Microsoft

#AzureEvent
#BuildWithAzure

Azure Workshop

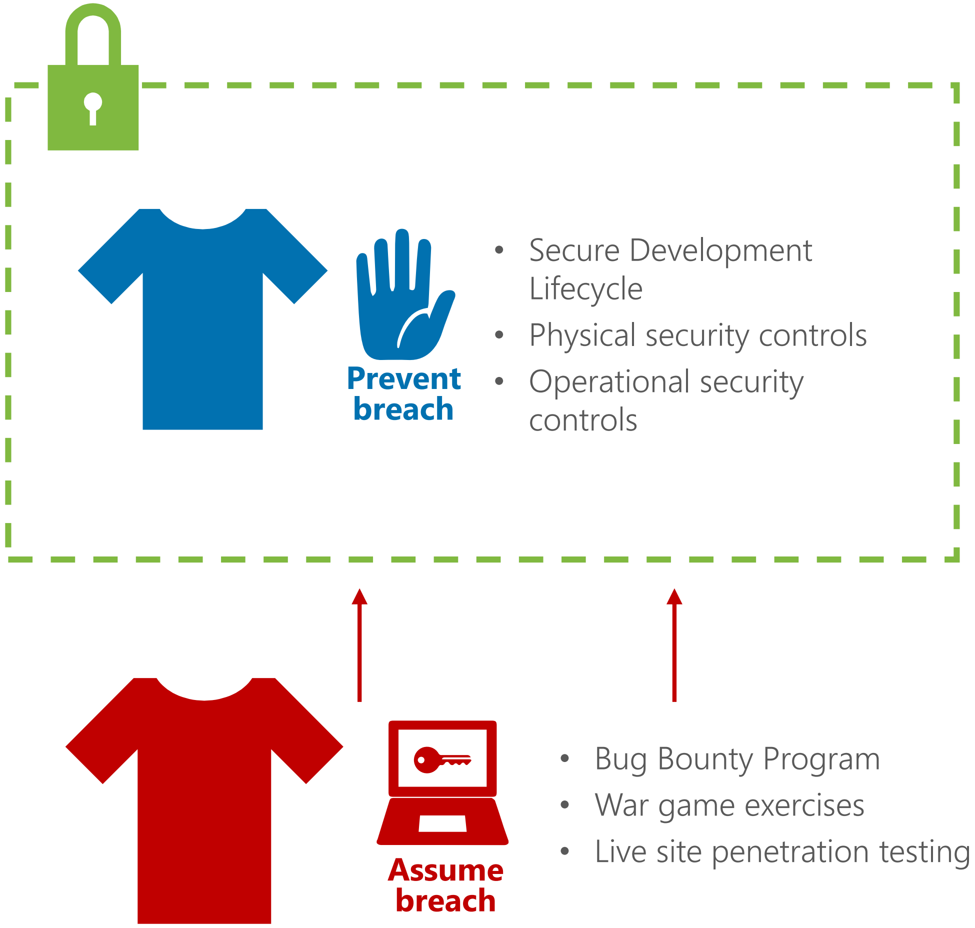
# GDPR, Security and Privacy features for cloud applications

Ben Roscorla, Mike Ormond, Robin Lester

*vipazure@microsoft.com*

# Monitoring and Operations

# Prevent & Assume Breach



- Secure Development Lifecycle
- Physical security controls
- Operational security controls

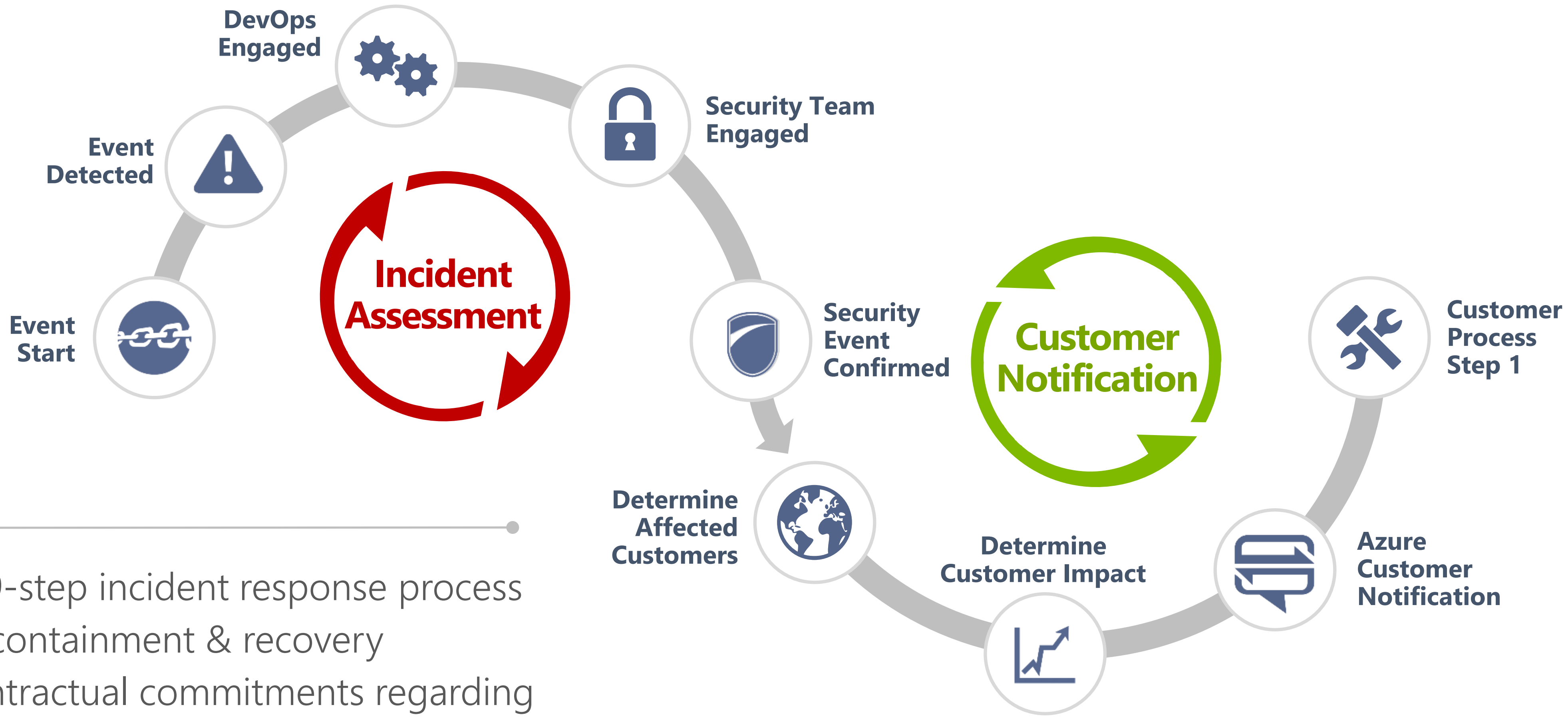
- Bug Bounty Program
- War game exercises
- Live site penetration testing

