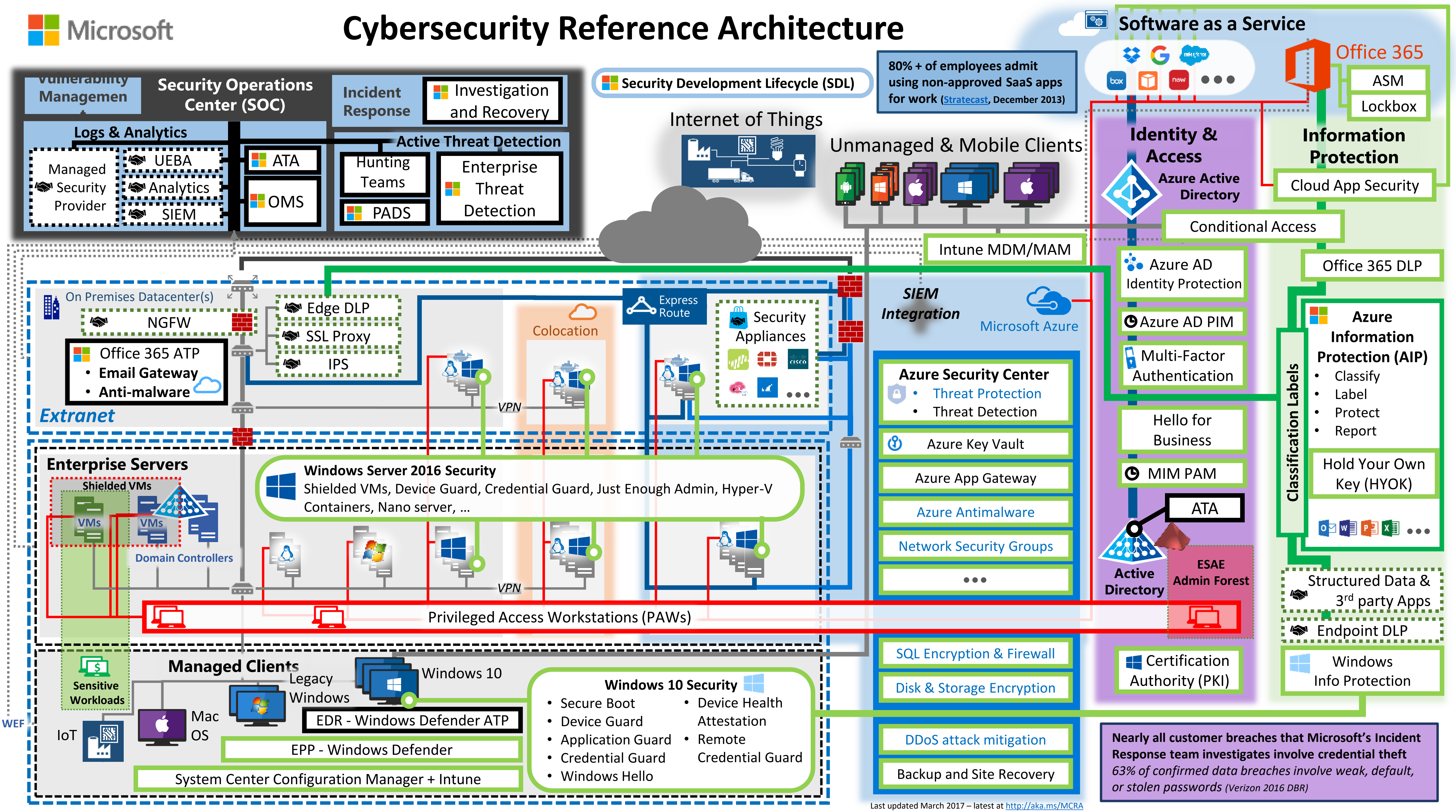
Azure Security Center

Vadym Popov
Head of Consulting Division
Comparex Ukraine

Microsoft

Cybersecurity Reference Architecture



Vulnerability Management

Security Operations Center (SOC)

Incident Response

Investigation and Recovery

Logs & Analytics

Managed Security Provider

UEBA

Analytics

SIEM

ATA

OMS

Active Threat Detection

Hunting Teams

PADS

Enterprise Threat Detection

Security Development Lifecycle (SDL)

80% + of employees admit using non-approved SaaS apps for work (Stratecast, December 2013)

Software as a Service

Office 365

ASM

Lockbox

Internet of Things

Unmanaged & Mobile Clients

Identity & Access

Azure Active Directory

Information Protection

Cloud App Security

Conditional Access

Intune MDM/MAM

Office 365 DLP

Azure AD Identity Protection

Azure AD PIM

Multi-Factor Authentication

Hello for Business

MIM PAM

ATA

Active Directory

ESAE Admin Forest

Certification Authority (PKI)

Classification Labels

Azure Information Protection (AIP)
- Classify
- Label
- Protect
- Report

Hold Your Own Key (HYOK)

Structured Data & 3rd party Apps

Endpoint DLP

Windows Info Protection

SIEM Integration

Microsoft Azure

Azure Security Center
- Threat Protection
- Threat Detection

Azure Key Vault

Azure App Gateway

Azure Antimalware

Network Security Groups

•••

SQL Encryption & Firewall

Disk & Storage Encryption

DDoS attack mitigation

Backup and Site Recovery

On Premises Datacenter(s)

NGFW

Office 365 ATP
- Email Gateway
- Anti-malware

Edge DLP

SSL Proxy

IPS

Extranet

Colocation

Express Route

Security Appliances

VPN

Enterprise Servers

Shielded VMs

VMs

VMs

Domain Controllers

Windows Server 2016 Security

Shielded VMs, Device Guard, Credential Guard, Just Enough Admin, Hyper-V Containers, Nano server, …

VPN

Privileged Access Workstations (PAWs)

Managed Clients

Sensitive Workloads

Legacy Windows

Windows 10

IoT

Mac OS

WEF

EDR - Windows Defender ATP

EPP - Windows Defender

System Center Configuration Manager + Intune

Windows 10 Security
- Secure Boot
- Device Guard
- Application Guard
- Credential Guard
- Windows Hello
- Device Health Attestation
- Remote Credential Guard

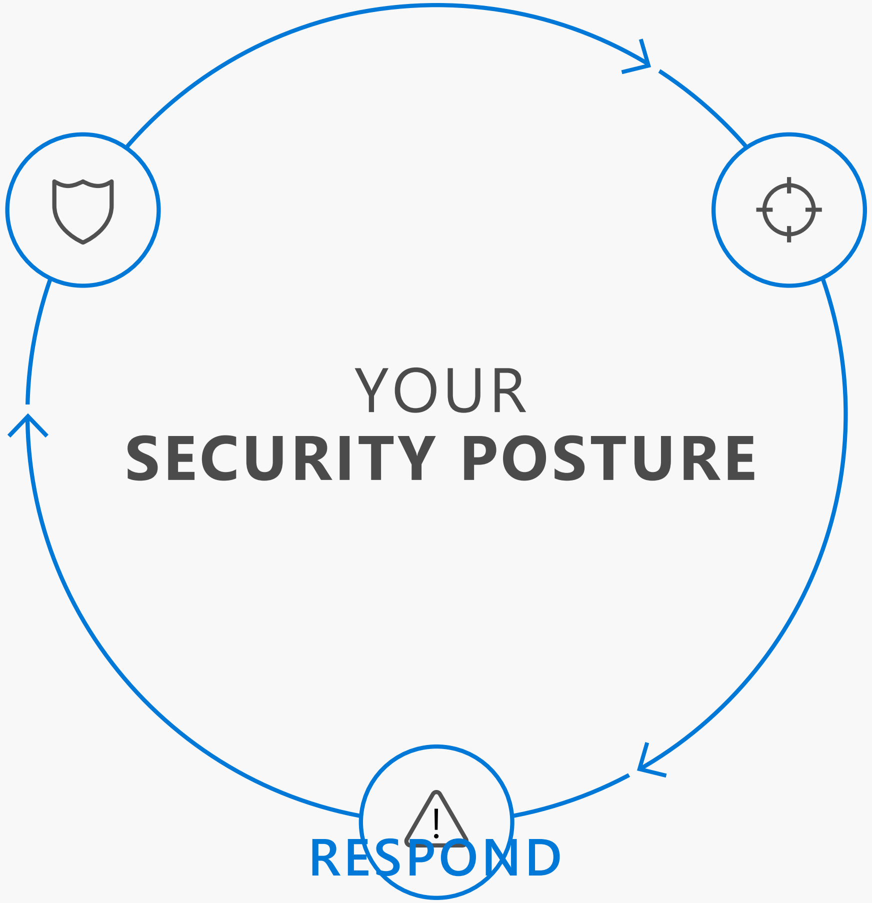
Nearly all customer breaches that Microsoft's Incident Response team investigates involve credential theft

63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

Last updated March 2017 – latest at http://aka.ms/MCRA

Top 10 Azure Security Features

- **Azure Security Center**
- **OMS Security and Compliance**
- **Azure Key Vault**
- **Azure Disk Encryption**
- **Azure Storage Encryption**
- **Azure Storage Service Encryption**
- **Azure SQL Transparent Data Encryption**
- **Azure SQL Cell Level Encryption**
- **Azure Log Integration**
- **Azure Active Directory Multi-Factor Authentication**
- **Azure Active Directory Privileged Identity Management**



YOUR
SECURITY POSTURE

PROTECT

across all endpoints, from
sensors to the datacenter

DETECT

using targeted signals, behavioral
monitoring, and machine learning

RESPOND

closing the gap between discovery and action

Hybrid cloud requires a new approach for security

- **Distributed infrastructure**

  Need better visibility and control

- **Rapidly changing cloud resources**

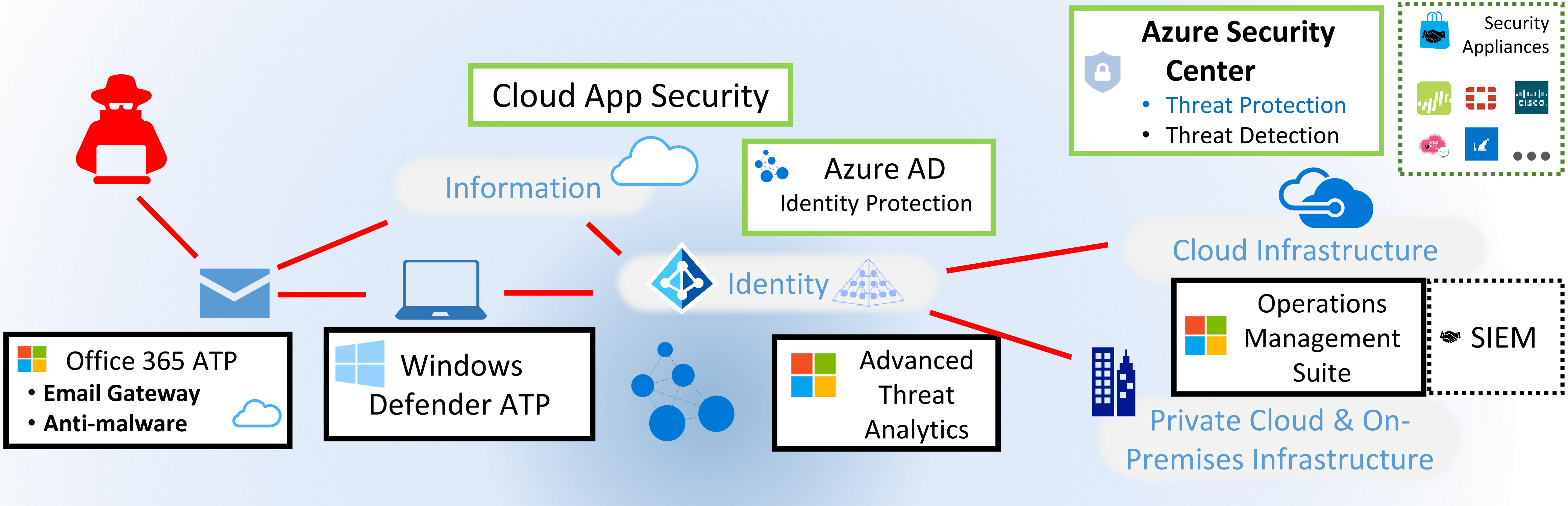
  Require solutions that keep pace with speed and agility of cloud

