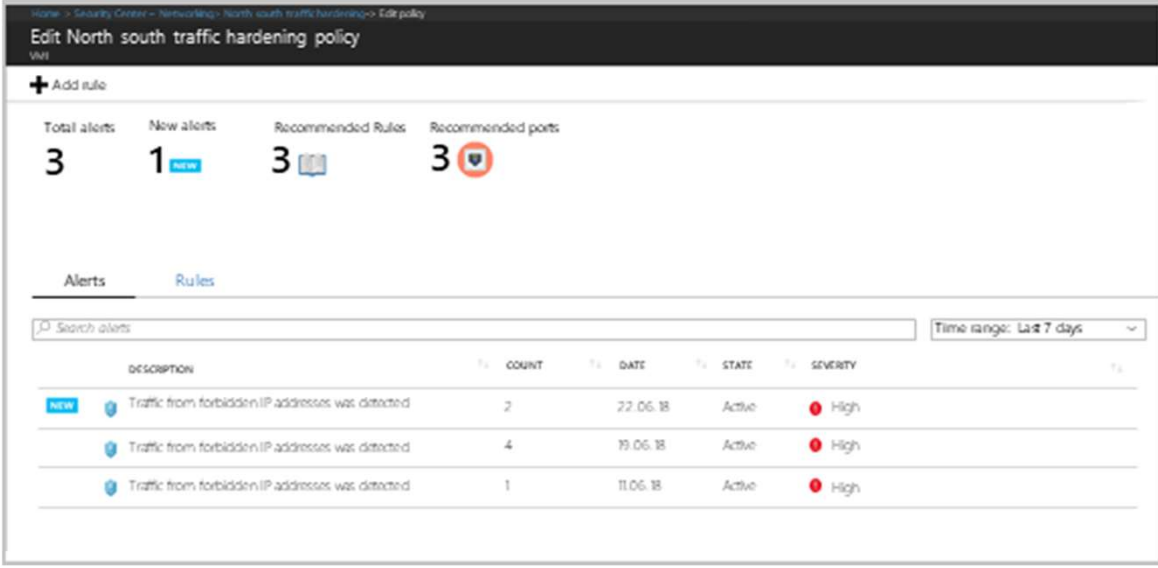
TVM will be available as a public preview for Microsoft Defender ATP customers within the next month.

Adaptive Network Hardening

Adaptive Network Hardening provides recommendations to further harden NSG rules

With this feature, Security Center learns the network traffic and connectivity patterns of Azure workloads and provides NSG rule recommendations, for internet facing virtual machines. This helps end users better configure their network access policies and limit their exposure to attacks.

Every internet facing virtual machine is analyzed for the traffic rules of the network security groups that protect it either on the subnet or the NIC level, as well as the actual traffic that's passing on to the virtual machine. Security Center then correlates this information, along with other indicators such as threat intelligence feeds and known attacker patterns, then recommends to restrict traffic according to the machine learning algorithm.



Home > Security Center > Networking > North south traffic hardening > Edit policy

Edit North south traffic hardening policy

VM

+ Add rule

Total alerts
3

New alerts
1 NEW

Recommended Rules
3

Recommended ports
3

Alerts Rules

Time range: Last 7 days

	DESCRIPTION	COUNT	DATE	STATE	SEVERITY
NEW	Traffic from forbidden IP addresses was detected	2	22.06.18	Active	High
	Traffic from forbidden IP addresses was detected	4	19.06.18	Active	High
	Traffic from forbidden IP addresses was detected	1	11.06.18	Active	High

Search (Ctrl+J)

GENERAL

Overview

Getting Started

Onboarding to advanced security

Events

Search

POLICY

Coverage

Security policy

RESOURCES

Recommendations

Security solutions

Compute & Apps

Networking

Data security

Identity & access

THREAT PROTECTION

Security alerts

Custom alert rules (Preview)

Threat intelligence

Action

Overview

131 Networking topology

22 Internet facing endpoints

Resource type: All

Severity: All

Status: All

Network map

Riskiest resources

32 VIRTUAL MACHINES

12 SUBNETS

See topology >

Adaptive Network Hardening

Just in time VM access - Last week

Healthy 30 VMs

Unhealthy 45 VMs

Unscanned 15 VMs

Top riskiest resources

classicvm1881

21 Recommendations

NEW

Virtual machine 2

16 Recommendations

NEW

Subnet-1

13 Recommendations

CONSTANT

Security controls

DESCRIPTION	RESOURCE TYPE	TOTAL RESOURCES	
NGFW not installed	Endpoints	15 of 60	
NSGs on subnets not enabled	Subnets	6 of 88	
NSGs on VMs not enabled	Virtual machines	5 of 66	
Restrict access through Internet facing endpoint	Virtual machines	16 of 66	
Healthy Internet facing endpoints	Endpoints	44 of 60	

Adaptive Network Hardening

Adaptive Network Hardening provides recommendations to further harden NSG rules

The feature will evaluate Internet facing Azure VMs for the IP ranges that should be allowed to communicate with specific ports. The result is an NSG rule recommendation ("allow" rules only).

Adaptive Network Hardening recommendations are supported on the following ports: 22, 3389, 21, 23, 445, 4333, 3306, 1433, 1434, 53, 20, 5985, 5986, 5432, 139, 66, 1128

Home > Security Center > Networking > North-south traffic hardening > Edit policy

Edit North-south traffic hardening policy

+ Add rule

Total alerts: 3

New alerts: 1 new

Recommended Rules: 3

Recommended ports: 3

Alerts Rules

Search rules

Type	Name	Destination port	Source IP ranges	Protocol	Alerts	
<input type="checkbox"/>	ASC NSG 1	22	192.11.1/24	TCP	4	...
<input type="checkbox"/>	ASC BT	3389	*	UDP	5	...
<input type="checkbox"/>	ASC NSG 3	111	192.1.2.3/32	TCP/UDP	6	...

Edit rule
Delete rule

Enforce

To learn more, visit

<https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-network-hardening>

Thank you!

Any questions?