✓ **Prevent Breach** is a defensive strategy aimed at predicting and preventing a security breach

✓ The **Assume Breach** strategy, unique to Microsoft, is a key operational practice that hardens cloud services

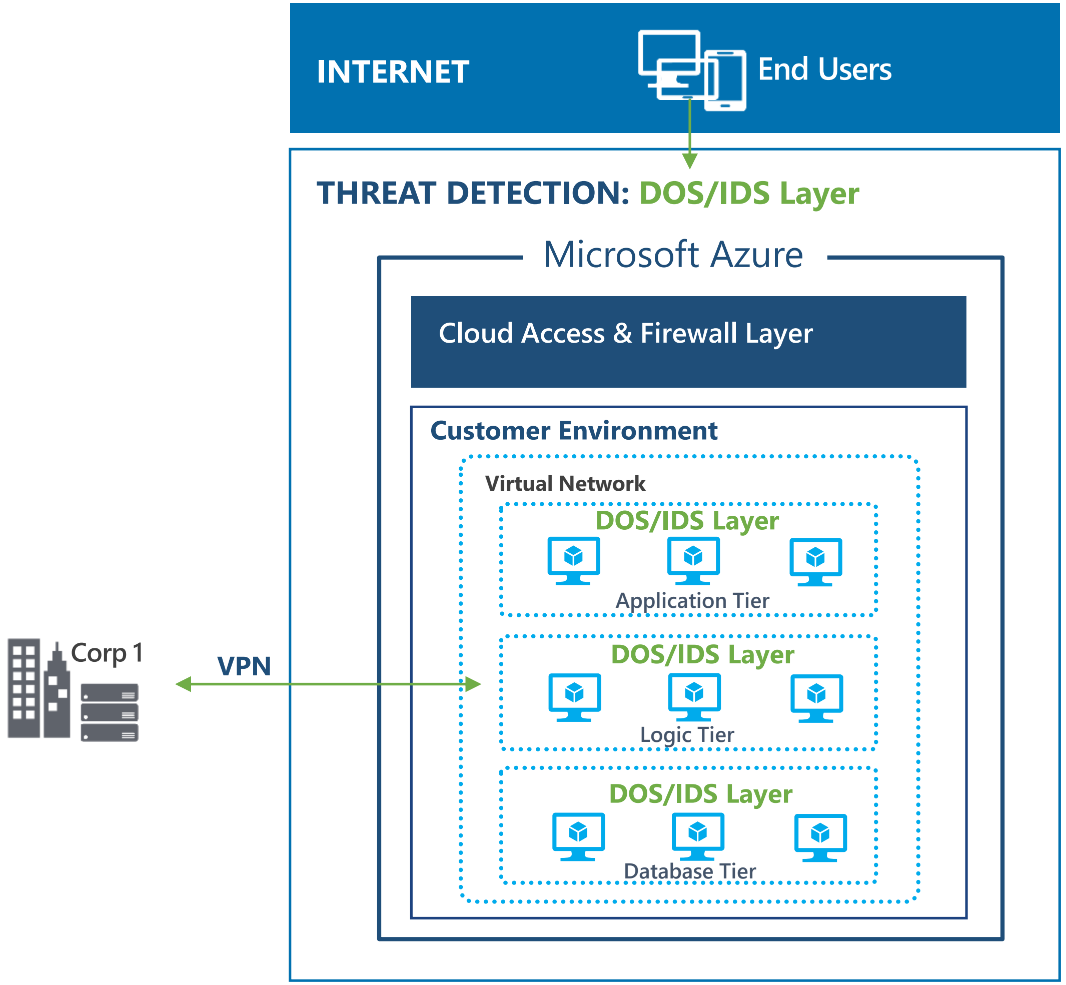
- ✓ Leverages Microsoft's vast threat intelligence
- ✓ Includes state of the art security monitoring and response