- **Increasingly sophisticated threats**

  Leverage analytics and threat intelligence to detect threats quickly

Microsoft Threat Detection

Deep insight across your environment



Cloud App Security

Azure AD
Identity Protection

Azure Security Center
- Threat Protection
- Threat Detection

Security Appliances

Information

Identity

Cloud Infrastructure

Office 365 ATP
- **Email Gateway**
- **Anti-malware**

Windows Defender ATP

Advanced Threat Analytics

Operations Management Suite

SIEM

Private Cloud & On-Premises Infrastructure

Microsoft Azure Security Center

Unify security management and enable advanced threat protection for hybrid cloud workloads

Unified visibility and control

Adaptive threat prevention

Intelligent detection and response

Unified visibility and control

Dynamically discover and manage the security of your hybrid cloud workloads in a single cloud-based console

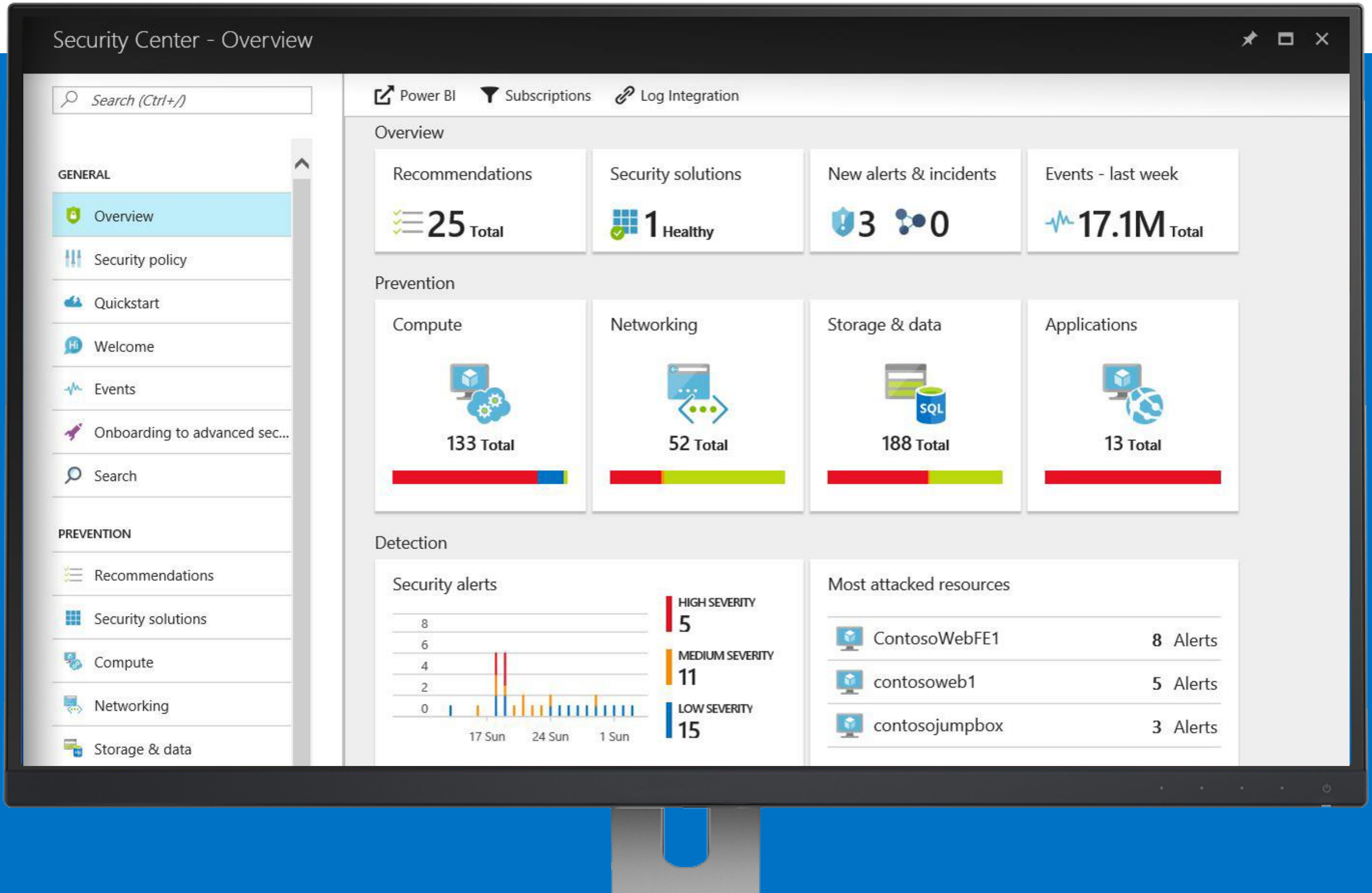
Understand security state across hybrid workloads

Built-in Azure, no setup required

- Automatically discover and monitor security of Azure resources

Gain insights for hybrid resources

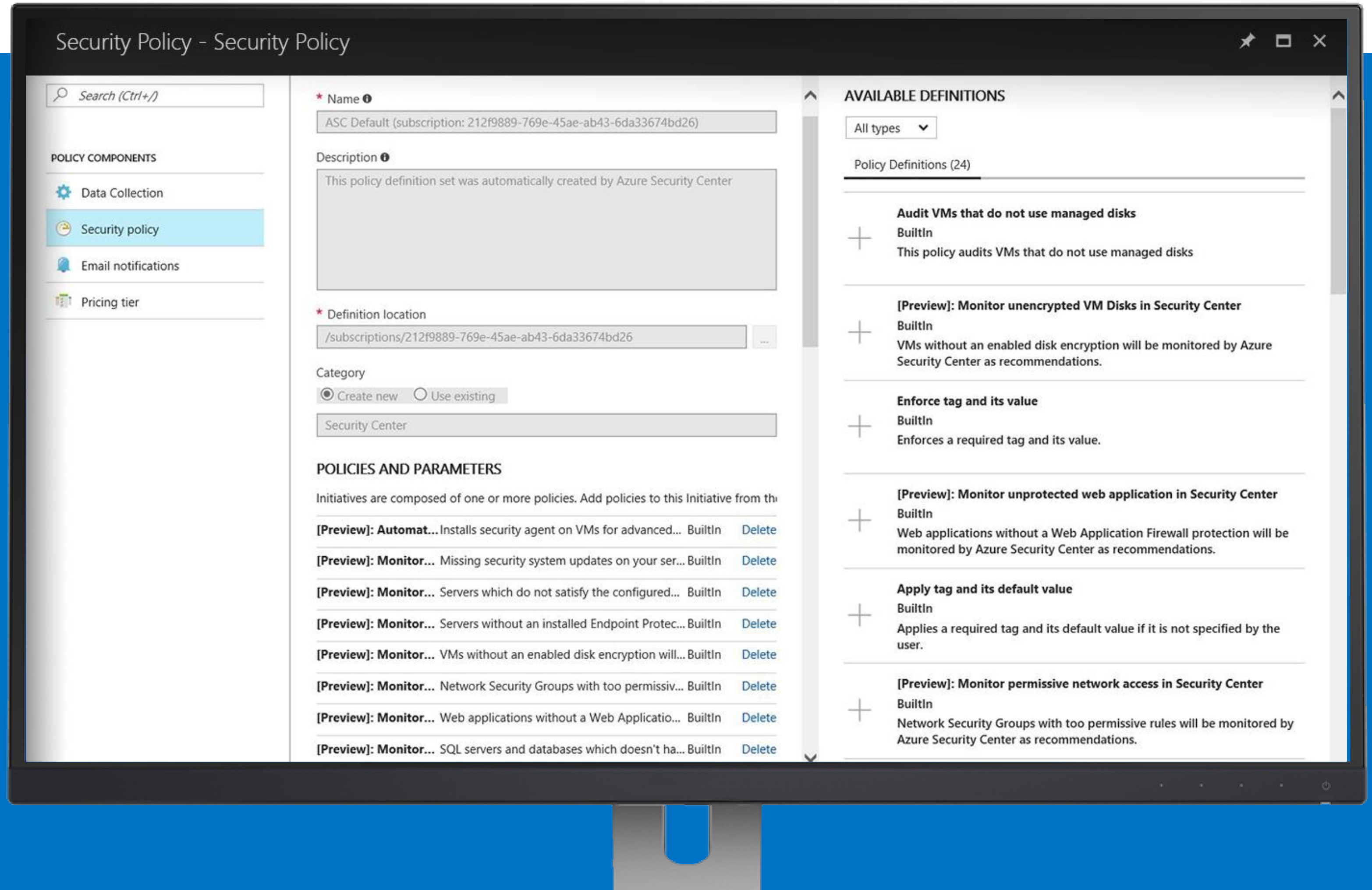
- Easily onboard resources running in other clouds and on-premises



Ensure compliance with policy management

Central policy management

- Define a security policy for each subscription in Security Center
- Apply across multiple subscriptions using Azure Management Groups



Security Policy - Security Policy

Search (Ctrl+/)

POLICY COMPONENTS

- Data Collection
- Security policy
- Email notifications
- Pricing tier

* Name: ASC Default (subscription: 212f9889-769e-45ae-ab43-6da33674bd26)

Description: This policy definition set was automatically created by Azure Security Center

* Definition location: /subscriptions/212f9889-769e-45ae-ab43-6da33674bd26

Category: ● Create new ○ Use existing

Security Center

POLICIES AND PARAMETERS

Initiatives are composed of one or more policies. Add policies to this Initiative from th

[Preview]: Automat...	Installs security agent on VMs for advanced...	BuiltIn	Delete
[Preview]: Monitor...	Missing security system updates on your ser...	BuiltIn	Delete
[Preview]: Monitor...	Servers which do not satisfy the configured...	BuiltIn	Delete
[Preview]: Monitor...	Servers without an installed Endpoint Protec...	BuiltIn	Delete
[Preview]: Monitor...	VMs without an enabled disk encryption will...	BuiltIn	Delete
[Preview]: Monitor...	Network Security Groups with too permissiv...	BuiltIn	Delete
[Preview]: Monitor...	Web applications without a Web Applicatio...	BuiltIn	Delete
[Preview]: Monitor...	SQL servers and databases which doesn't ha...	BuiltIn	Delete

AVAILABLE DEFINITIONS

All types

Policy Definitions (24)

Audit VMs that do not use managed disks
BuiltIn
This policy audits VMs that do not use managed disks

[Preview]: Monitor unencrypted VM Disks in Security Center
BuiltIn
VMs without an enabled disk encryption will be monitored by Azure Security Center as recommendations.

Enforce tag and its value
BuiltIn
Enforces a required tag and its value.

[Preview]: Monitor unprotected web application in Security Center
BuiltIn
Web applications without a Web Application Firewall protection will be monitored by Azure Security Center as recommendations.

Apply tag and its default value
BuiltIn
Applies a required tag and its default value if it is not specified by the user.

[Preview]: Monitor permissive network access in Security Center
BuiltIn
Network Security Groups with too permissive rules will be monitored by Azure Security Center as recommendations.

