Microsoft

RAZOR TECHNOLOGY

intel

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

Technology

Enterprise-class technology

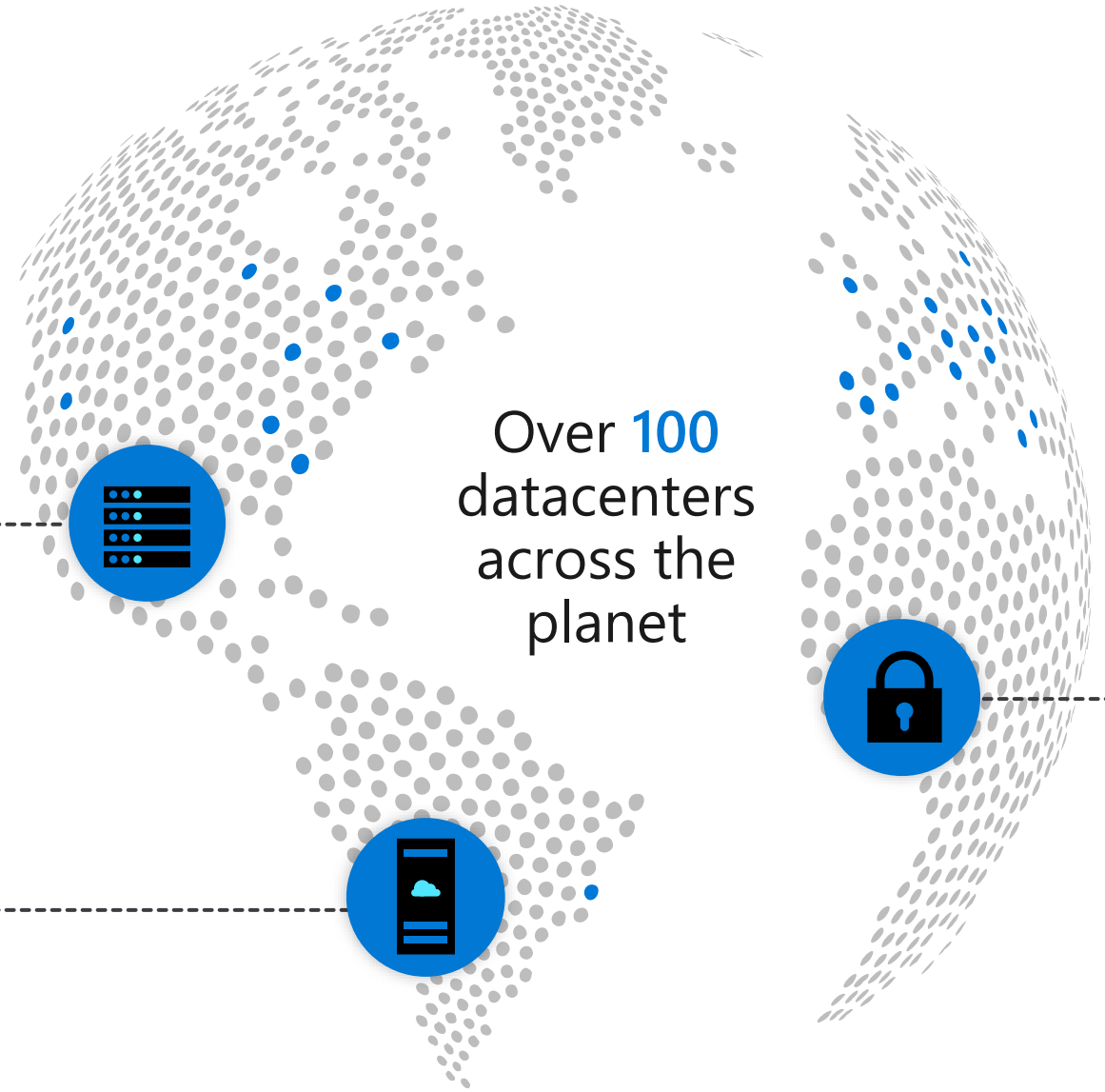
Partnerships

Partnerships for a heterogeneous world

A secure foundation at global scale

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

Global cloud infrastructure with custom hardware and network protection



Over **100** datacenters across the planet

Secured with cutting-edge **operational security**

- Restricted access
- 24x7 monitoring
- Global security experts

Azure infrastructure security

Secure foundation

Protect customer data

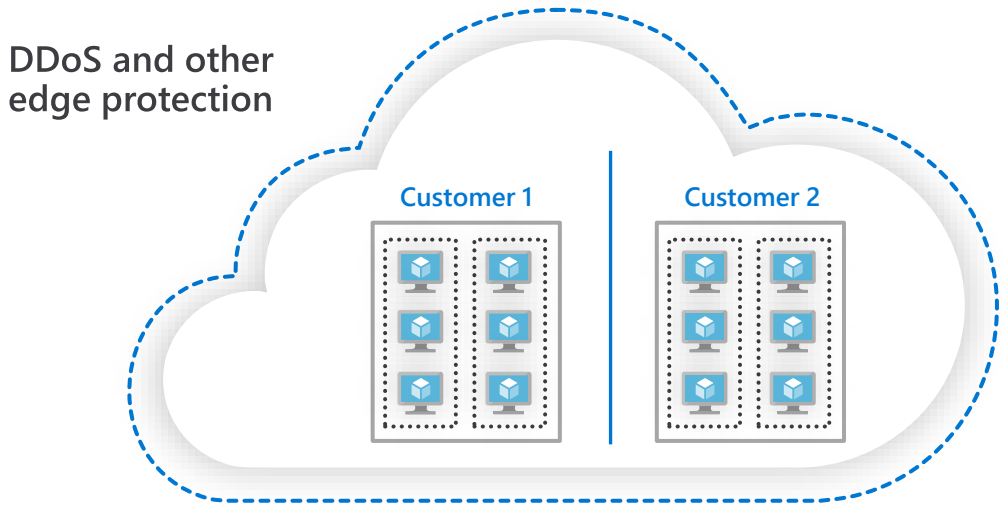
Data, network segregation. DDoS protection at the edge

Secure hardware

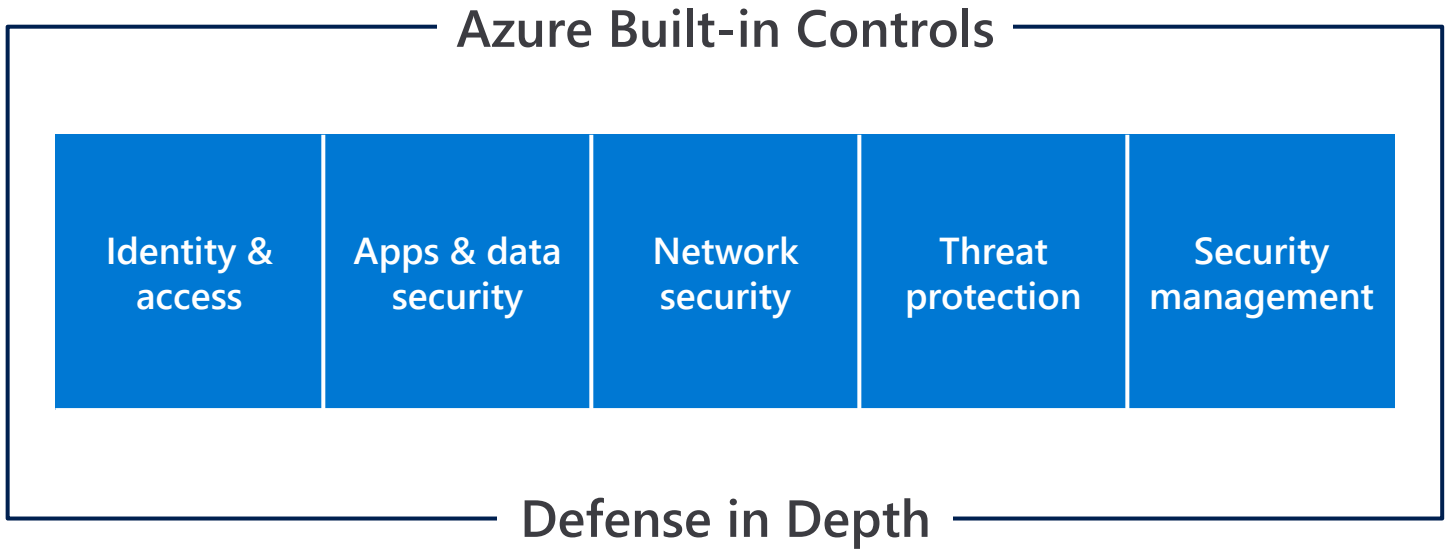
Custom-built hardware with integrated security and attestation

Continuous testing

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



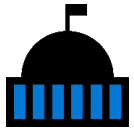
Technology


Azure Built-in Controls
Identity & access
Apps & data security
Network security
Threat protection
Security management
Defense in Depth

Partnerships for a heterogeneous world

Partner with peers

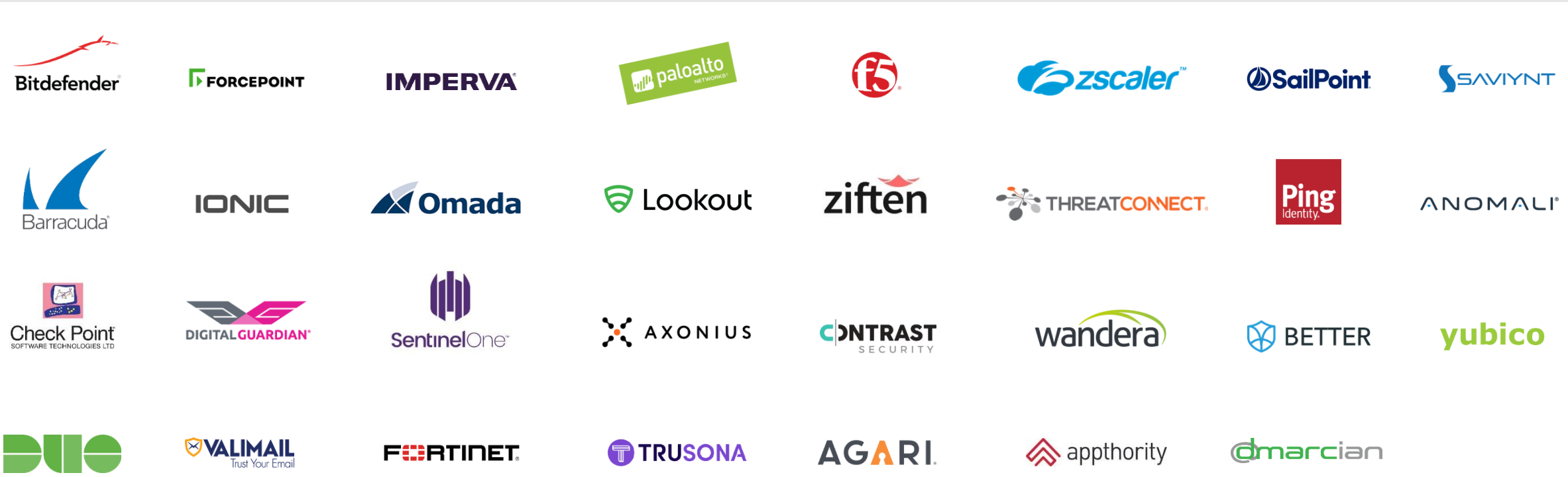
Work with industry alliances



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

RSA

Omada

PingIdentity.

