



RAZOR TECHNOLOGY



# Azure Security Strategy and Top 10 Best Security Practices

David J. Rosenthal  
VP, Digital Business  
March 31, 2021

# Operations

Security operations that work for you



## Azure Security



# Technology

Enterprise-class technology



# Partnerships

Partnerships for a heterogeneous world

# A secure foundation at global scale

Each **physical datacenter** protected with world-class, multi-layered protection



Over **100** datacenters across the planet

**Global cloud infrastructure** with custom hardware and network protection



Secured with cutting-edge **operational security**

- Restricted access
- 24x7 monitoring
- Global security experts



# Azure infrastructure security

## Secure foundation

### Protect customer data

Data, network segregation. DDoS protection at the edge

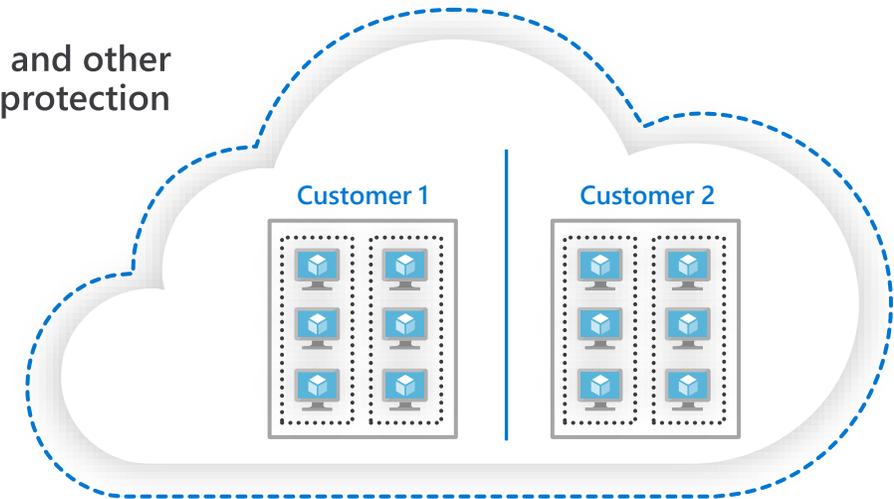
### Secure hardware

Custom-built hardware with integrated security and attestation

### Continuous testing

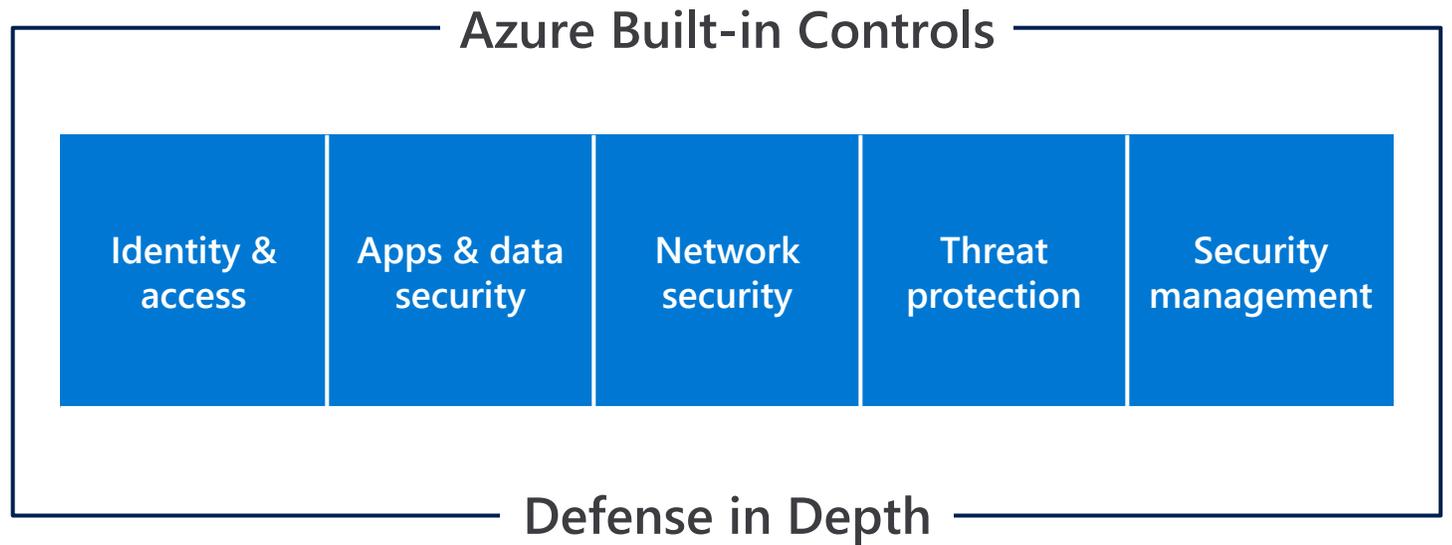
Red team exercises by Microsoft teams, vulnerability scanning & continuous monitoring

DDoS and other edge protection





Technology



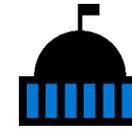
# Partnerships for a heterogeneous world



Partner  
with peers



Work with  
industry alliances



Work with  
government

# Microsoft Intelligent Security Association

Collaboration strengthens protection



Teaming up with our security partners to build an ecosystem of intelligent security solutions that better defend against a world of increased threats

# Extend your existing security solution to Azure with Marketplace

## Partner solutions



Identity & access management



Data protection



Network security



Palo Alto Networks



Check Point  
SOFTWARE TECHNOLOGIES LTD.



Threat protection



Security management



HPE ArcSight



Splunk



IBM QRadar

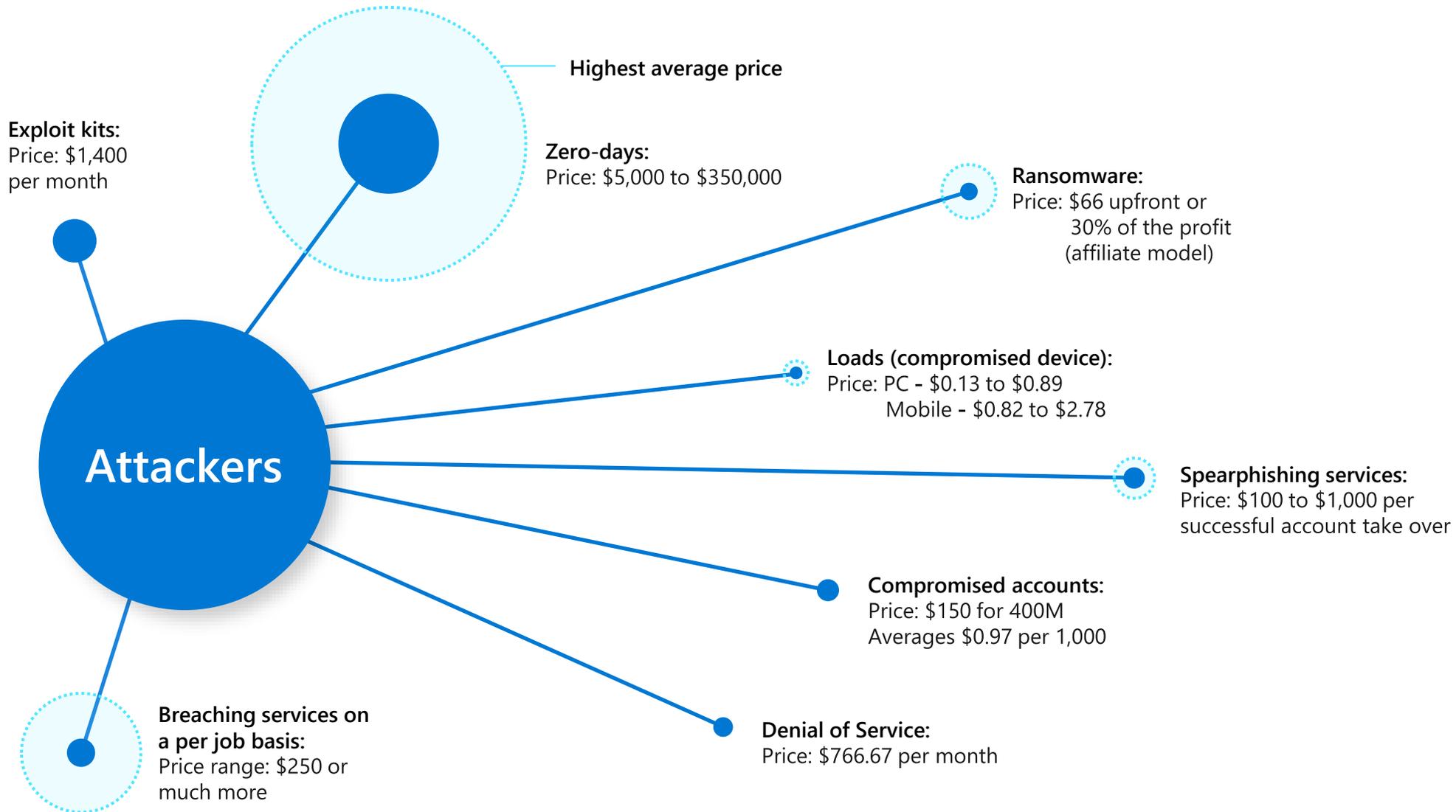


ALERT LOGIC

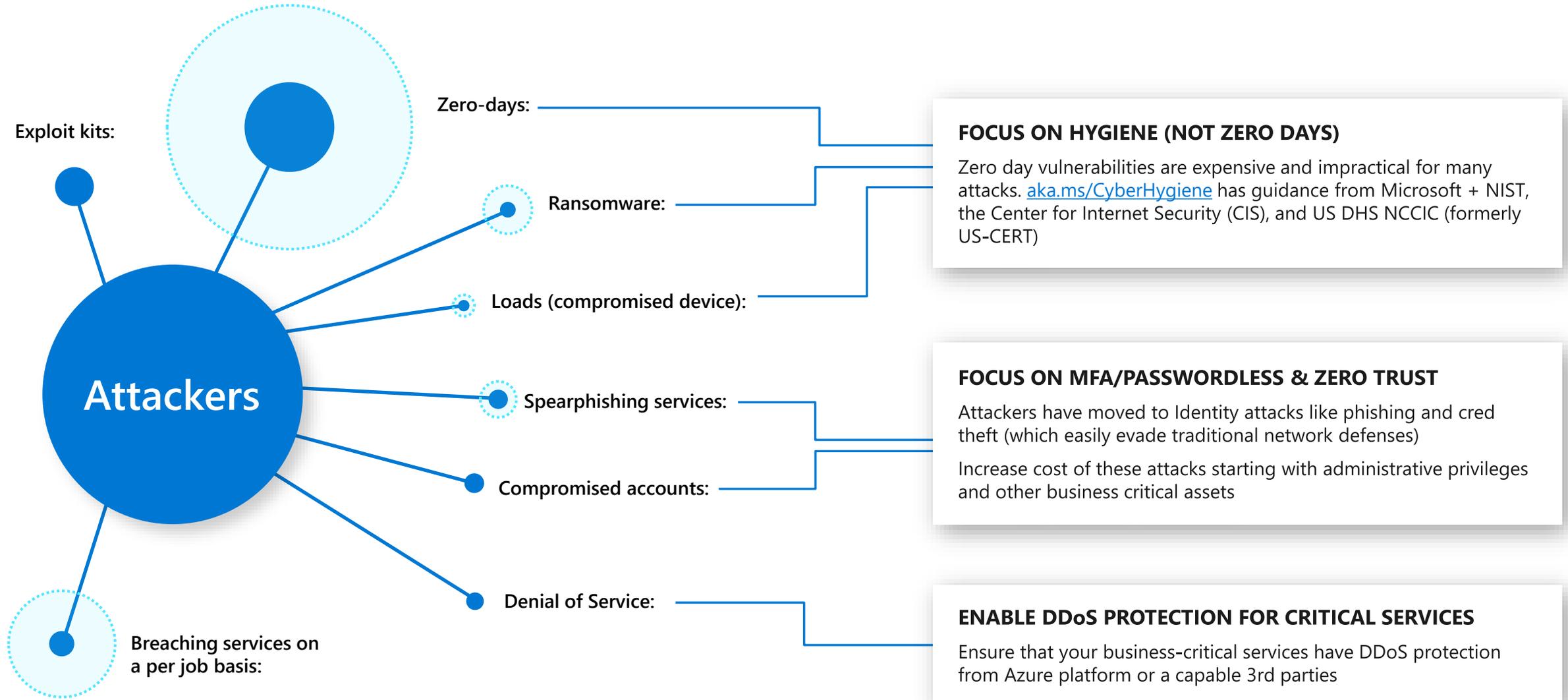
And **hundreds** more with new partners integrating every month