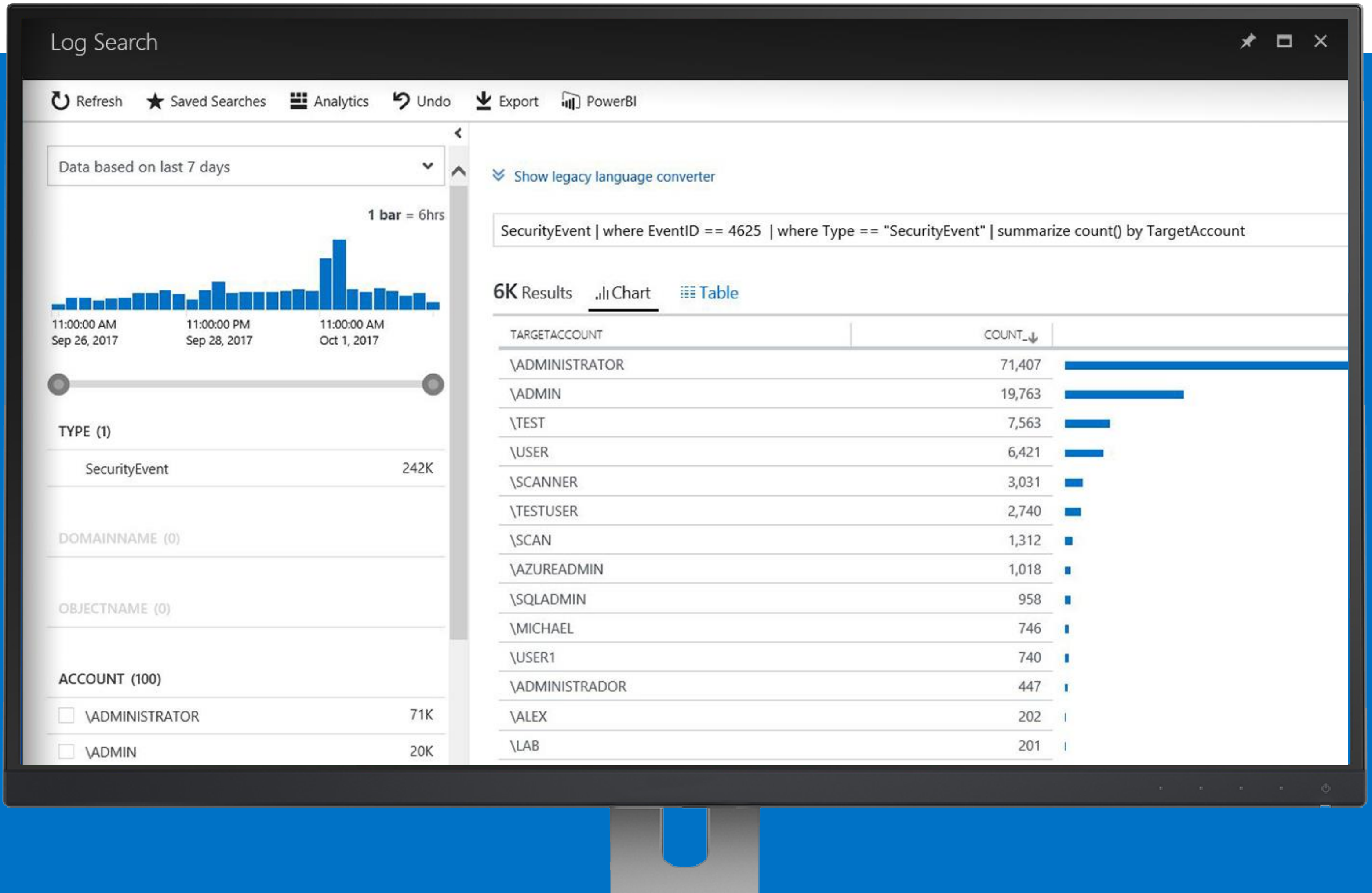
Gain deeper insights with integrated log analytics

Quickly identify list of notable events that require your attention

- Out of the box notable events in dashboard or create custom queries

Search and analyze security data using a flexible query language

- Use built-in or custom queries with Log Analytics search



Data based on last 7 days

TYPE (1)

SecurityEvent	242K

DOMAINNAME (0)

OBJECTNAME (0)

ACCOUNT (100)

□ \ADMINISTRATOR	71K
□ \ADMIN	20K

```
SecurityEvent | where EventID == 4625  | where Type == "SecurityEvent" | summarize count() by TargetAccount
```

TARGETACCOUNT	COUNT
\ADMINISTRATOR	71,407
\ADMIN	19,763
\TEST	7,563
\USER	6,421
\SCANNER	3,031
\TESTUSER	2,740
\SCAN	1,312
\AZUREADMIN	1,018
\SQLADMIN	958
\MICHAEL	746
\USER1	740
\ADMINISTRADOR	447
\ALEX	202
\LAB	201

Analyze security information from variety of sources

Integrated partners

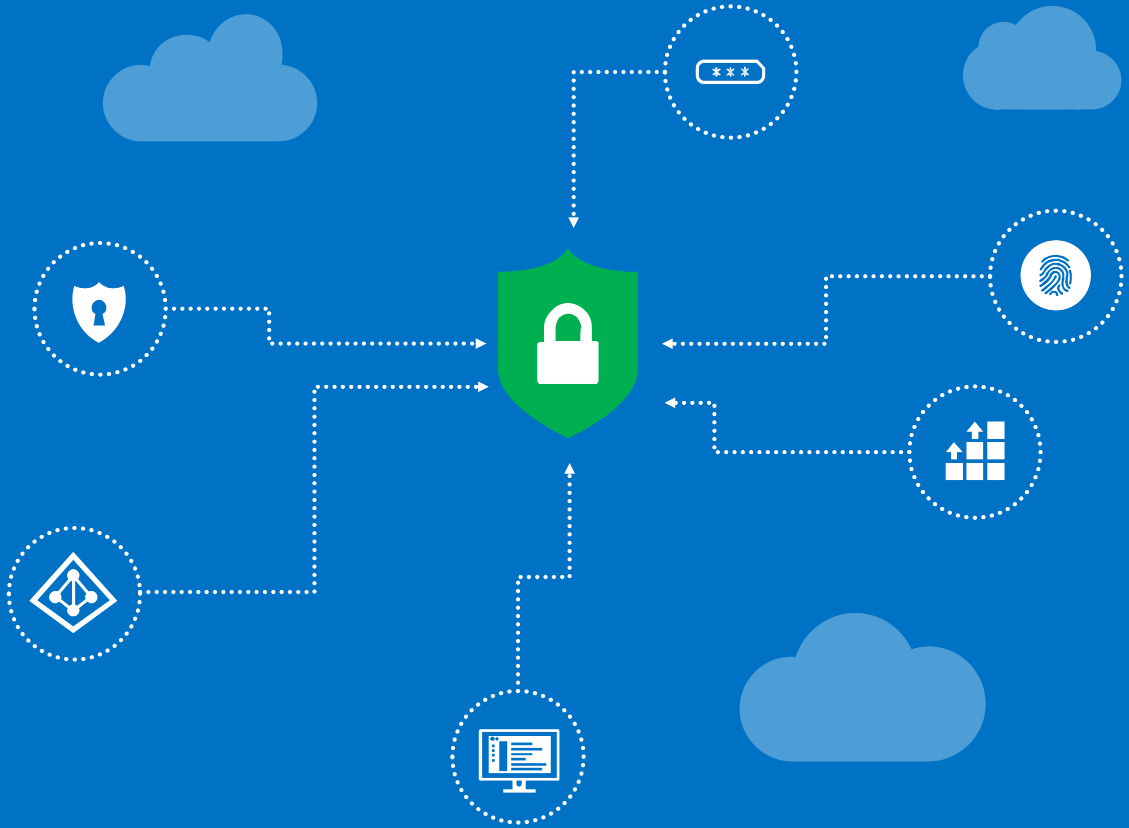
- Connected security solutions running in Azure, e.g. firewalls and antimalware solutions

Microsoft security

- Azure Active Directory Information Protection
- Advanced Threat Analytics

Many others

- Any security solution that supports Common Event Format (CEF)



Adaptive threat prevention

Enable actionable, adaptive protections that identify and mitigate risk to reduce exposure to attacks

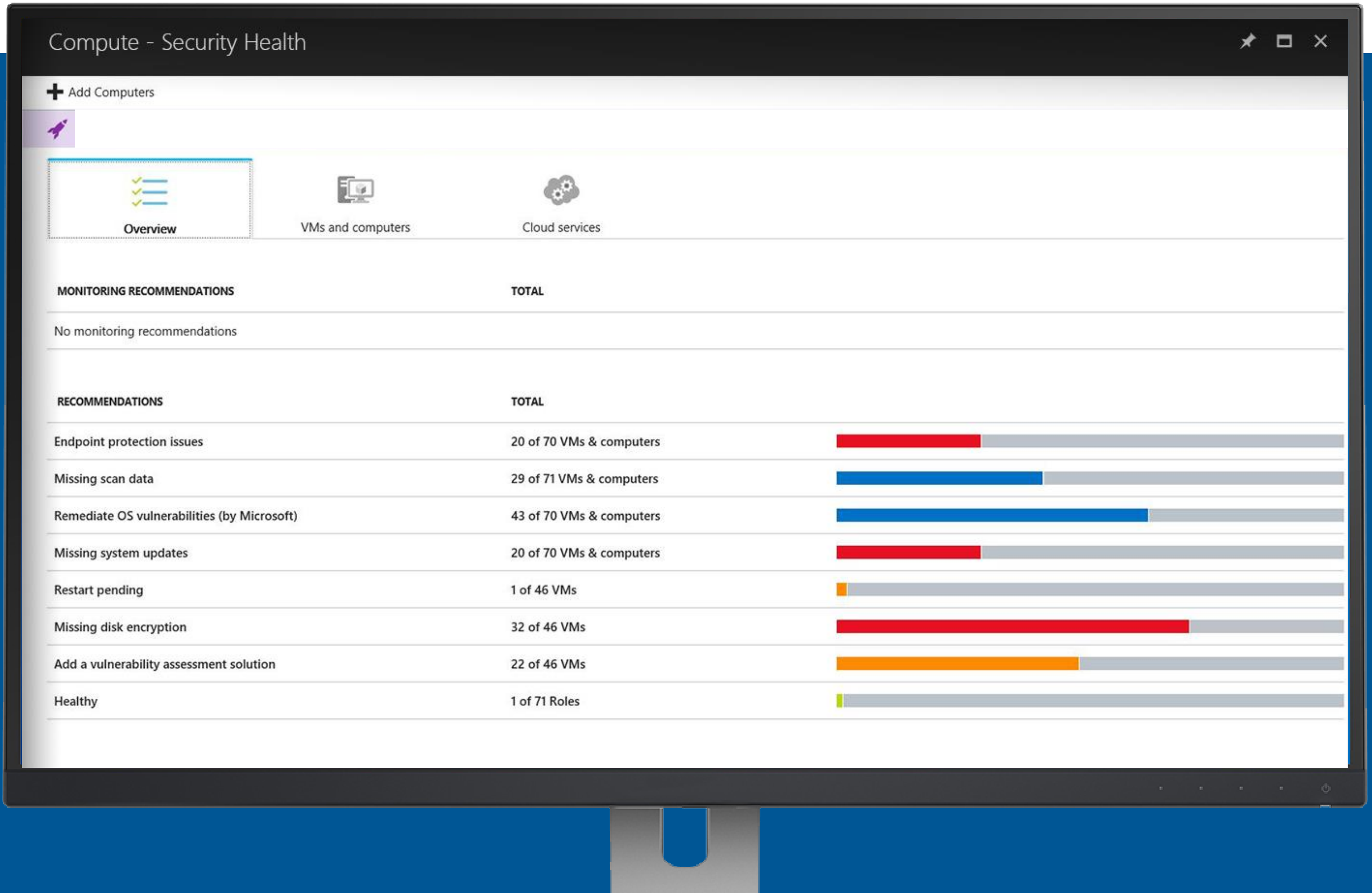
Identify and remediate vulnerabilities quickly