DUO

SailPoint

Data protection

gemalto
security to be free

THALES

SECURED BY CRYPTERON

Network security

Palo Alto Networks

Check Point
SOFTWARE TECHNOLOGIES LTD.

f5

cisco

Barracuda

Threat protection

Symantec

McAfee

Qualys Inc

RAPID7

aqua

Security management

HPE ArcSight

Splunk

IBM QRadar

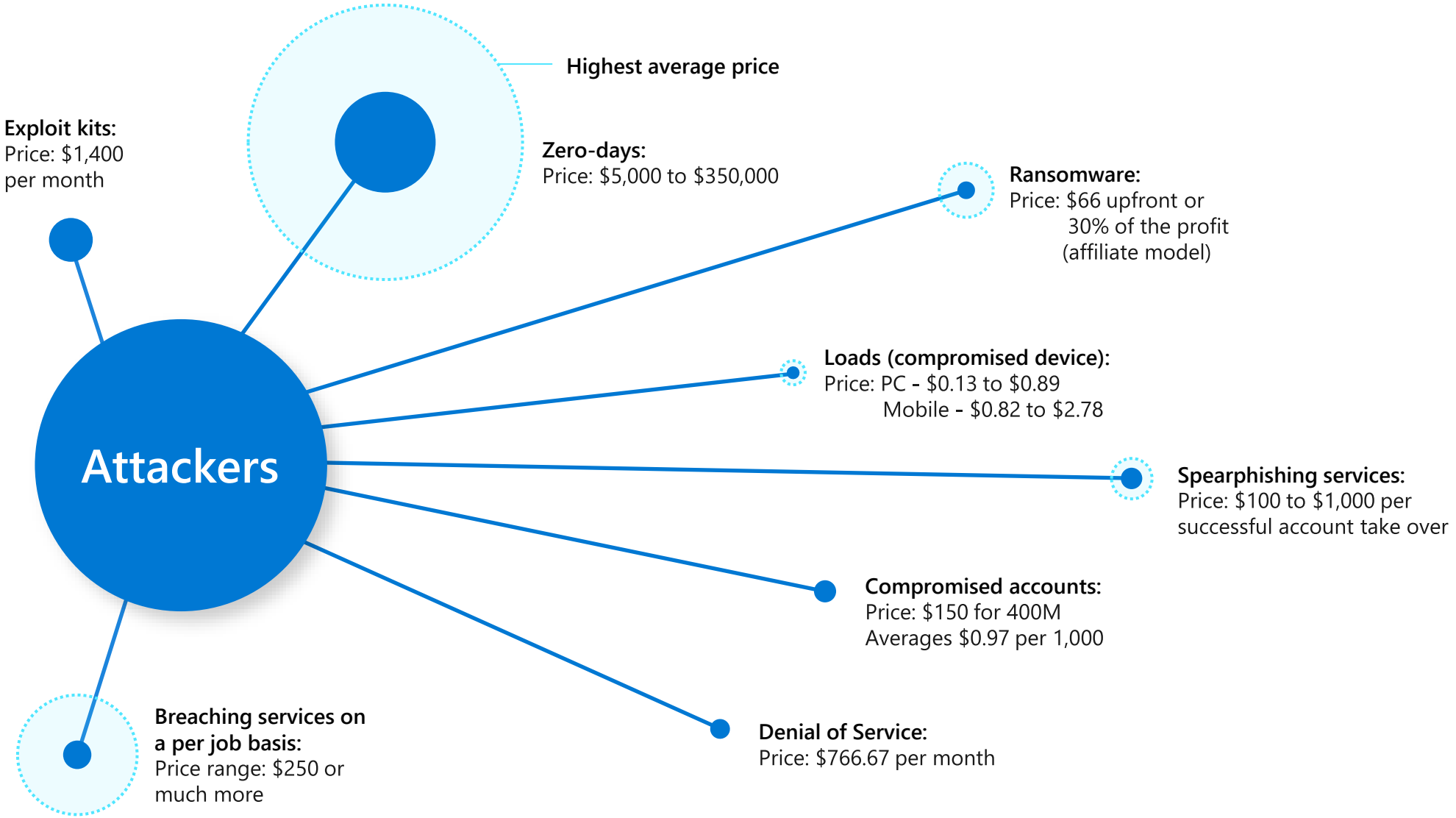
ALERT LOGIC

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

Microsoft Azure

Top 10 Best Security Practices for Azure

Attack services are cheap



Attack services are cheap

Zero-days:

Ransomware:

Loads (compromised device):

Spearphishing services:

Compromised accounts:

Denial of Service:

FOCUS ON HYGIENE (NOT ZERO DAYS)

Zero day vulnerabilities are expensive and impractical for many attacks. aka.ms/CyberHygiene has guidance from Microsoft + NIST, the Center for Internet Security (CIS), and US DHS NCCIC (formerly US-CERT)

FOCUS ON MFA/PASSWORDLESS & ZERO TRUST

Attackers have moved to Identity attacks like phishing and cred theft (which easily evade traditional network defenses)

Increase cost of these attacks starting with administrative privileges and other business critical assets

ENABLE DDoS PROTECTION FOR CRITICAL SERVICES

Ensure that your business-critical services have DDoS protection from Azure platform or a capable 3rd parties

Agenda

Introduction

- Azure Secure Score

Top 10 Best practices

Calls to Action

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

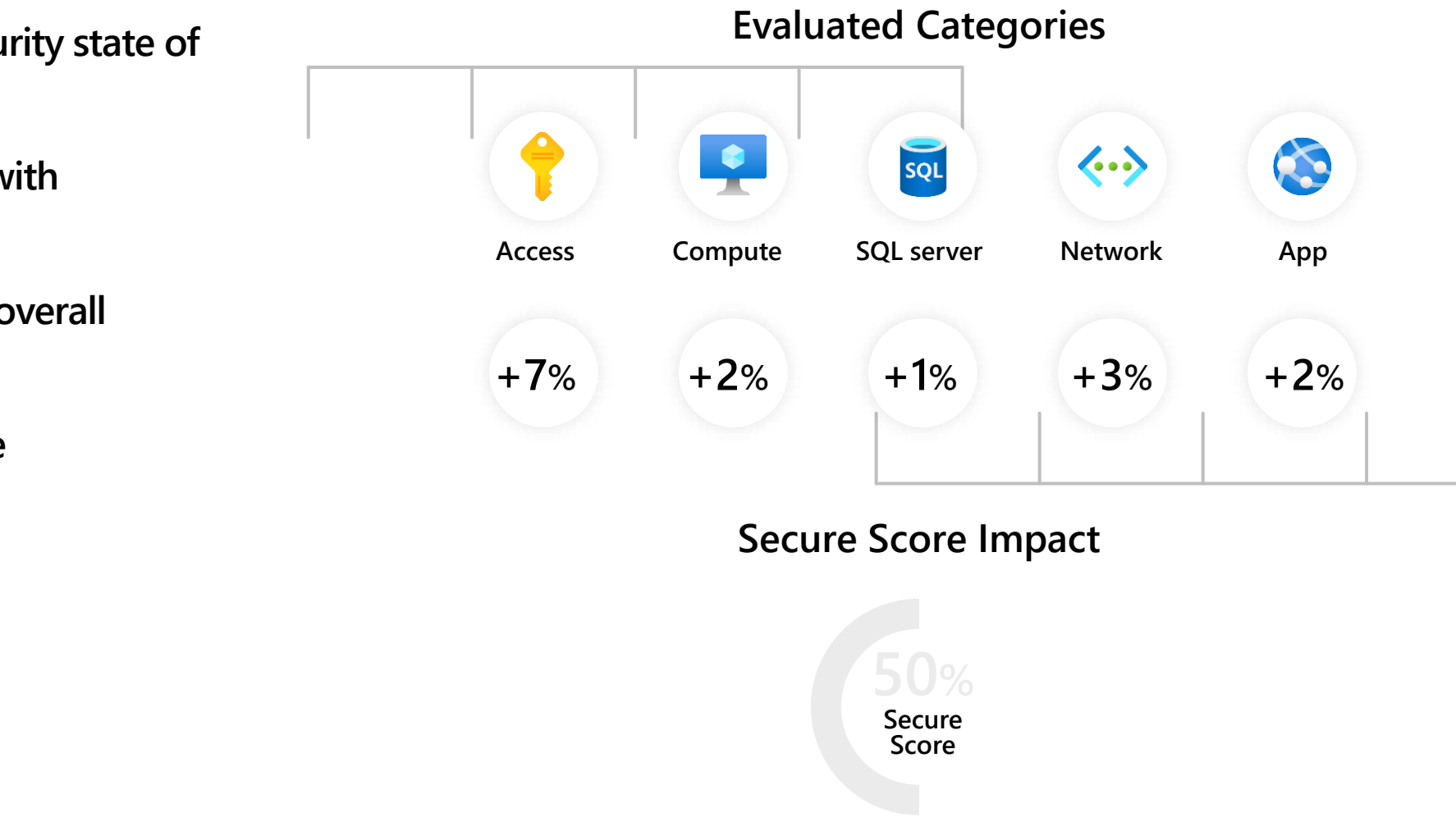
Security posture management with Azure Secure Score