# Incident Response



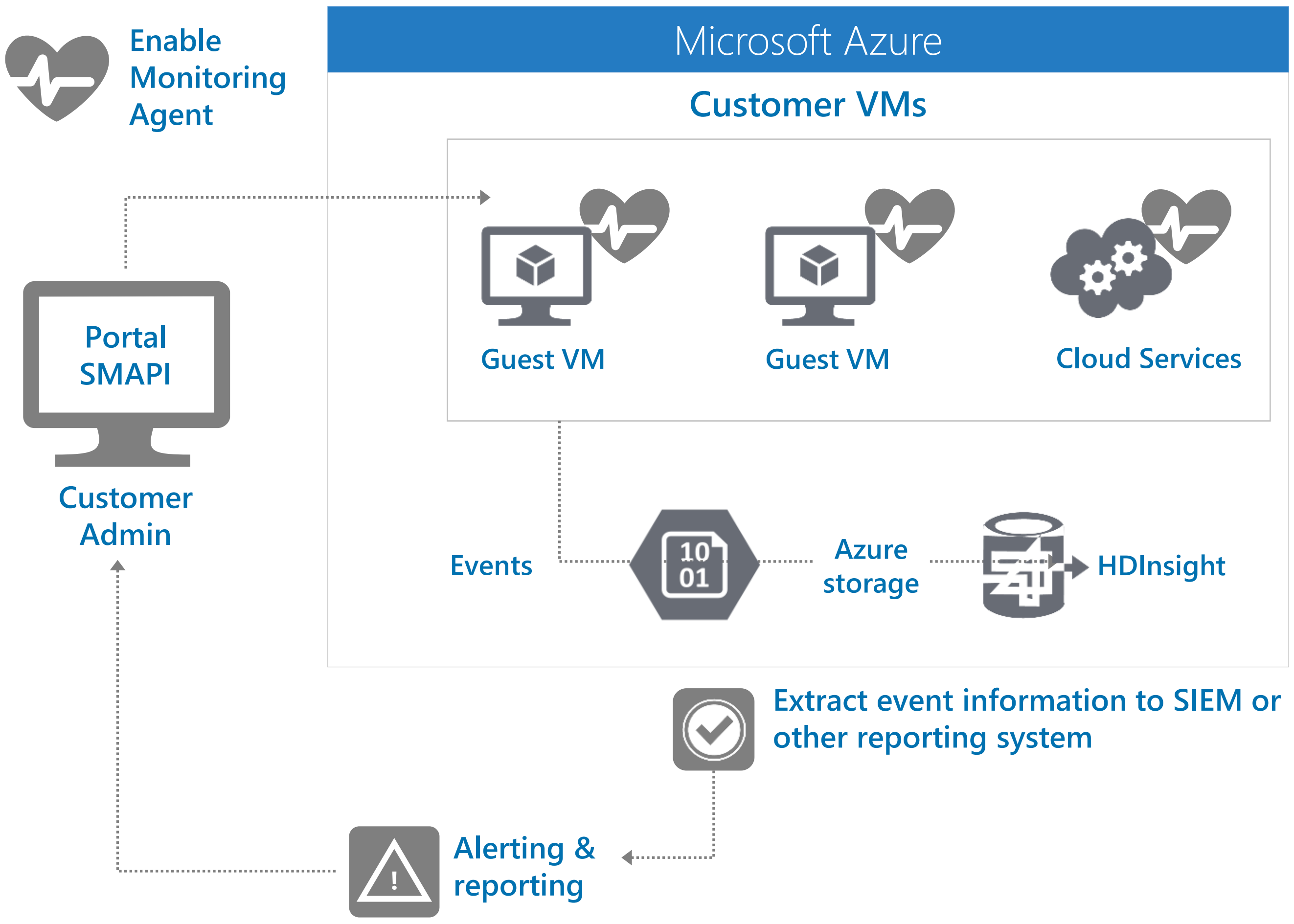
- ✓ In-depth 9-step incident response process
- ✓ Focus on containment & recovery
- ✓ Makes contractual commitments regarding customer notification + provides forensics

# Threat Detection



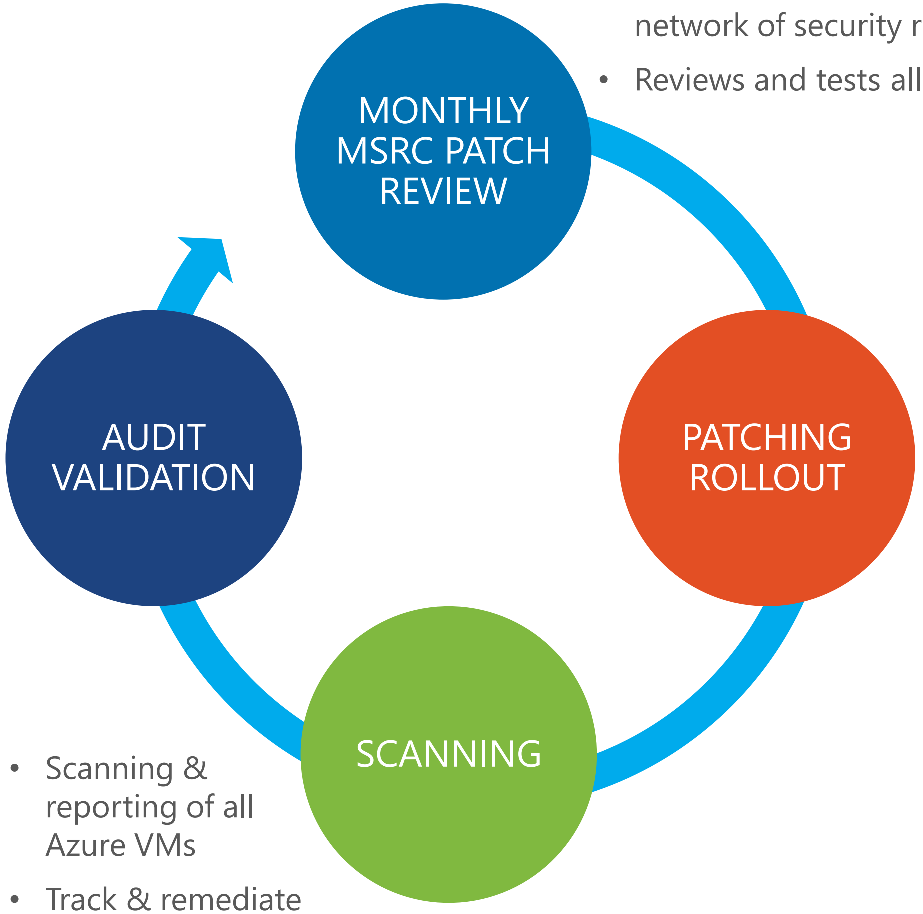
- ✓ Provides big data analysis of logs for intrusion detection & prevention for the platform
- ✓ Employs denial of service attack prevention measures for the platform
- ✓ Regularly performs penetration testing

