



Microsoft Ignite





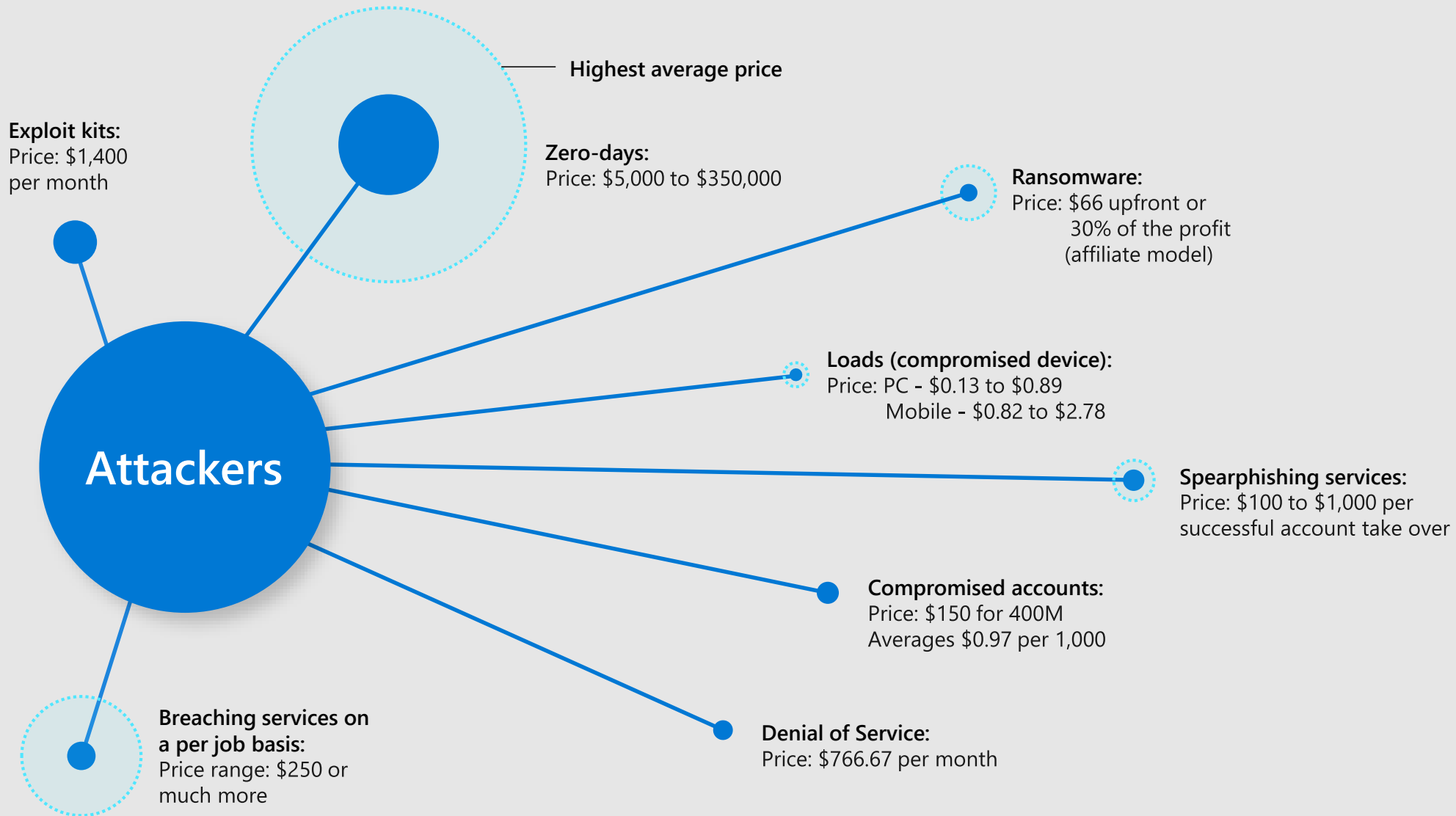
Top 10 Azure Security Best Practices

Mark Simos
Lead Cybersecurity Architect



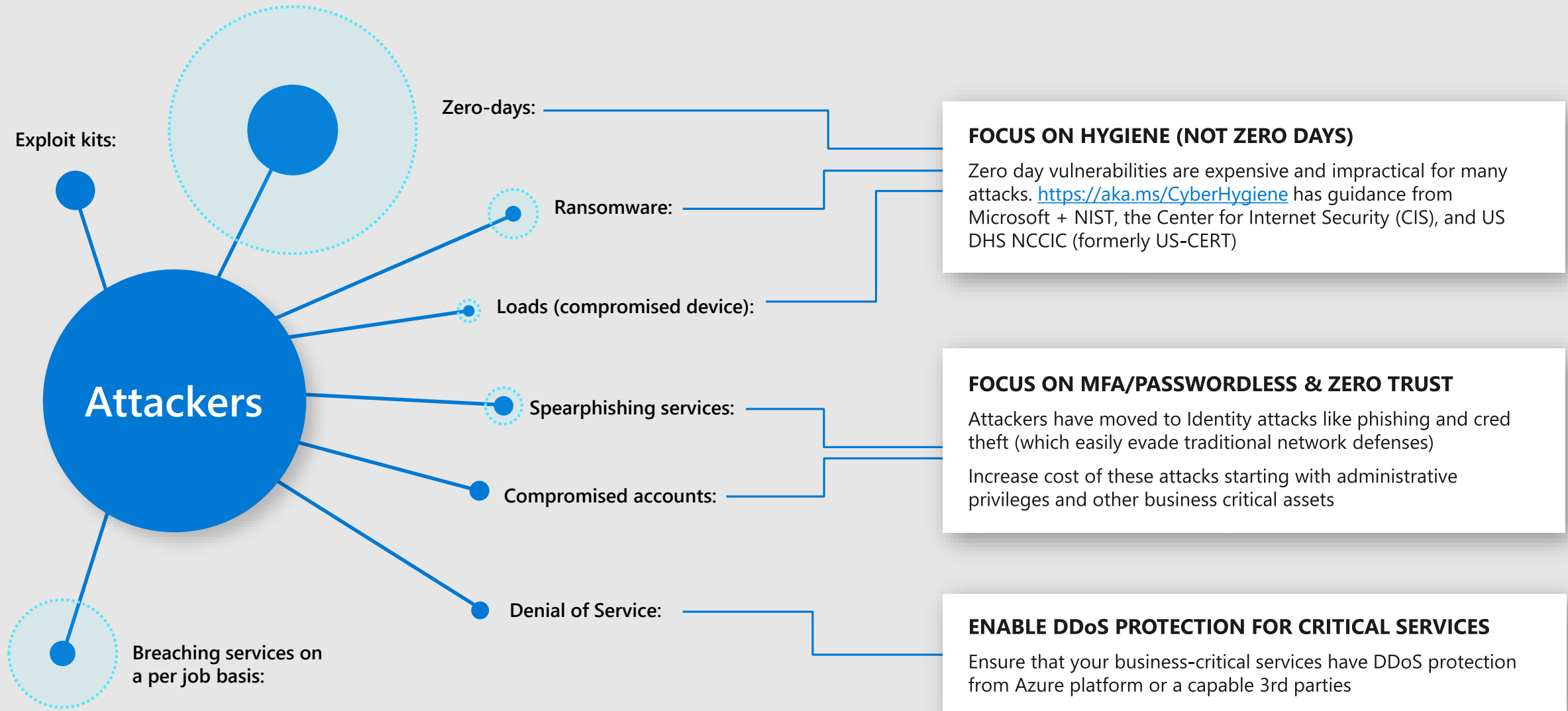
Attack services are cheap

More details at <https://aka.ms/CISOWorkshop>



Attack services are cheap

More details at <https://aka.ms/CISOWorkshop>



Agenda

Introduction:

- Azure Security Compass
- Secure Score

Top 10 Best practices

Calls to Action

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



What is Azure Security compass?