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

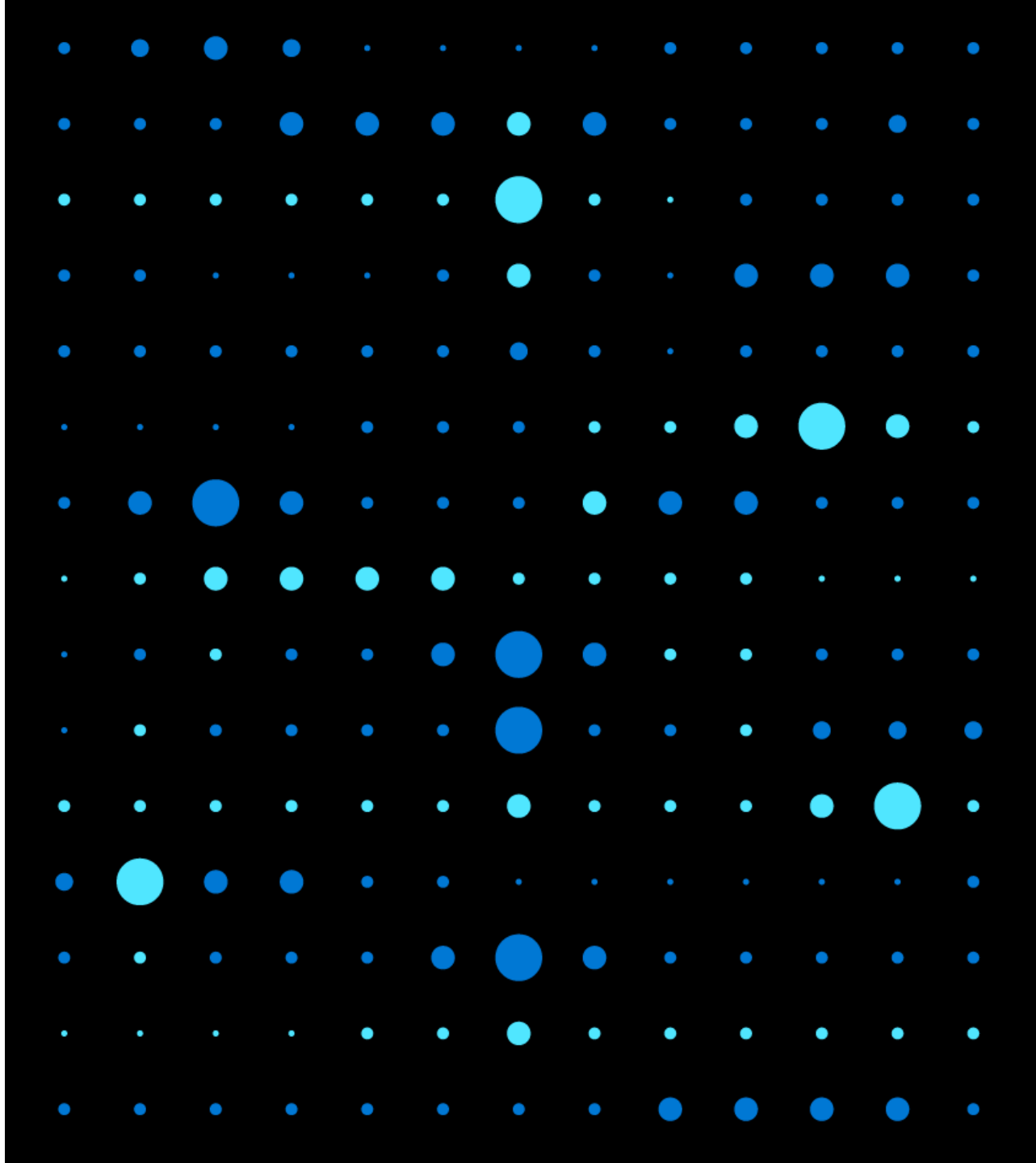
Speed up regulatory compliance



Microsoft Azure

Demo

Azure Secure Score



RAZOR TECHNOLOGY

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	• **Vulnerability Management (or Governance/Risk/Compliance team)** • Architecture Team • Responsible Technical Team (listed below)
Improve Score Area	**Responsible Technical Team**
Compute and Apps Resources	**App Services** ▪ Application Development/Security Team(s) **Containers** ▪ Application Development and/or Infrastructure/IT Operations **VMs/Scale sets/compute** ▪ IT/Infrastructure Operations **NOTE:** Each DevOps team may be responsible for their application resources
Data & Storage Resources	**SQL/Redis/Data Lake Analytics/Data Lake Store** ▪ Database Team **Storage Accounts** ▪ Storage/Infrastructure Team
Identity and Access Resources	**Subscriptions** ▪ Identity Team(s) **Key Vault** ▪ Information/Data Security Team
Networking Resources	▪ Networking Team ▪ Network Security Team
IoT Security	▪ IoT Operations Team

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.

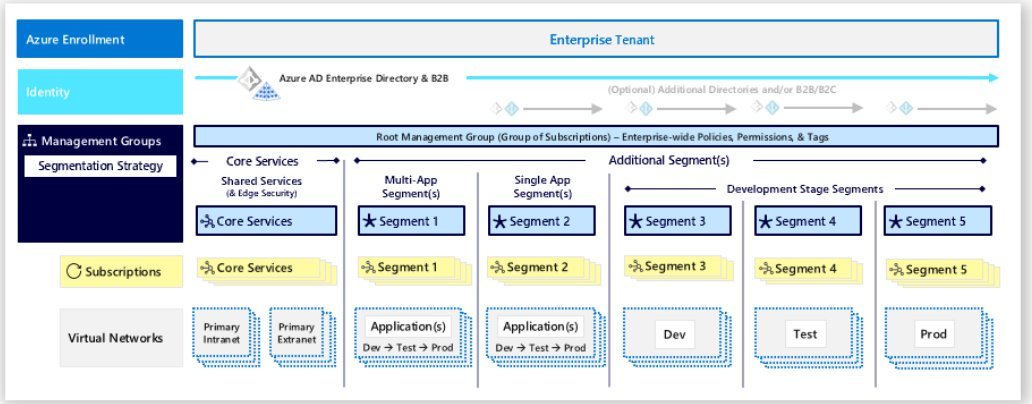
TIP **Minimize Complexity** - Always consider whether a segment is needed or whether security monitoring provides enough risk mitigation (each segments adds friction and overhead)

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.)

RAZOR TECHNOLOGY

Reference design - Azure administration model



RAZOR TECHNOLOGY

GRC – Segmentation

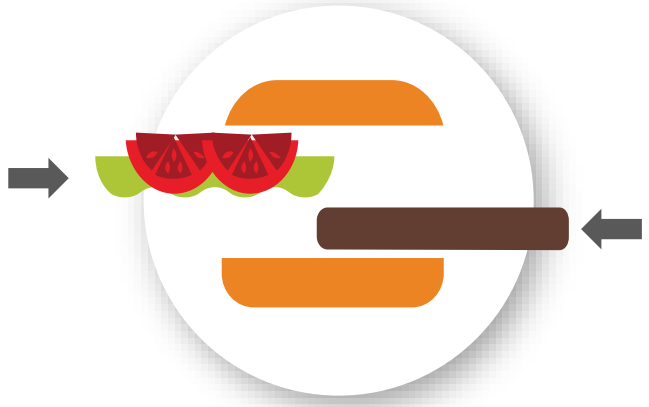
CRITICAL CHOICE

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

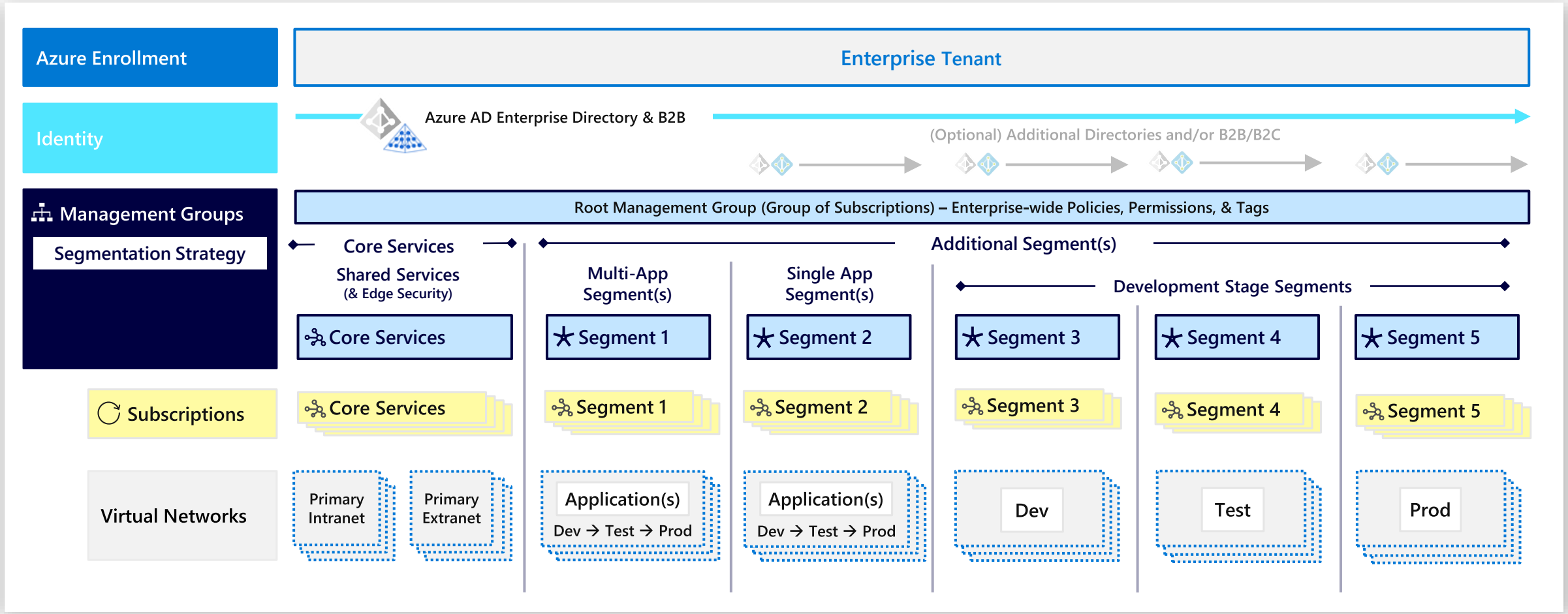
Minimize Complexity - Always consider whether a segment is needed or whether security monitoring provides enough risk mitigation
(each segments adds friction and overhead)



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 3rd 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