Continuous assessment of machines, networks, and Azure services

- Hundreds of built-in security assessments, or create your own

Fix vulnerabilities quickly

- Prioritized, actionable security recommendations



Compute - Security Health

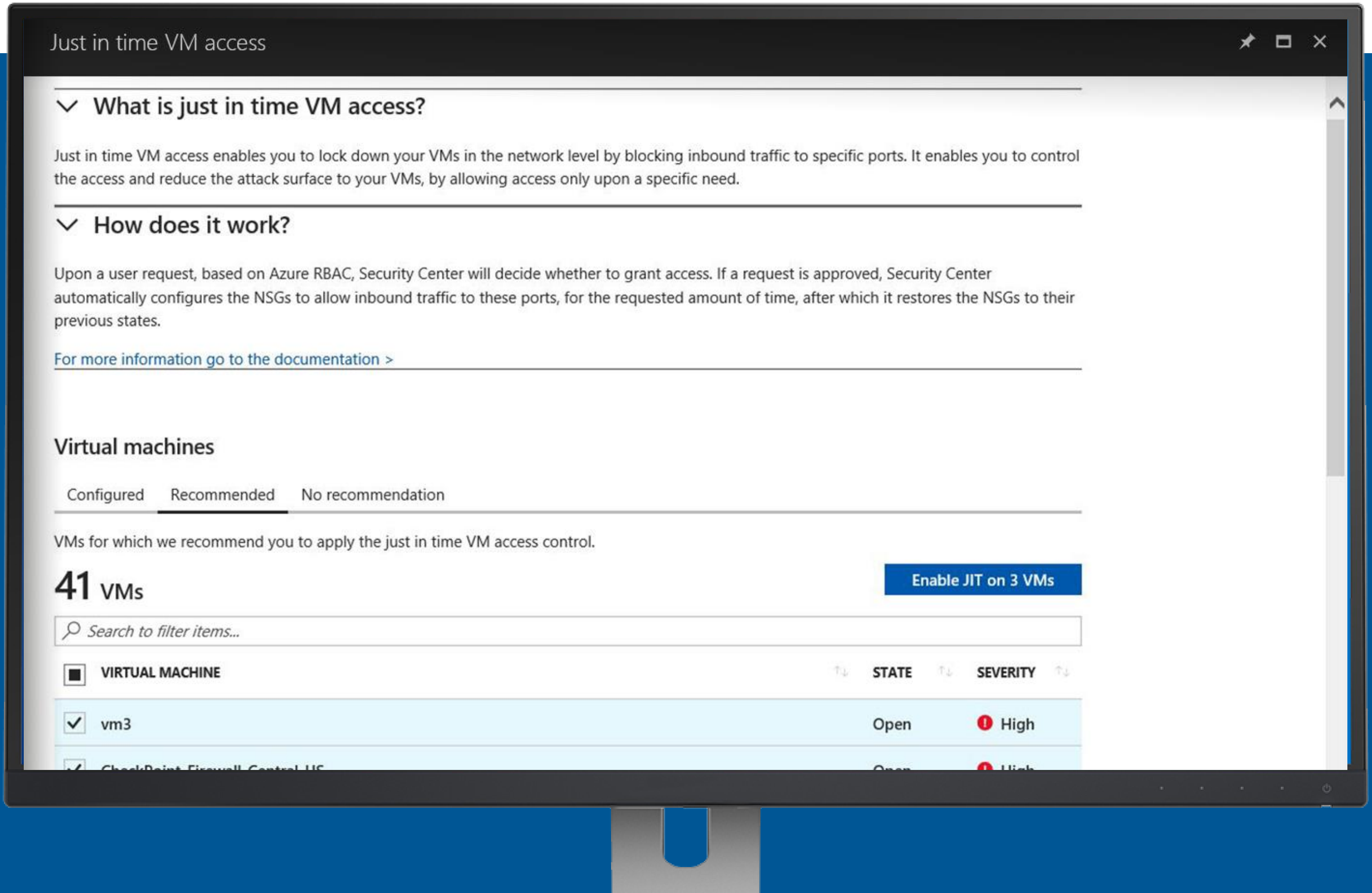
MONITORING RECOMMENDATIONS	TOTAL
No monitoring recommendations	

RECOMMENDATIONS	TOTAL
Endpoint protection issues	20 of 70 VMs & computers
Missing scan data	29 of 71 VMs & computers
Remediate OS vulnerabilities (by Microsoft)	43 of 70 VMs & computers
Missing system updates	20 of 70 VMs & computers
Restart pending	1 of 46 VMs
Missing disk encryption	32 of 46 VMs
Add a vulnerability assessment solution	22 of 46 VMs
Healthy	1 of 71 Roles

Limit exposure to brute-force attacks

Lock down ports on virtual machines

- Enable just-in-time access to virtual machines
- Access automatically granted for limited time



What is just in time VM access?

Just in time VM access enables you to lock down your VMs in the network level by blocking inbound traffic to specific ports. It enables you to control the access and reduce the attack surface to your VMs, by allowing access only upon a specific need.

How does it work?

Upon a user request, based on Azure RBAC, Security Center will decide whether to grant access. If a request is approved, Security Center automatically configures the NSGs to allow inbound traffic to these ports, for the requested amount of time, after which it restores the NSGs to their previous states.

For more information go to the documentation >

Virtual machines

VMs for which we recommend you to apply the just in time VM access control.

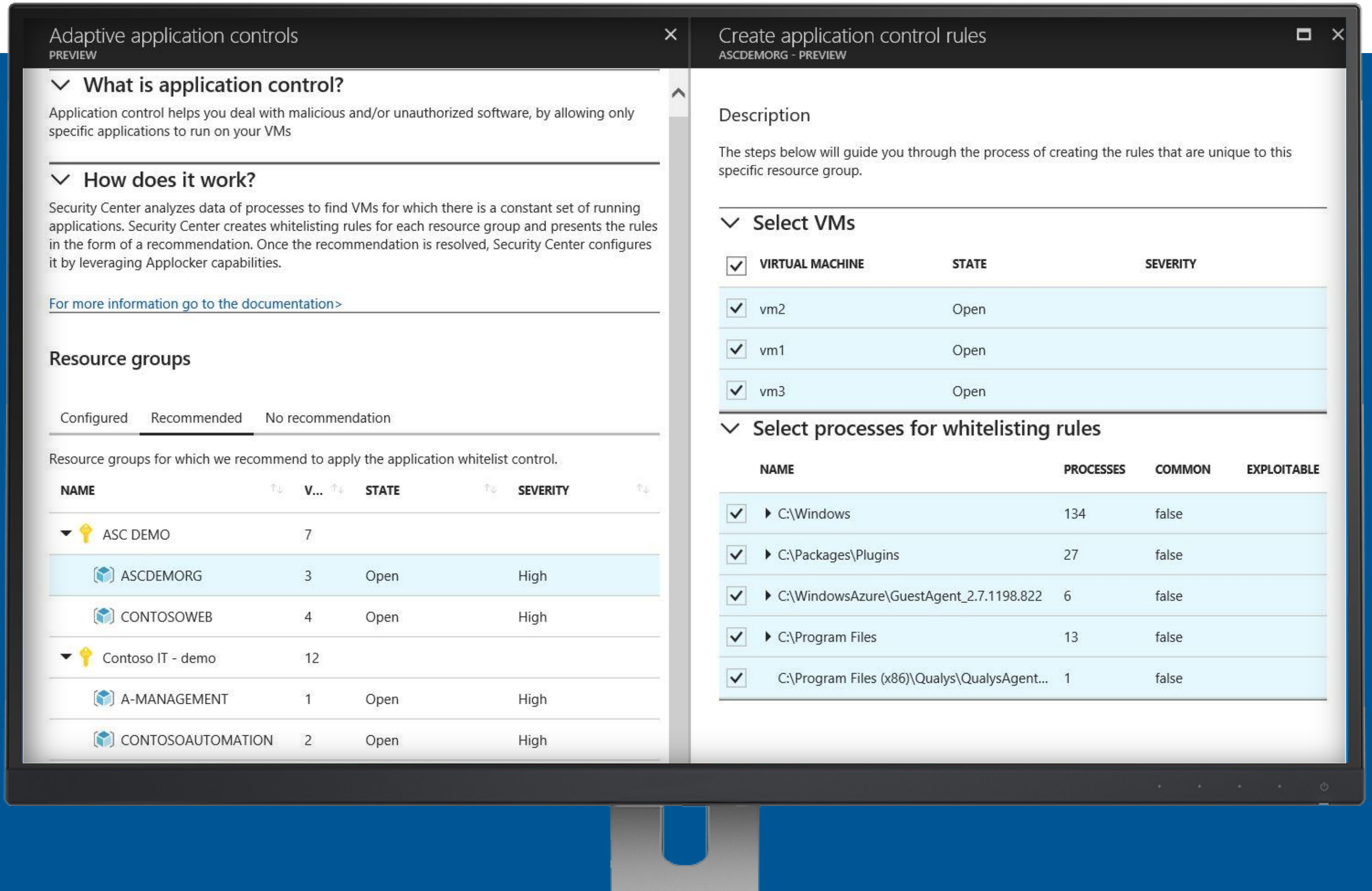
41 VMs

■	VIRTUAL MACHINE	STATE	SEVERITY
☑	vm3	Open	● High
☑	CheckPoint-Firewall-Central-US	Open	● High

Block malware and other unwanted applications

Allow safe applications only

- Adaptive whitelisting learns application patterns
- Simplified management with recommended whitelists



Adaptive application controls
PREVIEW

What is application control?

Application control helps you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your VMs

How does it work?

Security Center analyzes data of processes to find VMs for which there is a constant set of running applications. Security Center creates whitelisting rules for each resource group and presents the rules in the form of a recommendation. Once the recommendation is resolved, Security Center configures it by leveraging Applocker capabilities.

For more information go to the documentation>

Resource groups

Resource groups for which we recommend to apply the application whitelist control.

NAME	V...	STATE	SEVERITY
ASC DEMO	7		
ASCDEMORG	3	Open	High
CONTOSOWEB	4	Open	High
Contoso IT - demo	12		
A-MANAGEMENT	1	Open	High
CONTOSOAUTOMATION	2	Open	High

Create application control rules
ASCDEMORG - PREVIEW

Description

The steps below will guide you through the process of creating the rules that are unique to this specific resource group.