# Top 10 Best Security Practices for Azure

# Attack services are cheap



# Attack services are cheap



# Agenda

## Introduction

- Azure Secure Score

## Top 10 Best practices

## Calls to Action

- Follow Best Practices
- Learn More
- Share
- Provide Feedback



# Security posture management with Azure Secure Score

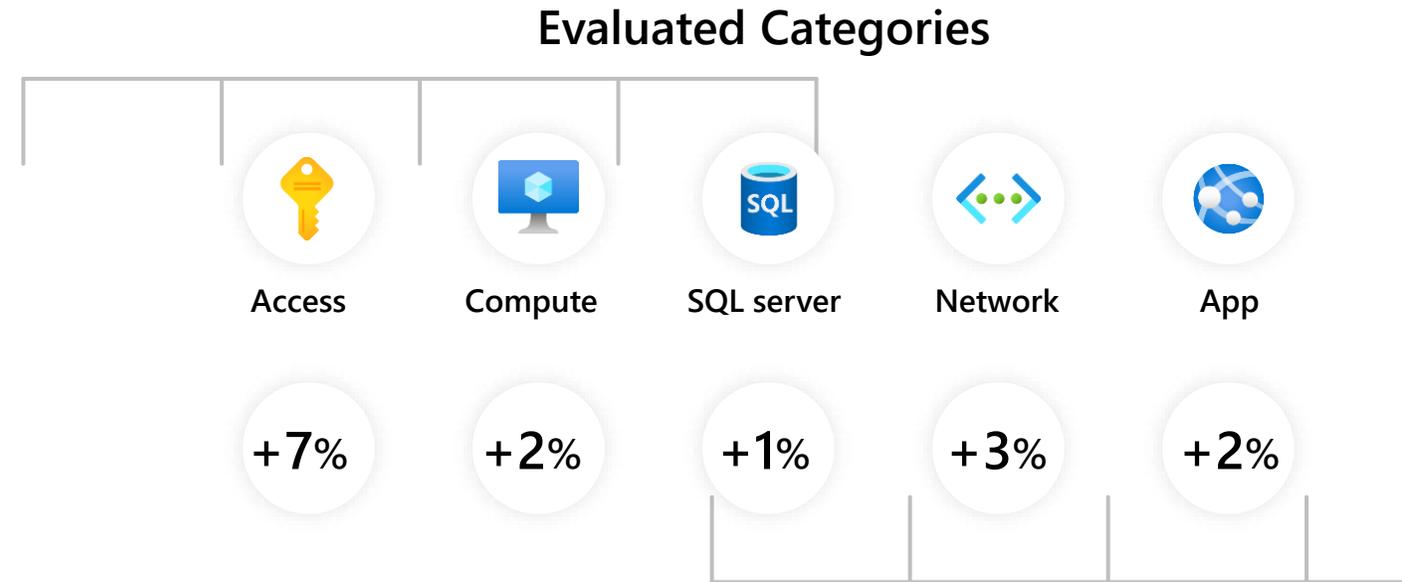


Gain instant insight into the security state of your cloud workloads

Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes

Speed up regulatory compliance

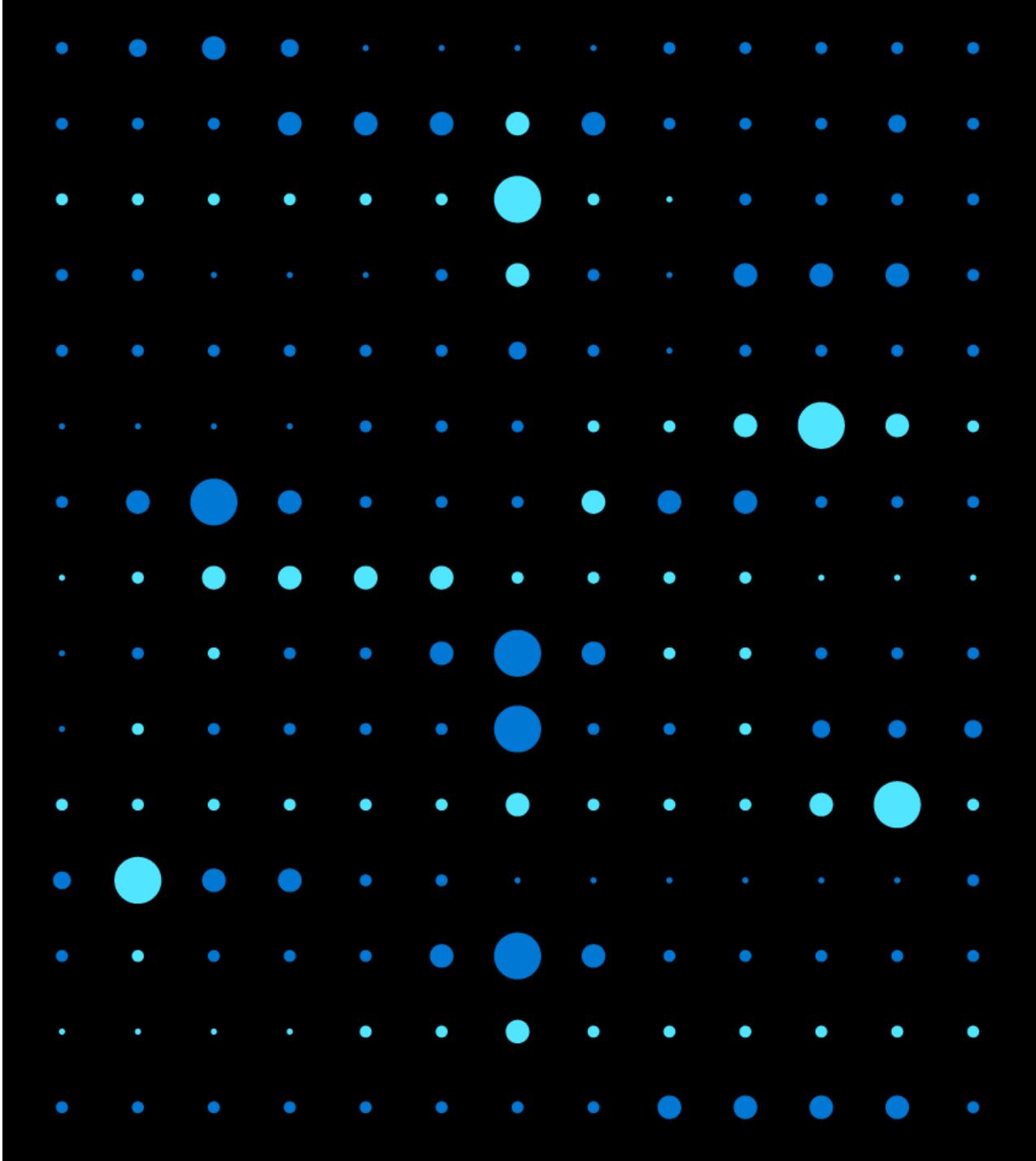


Secure Score Impact



# Demo

## Azure Secure Score



# Top 10 best practices

Focus on highest impact and rapid implementation

- 1 Operationalize Secure Score for cleaning up risk
- 2 Passwordless or MFA for admins
- 3 Enterprise segmentation & Zero Trust preparation
- 4 Enable Threat Protection for Azure Resources
- 5 Follow guidance to secure your DevOps
- 6 Assign and Publish Roles/ Responsibilities
- 7 Choose Firewall Strategy
- 8 Implement Web Application Firewalls
- 9 Choose DDoS Mitigation for Critical Apps
- 10 Consider Retiring Legacy/Classic Technology

# 1

# Operationalize secure score

## OPERATIONALIZE AZURE SECURE SCORE



- **What** – Assign stakeholders to use Secure Score in Azure Security Center to monitor risk profile and continuously improve security posture
- **Why** – Rapidly identifying and remediating common security hygiene risks can significantly reduce overall risk
- **How** – Set up a regular cadence (typically monthly) to review Azure secure score and plan initiatives with specific improvement goals. Gamify the activity if possible to increase engagement.

<https://docs.microsoft.com/en-us/azure/security-center/security-center-secure-score>



TIP

Important: The score you see depends on which subscriptions you have permission to

## SUGGESTED PROCESS OWNERS

Monitor Secure Score	<ul style="list-style-type: none"> <li>• Vulnerability Management (or Governance/Risk/Compliance team)</li> <li>• Architecture Team</li> <li>• Responsible Technical Team (listed below)</li> </ul>
Improve Score Area	Responsible Technical Team
Compute and Apps Resources	<p><b>App Services</b></p> <ul style="list-style-type: none"> <li>▪ Application Development/Security Team(s)</li> </ul> <p><b>Containers</b></p> <ul style="list-style-type: none"> <li>▪ Application Development and/or Infrastructure/IT Operations</li> </ul> <p><b>VMs/Scale sets/compute</b></p> <ul style="list-style-type: none"> <li>▪ IT/Infrastructure Operations</li> </ul> <p><b>NOTE:</b> Each DevOps team may be responsible for their application resources</p>
Data & Storage Resources	<p><b>SQL/Redis/Data Lake Analytics/Data Lake Store</b></p> <ul style="list-style-type: none"> <li>▪ Database Team</li> </ul> <p><b>Storage Accounts</b></p> <ul style="list-style-type: none"> <li>▪ Storage/Infrastructure Team</li> </ul>
Identity and Access Resources	<p><b>Subscriptions</b></p> <ul style="list-style-type: none"> <li>▪ Identity Team(s)</li> </ul> <p><b>Key Vault</b></p> <ul style="list-style-type: none"> <li>▪ Information/Data Security Team</li> </ul>
Networking Resources	<ul style="list-style-type: none"> <li>▪ Networking Team</li> <li>▪ Network Security Team</li> </ul>
IoT Security	<ul style="list-style-type: none"> <li>▪ IoT Operations Team</li> </ul>

## 2

# Account protection

## PASSWORDLESS / MFA FOR ADMINS

- **What** – Require all critical impact admins to be passwordless (preferred) or require Multi-factor Authentication (MFA).
- **Why** – Passwords cannot protect accounts against common attacks. <https://channel9.msdn.com/events/Ignite/Microsoft-Ignite-Orlando-2017/BRK3016>
- **How** –
  - **Passwordless (Windows Hello)**  
<http://aka.ms>HelloForBusiness>
  - **Passwordless (Authenticator App)**  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-phone-sign-in>
  - **Multifactor Authentication**  
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>
  - **3rd Party MFA Solution**

## NO STANDING ACCESS

- **What** – No standing access for critical impact admins
- **Why** – Permanent privileges increase business risk by increasing attack surface of accounts (time)
- **How** –
  - **Just in Time** - Enable Azure AD PIM or 3rd party solution) for all of these accounts
  - **Break glass** – Process for accounts (preferred for low use accounts like global admin)

**Note:** Text Message based MFA is now relatively inexpensive for attackers to bypass, so focus on passwordless & stronger MFA

**Key Related Item** is to increase administrator workstation security – <http://aka.ms/secureworkstation>

# 3

# Enterprise segmentation & Zero Trust preparation

1. **Align teams & strategy** to prioritize zero trust activities & create enterprise segmentation strategy spanning network, identity, app, etc. *(aligns naturally to Cloud adoption)*



## GRC – Segmentation

CRITICAL CHOICE



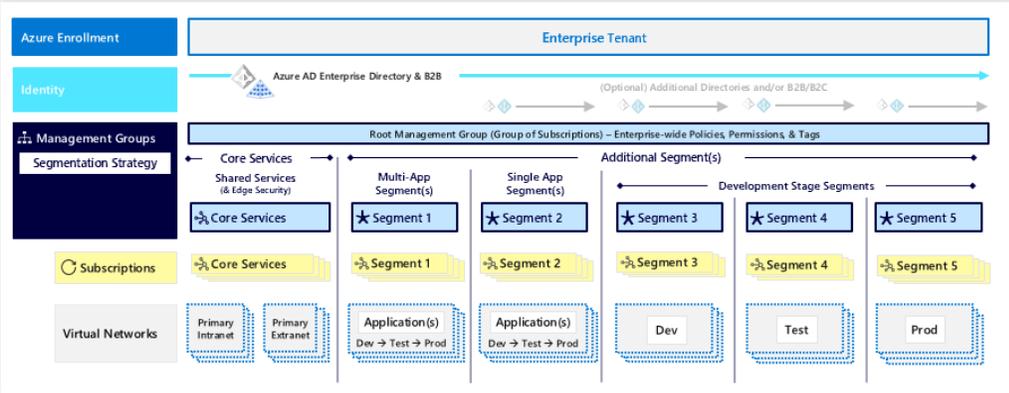
### SEGMENTATION STRATEGY

- **What** – Identify security segments that are needed for your organization to contain risk
- **Why** – A clear and simple segmentation strategy enables stakeholders (IT, Security, Business Units) can understand and support it. This clarity reduces the risk of human errors and automation failures that can lead to security vulnerabilities, operational downtime, or both
- **How** – Select the segmentation approaches from the reference design and assign permissions and network controls as appropriate.