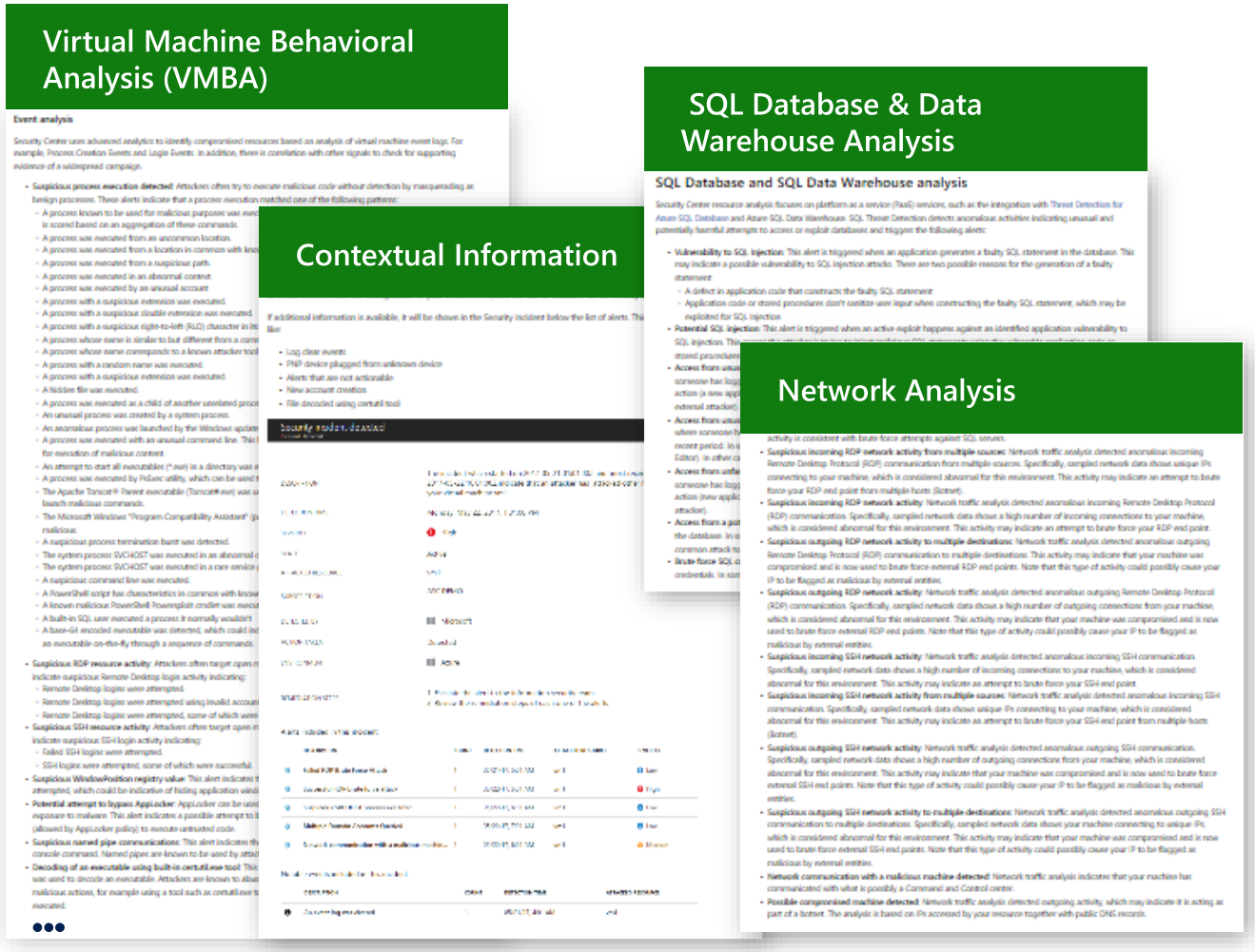
CRITICAL GUIDANCE

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



RAZOR TECHNOLOGY

Centralized Visibility

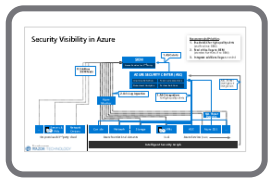
Azure Security Center | **Azure Sentinel**

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

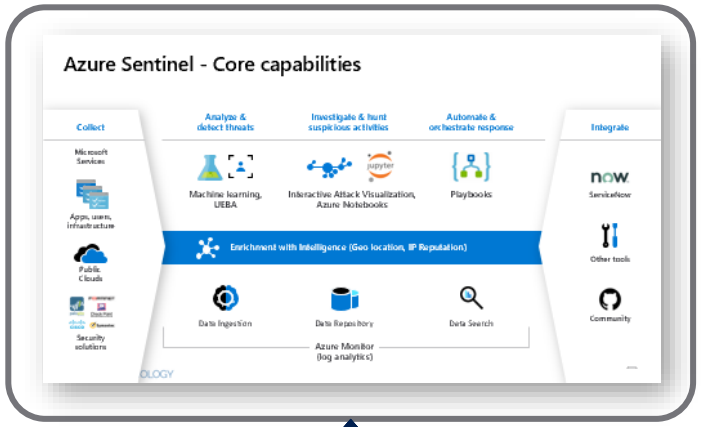
GRC Professional
Assess Risk & Compliance

IT / Security Professional
Implement Protections

SOC Analyst
Primary Console
Alerts, Investigation



Log Flow



Generate Alerts

Identity | Endpoint | Cloud | Network | and more

RAZOR TECHNOLOGY

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

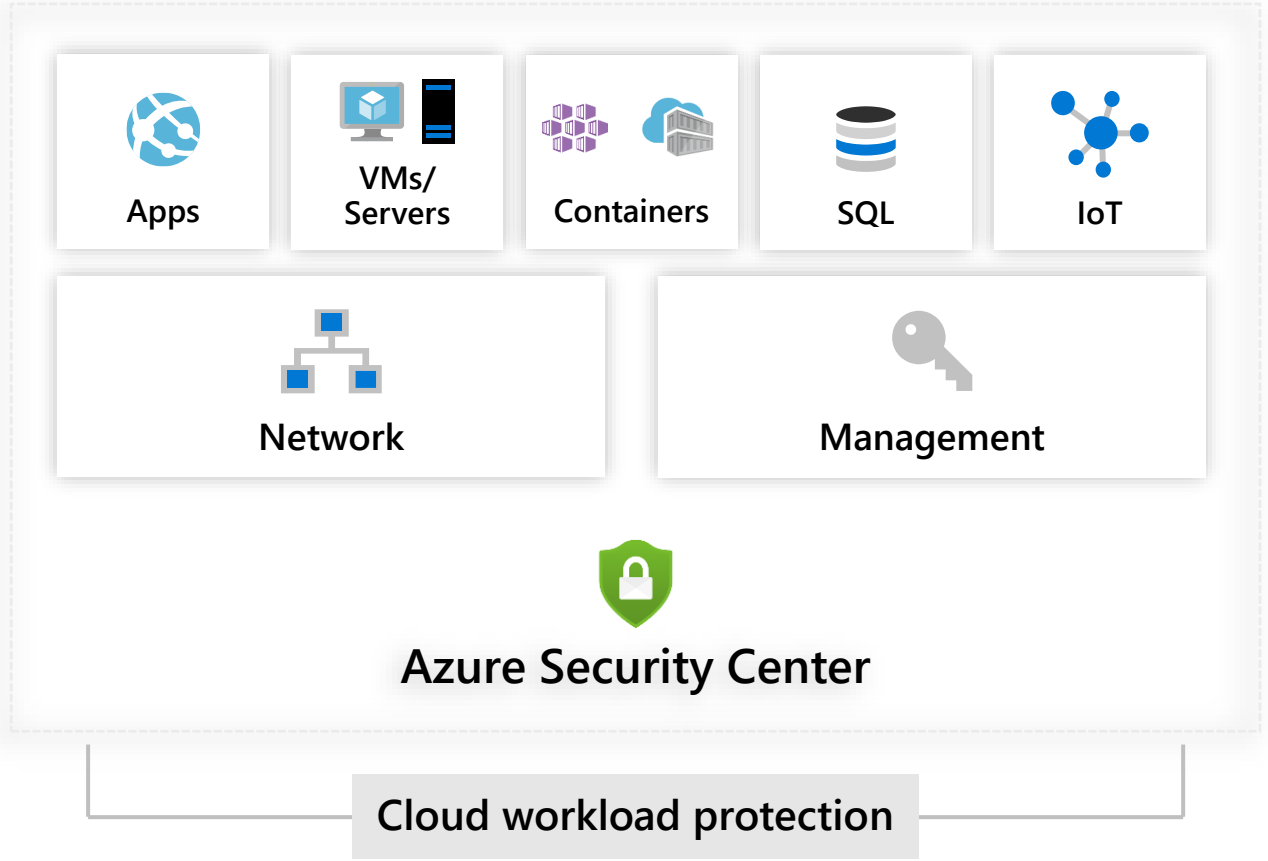
Use industry's most extensive threat intelligence to gain deep insights

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

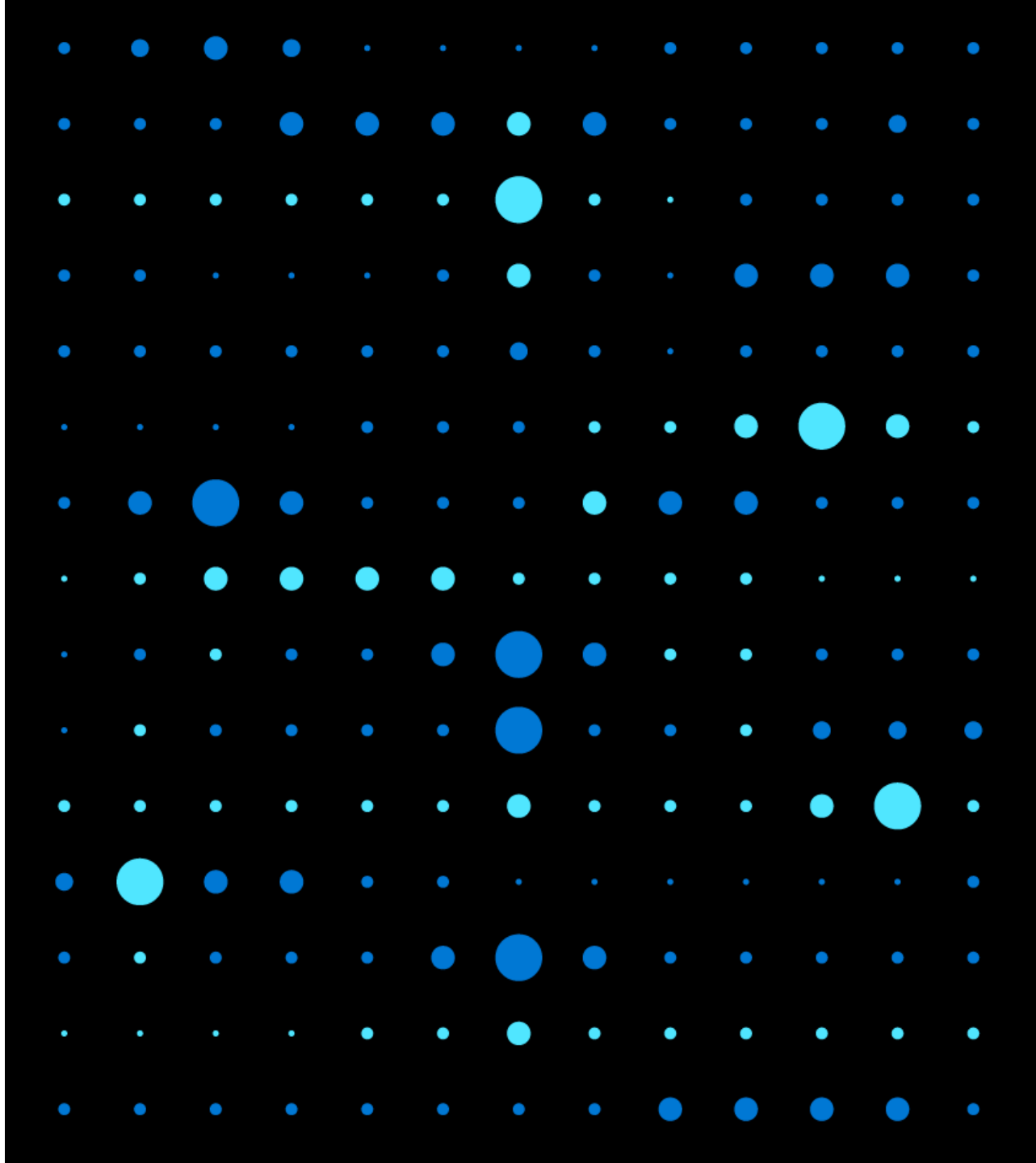
Protect your Azure IoT solutions with near real time monitoring