Select VMs

☑	VIRTUAL MACHINE	STATE	SEVERITY
☑	vm2	Open	
☑	vm1	Open	
☑	vm3	Open	

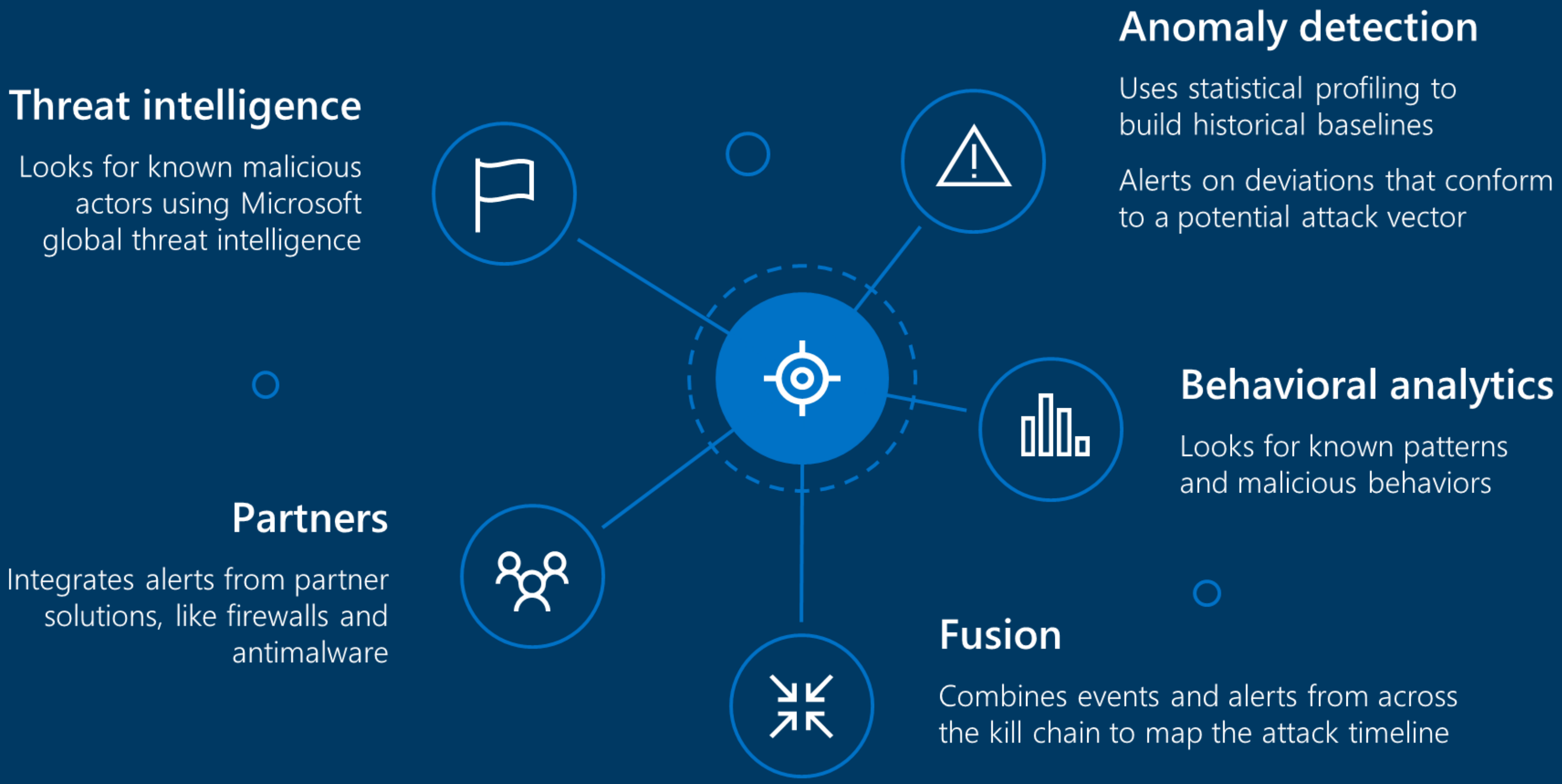
Select processes for whitelisting rules

	NAME	PROCESSES	COMMON	EXPLOITABLE
☑	C:\Windows	134	false	
☑	C:\Packages\Plugins	27	false	
☑	C:\WindowsAzure\GuestAgent_2.7.1198.822	6	false	
☑	C:\Program Files	13	false	
☑	C:\Program Files (x86)\Qualys\QualysAgent...	1	false	

Intelligent detection and response

Use advanced analytics and Microsoft Intelligent Security Graph to rapidly detect and respond to evolving cyber threats

Built-in Intelligence and advanced analytics



Threat intelligence

Looks for known malicious actors using Microsoft global threat intelligence

Anomaly detection

Uses statistical profiling to build historical baselines

Alerts on deviations that conform to a potential attack vector

Behavioral analytics

Looks for known patterns and malicious behaviors

Partners

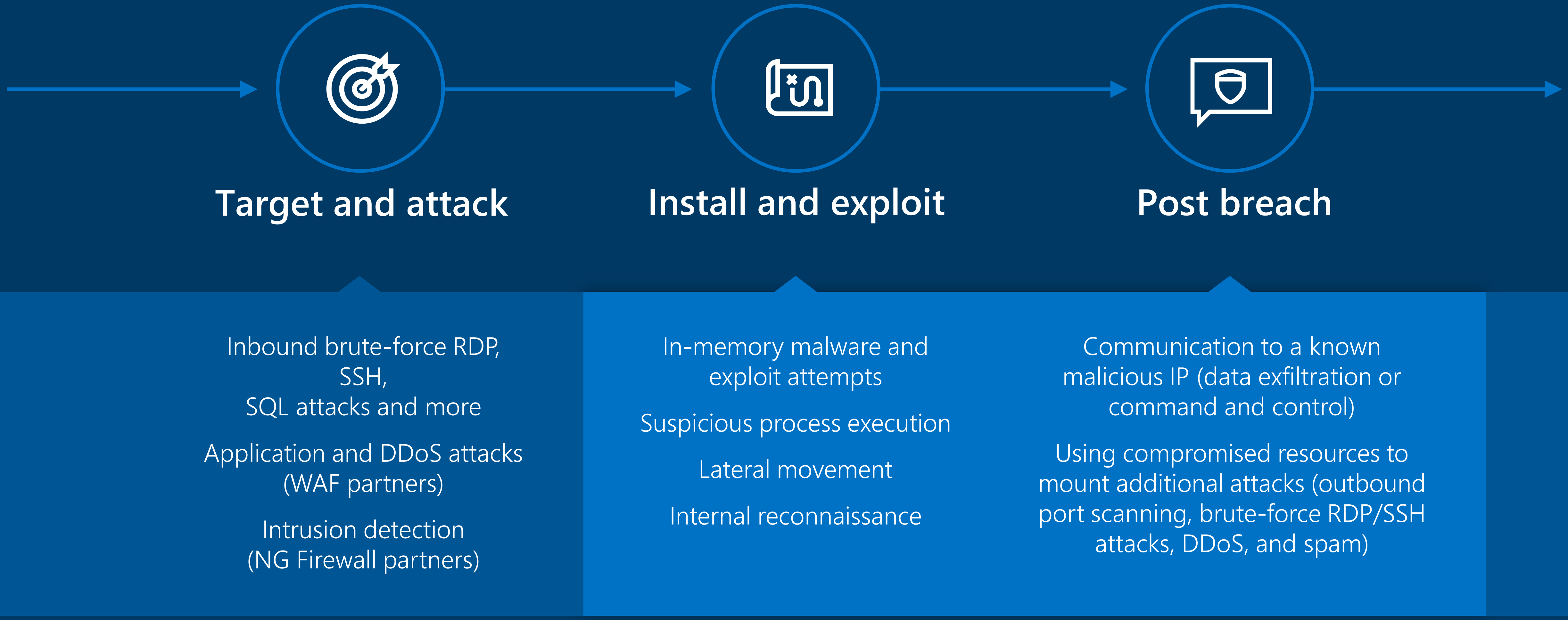
Integrates alerts from partner solutions, like firewalls and antimalware

Fusion

Combines events and alerts from across the kill chain to map the attack timeline

Powered by Microsoft Intelligent Security Graph

Detect threats across the kill chain



Target and attack

Inbound brute-force RDP,
SSH,
SQL attacks and more

Application and DDoS attacks
(WAF partners)

Intrusion detection
(NG Firewall partners)

Install and exploit

In-memory malware and
exploit attempts

Suspicious process execution

Lateral movement

Internal reconnaissance

Post breach

Communication to a known
malicious IP (data exfiltration or
command and control)

Using compromised resources to
mount additional attacks (outbound
port scanning, brute-force RDP/SSH
attacks, DDoS, and spam)

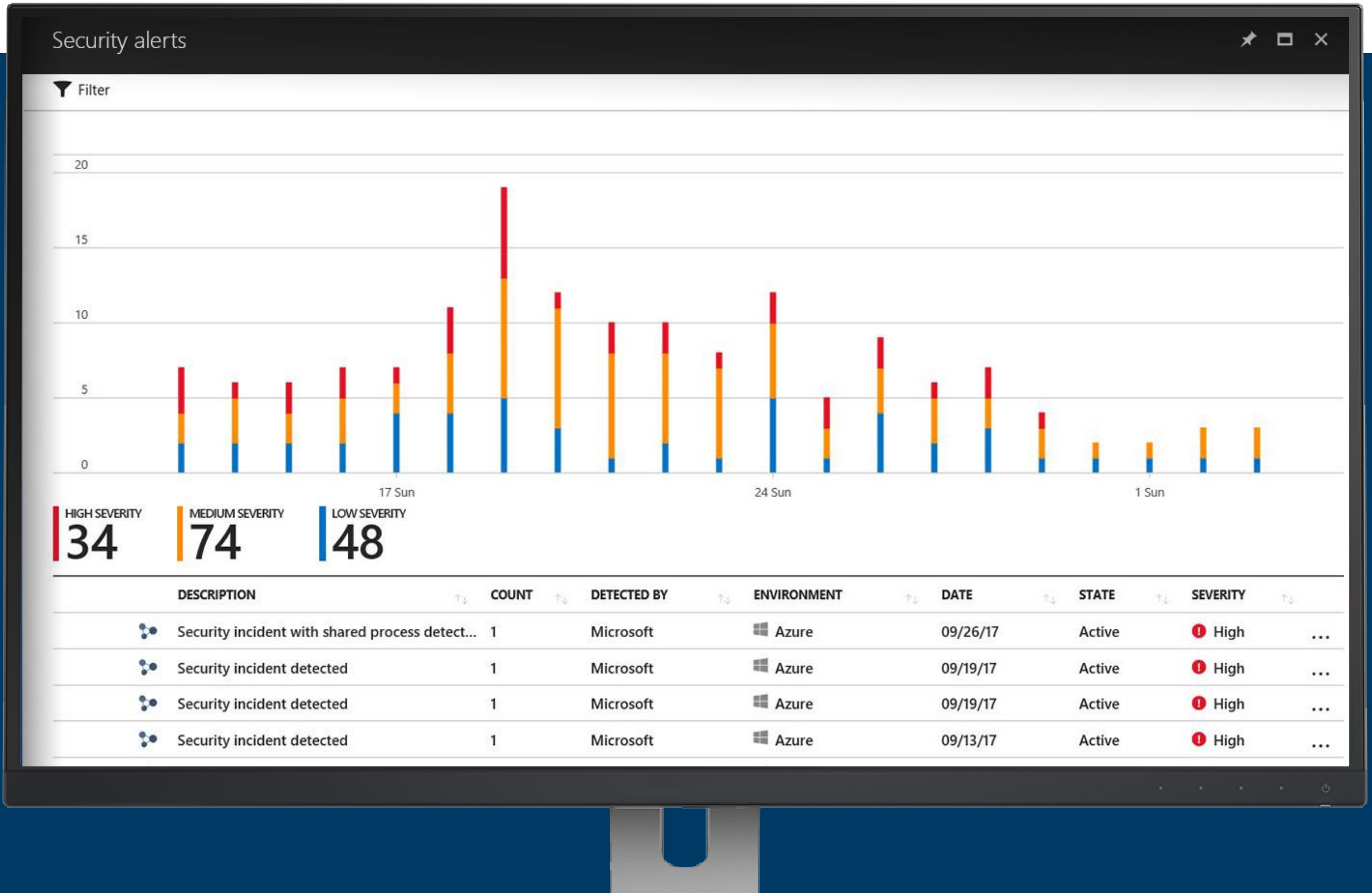
Focus on the most critical threats

Get prioritized security alerts

- Details about detected threats and recommendations

Detect threats across the kill chain

- Alerts that conform to kill chain patterns are fused into a single incident



HIGH SEVERITY 34

MEDIUM SEVERITY 74

LOW SEVERITY 48

DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY	
Security incident with shared process detect...	1	Microsoft	Azure	09/26/17	Active	High	...
Security incident detected	1	Microsoft	Azure	09/19/17	Active	High	...
Security incident detected	1	Microsoft	Azure	09/19/17	Active	High	...
Security incident detected	1	Microsoft	Azure	09/13/17	Active	High	...