# Host Protection: Monitoring, Firewalls, AV



- ✓ Configure monitoring, export events for analysis
- ✓ Configure Microsoft Antimalware or an AV/AM solution from a partner
- ✓ Apply corporate firewall using site-to-site VPN, configures endpoints
- ✓ Define access controls between tiers and provide additional protection via the OS firewall
- ✓ Monitor and respond to alerts

# Update Management



- Monitor 100,000+ vulnerability reports
- Sourced from customers & worldwide network of security researchers
- Reviews and tests all changes

- Prioritize critical updates
- Monthly OS releases with patches

- Scanning & reporting of all Azure VMs
- Track & remediate any findings

- Reconciliation report
- Resolution summary

## AZURE:

✓ Apply patch management as a service

✓ Rigorously reviews & tests all changes

## CUSTOMER:

✓ Applies similar patch management strategies for their Virtual Machines

# Azure Security and Operations Management

Collect security-related events and perform forensic, audit, and breach analysis

## Identification of missing system updates across data centers or in a public cloud

Comprehensive updates assessment across datacenters and public clouds

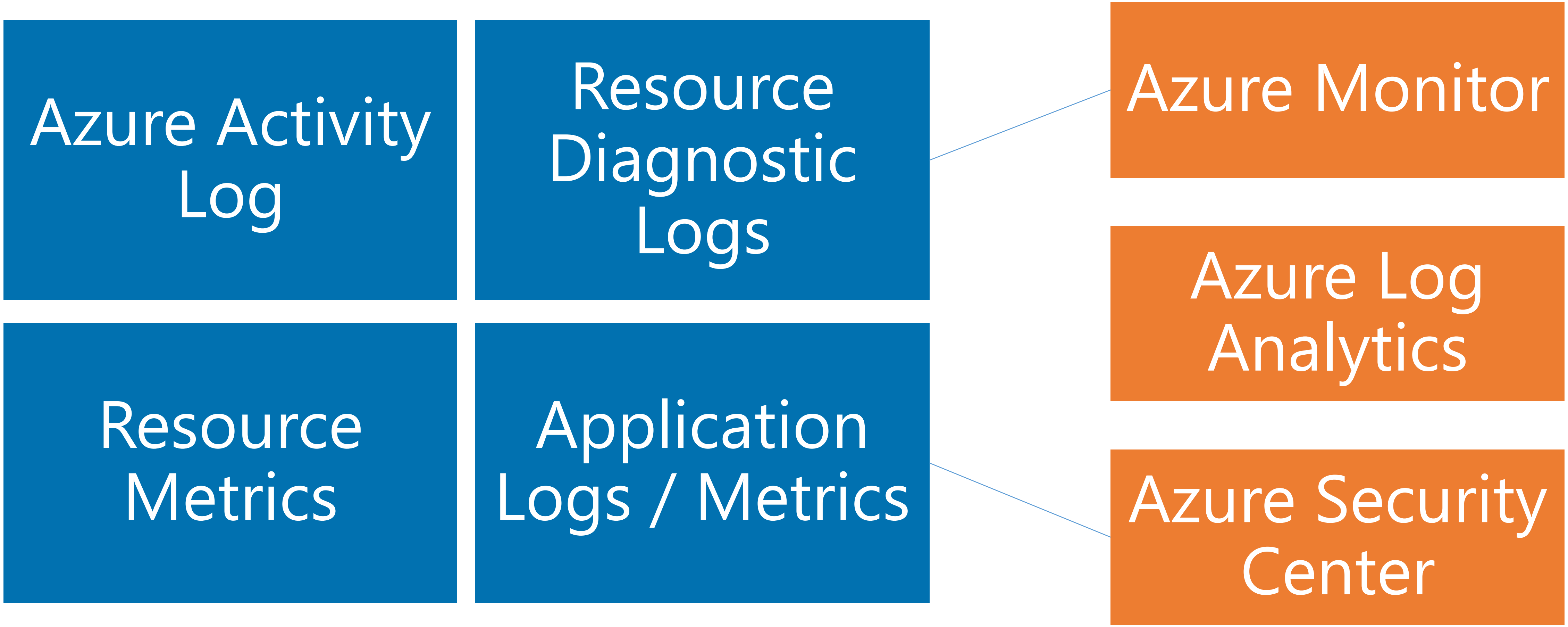
## Comprehensive view into your organization's IT security posture

