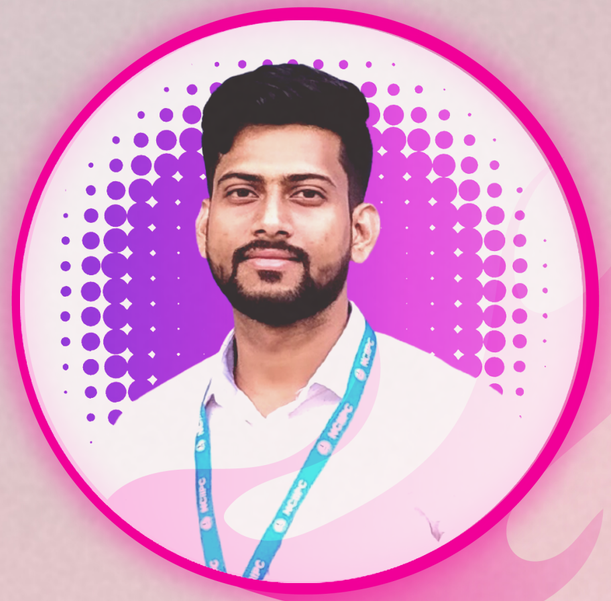
Sponsored by

Microsoft Azure | Azure Developer Community

AZURE DEFENDER

iNeuron

Azure Developer Community



#whoami

Cyber Security Analyst at iNeuron

AzDev Lead Member

Cyber Security Consultant at Cyber Security Society | Secuneus Cyber Security | Techtwins Technologies | Ground Cyber Pvt Ltd.