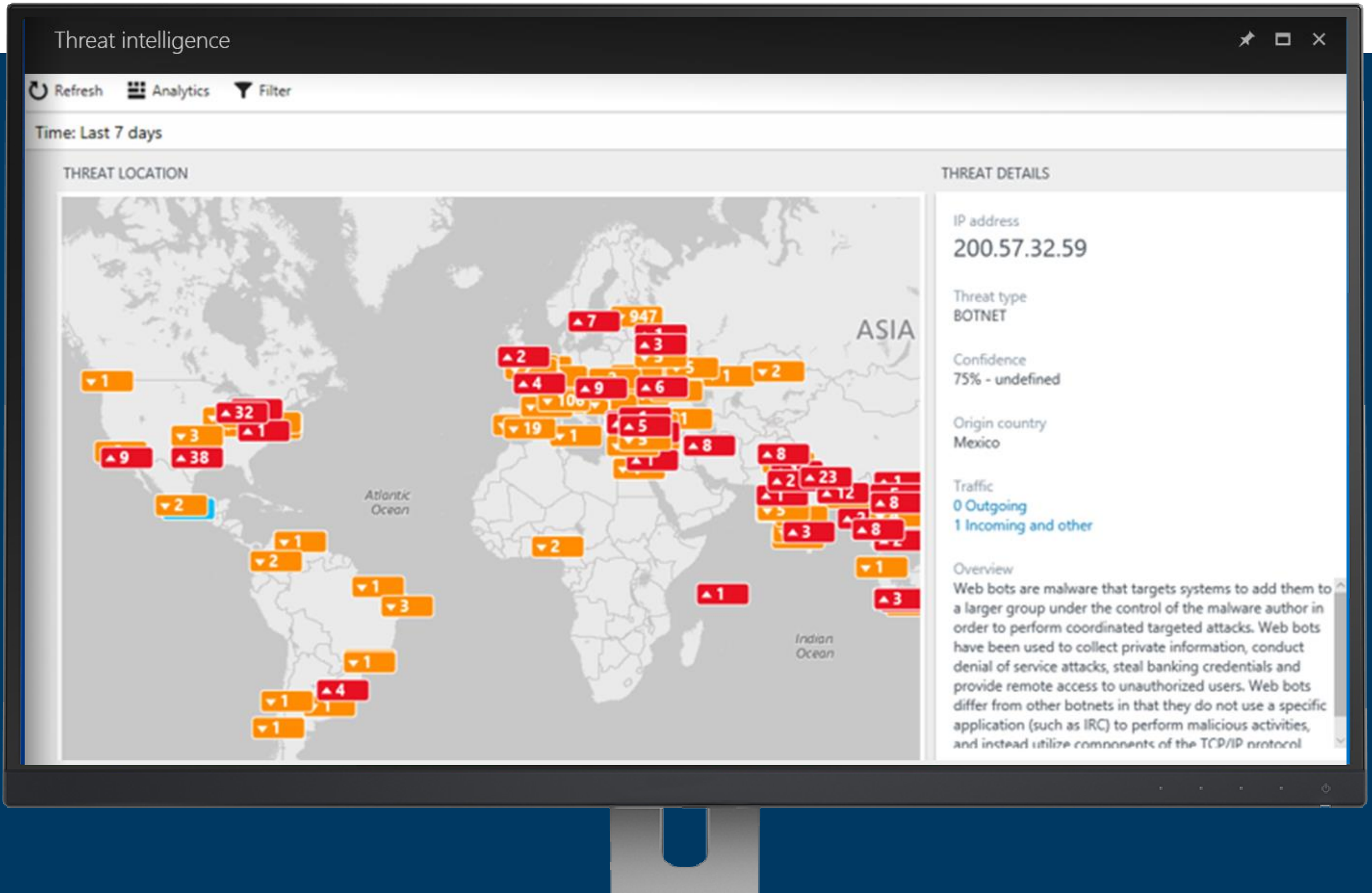
Gain valuable insights about attackers

Visualize source of attacks with interactive map

- Analyzes data from your computers and firewalls logs

Gain insights through threat reports

- Attacker's known objectives, tactics, and techniques



Time: Last 7 days

THREAT LOCATION

THREAT DETAILS

IP address
200.57.32.59

Threat type
BOTNET

Confidence
75% - undefined

Origin country
Mexico

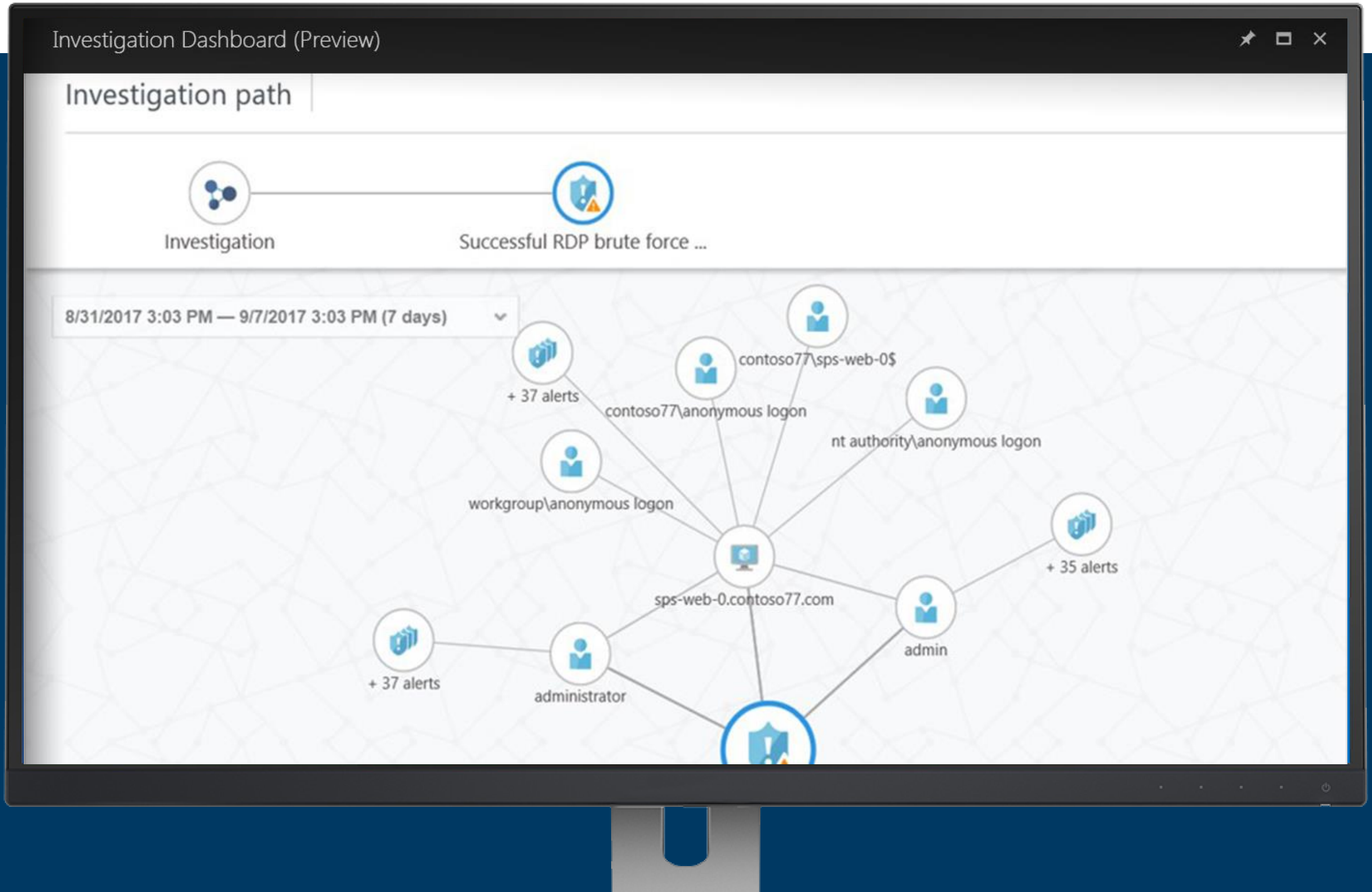
Traffic
0 Outgoing
1 Incoming and other

Overview
Web bots are malware that targets systems to add them to a larger group under the control of the malware author in order to perform coordinated targeted attacks. Web bots have been used to collect private information, conduct denial of service attacks, steal banking credentials and provide remote access to unauthorized users. Web bots differ from other botnets in that they do not use a specific application (such as IRC) to perform malicious activities, and instead utilize components of the TCP/IP protocol

Simplify security operations and investigation

Quickly assess the scope and impact of an attack

- Interactive experience to explore links across alerts, computers and users
- Use predefined or ad hoc queries for deeper examination



Investigation Dashboard (Preview)

Investigation path

8/31/2017 3:03 PM — 9/7/2017 3:03 PM (7 days)

Investigation
Successful RDP brute force ...
+ 37 alerts
contoso77\sps-web-0$
contoso77\anonymous logon
nt authority\anonymous logon
workgroup\anonymous logon
+ 35 alerts
sps-web-0.contoso77.com
admin
+ 37 alerts
administrator

Respond quickly to threats

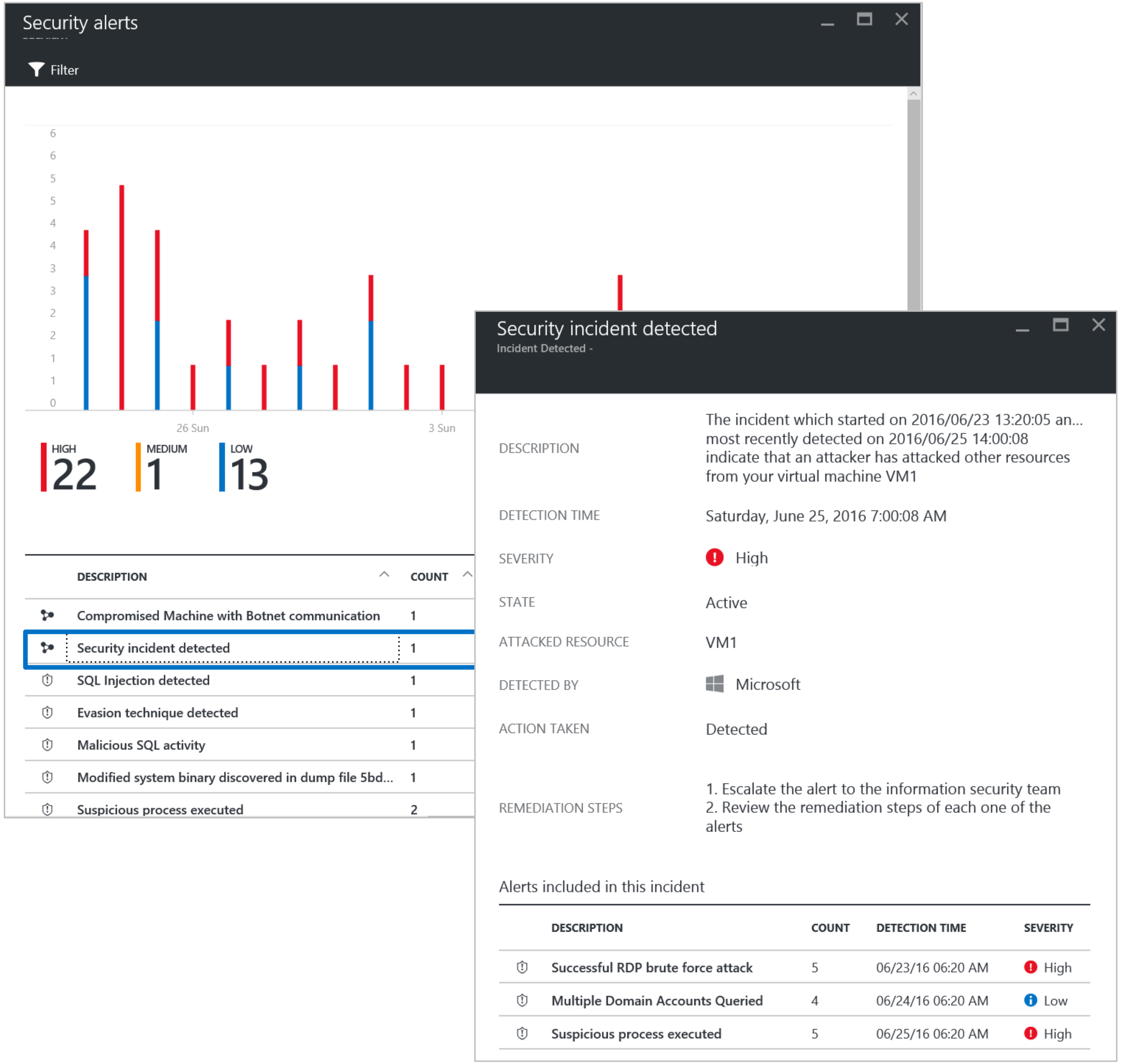
Automate and orchestrate common security workflows