**TIP** **Minimize Complexity** - Always consider whether a segment is needed or whether security monitoring provides enough risk mitigation (each segment adds friction and overhead)

- A GOOD SEGMENTATION STRATEGY:**
1. **Enables Operations** – Minimizes operation friction by aligning to business practices and applications
    - Isolating sensitive workloads from compromise of other assets
    - Isolating high exposure systems from being used as a pivot to other systems
  2. **Contains Risk** - Adds cost and friction to attackers by
    - Isolating sensitive workloads from compromise of other assets
    - Isolating high exposure systems from being used as a pivot to other systems
  3. **Is Monitored** – Security Operations should monitor for potential violations of the integrity of the segments (account usage, unexpected traffic, etc.)

## Reference design - Azure administration model



# GRC – Segmentation

## CRITICAL CHOICE

### SEGMENTATION STRATEGY

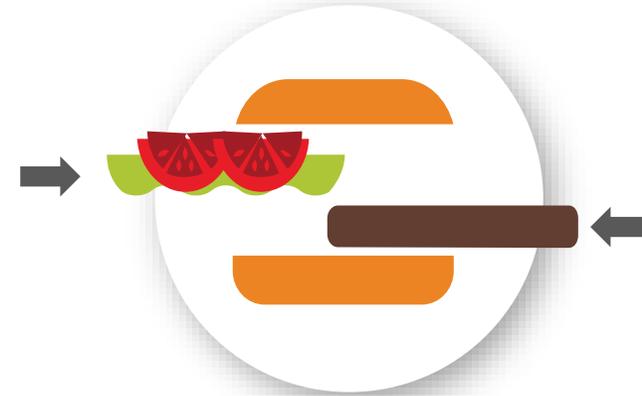


- **What** – Identify security segments that are needed for your organization to contain risk
- **Why** – A clear and simple segmentation strategy enables stakeholders (IT, Security, Business Units) can understand and support it. This clarity reduces the risk of human errors and automation failures that can lead to security vulnerabilities, operational downtime, or both
- **How** – Select the segmentation approaches from the reference design and assign permissions and network controls as appropriate.



TIP

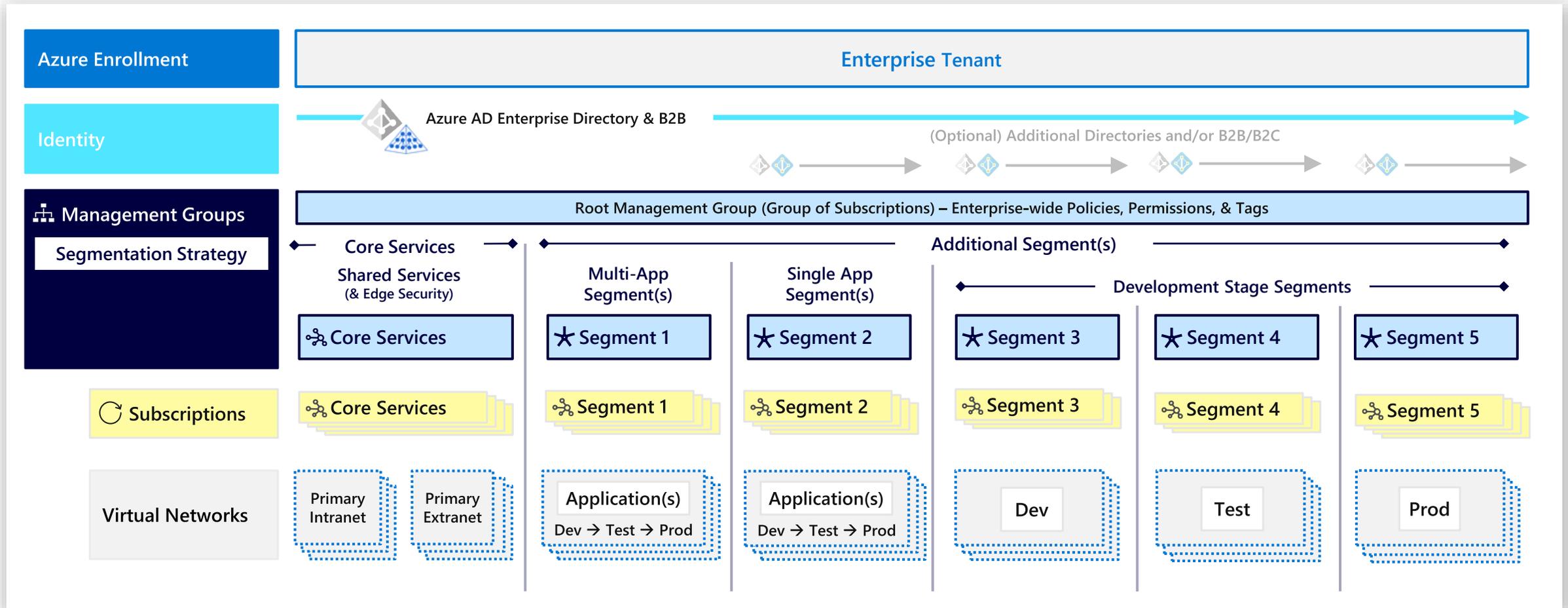
**Minimize Complexity** - Always consider whether a segment is needed or whether security monitoring provides enough risk mitigation (each segments adds friction and overhead)



### A GOOD SEGMENTATION STRATEGY:

- 1. Enables Operations** – Minimizes operation friction by aligning to business practices and applications
- 2. Contains Risk** - Adds cost and friction to attackers by
  - Isolating sensitive workloads from compromise of other assets
  - Isolating high exposure systems from being used as a pivot to other systems
- 3. Is Monitored** – Security Operations should monitor for potential violations of the integrity of the segments (account usage, unexpected traffic, etc.)

# Reference design - Azure administration model



## 4

# Monitor for Attacks

## Monitor for Potential Attacks

- ✓ VMs on Azure (Windows, Linux, and Installed Applications)
- ✓ VMs on 3<sup>rd</sup> party clouds and IaaS
- ✓ Azure Container and Azure Kubernetes Services (AKS)
- ✓ Azure SQL Database and Azure SQL Data Warehouse
- ✓ Azure Storage Accounts
- ✓ Azure Cosmos DB
- ✓ SQL Server running on IaaS VMs
- ✓ IoT Devices
- ✓ On-premises servers
- ✓ Azure App Service
- ✓ And More...



As Required, Export to or integrate with your SIEM / analytics

# Security Operations – Azure Alerts

## CRITICAL GUIDANCE



### ASC BUILT IN SECURITY ALERTS

- **What** – Enable Azure Security Center security Alerts
- **Why** – Azure Security Center provides actionable detections for common attack methods ([Alert List](#) depicted on this slide), which can save your team significant effort on query development.

These alerts are focused on high true positive rate by leveraging Microsoft's [extensive threat intelligence](#), advanced machine learning, industry leading Endpoint Detection & Response (EDR) ([MITRE report](#)), and other approaches.

- **How** – Enable Azure Security Center (Recommend Standard Tier) <https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started>

## AZURE SECURITY CENTER ALERTS

### Virtual Machine Behavioral Analysis (VMBA)

#### Event analysis

Security Center uses advanced analysis to identify compromised resources based on analysis of virtual machine event logs. For example, Process Creation Events and Login Events. In addition, there is correlation with other signals to check for supporting evidence of a widespread campaign.

- Suspicious process execution detected: Attackers often try to execute malicious code without detection by masquerading as benign processes. These alerts indicate that a process execution matched one of the following patterns:
  - A process known to be used for malicious purposes was executed based on an aggregation of these commands:
  - A process was executed from an uncommon location.
  - A process was executed from a location in common with known malware.
  - A process was executed from a suspicious path.
  - A process was executed in an abnormal context.
  - A process was executed by an unusual account.
  - A process with a suspicious extension was executed.
  - A process with a suspicious double extension was executed.
  - A process with a suspicious right-to-left (RTL) character in its name.
  - A process whose name is similar to but different from a common process.
  - A process whose name corresponds to a known attacker tool.
  - A process with a random name was executed.
  - A process with a suspicious extension was executed.
  - A hidden file was executed.
- A process with a suspicious extension was executed.
- A process with a suspicious double extension was executed.
- A process with a suspicious right-to-left (RTL) character in its name.
- A process whose name is similar to but different from a common process.
- A process whose name corresponds to a known attacker tool.
- A process with a random name was executed.
- A process with a suspicious extension was executed.
- A hidden file was executed.
- An unusual process was created by a system process.
- An abnormal process was launched by the Windows update service.
- A process was executed with an unusual command line that is evocative of malicious content.
- An attempt to start all executables (\*.exe) in a directory was attempted.
- A process was executed by PsExec utility, which can be used to launch malicious commands.
- The Apache Tomcat's JRebel executable (Jrebel.exe) was used to launch malicious commands.
- The Microsoft Windows "Program Compatibility Assistant" (pca.exe) was executed.
- A suspicious process termination event was detected.
- The system process SVCHOST was executed in an abnormal context.
- The system process SVCHOST was executed in a new session.
- A suspicious command line was executed.
- A PowerShell script has characteristics in common with known malware.
- A known malicious PowerShell Powershell cmdlet was executed.
- A built-in SQL user executed a process it normally wouldn't.
- A Base-64 encoded executable was detected, which could indicate an executable on-the-fly through a sequence of commands.

- Suspicious RDP resource activity: Attackers often target open Remote Desktop Protocol (RDP) connections to gain access to your virtual machines.
  - Remote Desktop logins were attempted.
  - Remote Desktop logins were attempted using invalid accounts.
  - Remote Desktop logins were attempted, some of which were successful.
- Suspicious SSH resource activity: Attackers often target open Secure Shell (SSH) connections to gain access to your virtual machines.
  - Failed SSH logins were attempted.
  - SSH logins were attempted, some of which were successful.
  - Suspicious Windows/Position registry value: This alert indicates an attempt to modify the registry, which could be indicative of hiding applications used by malware. This alert indicates a possible attempt to bypass (followed by AppLocker policy) to execute untrusted code.
  - Suspicious named pipe communications: This alert indicates the use of a named pipe, which is known to be used by attackers to execute code. Named pipes are known to be used by attackers to execute code. This alert indicates the use of a named pipe to execute code. This alert indicates the use of a named pipe to execute code.
  - Decoding of an executable using built-in certutil.exe tool: This alert indicates the use of a built-in tool to decode an executable. Attackers are known to abuse this tool to decode an executable. This alert indicates the use of a built-in tool to decode an executable.