Microsoft Azure

Demo

Azure Security Center

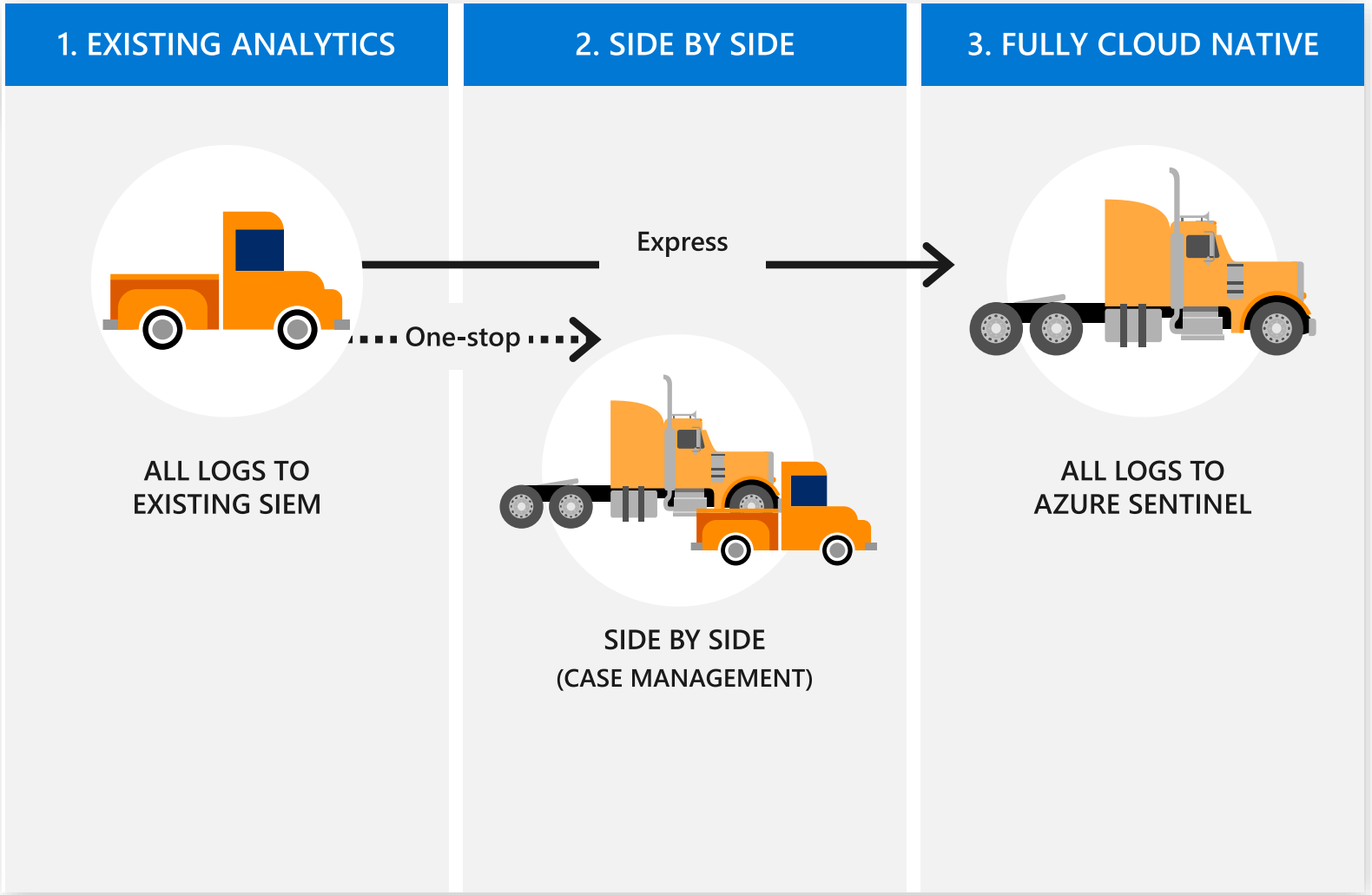


RAZOR TECHNOLOGY

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.



Introducing Azure Sentinel

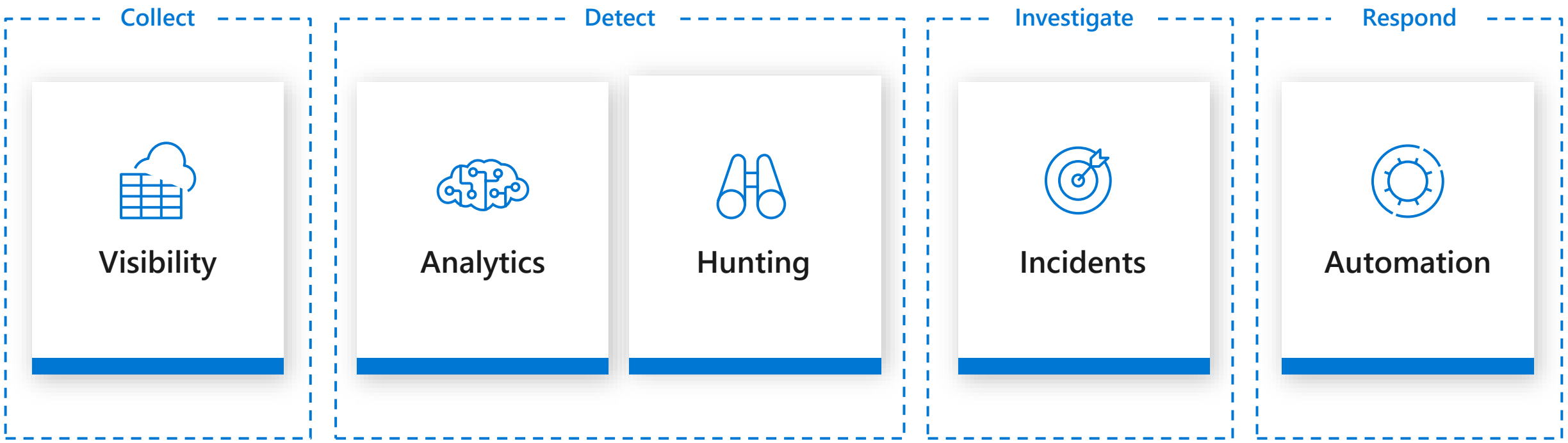
INTELLIGENT, CLOUD-NATIVE SIEM

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

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (log analytics)