Detection of breaches and threats with malware assessment

## Collection and analysis of security related events

Perform forensic, audit and breach analysis

# Data Sources



Azure Activity Log

Resource Diagnostic Logs

Resource Metrics

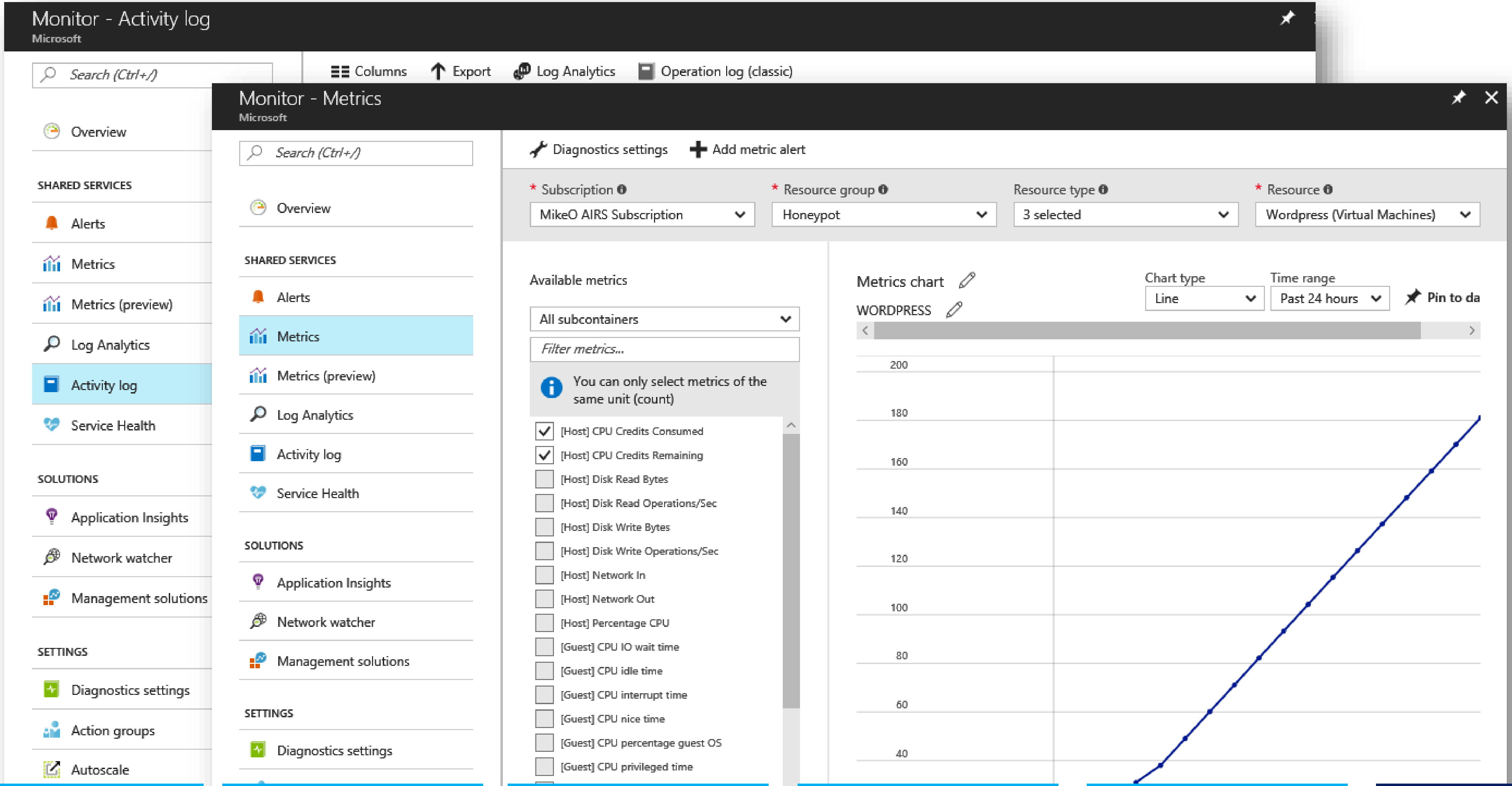
Application Logs / Metrics

Azure Monitor

Azure Log Analytics

Azure Security Center

# Azure Monitor



Monitor - Activity log
Microsoft

Monitor - Metrics
Microsoft

* Subscription: MikeO AIRS Subscription

* Resource group: Honeypot

Resource type: 3 selected

* Resource: Wordpress (Virtual Machines)

Available metrics: All subcontainers

Filter metrics...

You can only select metrics of the same unit (count)

- ☑ [Host] CPU Credits Consumed
- ☑ [Host] CPU Credits Remaining
- □ [Host] Disk Read Bytes
- □ [Host] Disk Read Operations/Sec
- □ [Host] Disk Write Bytes
- □ [Host] Disk Write Operations/Sec
- □ [Host] Network In
- □ [Host] Network Out
- □ [Host] Percentage CPU
- □ [Guest] CPU IO wait time
- □ [Guest] CPU idle time
- □ [Guest] CPU interrupt time
- □ [Guest] CPU nice time
- □ [Guest] CPU percentage guest OS
- □ [Guest] CPU privileged time