### Contextual Information

If additional information is available, it will be shown in the Security Incident below the list of alerts. This includes:

- Log clear events
- PHP device plugged from unknown device
- Alerts that are not actionable
- New account creation
- File decoded using certutil tool

Time	Alert Name	Severity	Category	Resolution
2020-10-01 10:00:00	Failed RDP login from external IP	High	Remote Desktop Protocol	Low
2020-10-01 10:00:00	Failed SSH login from external IP	High	Secure Shell	High
2020-10-01 10:00:00	Failed RDP login from external IP	High	Remote Desktop Protocol	Low
2020-10-01 10:00:00	Failed SSH login from external IP	High	Secure Shell	High

### SQL Database & Data Warehouse Analysis

#### SQL Database and SQL Data Warehouse analysis

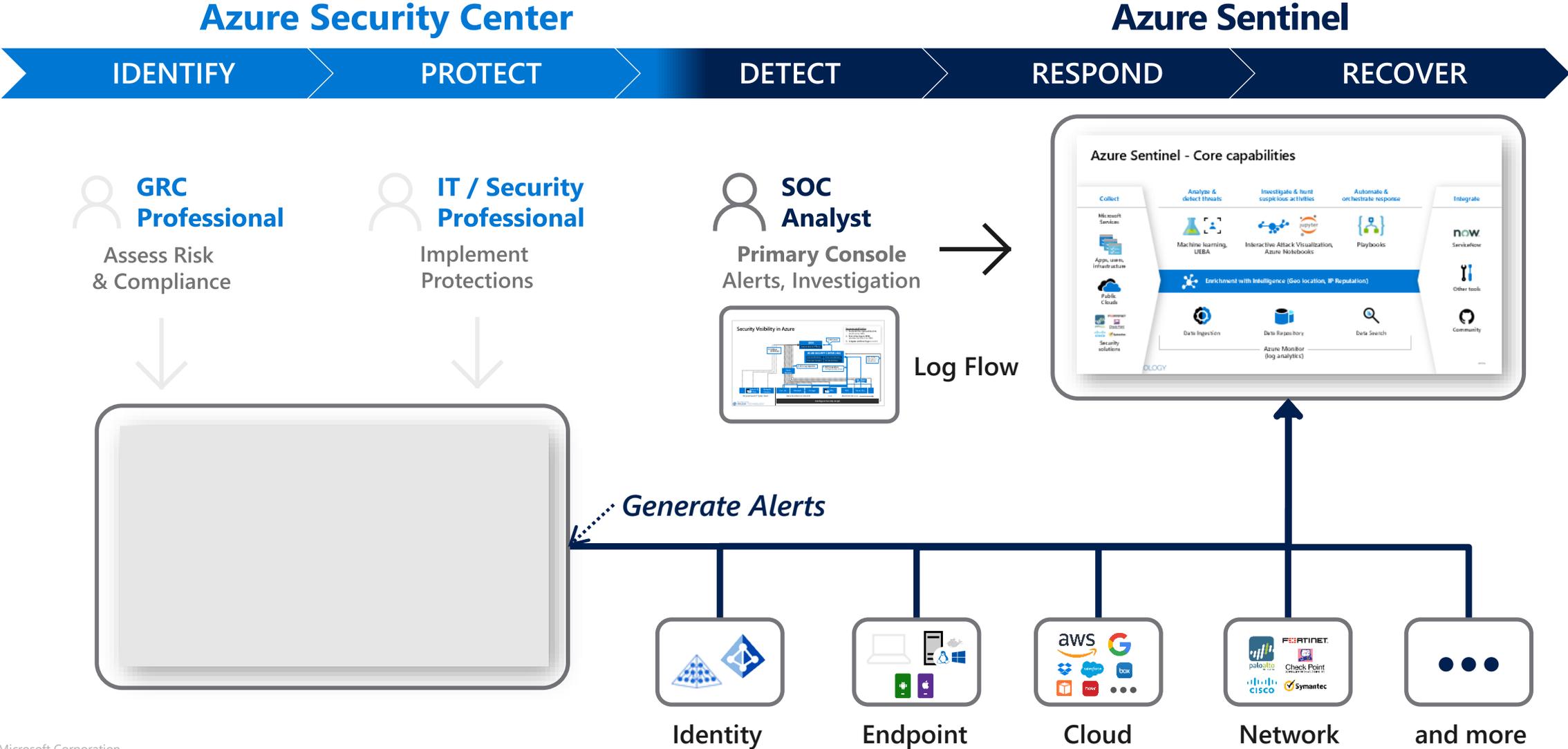
Security Center resource analysis focuses on platforms as a service (PaaS) services, such as the integration with Threat Detection for Azure SQL Database and Azure SQL Data Warehouse. These detections detect anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases and trigger the following alerts:

- Vulnerability to SQL injection: This alert is triggered when an application generates a faulty SQL statement in the database. This may indicate a possible vulnerability to SQL injection attacks. There are two possible reasons for the generation of a faulty statement:
  - A defect in application code that constructs the faulty SQL statement.
  - Application code or stored procedures don't create user input when constructing the faulty SQL statement, which may be exploited for SQL injection.
- Potential SQL injection: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This stored procedure:
  - Access from usual someone has logged action (new application external attack).
  - Access from usual someone has logged action (new application external attack).

### Network Analysis

- Suspicious incoming RDP network activity from multiple sources: Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication from multiple sources. Specifically, sampled network data shows unique IP addresses connecting to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point from multiple hosts (bots).
- Suspicious incoming RDP network activity: Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication. Specifically, sampled network data shows a high number of incoming connections to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point.
- Suspicious outgoing RDP network activity to multiple destinations: Network traffic analysis detected anomalous outgoing Remote Desktop Protocol (RDP) communication to multiple destinations. Specifically, sampled network data shows a high number of outgoing connections from your machine, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external RDP end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- Suspicious outgoing RDP network activity: Network traffic analysis detected anomalous outgoing Remote Desktop Protocol (RDP) communication. Specifically, sampled network data shows a high number of outgoing connections from your machine, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external RDP end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- Suspicious incoming SSH network activity from multiple sources: Network traffic analysis detected anomalous incoming Secure Shell (SSH) communication from multiple sources. Specifically, sampled network data shows unique IP addresses connecting to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your SSH end point from multiple hosts (bots).
- Suspicious incoming SSH network activity: Network traffic analysis detected anomalous incoming Secure Shell (SSH) communication. Specifically, sampled network data shows a high number of incoming connections to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your SSH end point.
- Suspicious outgoing SSH network activity to multiple destinations: Network traffic analysis detected anomalous outgoing Secure Shell (SSH) communication to multiple destinations. Specifically, sampled network data shows outgoing connections from your machine, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external SSH end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- Suspicious outgoing SSH network activity: Network traffic analysis detected anomalous outgoing Secure Shell (SSH) communication. Specifically, sampled network data shows a high number of outgoing connections from your machine, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external SSH end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- Network communication with a malicious machine detected: Network traffic analysis indicates that your machine has communicated with what is possibly a Command and Control center.
- Possible compromised machine detected: Network traffic analysis detected outgoing activity, which may indicate it is acting as part of a botnet. This analysis is based on IP addresses by your resource together with public DNS records.

# Centralized Visibility



# Azure Security Center



Strengthen security posture

Cloud security posture management  
Secure Score | Policies and compliance



Protect against threats

For servers

For cloud native workloads

For databases and storage



Get secure faster

# Azure Security Center



**Cloud Security Posture Management**  
Secure Score | Policies and compliance

**Integrate Threat Intelligence**  
Intelligent Security Graph (Vast & Diverse Data)



## Prevent Attacks

Measure & Improve Security Posture



## Detect & Respond to Attacks

Monitor & Respond Across Resources



Apps



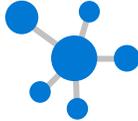
VMs & Servers



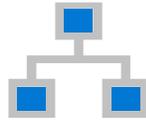
Containers



SQL



IoT



Network



Keys



On-Prem



aws ...



Get secure faster



# Protect your workloads from threats

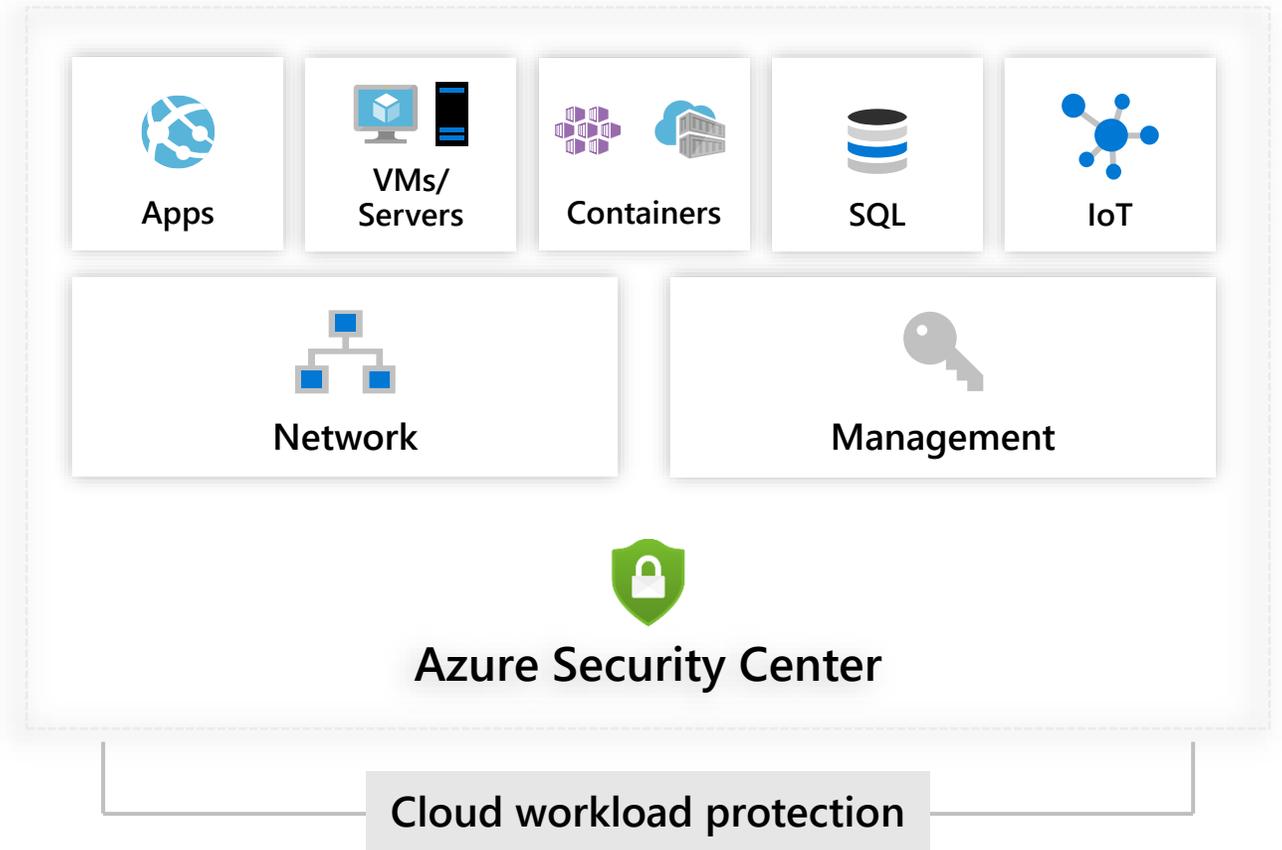
Use industry's most extensive threat intelligence to gain deep insights

Detect & block advanced malware and threats for Linux and Windows Servers on any cloud