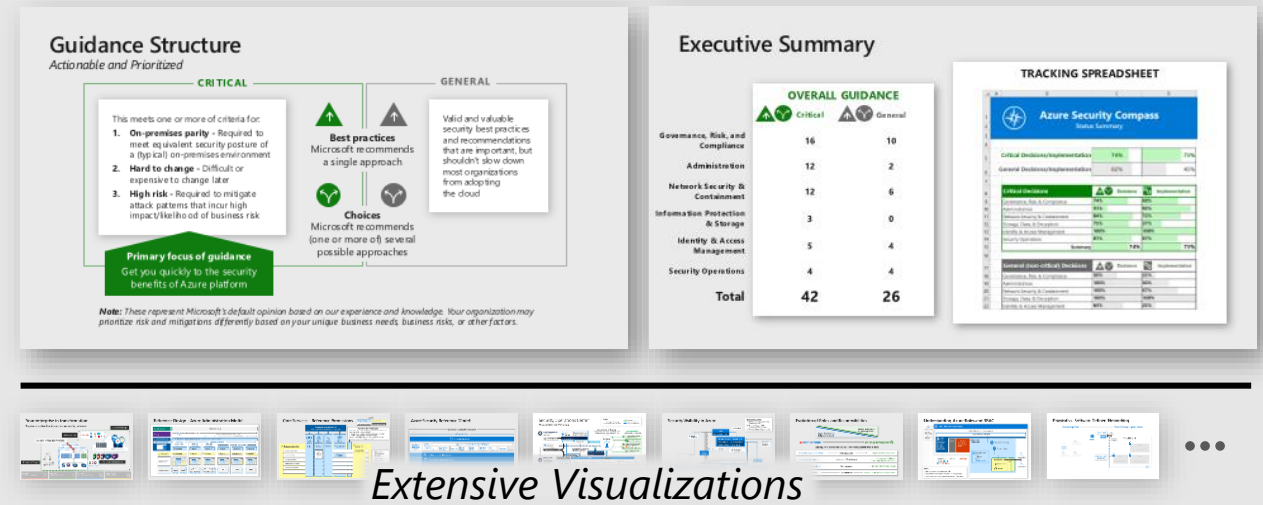
Azure Security Guidance

Strategy Transformation Guidance

Changes from On-premises Security

Reference Models / Diagrams

Actionable Best Practices (Top 10 is a subset)

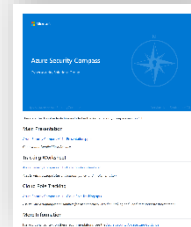


Extensive Visualizations

Architecture
Documentation
aka.ms/AzureSecurityArchitecture

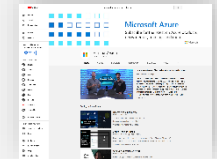


Download Site
aka.ms/AzureSecurityCompass



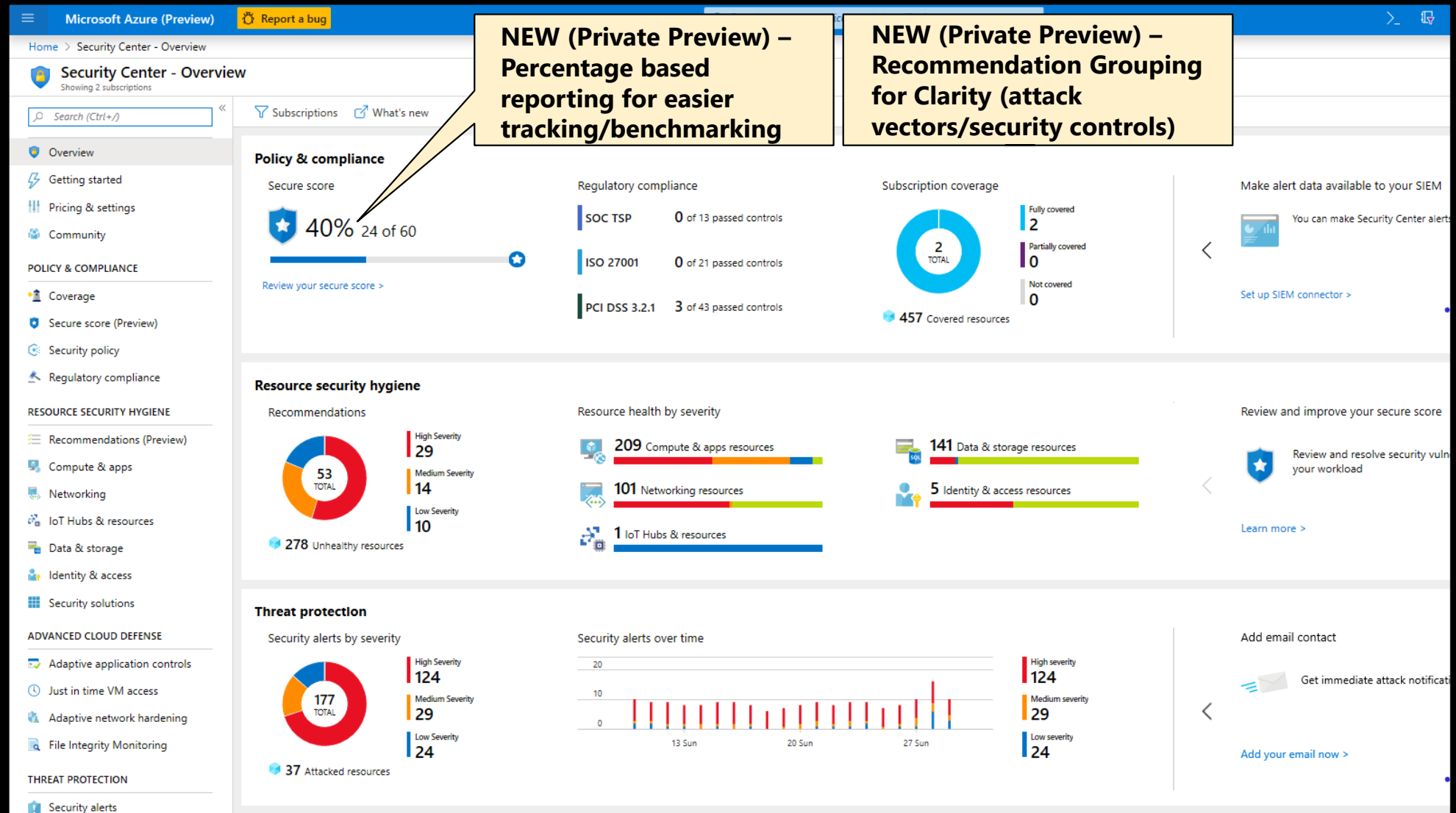
- Slides –
- Tracking Spreadsheets
- And more...