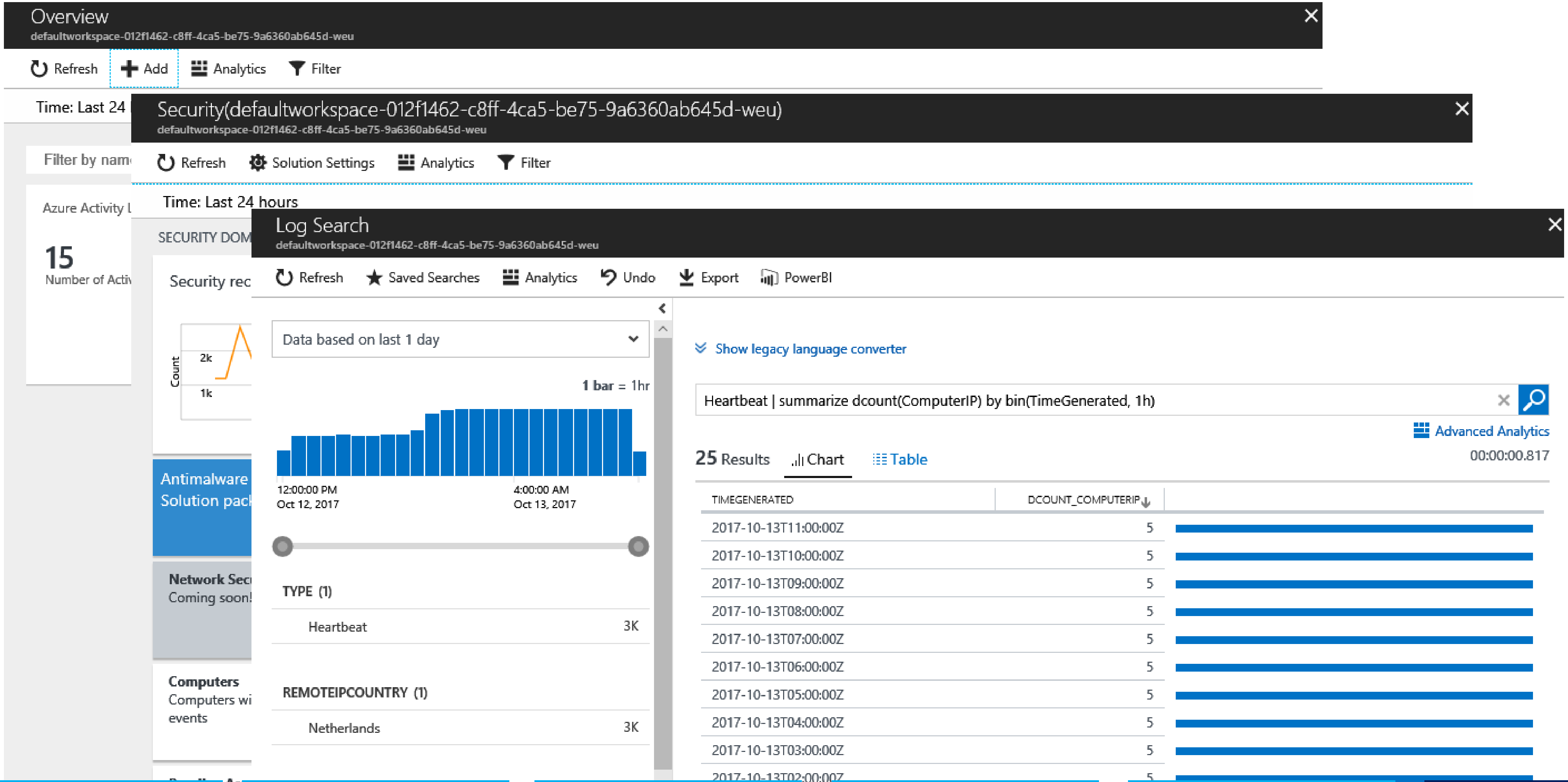
Metrics chart

WORDPRESS

Chart type: Line

Time range: Past 24 hours

# Azure Log Analytics



Overview
defaultworkspace-012f1462-c8ff-4ca5-be75-9a6360ab645d-weu

Time: Last 24

Filter by nam

Azure Activity L

15
Number of Activ

Security(defaultworkspace-012f1462-c8ff-4ca5-be75-9a6360ab645d-weu)
defaultworkspace-012f1462-c8ff-4ca5-be75-9a6360ab645d-weu

Time: Last 24 hours

SECURITY DOM

Security rec

Antimalware
Solution pack

Network Secu
Coming soon!

Computers
Computers wi
events

Log Search
defaultworkspace-012f1462-c8ff-4ca5-be75-9a6360ab645d-weu

Data based on last 1 day

TYPE (1)

| | |
|---|---|
| Heartbeat | 3K |

REMOTEIPCOUNTRY (1)

| | |
|---|---|
| Netherlands | 3K |

Show legacy language converter

```
Heartbeat | summarize dcount(ComputerIP) by bin(TimeGenerated, 1h)
```