Protect cloud-native services from threats

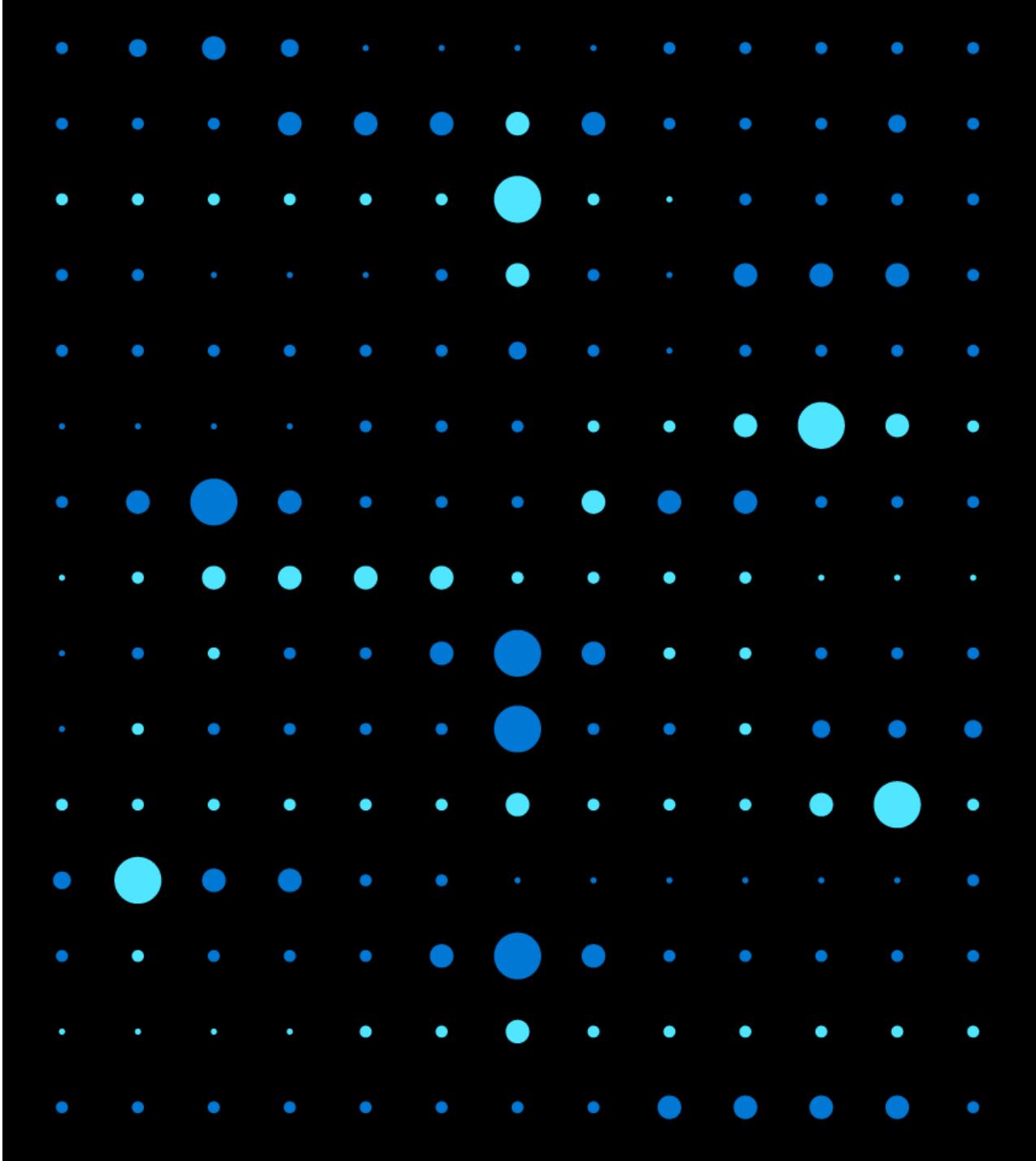
Protect data services against malicious attacks

Protect your Azure IoT solutions with near real time monitoring



# Demo

## Azure Security Center



# Integrate Cloud Security Analytics

## CLOUD ANALYTICS STRATEGY

- **What** – Choose when and how to integrate cloud-based security analytics/SIEM (such as Azure Sentinel, ELK stack, etc.)
- **Why** – As more enterprise services generate security data in the cloud, hauling this data back to on premises becomes expensive and inefficient. This '[Data Gravity](#)' will increasingly require security analytics to be hosted in the cloud as you migrate workloads.
- **How** – Ensure your strategy for security analytics & SIEM plans for this transition and includes thresholds & timing for progression into each phase.

### 1. EXISTING ANALYTICS



ALL LOGS TO  
EXISTING SIEM

### 2. SIDE BY SIDE



SIDE BY SIDE  
(CASE MANAGEMENT)

### 3. FULLY CLOUD NATIVE



ALL LOGS TO  
AZURE SENTINEL

Express

One-stop

# Introducing Azure Sentinel

INTELLIGENT, CLOUD-NATIVE SIEM



Delivers instant value to  
your defenders

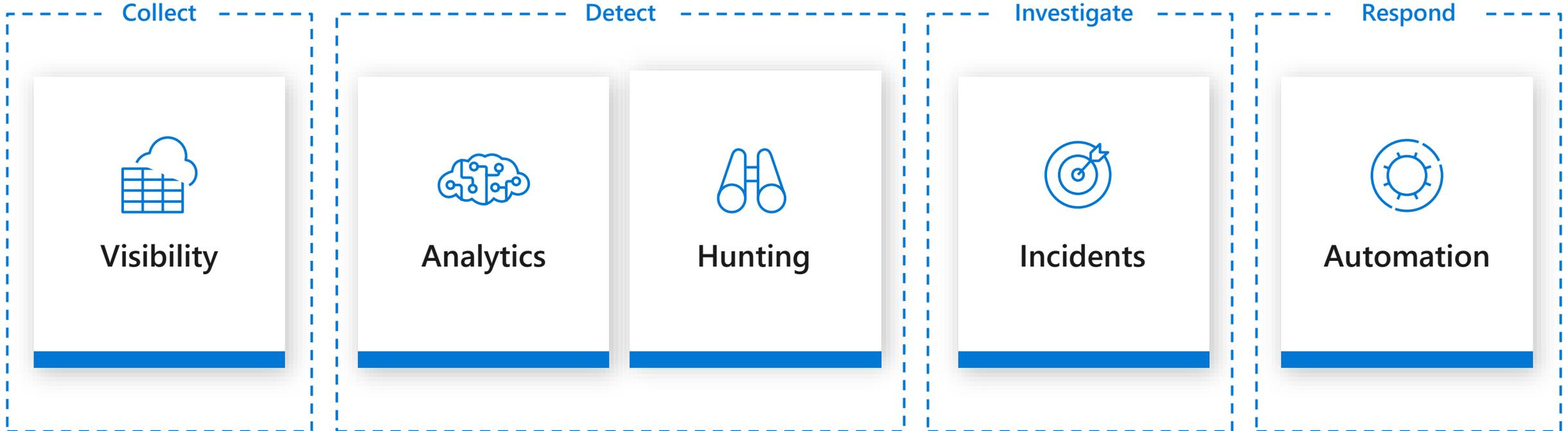


Scales to support your  
growing digital estate



Uses AI and automation to  
improve effectiveness

# End-to-end solution for security operations



Powered by community + backed by Microsoft's security experts

# Azure Sentinel - Core capabilities

## Collect

Microsoft Services



Apps, users, infrastructure

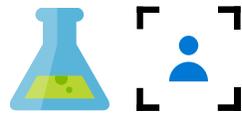


Public Clouds



Security solutions

## Analyze & detect threats



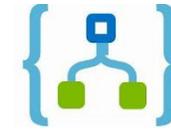
Machine learning, UEBA

## Investigate & hunt suspicious activities



Interactive Attack Visualization, Azure Notebooks

## Automate & orchestrate response



Playbooks

## Integrate

now™

ServiceNow



Other tools



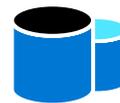
Community



Enrichment with Intelligence (Geo location, IP Reputation)



Data Ingestion



Data Repository

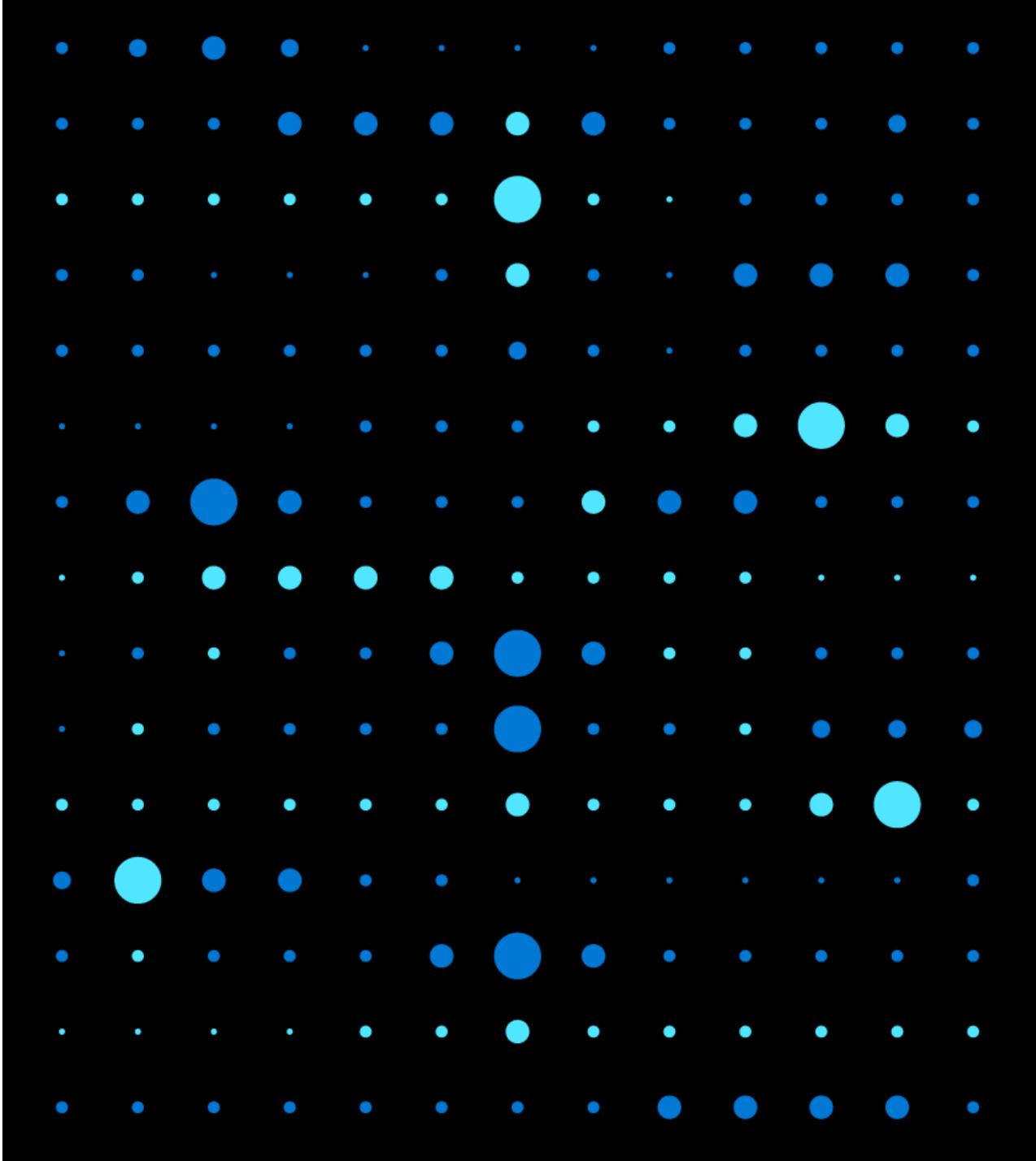


Data Search

Azure Monitor (log analytics)