Integrate

ServiceNow

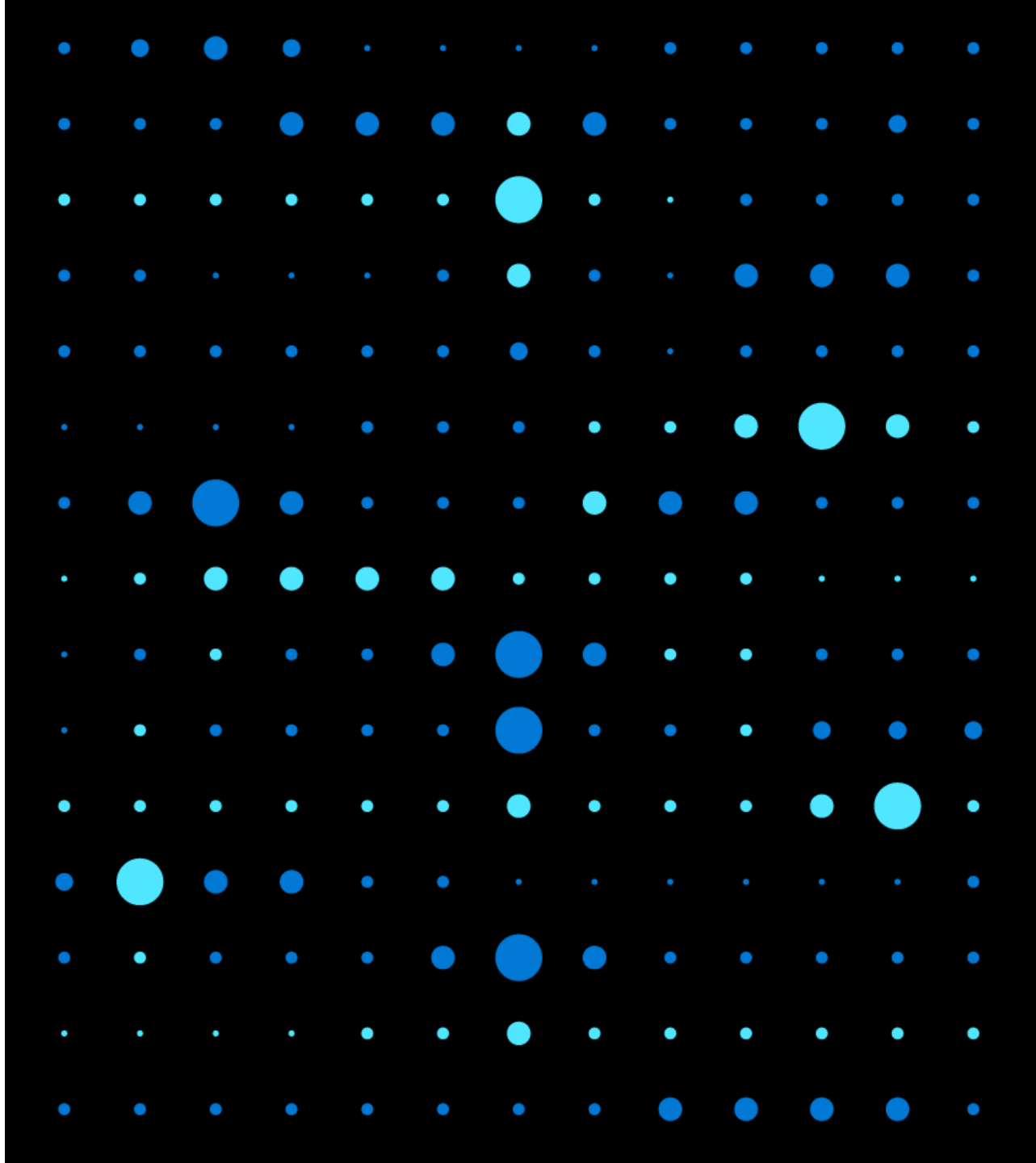
Other tools

Community

Microsoft Azure

Demo

Azure Sentinel

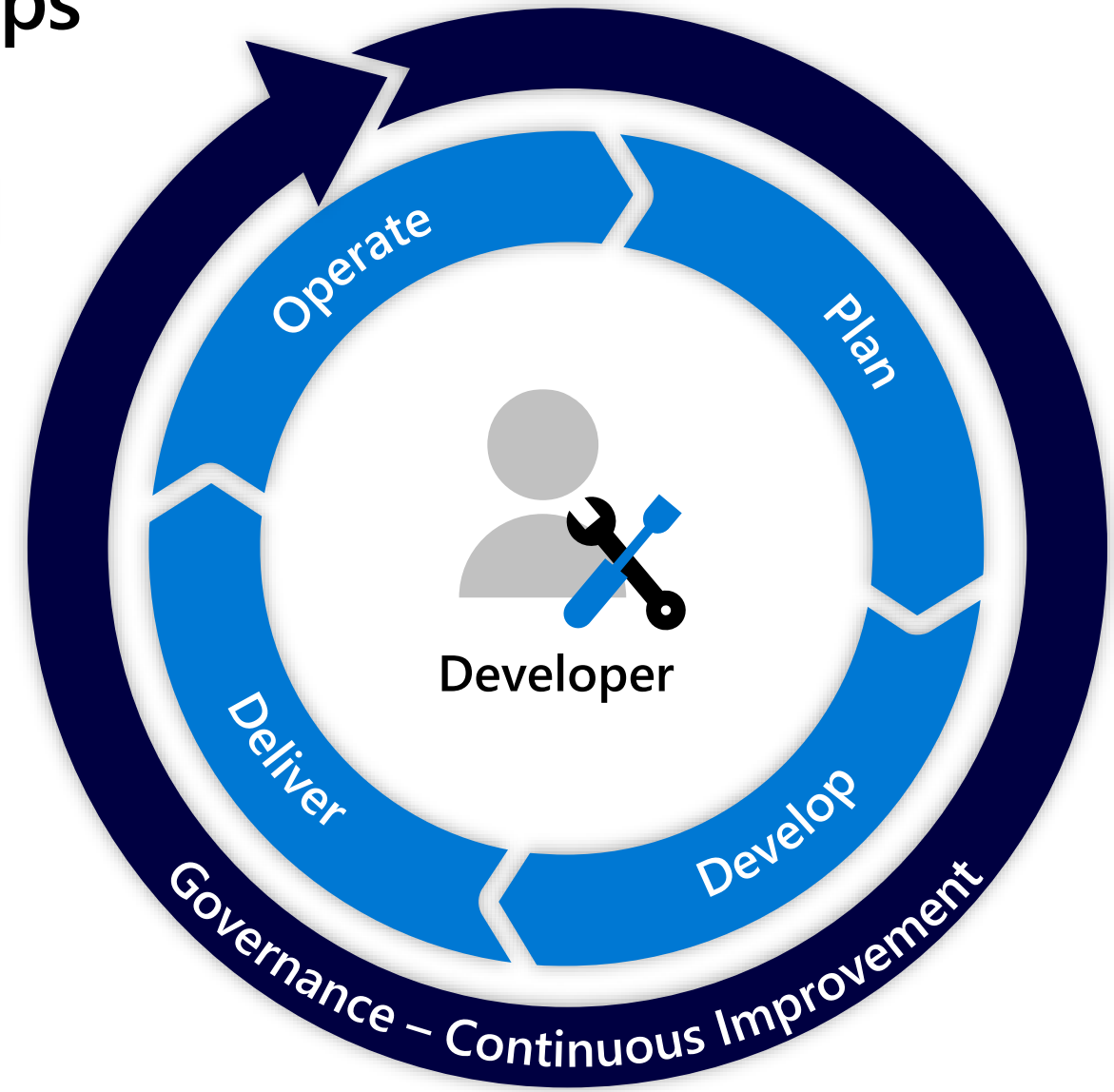


RAZOR TECHNOLOGY

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

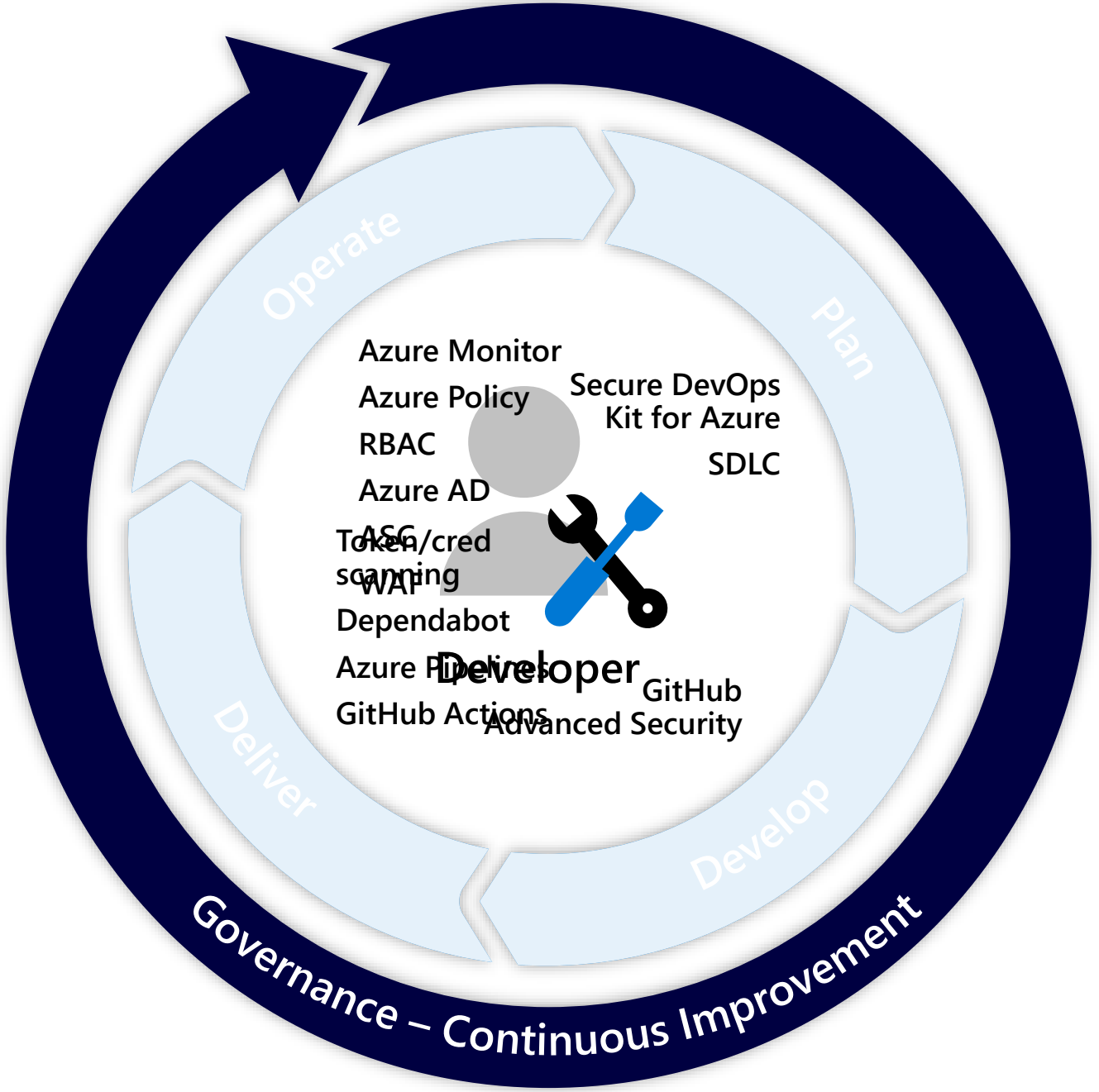


Securing DevOps: Integrate security into the process

Define security requirements:

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

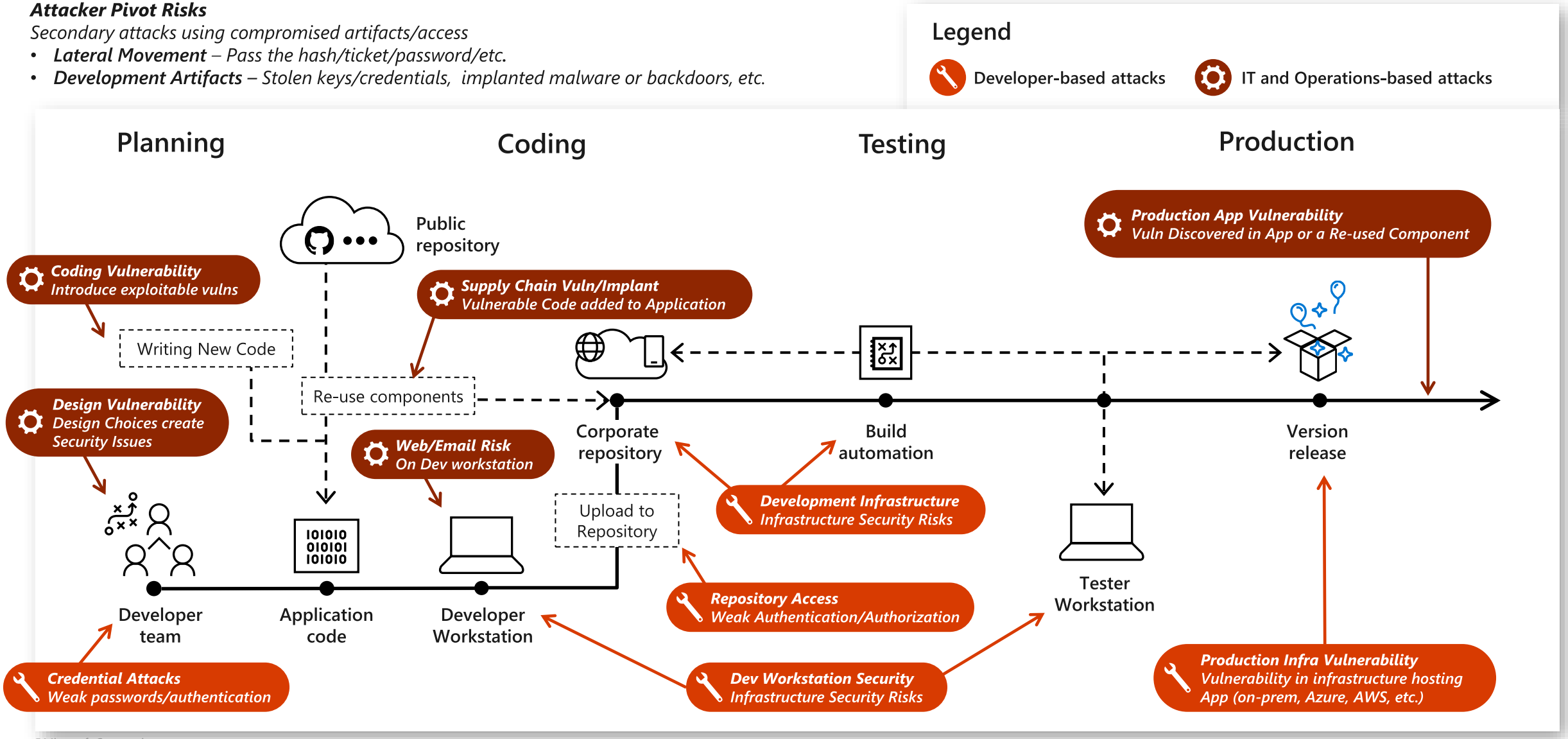
Establish a standard Incident Response Procedure