Certified Ethical Hacker - CEHv11

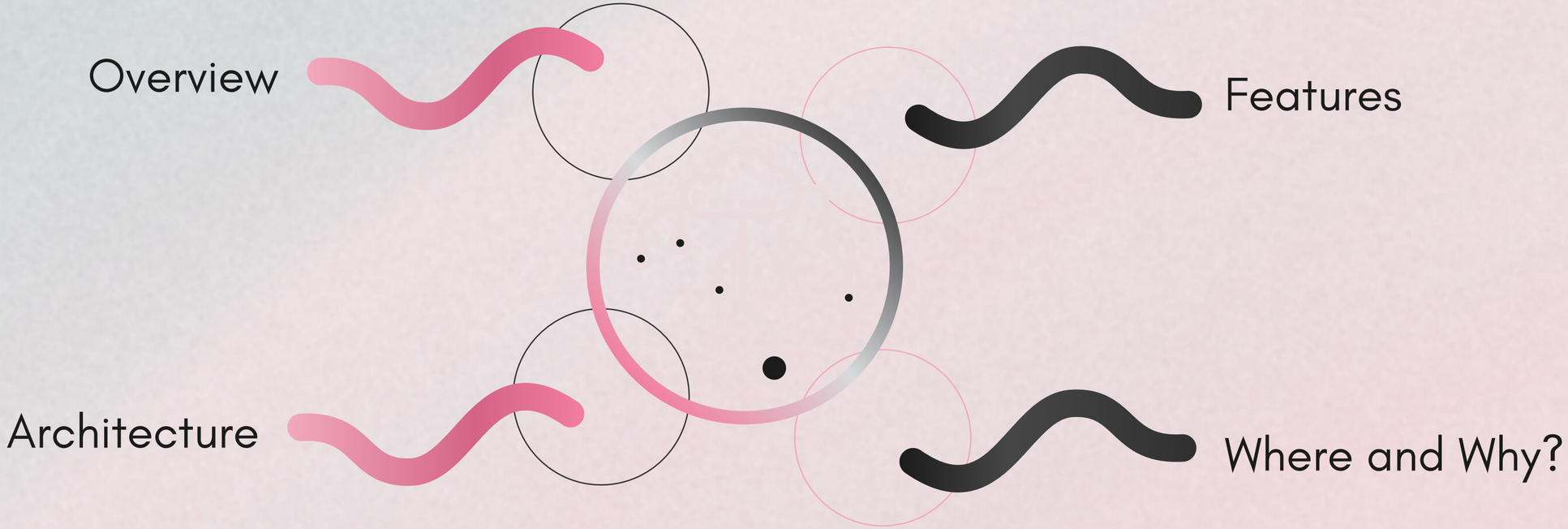
FOLLOW ME

Azure Developer
Community

WHAT WE COVERING

Azure Developer Community

AZURE DEFENDER



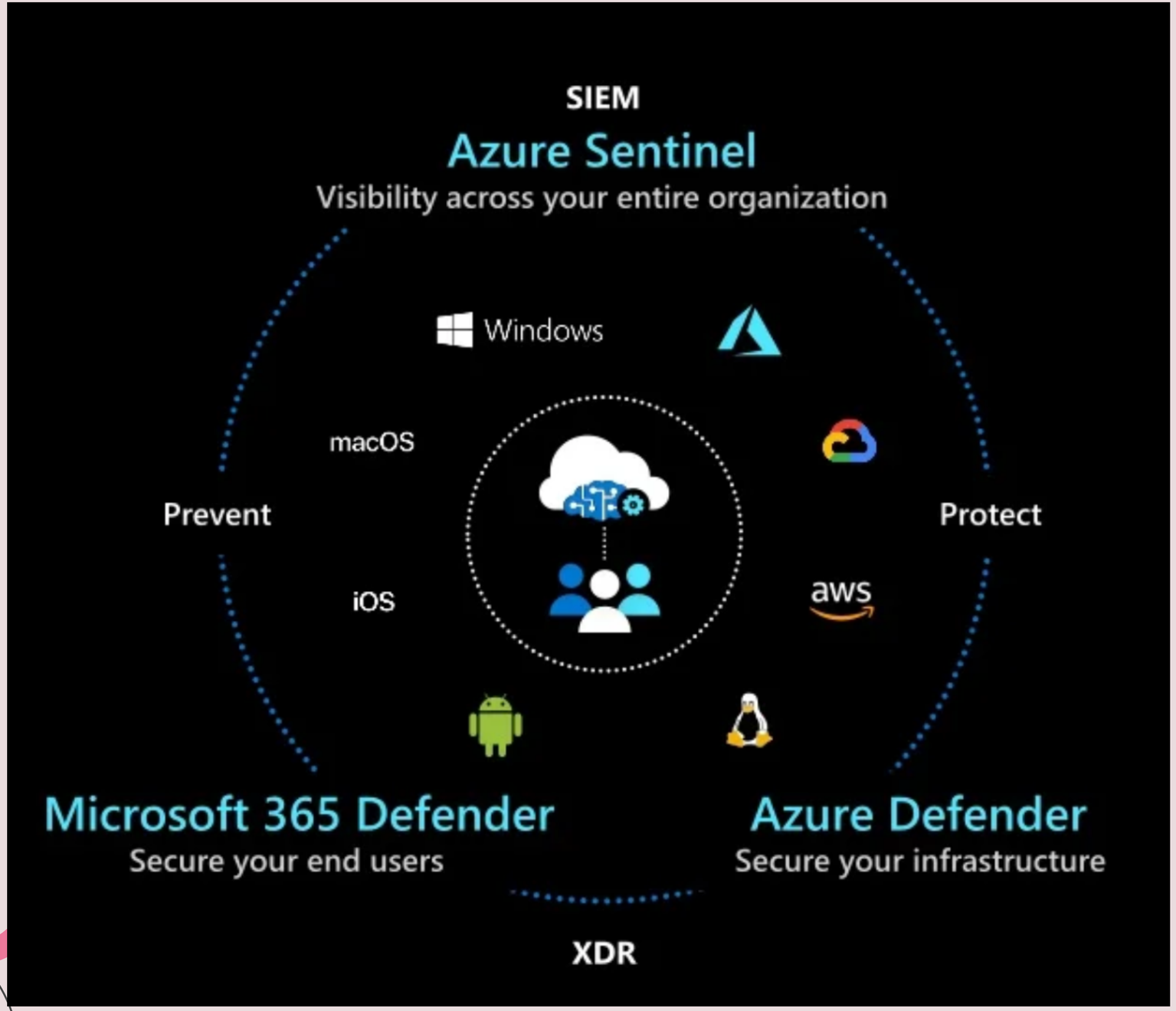
Integrate with 360 degree security solutions