# Demo

## Azure Sentinel

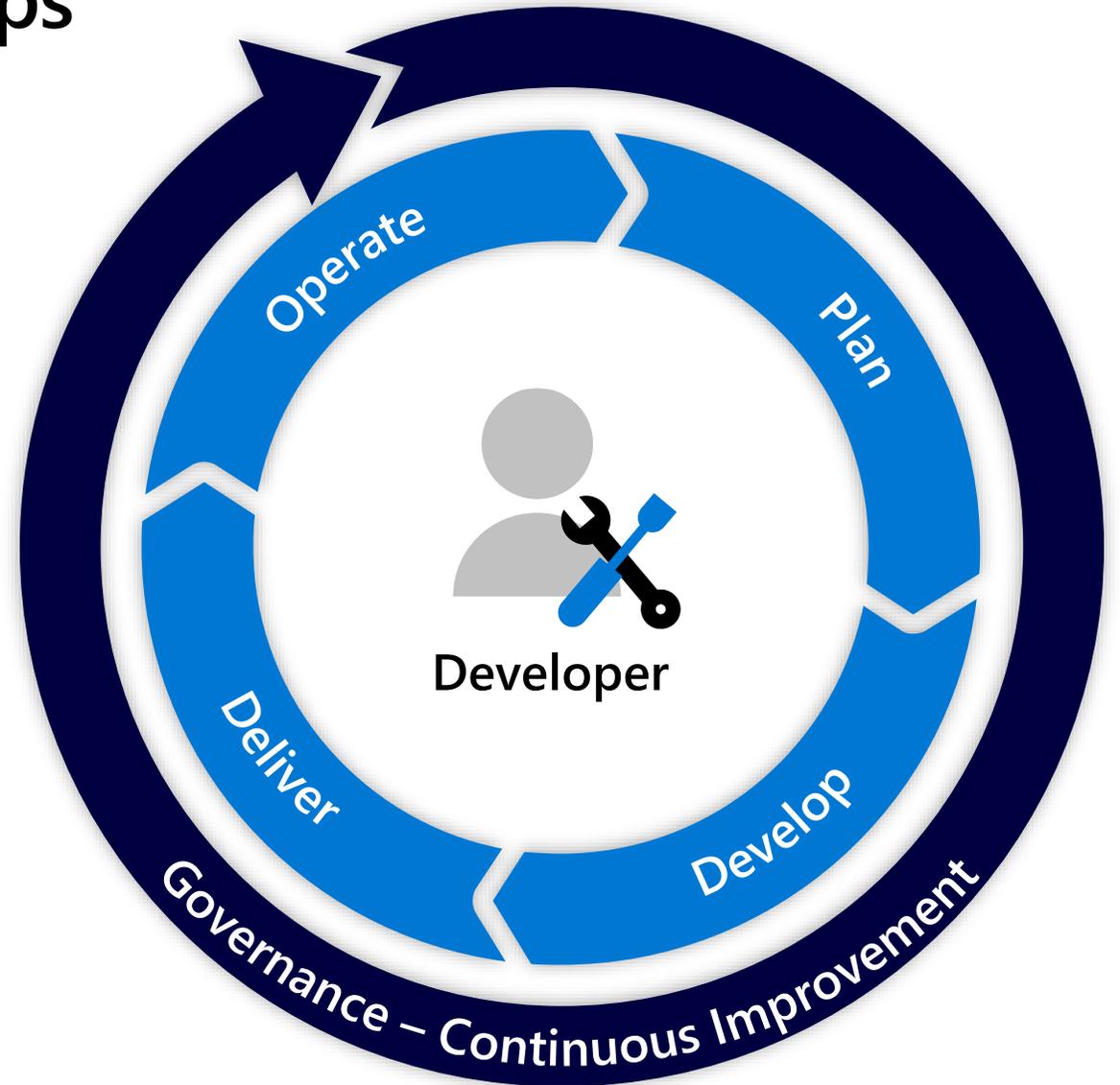


5

# Applications – Secure DevOps

## FOLLOW DEVOPS SECURITY GUIDANCE

- **What** – Integrate guidance and automation for securing applications on the cloud.
- **Why** – Using resources and lessons learned by external organizations that are early adopters of these models can accelerate the improvement of an organization's security posture with less expenditure of effort and resources.
- **How** – Secure your application development / DevOps process by integrating existing guidance such as
  - Microsoft Secure DevOps Toolkit – <https://azsk.azurewebsites.net/>
  - Organization for Web App Security Project (OWASP) DevOps Pipeline security [https://www.owasp.org/index.php/OWASP\\_AppSec\\_Pipeline#tab=Main](https://www.owasp.org/index.php/OWASP_AppSec_Pipeline#tab=Main)

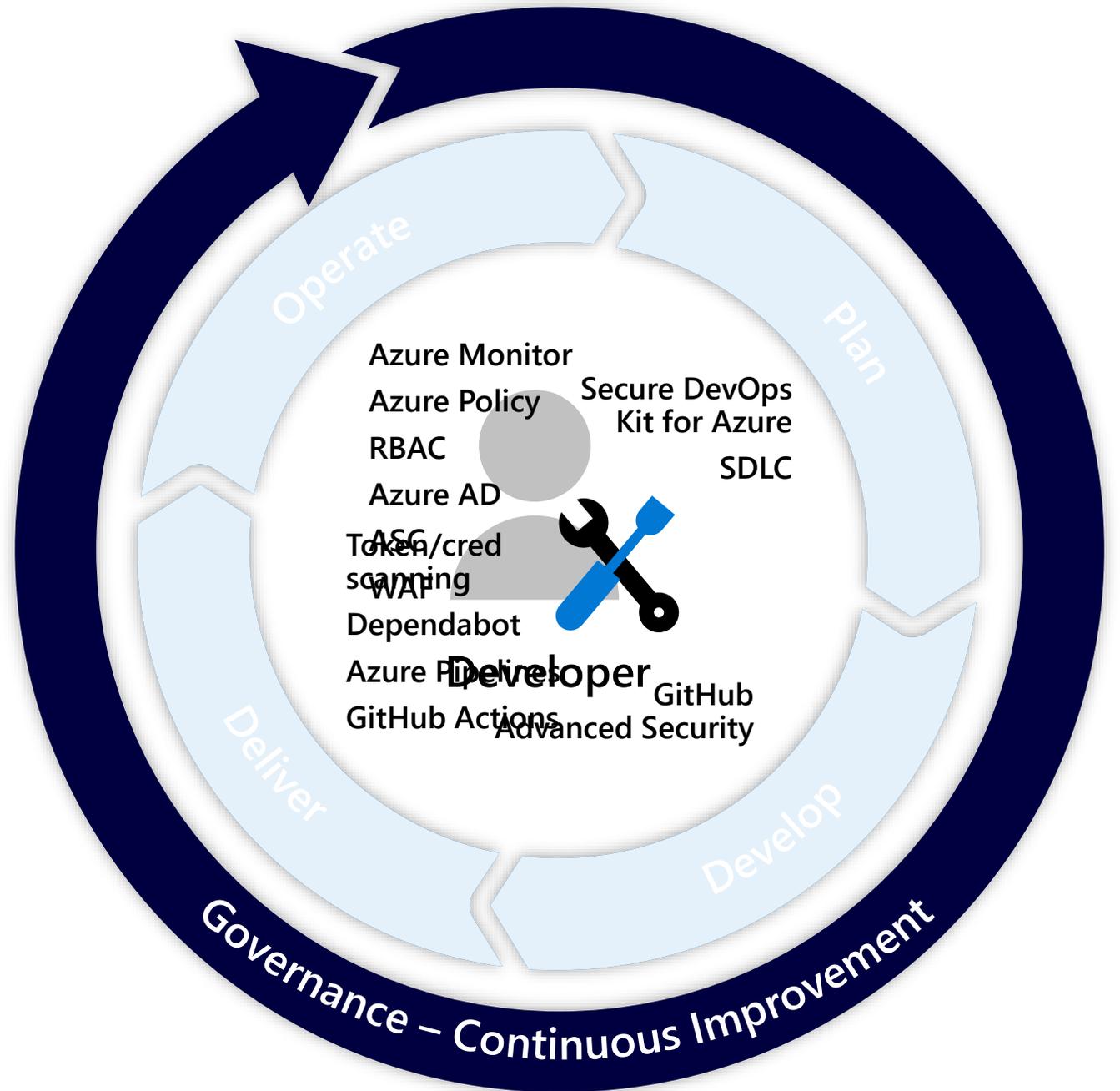


# Securing DevOps: Integrate security into the process

## Define security requirements:

- Threat modeling on major releases
- Run Microsoft Security Code Analysis
- All secrets will be stored in Azure Key Vault

## Establish a standard Incident Response Procedure



# Attacker Opportunities

## Attacker Pivot Risks

Secondary attacks using compromised artifacts/access

- **Lateral Movement** – Pass the hash/ticket/password/etc.
- **Development Artifacts** – Stolen keys/credentials, implanted malware or backdoors, etc.

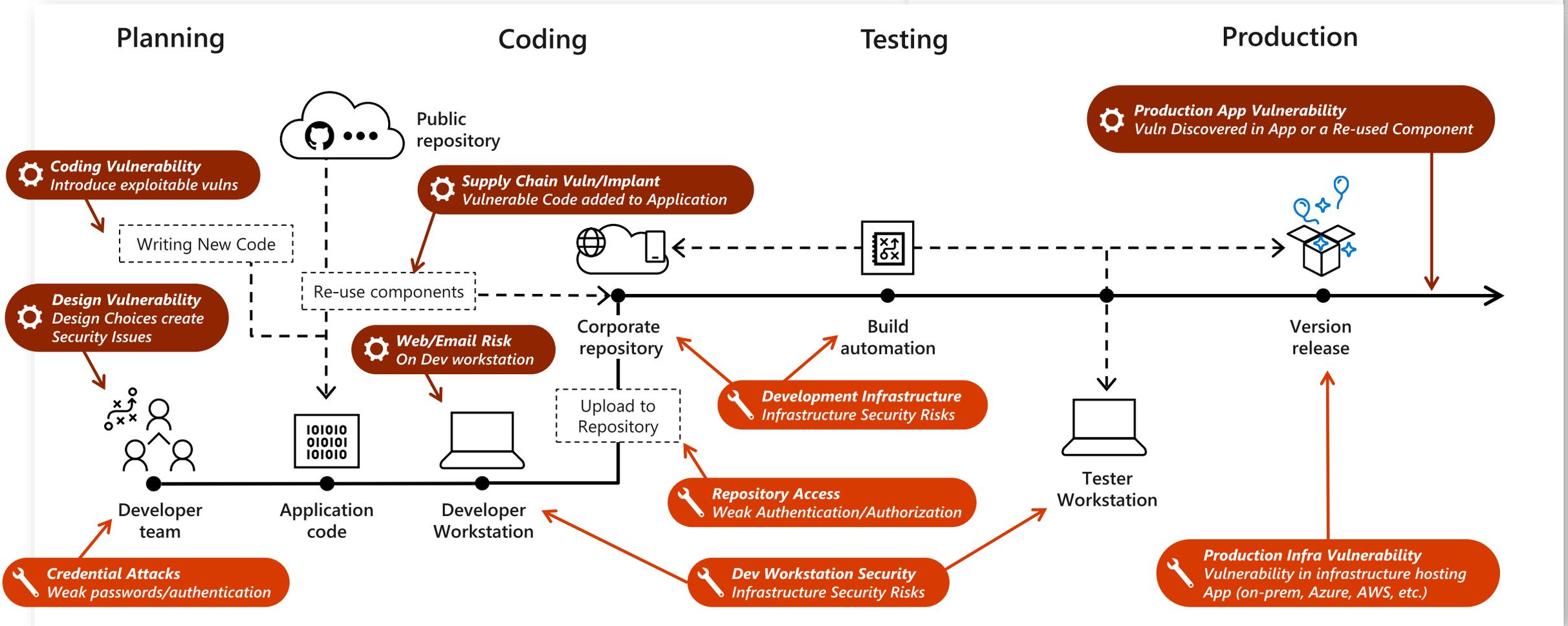
## Legend



Developer-based attacks

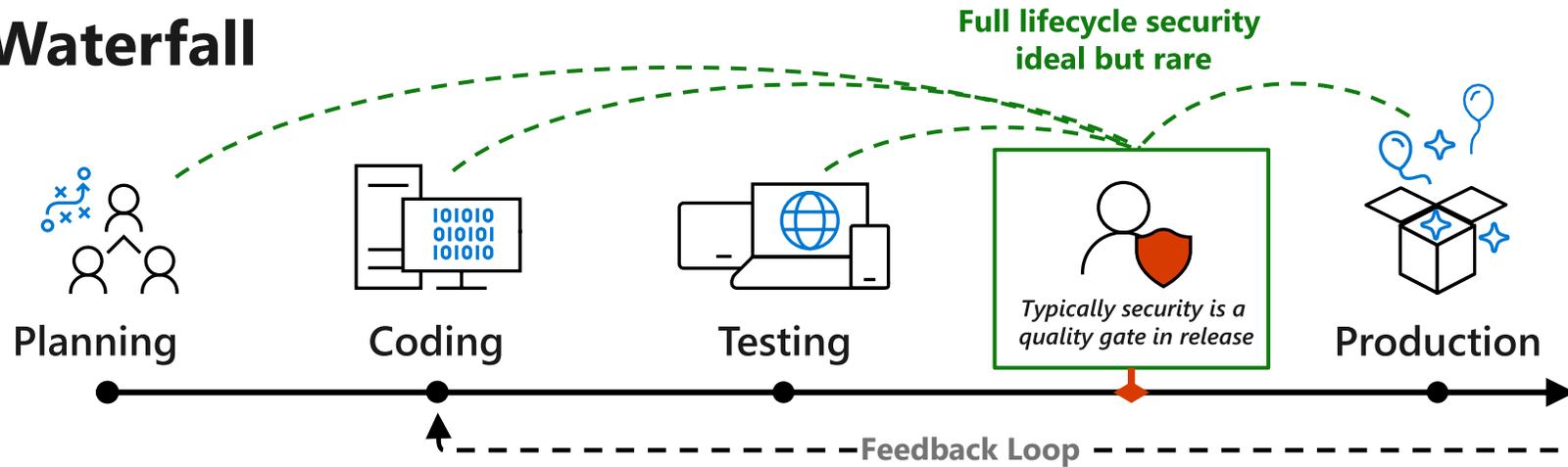


IT and Operations-based attacks



# Role of Security in Development

## Waterfall



Bias to Plan  
& Quality  
(Weeks/Months)

## DevOps

Quality and Security risk mitigated by rapidly release of fixes



Bias to Speed  
& Agility  
(Hours/Days)

# 6

## Ensure clear ownership through the transition

### CLEAR LINES OF RESPONSIBILITY



- **What** – Designate the parties responsible for specific functions in Azure
- **Why** – Consistency helps avoid confusion that can lead to human and automation errors that create security risk.
- **How** – Designate groups (or individual roles) that will be responsible for key centralized functions

Most organizations map these closely to current on premises models.