RAZOR TECHNOLOGY

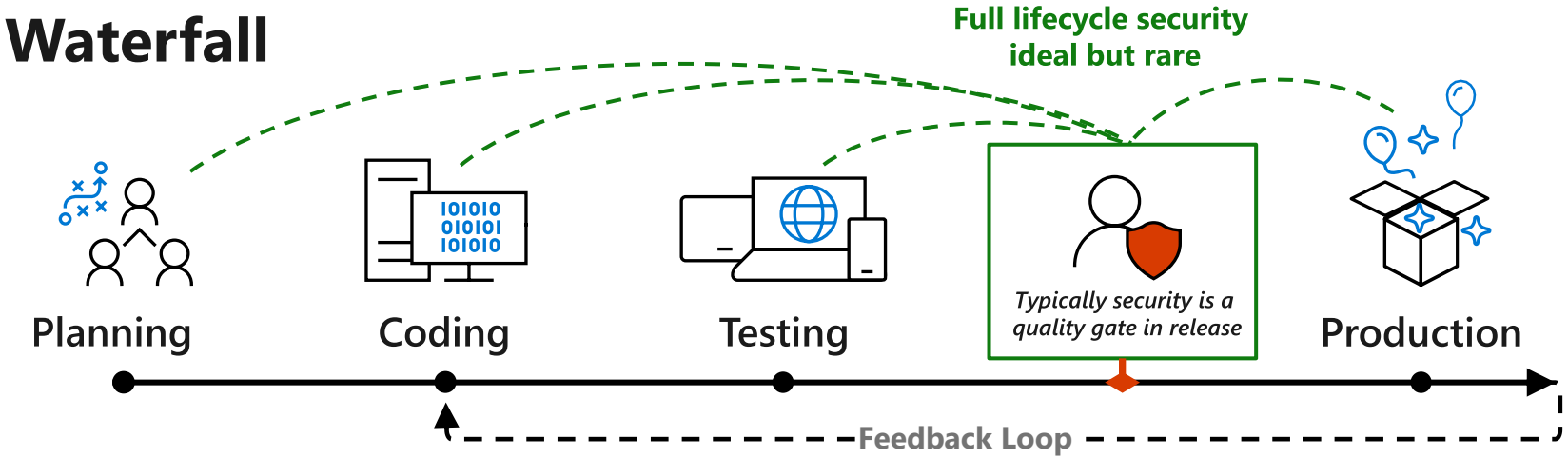
Attacker Opportunities

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.*



Role of Security in Development

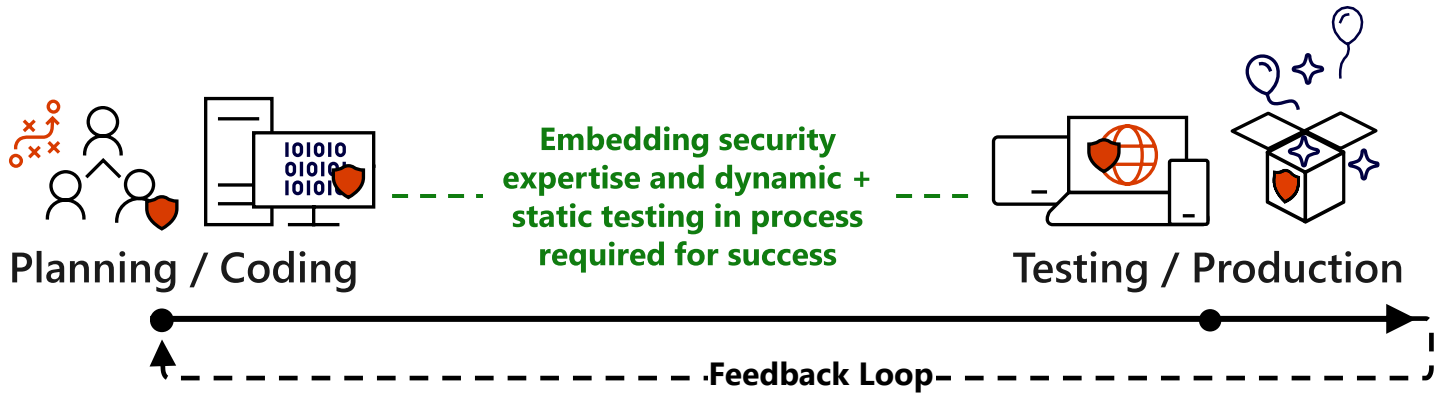
Waterfall



Bias to Plan & Quality *(Weeks/Months)*

DevOps

Quality and Security risk mitigated by rapidly release of fixes



Bias to Speed & Agility *(Hours/Days)*

RAZOR TECHNOLOGY

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	*Typically existing network security team* Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.
Network Management	*Typically existing network operations team* Enterprise-wide virtual network and subnet allocation
Server Endpoint Security	*Typically IT operations, security, or jointly* Monitor and remediate server security (patching, configuration, endpoint security, etc.)
Incident Monitoring and Response	*Typically security operations team* Investigate and remediate security incidents in SIEM or source console: • Azure Security Center • Azure AD Identity Protection
Policy Management	*Typically GRC team + Architecture* 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	*Typically Security Team + Identity Team Jointly* 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

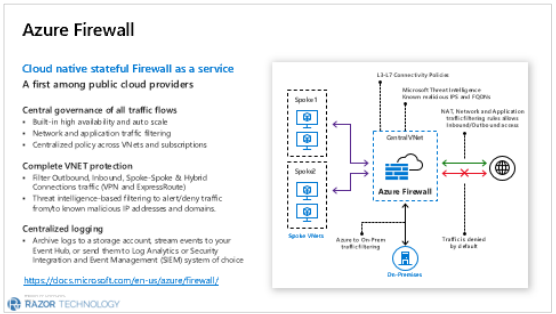
Next Generation Firewall (NGFW) and other 3rd party offerings

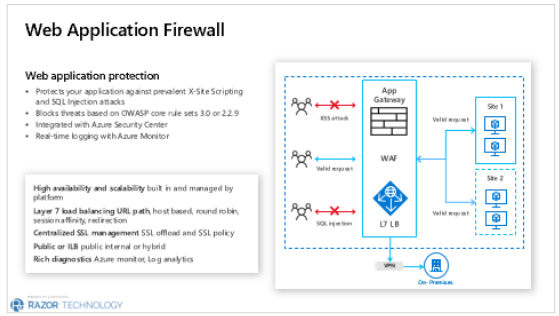
Network virtual appliances in the Azure Marketplace include familiar security tools that provide enhanced network security capabilities

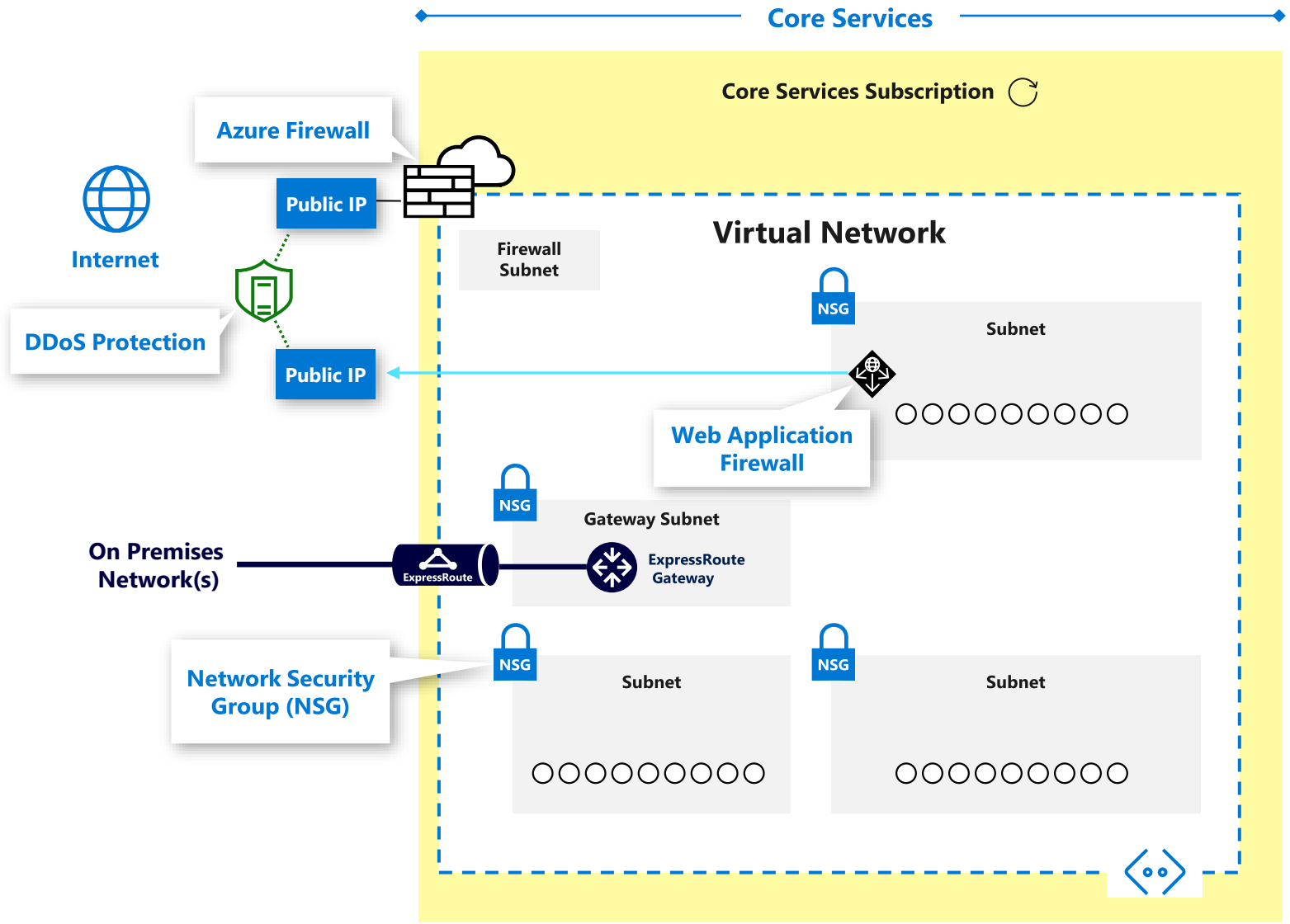
Configuration is more complex, but allows you to leverage existing capabilities, and skillets