Videos
aka.ms/AzureSecurityCompass-Videos



COMING SOON

Visibility Across Your Estate with **Secure Score**



Top 10 Best Practices

Focused on Highest Impact
and Rapid Implementation



Best Practices 1 - 5

1 Operationalize Secure Score

- OPERATIONALIZE AZURE SECURE SCORE**
- What** - Assign stakeholders to use Secure Score in Azure Security Center to monitor risk profiles and continuously improve security posture.
- Why** - Regularly 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. Clarify the activity if possible to increase engagement.

2 Administration - Account protection

- PASSWORDLESS OR MULTI-FACTOR AUTHENTICATION FOR ADMINS**
- What** - Require all critical impact admins to be passwordless (preferred) or require MFA.
- Why** - Passwords cannot protect accounts against common attacks.
- How** - Passwordless (Windows Hello, FIDO2, etc.)
- NO STANDING ACCESS**
- What** - No standing access for critical impact admins.
- Why** - Permanent privileges increase business risk by increasing attack surface of accounts (keys).
- How** - Just in Time - For Azure AD PIM and just party solutions for all other accounts.

3 Enterprise segmentation & Zero Trust preparation

- Align segmentation strategy & teams** by unifying network, identity, apps, etc. into a single enterprise segmentation strategy (as you migrate to Azure).

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 via Windows Admin Center (WAC)
- Azure App Service
- And more...

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 overall time of effort and resources.
- How** - Secure your application development / DevOps process by integrating existing guidance such as:

Operationalize Secure Score for cleaning up risk

Passwordless or MFA for admins

Enterprise segmentation & Zero Trust preparation

Enable Threat Protection for Azure Resources

Follow guidance to secure your DevOps

Best Practices 6 - 10

6 GRC – Key Responsible Parties

CRITICAL BEST PRACTICES

CLEAR LINES OF RESPONSIBILITY

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

Key responsibilities map new roles to governing process needs

Document and Socialize the results with all those involved in Azure

Network Security

Specify multi-tenant security from Configuration and membership of Azure Firewall, Network Virtual Appliances (for on-premises routing), VMs, VMs, Azure, etc.

Network Management

Specify management operations from Enterprise-wide or last network and select a location

Service Endpoint Security

Specify operations, usage, or policy: Monitor and maintain server security (patching, configurations, endpoint security, etc.)

Incident Monitoring and Response

Specify security operations team: Investigate incidents to notify incidents in SIEM or external console

- Azure Security Center
- Azure Active Directory Protection

Policy Management

Specify GRC team + authorization

Set policies for use of Azure-based Access Control (RBAC), Azure Security Center, Advanced or protection strategy, and Azure Policy to govern Azure resources

Specify security from + identity, team, security

Get strategy for Azure AD, connectors, RBAC, logs, MFA, permissions management, configurations, application security standards

Identify Security and Standards

7 Networks and Containment

CRITICAL BEST PRACTICES

INTERNET EDGE STRATEGY

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

Note – Some organizations choose a hybrid solution where some VMs are protected by 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 checked Firewall as a service, built-in high availability, server-side cloud scalability, EDRN filtering, support for DMZP use side view, and simple setup and configuration

3rd PARTY CAPABILITIES

Advanced security capabilities from existing vendors

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

Network or host appliances in the Azure Management include flexible security tools that provide enhanced network security capabilities. Configuration is more complex, but allows you to leverage existing capabilities, and scaling.