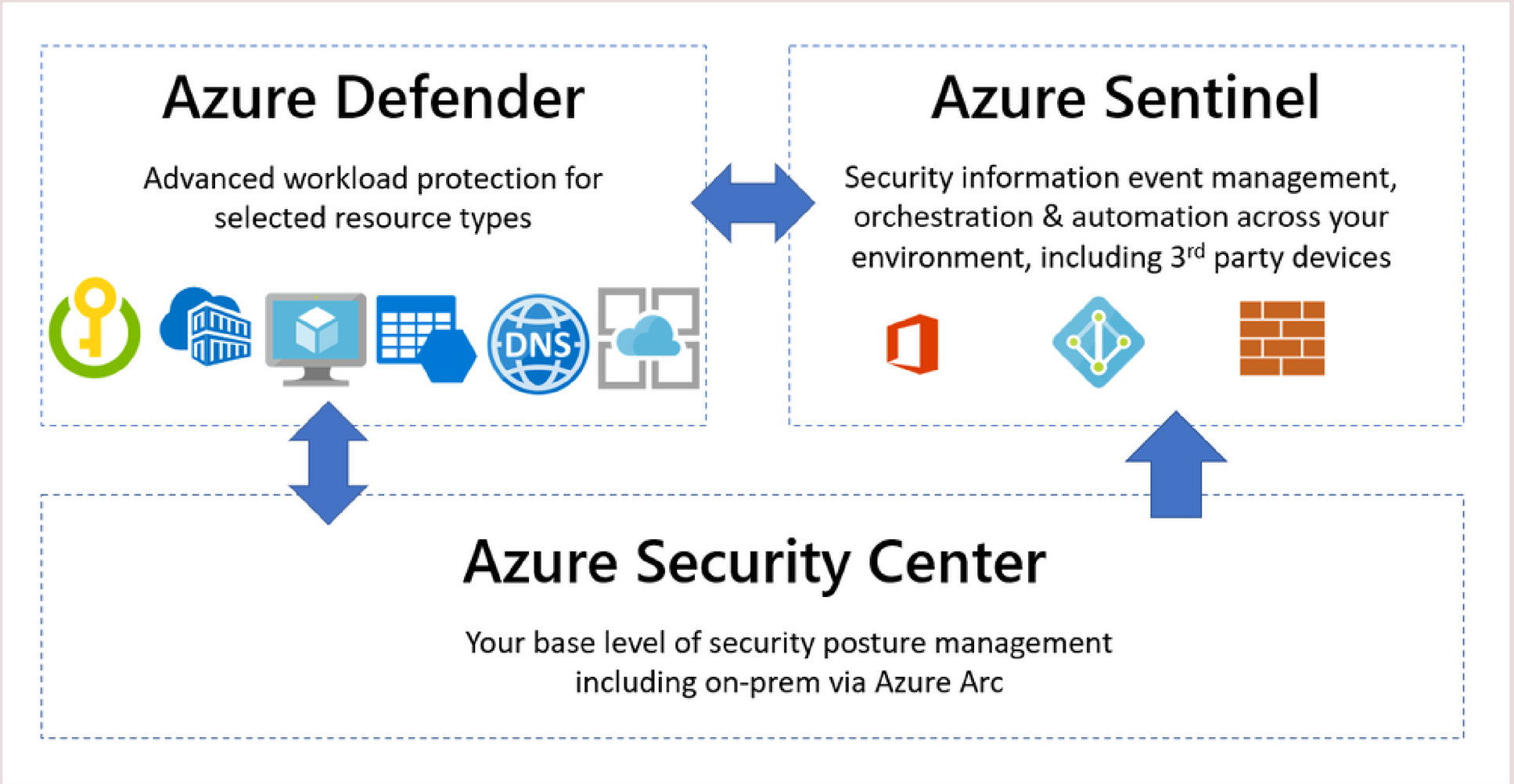
Azure Developer Community

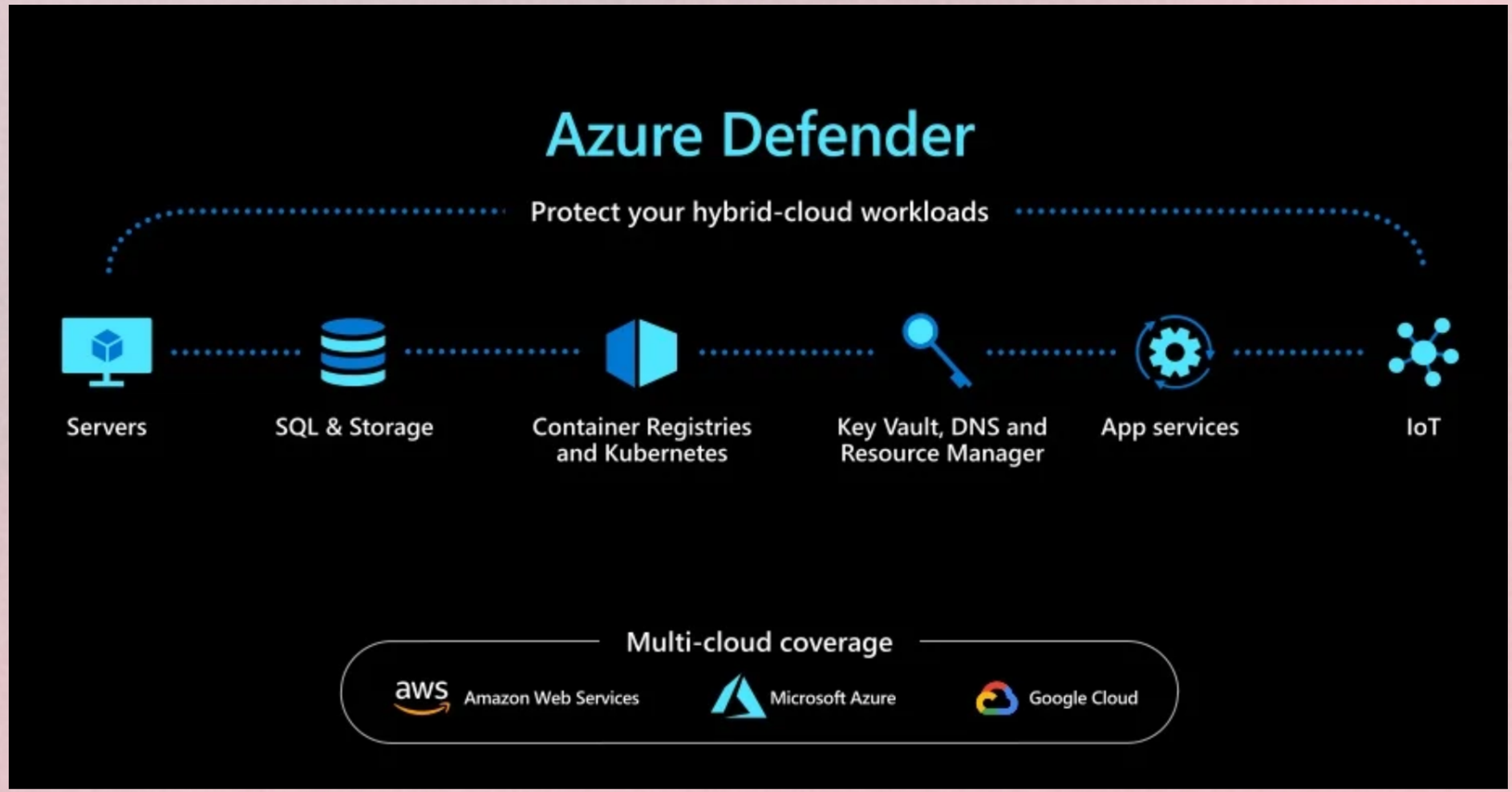
Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for all of your Azure, on-premises, and multicloud (Amazon AWS and Google GCP) resources.

CSPM

Hardening guidance - to help you efficiently and effectively improve your security
Visibility - to help you understand your current security situation