- Create playbooks with integration of Azure Logic Apps
- Trigger workflows from any alert to enable conditional actions

Common workflows

- Route alerts to a ticketing system
- Gather additional information
- Apply additional security controls
- Ask a user to validate an action
- Block a suspicious user account
- Restrict traffic from an IP address

Alerts that conform to kill chain patterns are fused into a single incident



Security alerts

HIGH	MEDIUM	LOW
22	1	13

DESCRIPTION	COUNT
Compromised Machine with Botnet communication	1
Security incident detected	1
SQL Injection detected	1
Evasion technique detected	1
Malicious SQL activity	1
Modified system binary discovered in dump file 5bd...	1
Suspicious process executed	2

Security incident detected

Incident Detected -

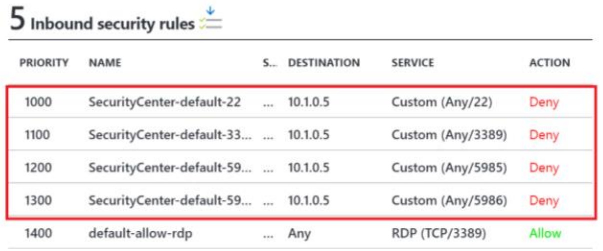
DESCRIPTION	The incident which started on 2016/06/23 13:20:05 an... most recently detected on 2016/06/25 14:00:08 indicate that an attacker has attacked other resources from your virtual machine VM1
DETECTION TIME	Saturday, June 25, 2016 7:00:08 AM
SEVERITY	! High
STATE	Active
ATTACKED RESOURCE	VM1
DETECTED BY	Microsoft
ACTION TAKEN	Detected
REMEDIATION STEPS	1. Escalate the alert to the information security team 2. Review the remediation steps of each one of the alerts

Alerts included in this incident

DESCRIPTION	COUNT	DETECTION TIME	SEVERITY
Successful RDP brute force attack	5	06/23/16 06:20 AM	! High
Multiple Domain Accounts Queried	4	06/24/16 06:20 AM	i Low
Suspicious process executed	5	06/25/16 06:20 AM	! High

Just in time Access

ASC locks VMs for inbound traffic on management ports leveraging NSG rules

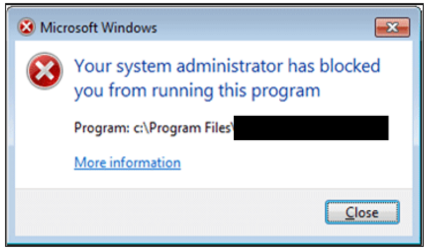


5 Inbound security rules

PRIORITY	NAME	S...	DESTINATION	SERVICE	ACTION
1000	SecurityCenter-default-22	...	10.1.0.5	Custom (Any/22)	Deny
1100	SecurityCenter-default-33...	...	10.1.0.5	Custom (Any/3389)	Deny
1200	SecurityCenter-default-59...	...	10.1.0.5	Custom (Any/5985)	Deny
1300	SecurityCenter-default-59...	...	10.1.0.5	Custom (Any/5986)	Deny
1400	default-allow-rdp	...	Any	RDP (TCP/3389)	Allow

Predictive application Whitelisting

Stopping the execution of unapproved (whitelisted) software on managed machines

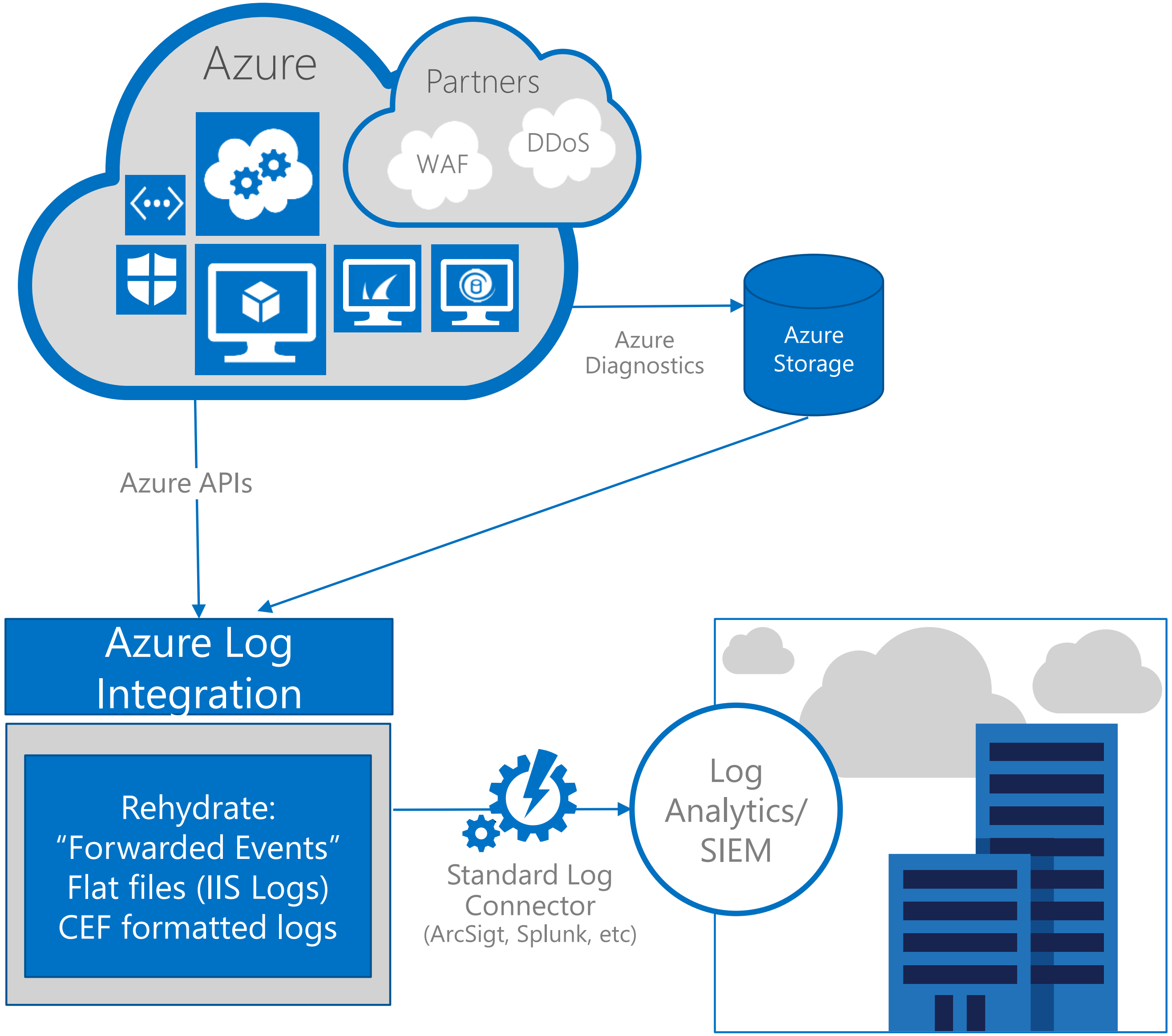


Your system administrator has blocked you from running this program

Program: c:\Program Files\ [redacted]

More information

Access security data in near real-time from your Security Information and Event Management (SIEM)



Public Preview

Azure Security Center

Unified visibility and control

Dynamically discover and manage the security of your hybrid cloud workloads in a single cloud-based console

Adaptive threat prevention

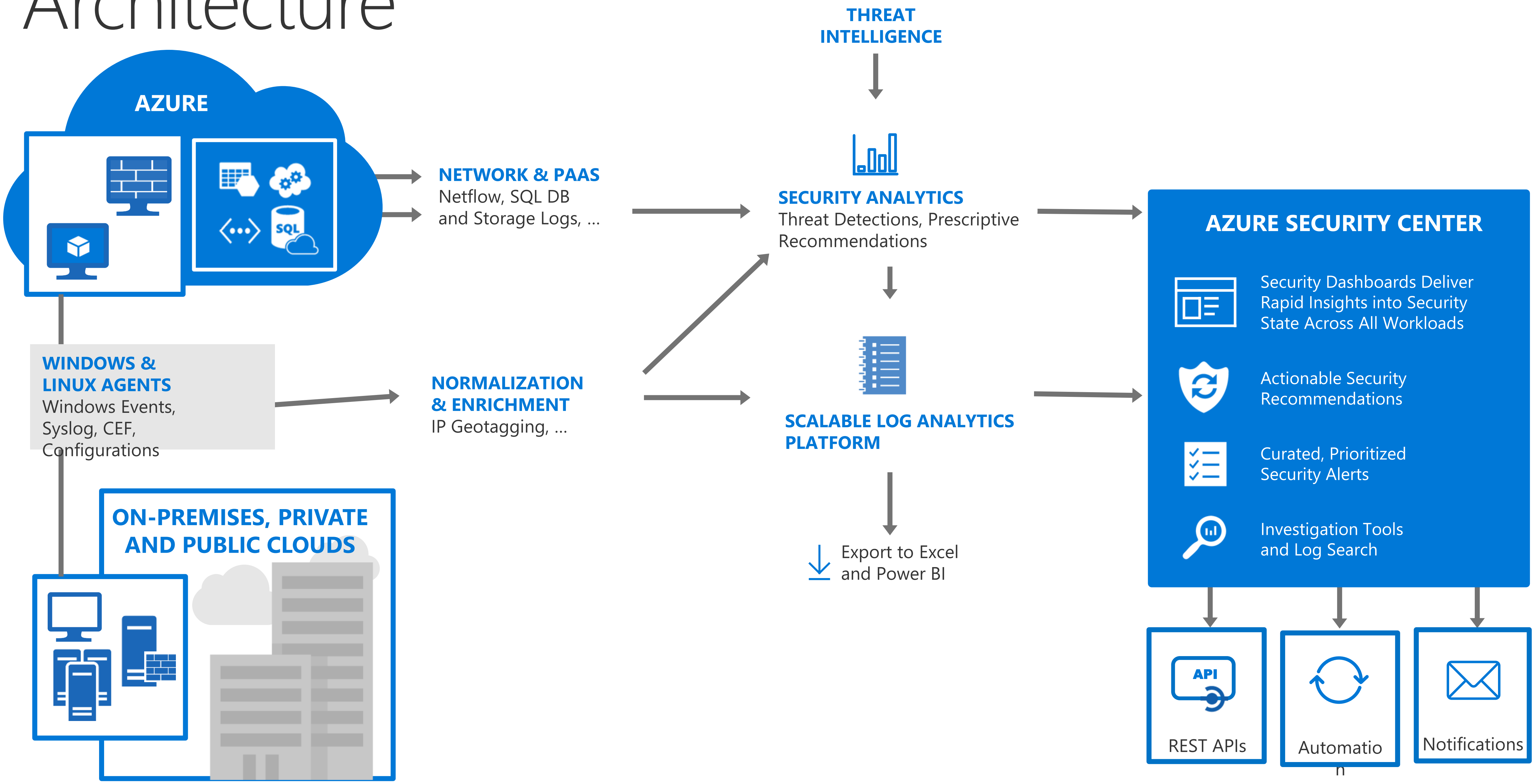
Enable actionable, adaptive protections that identify and mitigate risk to reduce exposure to attacks