TIP

Document and Socialize this widely with all teams working on Azure

Network Security	<i>Typically existing network security team</i> Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.
Network Management	<i>Typically existing network operations team</i> Enterprise-wide virtual network and subnet allocation
Server Endpoint Security	<i>Typically IT operations, security, or jointly</i> Monitor and remediate server security (patching, configuration, endpoint security, etc.)
Incident Monitoring and Response	<i>Typically security operations team</i> Investigate and remediate security incidents in SIEM or source console: <ul style="list-style-type: none"> <li>• Azure Security Center</li> <li>• Azure AD Identity Protection</li> </ul>
Policy Management	<i>Typically GRC team + Architecture</i> Set direction for use of Roles Based Access Control (RBAC), Azure Security Center, Administrator protection strategy, and Azure Policy to govern Azure resources
Identity Security and Standards	<i>Typically Security Team + Identity Team Jointly</i> Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards

# 7 Networks and containment

## INTERNET EDGE STRATEGY

- **What** – Choose whether to use Native Azure Controls or 3rd party Network Virtual Appliances (NVAs) for internet edge security (North-South)
- **Why** – Legacy workloads require network protection from internet sources and there are advantages to using either 1st or 3rd party controls to provide this.
- **How** – Select a strategy using the comparison information →

**Note** - Some organizations choose a hybrid configuration where some VNets use advanced 3rd party controls and others use native controls

### AZURE NATIVE CONTROLS

Basic capabilities with simple integration & management

#### Azure Firewall + Web App Firewall (in Application Gateway)

These offer basic security that is good enough for some scenarios with a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration

VS.

### 3RD PARTY CAPABILITIES

Advanced security capabilities from existing vendors

#### Next Generation Firewall (NGFW) and other 3rd party offerings

Network virtual appliances in the Azure Marketplace include familiar security tools that provide enhanced network security capabilities

Configuration is more complex, but allows you to leverage existing capabilities, and skillsets

# Reference Configuration with Native Controls

## Azure Firewall + Application Gateway with Web App Firewall (WAF)

**Azure Firewall**

Cloud native stateful Firewall as a service  
A first among public cloud providers

**Central governance of all traffic flows**

- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNETs and subscriptions

**Complete VNET protection**

- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)
- These intelligence-based filtering to also deny traffic from/to known malicious IP addresses and domains.

**Centralized logging**

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice

<https://docs.microsoft.com/en-us/azure/firewall/>

RAZOR TECHNOLOGY

**Web Application Firewall**

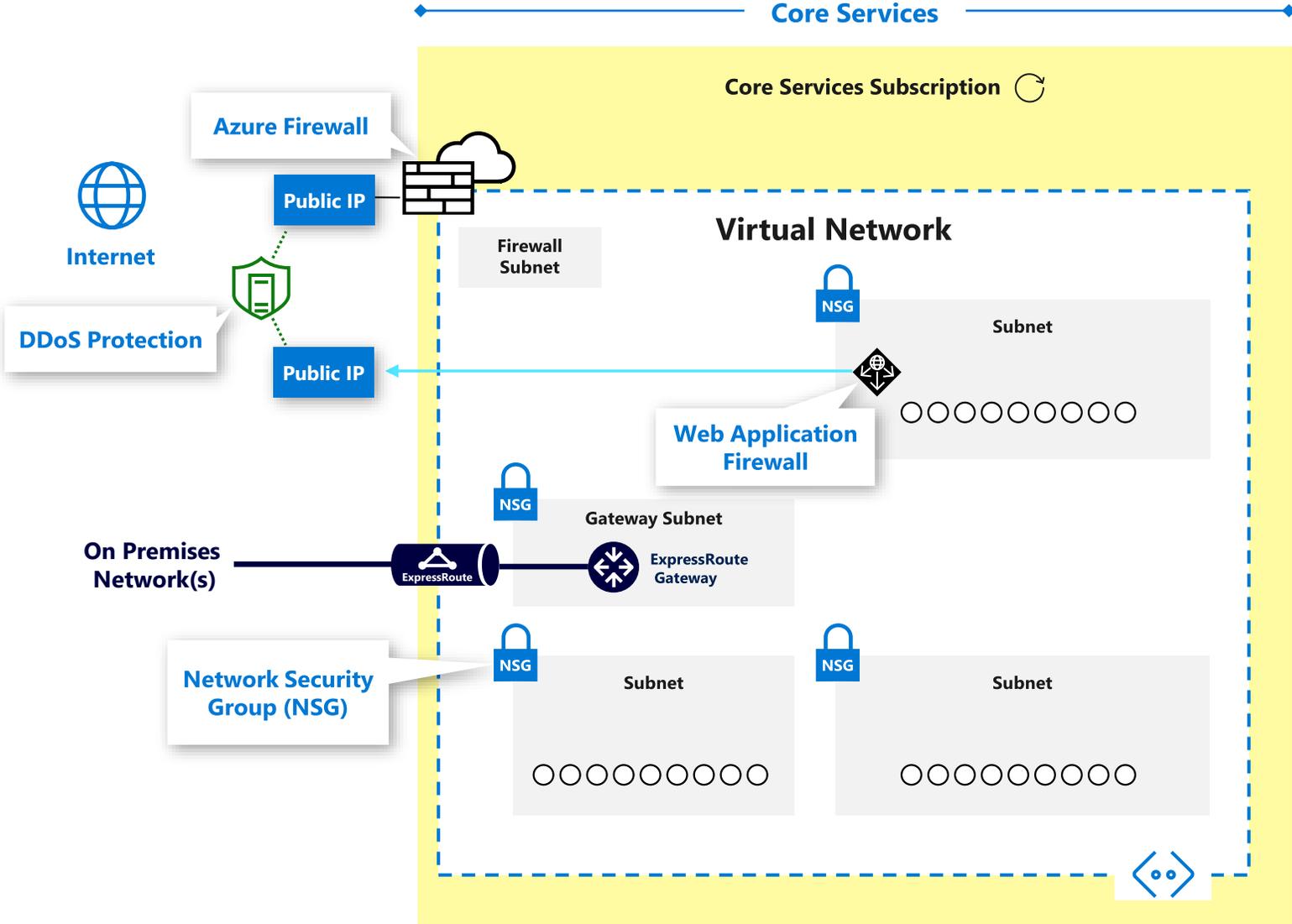
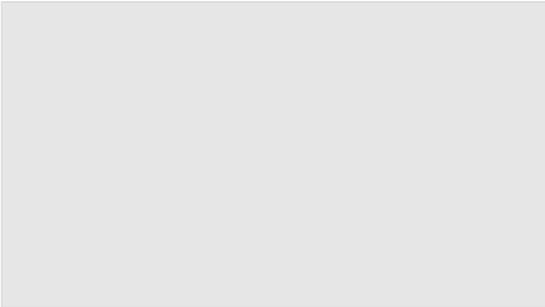
Web application protection

- Protects your application against prevalent XSSe Scripting and SQL Injection attacks
- Blocks threats based on OWASP core rule sets 3.0 or 2.2.9
- Integrated with Azure Security Center
- Real-time logging with Azure Monitor

**High availability and scalability built in and managed by platform**

- Layer 7 load balancing URL path, host based, round robin, session affinity, redirection
- Centralized SSL management SSL offload and SSL policy
- Public or IIS public internal or hybrid
- Rich diagnostics Azure monitor, Log analytics

RAZOR TECHNOLOGY



# Azure Firewall

## Cloud native stateful Firewall as a service

### A first among public cloud providers

#### Central governance of all traffic flows

- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

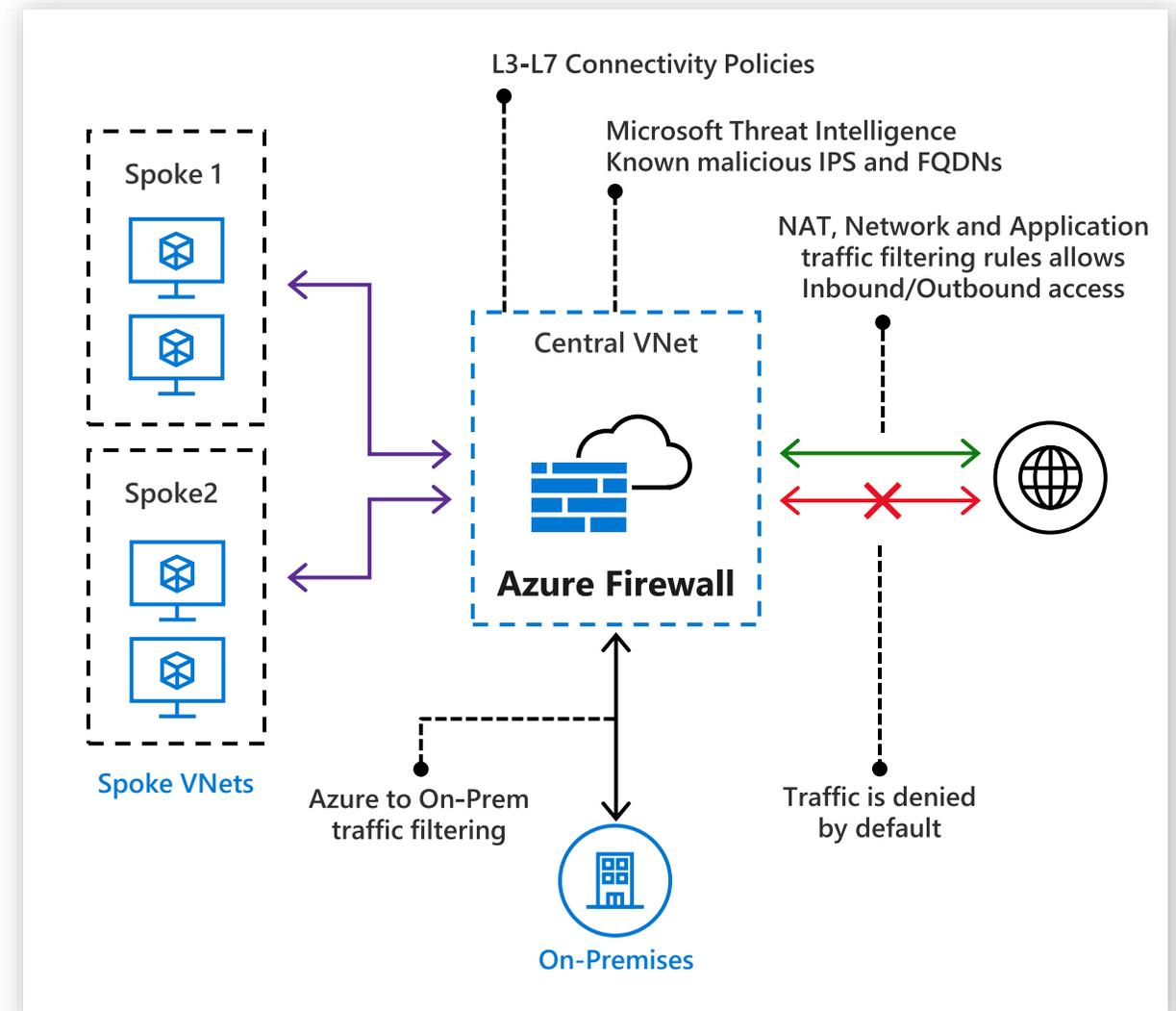
#### Complete VNET protection

- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)
- Threat intelligence-based filtering to alert/deny traffic from/to known malicious IP addresses and domains.