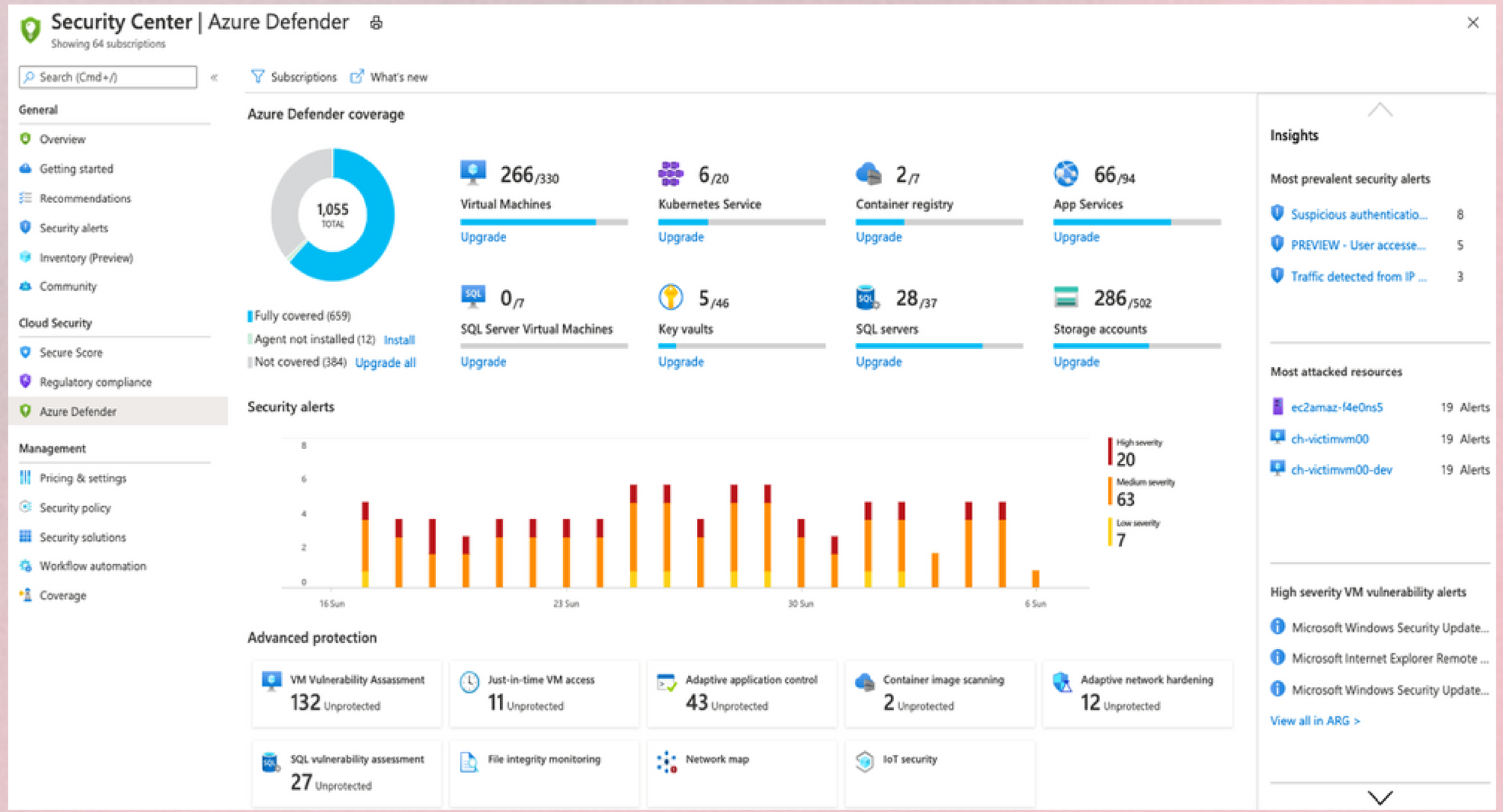

SIEM
Azure Sentinel
Visibility across your entire organization
Windows
macOS
iOS
Prevent
Protect
aws
Microsoft 365 Defender
Secure your end users
Azure Defender
Secure your infrastructure
XDR