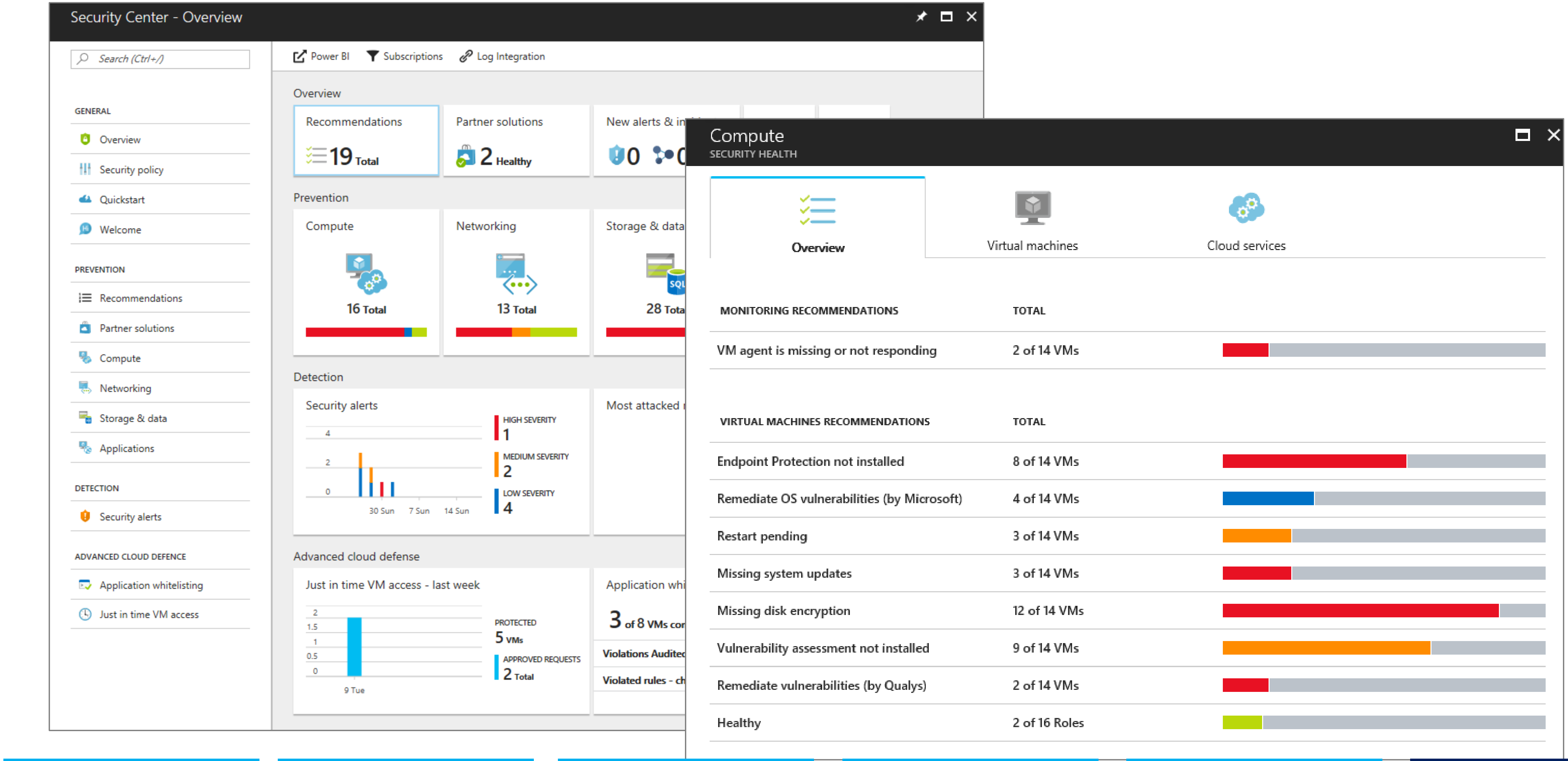
Advanced Analytics

25 Results  Chart  Table

00:00:00.817

| TIMEGENERATED | DCOUNT_COMPUTERIP |
|---|---|
| 2017-10-13T11:00:00Z | 5 |
| 2017-10-13T10:00:00Z | 5 |
| 2017-10-13T09:00:00Z | 5 |
| 2017-10-13T08:00:00Z | 5 |
| 2017-10-13T07:00:00Z | 5 |
| 2017-10-13T06:00:00Z | 5 |
| 2017-10-13T05:00:00Z | 5 |
| 2017-10-13T04:00:00Z | 5 |
| 2017-10-13T03:00:00Z | 5 |
| 2017-10-13T02:00:00Z | 5 |