#### Centralized logging

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice

<https://docs.microsoft.com/en-us/azure/firewall/>



# Web Application Firewall

## Web application protection

- Protects your application against prevalent X-Site Scripting and SQL Injection attacks
- Blocks threats based on OWASP core rule sets 3.0 or 2.2.9
- Integrated with Azure Security Center
- Real-time logging with Azure Monitor

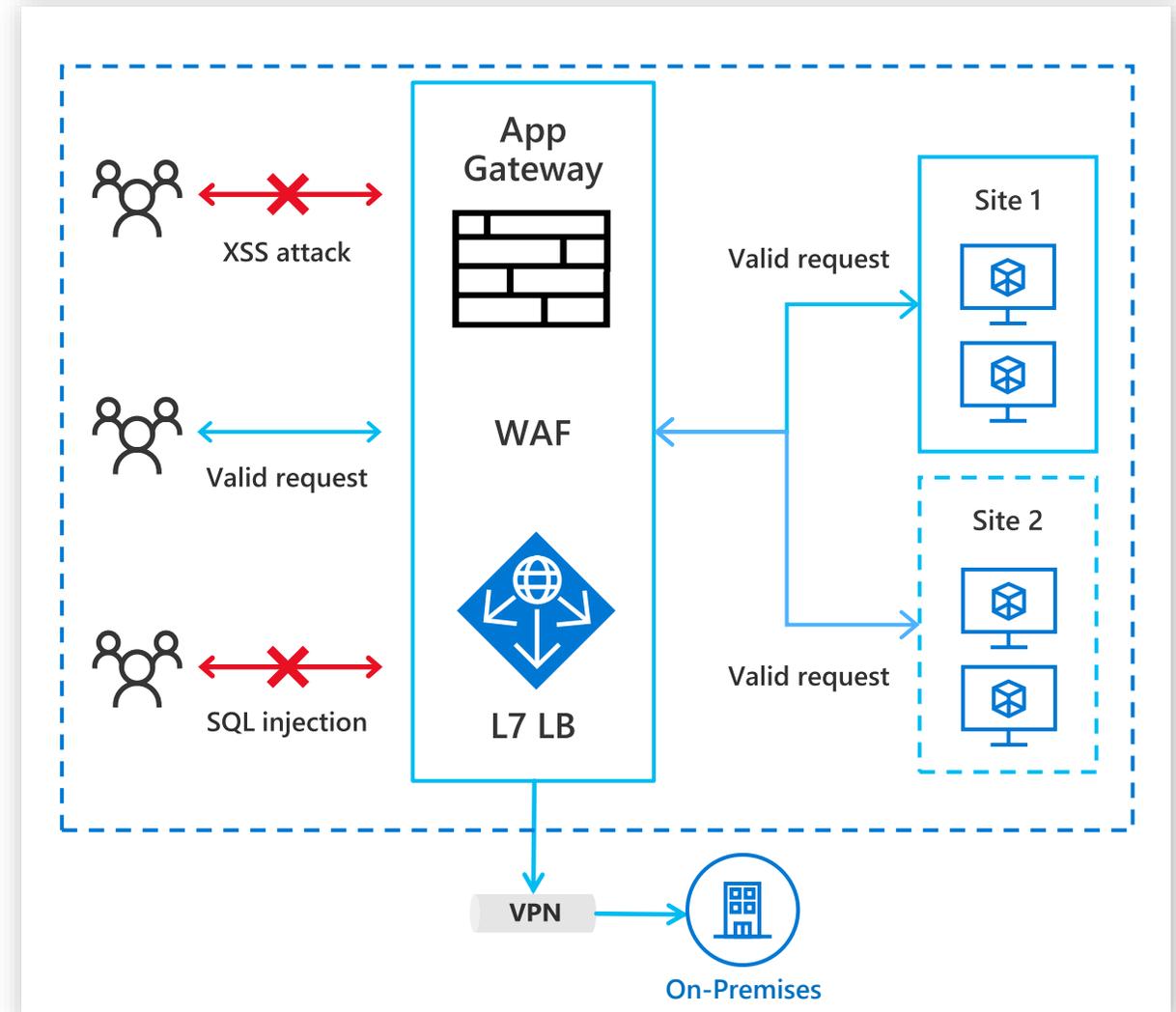
**High availability and scalability** built in and managed by platform

**Layer 7 load balancing** URL path, host based, round robin, session affinity, redirection

**Centralized SSL management** SSL offload and SSL policy

**Public or ILB** public internal or hybrid

**Rich diagnostics** Azure monitor, Log analytics



# Reference Configuration with Virtual Appliance(s)

## Next Generation Firewall with Integrated WAF/Proxy



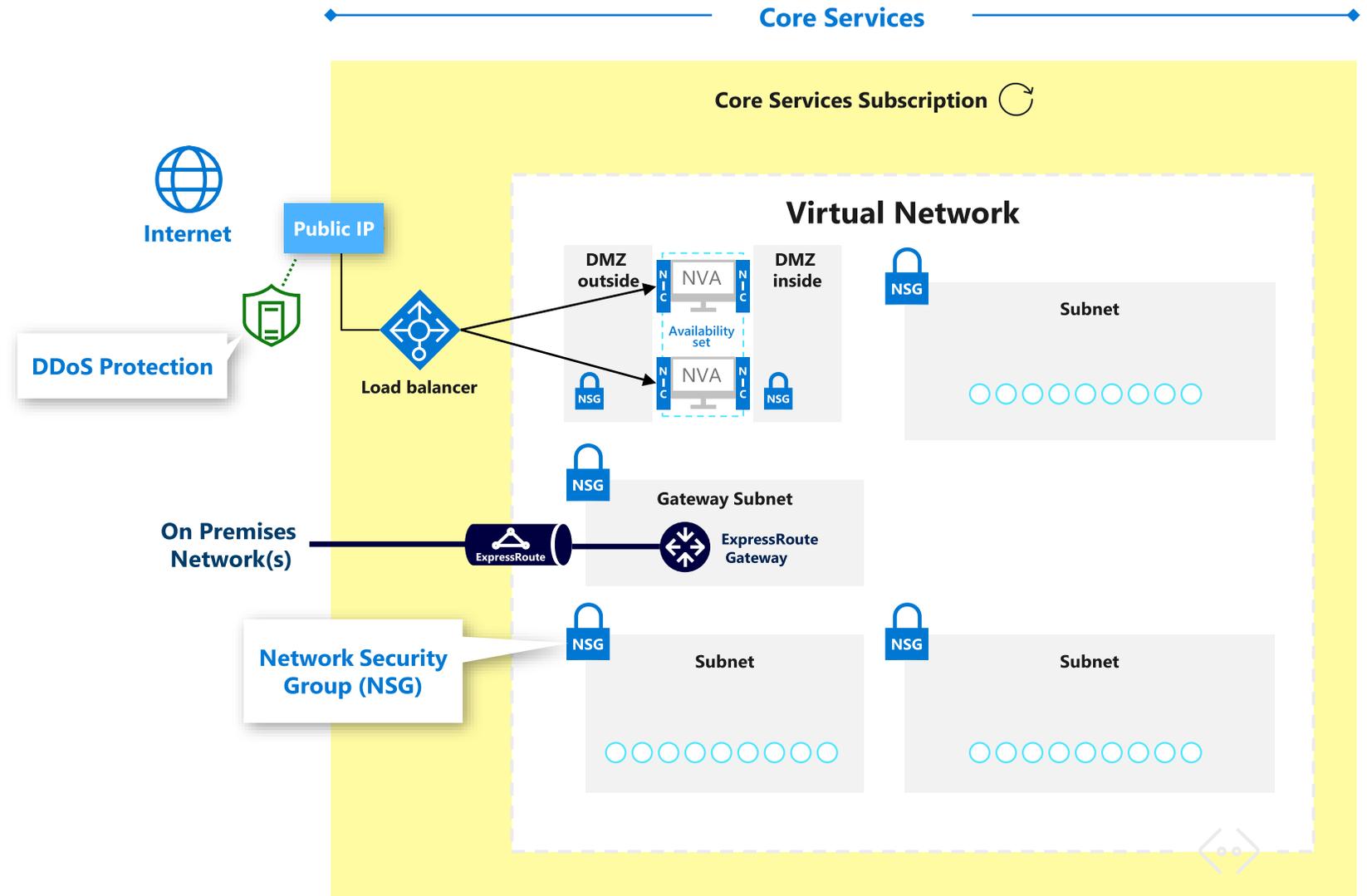
Popular Next Generation Firewalls available in Azure Marketplace

Load balancer enables scalability and availability

DDoS Protection Standard can be applied to public IP addresses.

More Information online

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/shared-services>



## USE WEB APP FIREWALL ON ALL INTERNET FACING APPLICATIONS



- **What** – Configure web application firewalls (WAFs) to protect all internet facing applications.
- **Why** – Common security vulnerability types are often exploited by attackers targeting applications (either as an ingress point to the environment or as the ultimate objective).
  - WAFs are a critical mitigation for these attacks if you don't have a mature security development lifecycle (SDL) to find/fix these vulnerabilities.
  - WAFs also serve as an important safety measure even if you don't have a mature SDL (much like a parachute in a plane).
- **How** – Microsoft includes WAF capabilities in Azure Application Gateway and many vendors offer these capabilities as standalone security appliances or as part of next generation firewalls.

# 9 Implement DDOS mitigations

## DDOS MITIGATIONS



- **What** – Enable DDoS Mitigations for all business-critical web applications, and services.
- **Why** – DDoS attacks are prevalent and are very inexpensive to access on the dark markets.
- **How** – Evaluate and select the best option for protecting your critical applications and services.
  - [Azure DDoS standard](#)
  - 3rd party service

# Deprecating legacy technology

## CLASSIC NETWORK INTRUSION DETECTION/ PREVENTION SYSTEMS (NIDS/NIPS)



- **What** – Choose whether to add existing NIDS/NIPS capabilities on Azure.
- **Why** – The Azure platform already filters malformed packets and most classic NIDS/NIPS solutions are typically based on outdated signature-based approaches which are easily evaded by attackers and typically produce high rate of false positives.
- **How** –
  - Do Not Add (Default Recommendation)
  - Add to Azure tenant

## NETWORK DATA LOSS PREVENTION (DLP)



- **What** – Choose whether to add Network DLP capabilities on Azure
- **Why** – Network DLP is increasingly ineffective at identifying both inadvertent and deliberate data loss. This is because most modern protocols and most attackers use encryption (most available attacker toolkits have encryption built in)
- **How** –
  - Do Not Add (Default Recommendation)
  - Add to Azure tenant

# Calls To Action

## Follow Best Practices

- in your Design → Build → Operations

## Learn More

- Documentation  
<https://docs.microsoft.com/en-us/security/>
- Architecture Guidance  
[aka.ms/AzureSecurityArchitecture](https://aka.ms/AzureSecurityArchitecture)

## Share

- Architecture → architects & technical teams
- Slides → all of your teams

## Provide Feedback

- Security and Identity Forum in  
<https://aka.ms/SecurityCommunity>



# Contact Information



**David Rosenthal**  
VP & General Manager  
Digital Business

[@DavidJRosenthal](#)  
[SlideShare](#)  
Blog: [www.razor-tech.com](http://www.razor-tech.com)

Let's keep in touch

5 Tower Bridge  
300 Barr Harbor Dr., Suite 705  
West Conshohocken, PA 19428

[www.razor-tech.com](http://www.razor-tech.com)  
[David.Rosenthal@razor-tech.com](mailto:David.Rosenthal@razor-tech.com)

Office : 866.RZR.DATA