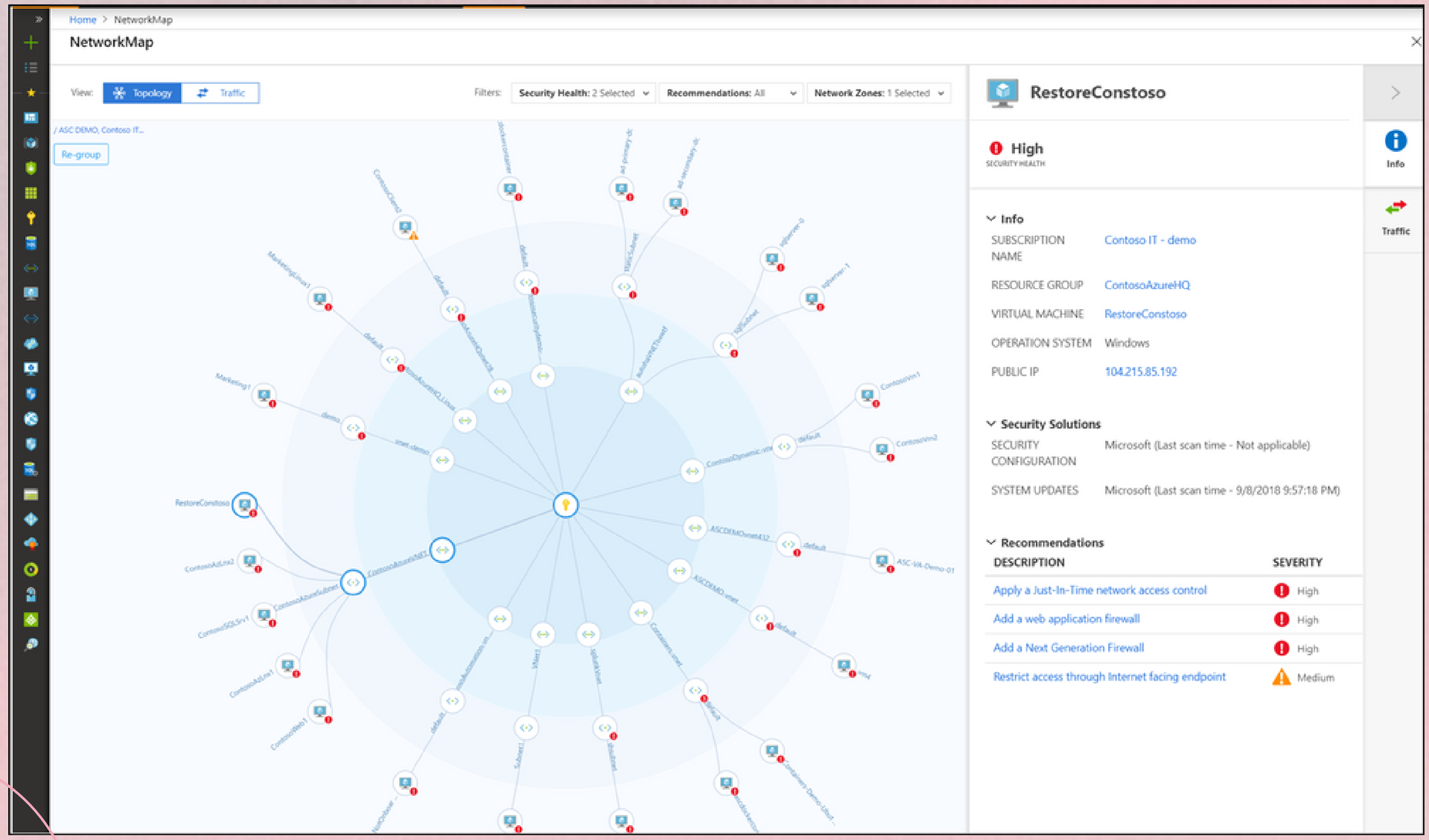

Azure Defender
Advanced workload protection for selected resource types
DNS
Azure Sentinel
Security information event management, orchestration & automation across your environment, including 3rd party devices
Azure Security Center
Your base level of security posture management including on-prem via Azure Arc