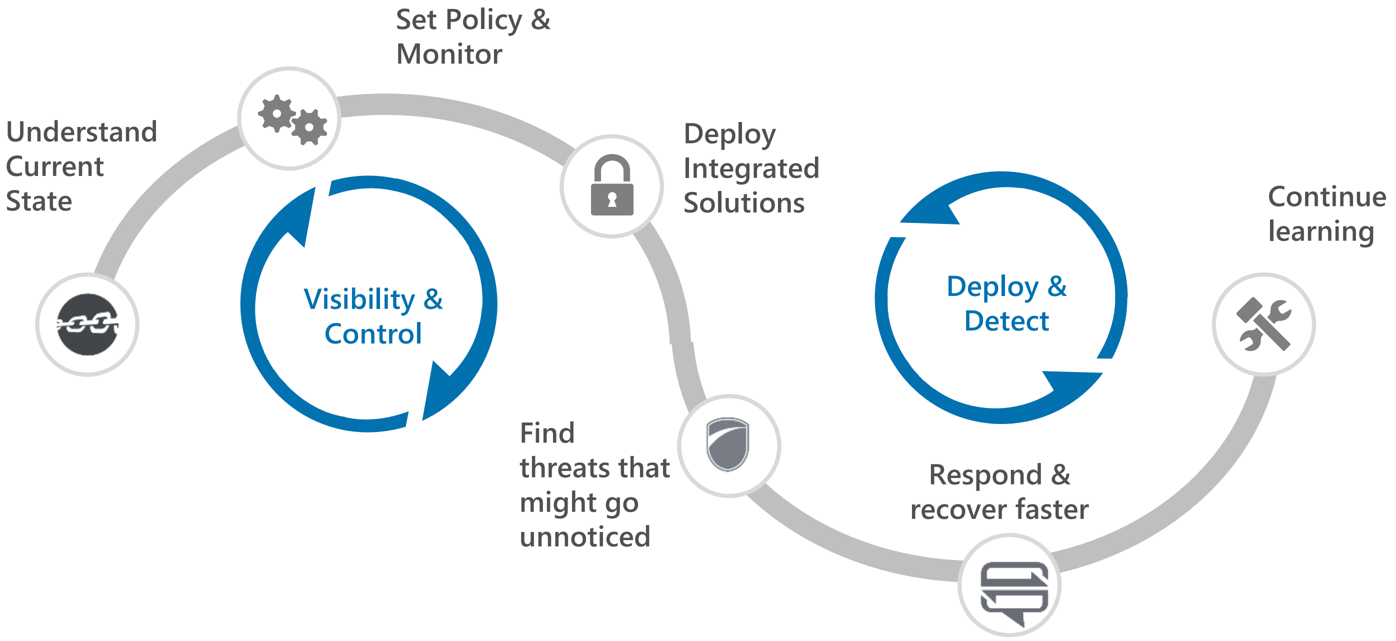
# Azure Security Center



| MONITORING RECOMMENDATIONS | TOTAL |
|---|---|
| VM agent is missing or not responding | 2 of 14 VMs |

| VIRTUAL MACHINES RECOMMENDATIONS | TOTAL |
|---|---|
| Endpoint Protection not installed | 8 of 14 VMs |
| Remediate OS vulnerabilities (by Microsoft) | 4 of 14 VMs |
| Restart pending | 3 of 14 VMs |
| Missing system updates | 3 of 14 VMs |
| Missing disk encryption | 12 of 14 VMs |
| Vulnerability assessment not installed | 9 of 14 VMs |
| Remediate vulnerabilities (by Qualys) | 2 of 14 VMs |
| Healthy | 2 of 16 Roles |

# Protect, Detect and Respond to Threats with Native Azure Security Center



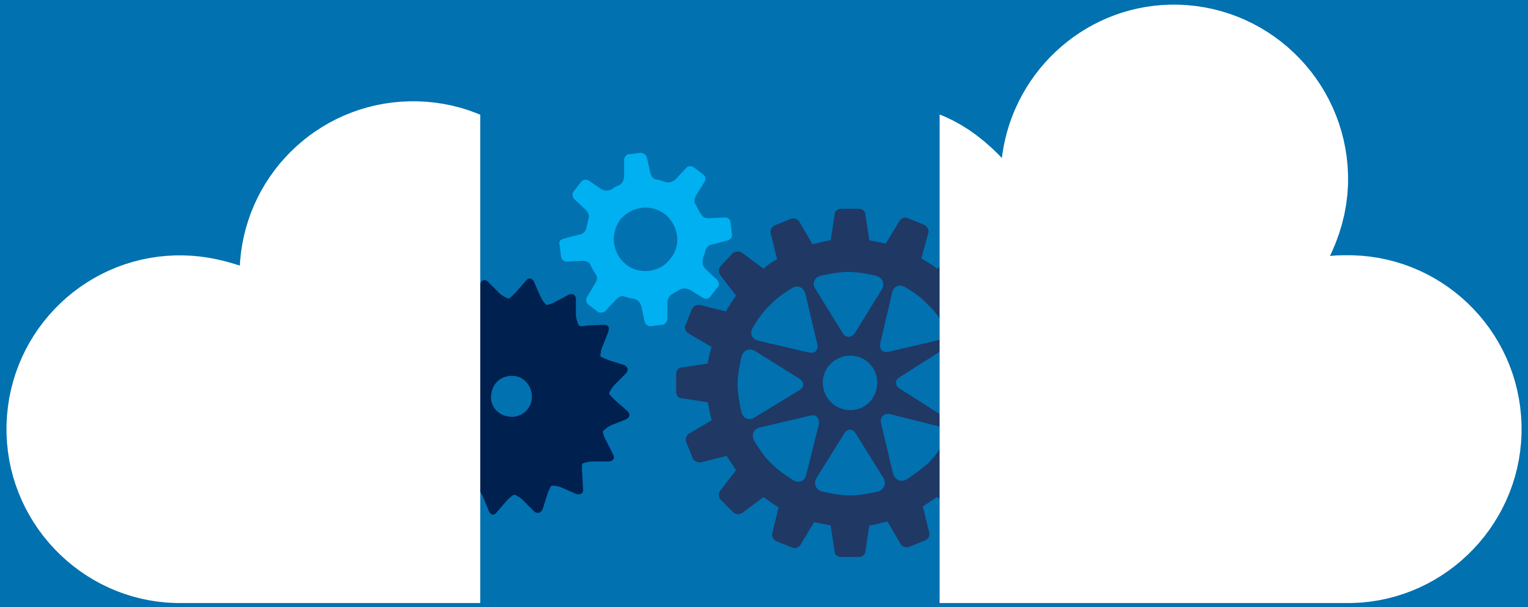
- ✓ Gain visibility and control
- ✓ Integrated security, monitoring, policy management
- ✓ Built in threat detections and alerts
- ✓ Works with broad ecosystem of security solutions

Check Point SOFTWARE TECHNOLOGIES LTD.
TREND MICRO
IMPERVA SECURESPHERE
CLOUDFLARE
Barracuda
f5
CISCO
IMPERVA INCAPSULA
FORTINET

Microsoft

# Demo

Azure Monitor
Azure Log Analytics
Azure Security Center



Microsoft

# Resources

[Azure Monitor](#)
[Azure Log Analytics](#)
[Azure Security Center](#)