Intelligent detection and response

Use advanced analytics and Microsoft Intelligent Security Graph to rapidly detect and respond to evolving cyber threats

Demo

Architecture



AZURE

NETWORK & PAAS
Netflow, SQL DB
and Storage Logs, …

WINDOWS & LINUX AGENTS
Windows Events,
Syslog, CEF,
Configurations

ON-PREMISES, PRIVATE AND PUBLIC CLOUDS

NORMALIZATION & ENRICHMENT
IP Geotagging, …

THREAT INTELLIGENCE

SECURITY ANALYTICS
Threat Detections, Prescriptive
Recommendations

SCALABLE LOG ANALYTICS PLATFORM

Export to Excel
and Power BI

AZURE SECURITY CENTER

Security Dashboards Deliver
Rapid Insights into Security
State Across All Workloads

Actionable Security
Recommendations

Curated, Prioritized
Security Alerts

Investigation Tools
and Log Search

REST APIs

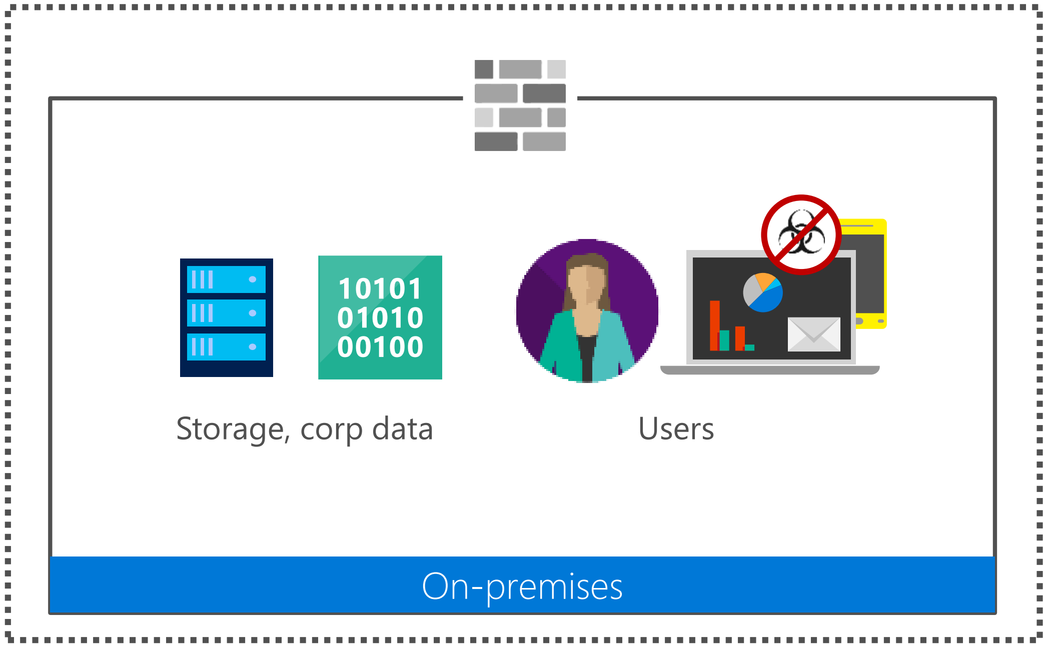
Automatio
n

Notifications

- Cloud App Security

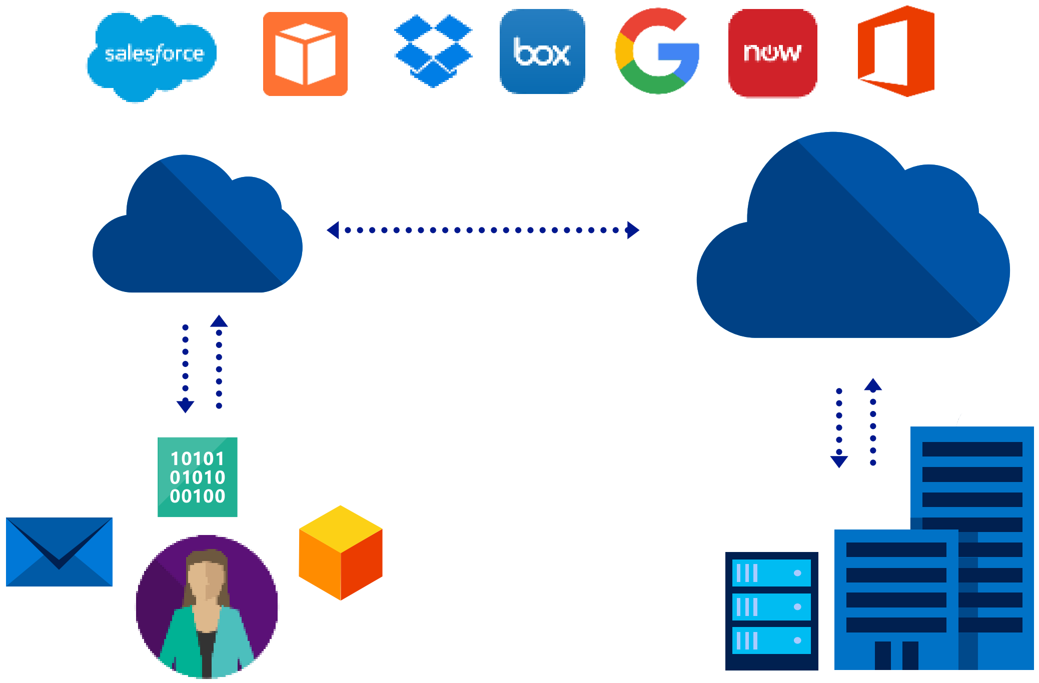
How the cloud changed the enterprise?

Life before cloud



- Only sanctioned apps are installed
- Resources accessed via managed devices/networks
- IT had layers of defense protecting internal apps
- IT has a known security perimeter

Life with cloud



- User chooses apps (unsanctioned, shadow IT)
- User can access resources from anywhere
- Data is shared by user and cloud apps
- IT has limited visibility and protection

Complete framework to secure your cloud apps

Cloud discovery

Discover all cloud usage in your organization

Information protection

Monitor and control your data in the cloud

Threat detection

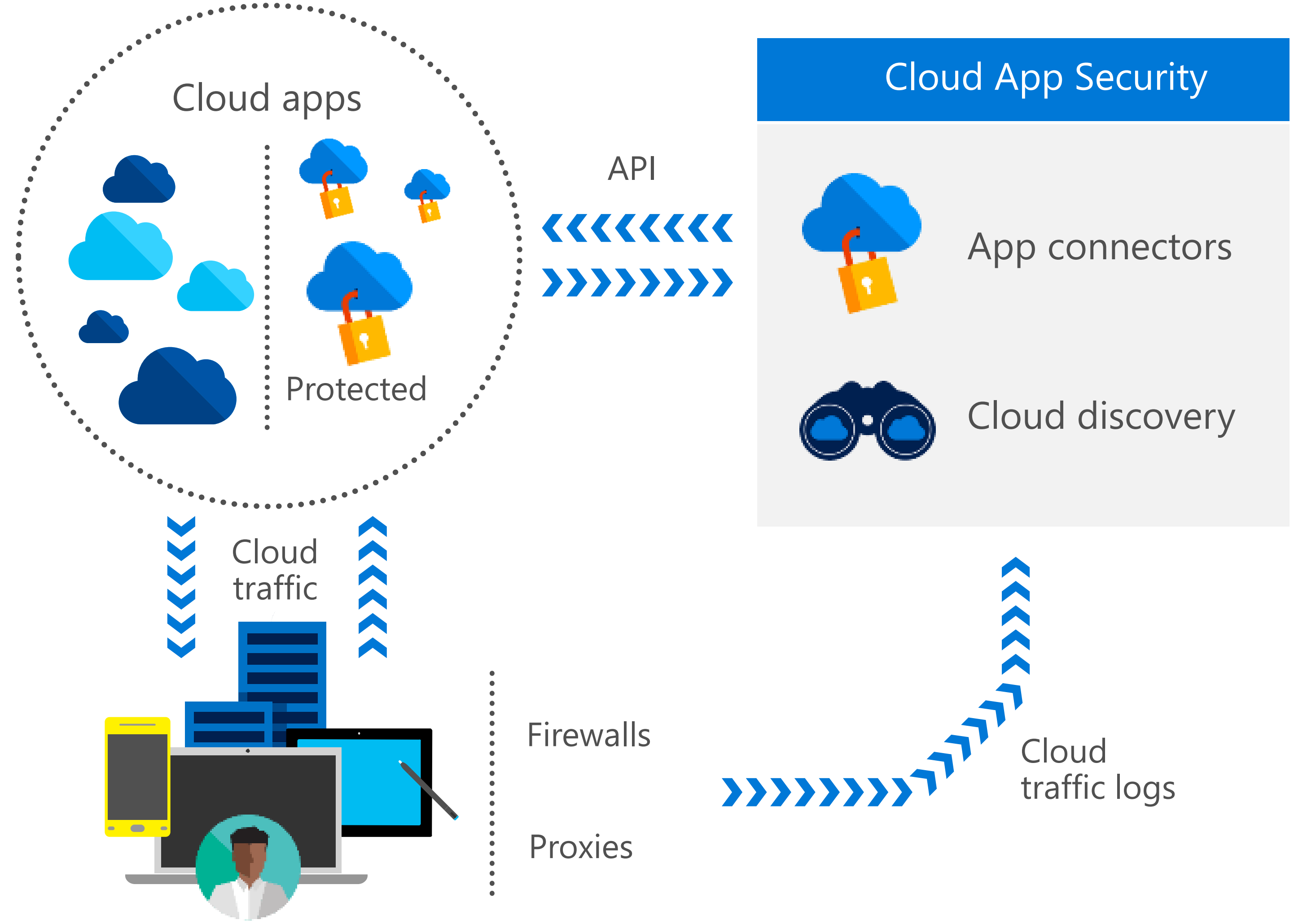
Detect usage anomalies and security incidents

In-session control

Control and limit user access based on session context

DISCOVER › INVESTIGATE › CONTROL › PROTECT

Architecture and how it works



Your organization from any location

Discovery

- Use traffic logs to discover and analyze which cloud apps are in use
- Manually or automatically upload log files for analysis from your firewalls and proxies

Sanctioning and un-sanctioning

- Sanction or block apps in your organization using the cloud app catalog

App connectors

- Leverage APIs provided by various cloud app providers
- Connect an app and extend protection by authorizing access to the app. Cloud App Security queries the app for activity logs and scans data, accounts, and cloud content