Reference Configuration with Native Controls

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







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

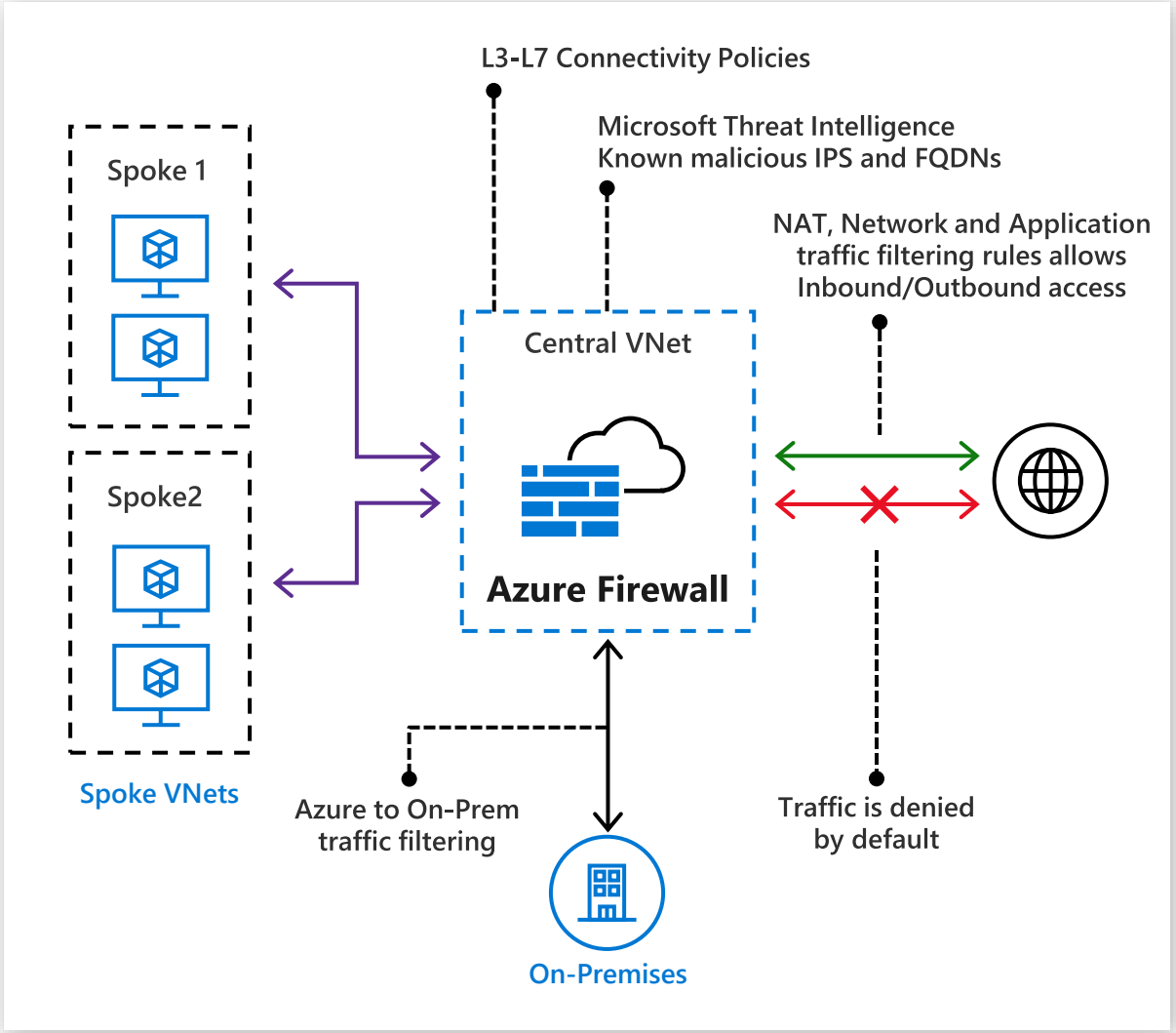
Complete VNET protection

- 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

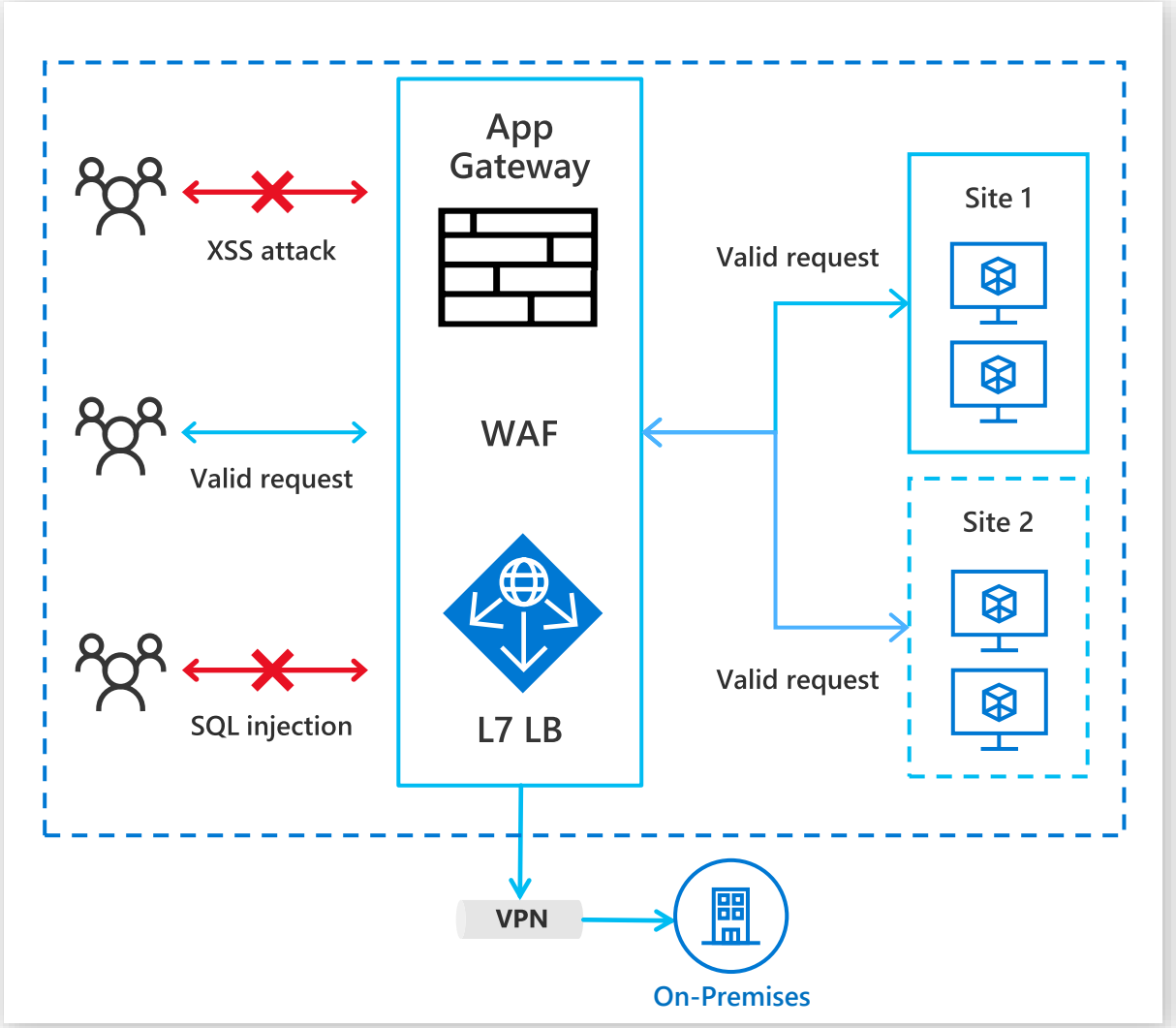
High availability and scalability built in and managed by platform

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

Centralized SSL management SSL offload and SSL policy

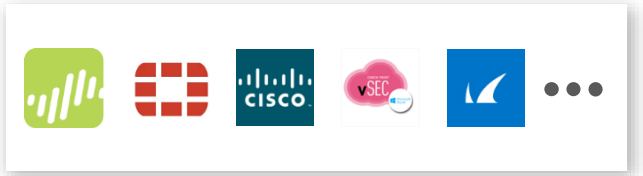
Public or ILB public internal or hybrid

Rich diagnostics Azure monitor, Log analytics



Reference Configuration with Virtual Appliance(s)

Next Generation Firewall with Integrated WAF/Proxy



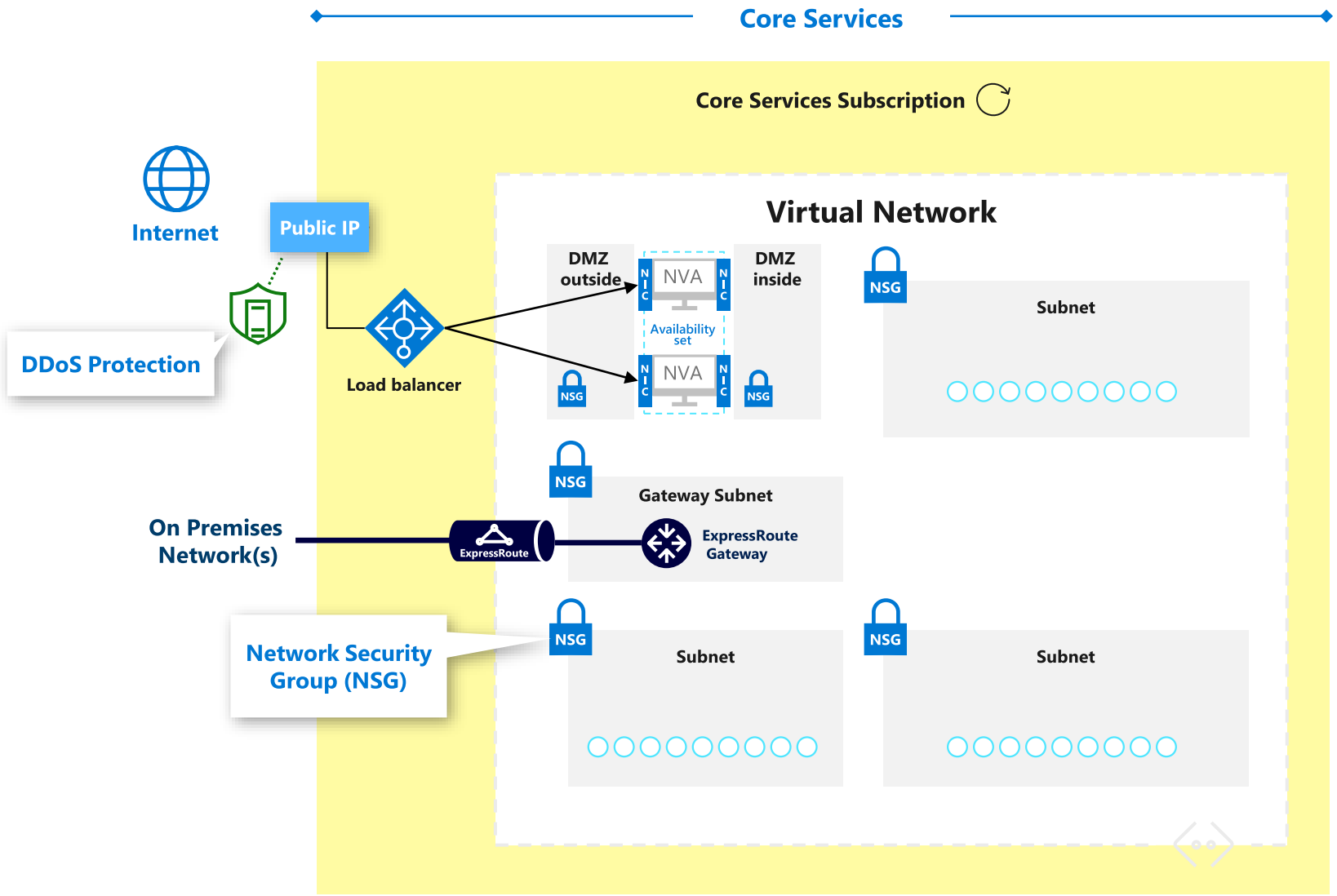
Popular Next Generation Firewalls available in Azure Marketplace

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



RAZOR TECHNOLOGY

8 Implement WAFs

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**

10 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

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

Let's keep in touch

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

www.razor-tech.com
David.Rosenthal@razor-tech.com

Office : 866.RZR.DATA