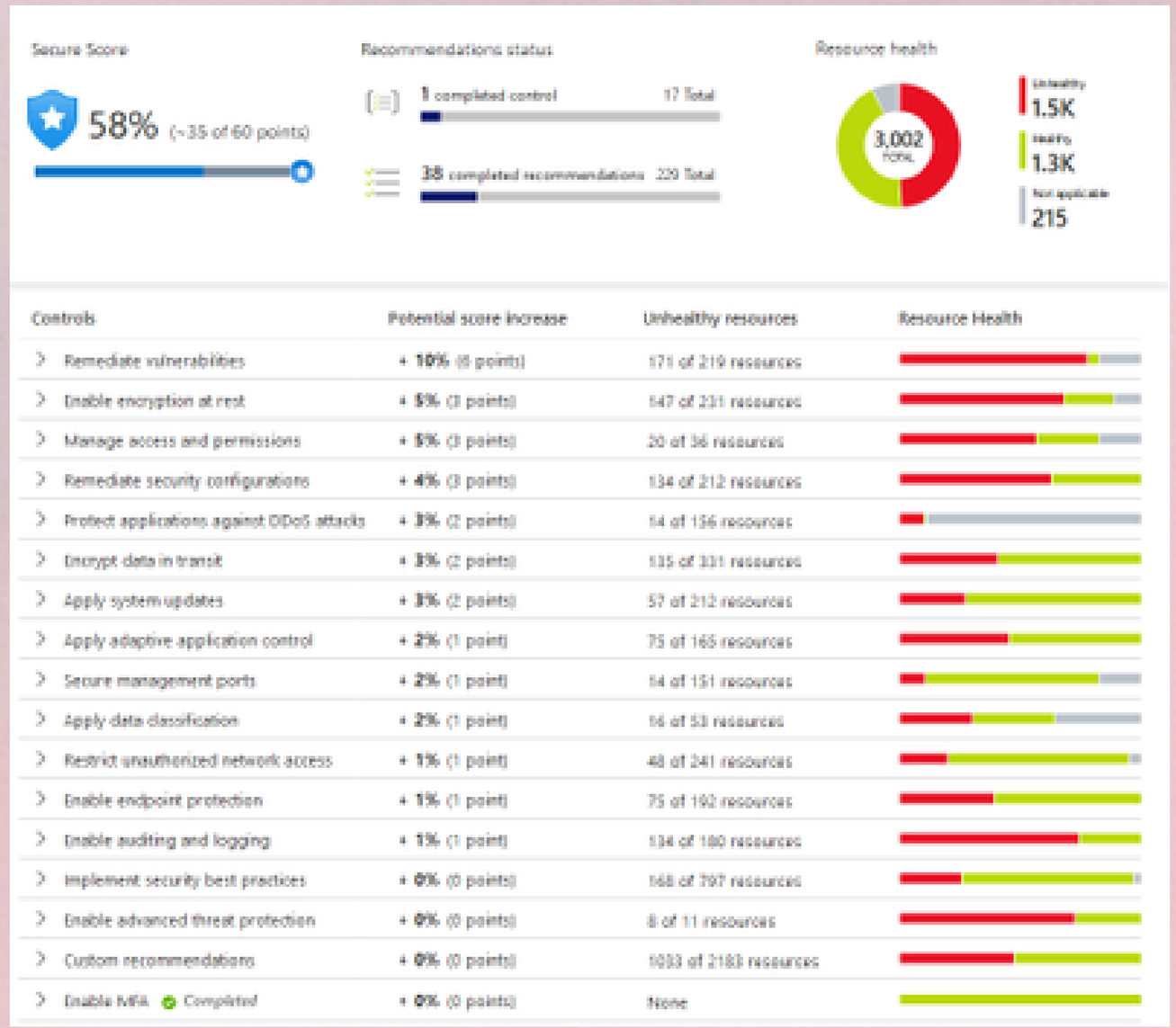


GLANCE AT DEPTH

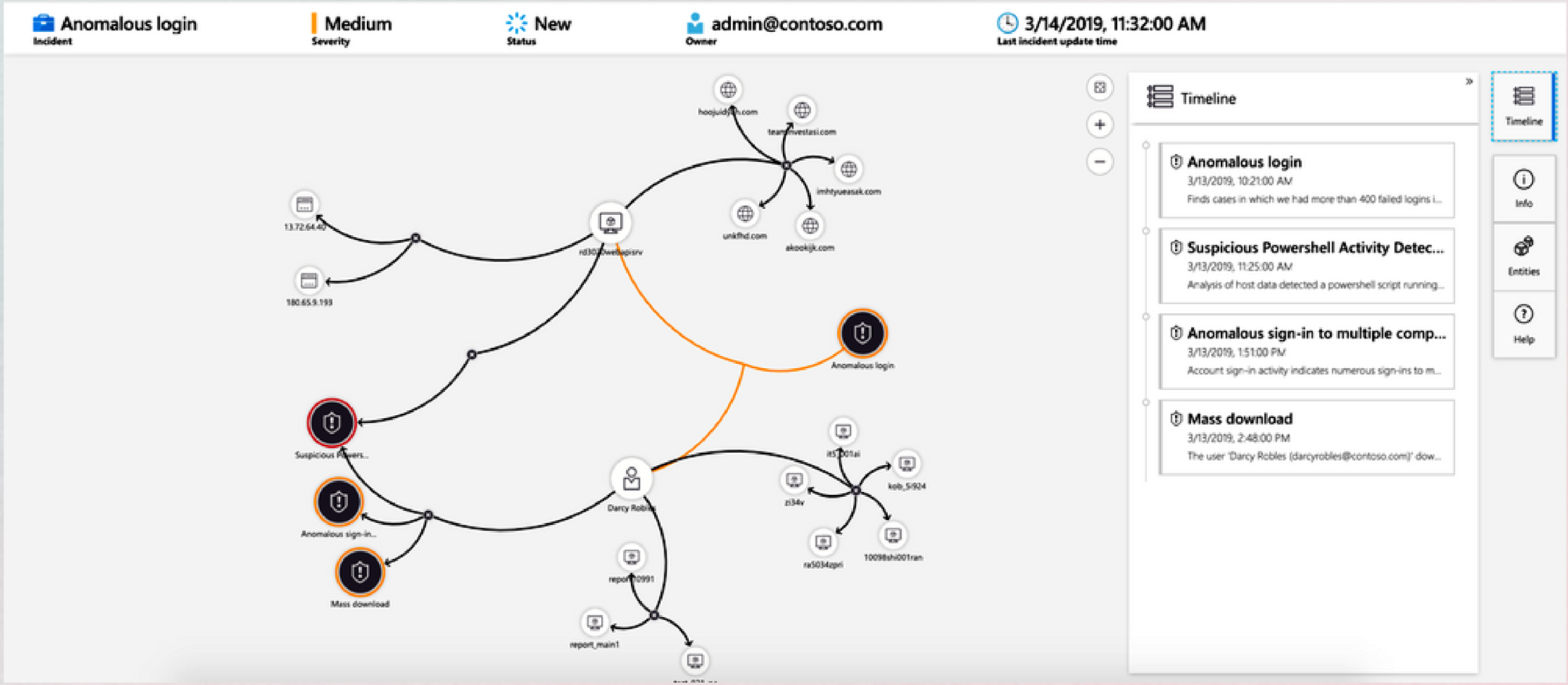
Azure Defender for Azure VMs
Azure Defender for Storage
Azure Defender for Key Vault
Azure Defender for Azure Kubernetes
Azure Defender for Azure App Service
Azure Defender for Azure SQL
Azure Defender for Azure files
Azure Defender for Azure Synapse
Azure Defender for Managed Instance
Azure Defender for Azure Network Layer V1


Security Center | Azure Defender
Showing 64 subscriptions
Search (Cmd+/)
Subscriptions
What's new
General
Overview
Getting started
Recommendations
Security alerts
Inventory (Preview)
Community
Cloud Security
Secure Score
Regulatory compliance
Azure Defender
Management
Pricing & settings
Security policy
Security solutions
Workflow automation
Coverage
Azure Defender coverage
1,055
TOTAL
Fully covered (659)
Agent not installed (12) Install
Not covered (384) Upgrade all
266/330
Virtual Machines
Upgrade
6/20
Kubernetes Service
Upgrade
2/7
Container registry
Upgrade
66/94
App Services
Upgrade
0/7
SQL Server Virtual Machines
Upgrade
5/46
Key vaults
Upgrade
28/37
SQL servers
Upgrade
286/502
Storage accounts
Upgrade
Security alerts
8
6
4
2
0
16 Sun
23 Sun
30 Sun
6 Sun
High severity
20
Medium severity
63
Low severity
7
Advanced protection
VM Vulnerability Assessment
132 Unprotected
Just-in-time VM access
11 Unprotected
Adaptive application control
43 Unprotected
Container image scanning
2 Unprotected
Adaptive network hardening
12 Unprotected
SQL vulnerability assessment
27 Unprotected
File integrity monitoring
Network map
IoT security
Insights
Most prevalent security alerts
Suspicious authenticatio... 8
PREVIEW - User accesse... 5
Traffic detected from IP ... 3
Most attacked resources
ec2amaz-f4e0ns5 19 Alerts
ch-victimvm00 19 Alerts
ch-victimvm00-dev 19 Alerts
High severity VM vulnerability alerts
Microsoft Windows Security Update...
Microsoft Internet Explorer Remote ...
Microsoft Windows Security Update...
View all in ARG >


Home > NetworkMap
NetworkMap
View: Topology Traffic
Filters: Security Health: 2 Selected Recommendations: All Network Zones: 1 Selected
/ ASC DEMO, Contoso IT...
Re-group
RestoreConstoso
High
SECURITY HEALTH
Info
Traffic
Info
SUBSCRIPTION NAME Contoso IT - demo
RESOURCE GROUP ContosoAzureHQ
VIRTUAL MACHINE RestoreConstoso
OPERATION SYSTEM Windows
PUBLIC IP 104.215.85.192
Security Solutions
SECURITY CONFIGURATION Microsoft (Last scan time - Not applicable)
SYSTEM UPDATES Microsoft (Last scan time - 9/8/2018 9:57:18 PM)
Recommendations
DESCRIPTION SEVERITY
Apply a Just-In-Time network access control High
Add a web application firewall High
Add a Next Generation Firewall High
Restrict access through Internet facing endpoint Medium



Security Review and Suggestion



Threat Investigation

Pricing Plan

Feature	Defender for Servers Plan 1	Defender for Servers Plan 2
Automatic onboarding for resources in Azure, AWS, GCP	✓	✓
Microsoft threat and vulnerability management	✓	✓
Flexibility to use Microsoft Defender for Cloud or Microsoft 365 Defender portal	✓	✓
Integration of Microsoft Defender for Cloud and Microsoft Defender for Endpoint (alerts, software inventory, Vulnerability Assessment)	✓	✓
Security Policy and Regulatory Compliance		✓
Log-analytics (500 MB free)		✓
Vulnerability Assessment using Qualys		✓
Threat detections: OS level, network layer, control plane		✓
Adaptive application controls		✓
File integrity monitoring		✓
Just-in time VM access		✓
Adaptive network hardening		✓

STUDY RESOURCES:

- https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
- https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
- https://www.microsoft.com/en-us/insidetrack/microsoft-uses-threat-intelligence-to-protect-detect-and-respond-to-threats
- https://techcommunity.microsoft.com/t5/itops-talk-blog/what-is-azure-defender/ba-p/1843528
- https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction
- https://www.slideshare.net/d501159/microsoft-defender-and-azure-sentinel
- https://techcommunity.microsoft.com/t5/itops-talk-blog/what-s-the-difference-between-azure-security-center-azure/ba-p/2155188
- https://charbelnemnom.com/azure-security-center-and-microsoft-defender-atp-integration/

Sponsored by

Microsoft Azure | Azure Developer Community

iNeuron

JOIN US

https://discord.gg/pqcw9bnq

Connect With Me

https://bit.ly/3yDMGHP

Azure Developer Community

THANK YOU

for your attention

Any Questions DO FIRE

Sponsored by

Microsoft Azure

iNeuron