8 Applications – WAF

CRITICAL BEST PRACTICE

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 that be an integral part 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 life cycle (SDLC) to find/fix these vulnerabilities. WAFs also serve as an important safety measure even if you don't have a mature SDLC (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 as a part of their penetration firewalls.

Web Application Firewall

Web application protection

- Microsoft Azure Application Gateway
- Microsoft Azure Front Door
- Microsoft Azure Front Door Premium
- Microsoft Azure Front Door Premium with WAF
- Microsoft Azure Front Door Premium with WAF and Bot Protection
- Microsoft Azure Front Door Premium with WAF and Bot Protection and Bot Management
- Microsoft Azure Front Door Premium with WAF and Bot Protection and Bot Management and Bot Management
- Microsoft Azure Front Door Premium with WAF and Bot Protection and Bot Management and Bot Management and Bot Management

9 Networks and Containment – DDoS Mitigations

GENERAL GUIDANCE

DDoS MITIGATIONS

- What** – Enable DDoS Mitigation for all business-critical web applications and services
- Why** – DDoS attacks are prevalent and are very expensive to access on the dark market
- How** – Evaluate and select the best option for protecting your critical applications and services

- [Azure DDoS standard](#)
- [Azure DDoS premium](#)

Attack services on Azure

Azure DDoS Protection

10 Network – Deprecating Legacy Technology

CRITICAL CHOICES

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/Drop Recommendation
 - Add to Azure Incent

NETWORK DATA LOSS PREVENTION (DLP)

- What** – Choose whether to add Network DLP capabilities on Azure
- Why** – Network DLP is increasingly ineffective at identifying both inbound and outbound attacks. This is because most data protocols and most attackers use one system (most available at the host) to have encryption built-in.
- How** –
 - Do Not Add/Drop Recommendation
 - Add to Azure Incent

Assign and Publish Roles/Responsibilities

Choose Firewall Strategy

Implement Web Application Firewalls

Choose DDoS Mitigation for Critical Apps

Consider Retiring Legacy/Classic Technology

Calls To Action

Follow Best Practices

- in your Design → Build → Operations

Learn More

- **Videos**
aka.ms/AzureSecurityCompass-Videos
- **Download slides** aka.ms/AzureSecurityCompass
- **Architecture Guidance**
aka.ms/AzureSecurityArchitecture

Share

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

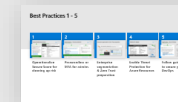
Provide Feedback

- **Compass** - Security and Identity Forum in
<https://aka.ms/SecurityCommunity>
- **Join Secure Score Private Preview**
<https://aka.ms/MicrosoftSecurityPreviewProgram>



Operationalize Secure Score

 Back



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>

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

Administration – Account protection

CRITICAL BEST PRACTICES

 [Back](#)



PASSWORDLESS OR MULTI-FACTOR AUTHENTICATION FOR ADMINS

- **What** – Require all critical impact admins to be passwordless (preferred) or require 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>

Enterprise segmentation & Zero Trust preparation



Align segmentation strategy & teams by unifying network, identity, app, etc. into a single enterprise segmentation strategy (as you migrate to Azure)

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.

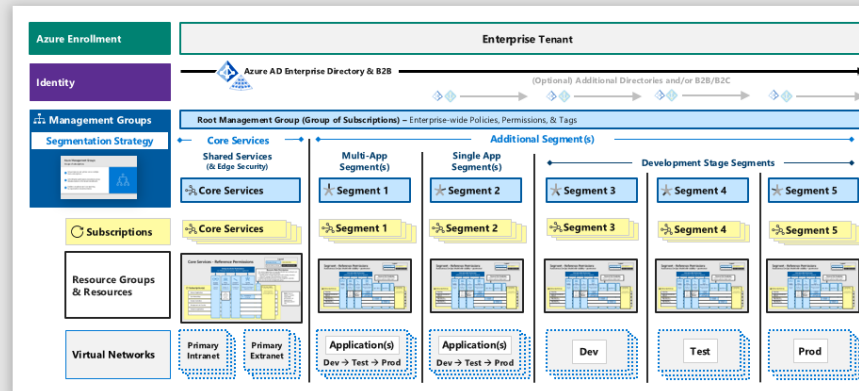
TIP **Minimize Complexity** – Always consider whether a segment is needed or whether security monitoring provides enough risk mitigation (each segment adds friction and overhead)



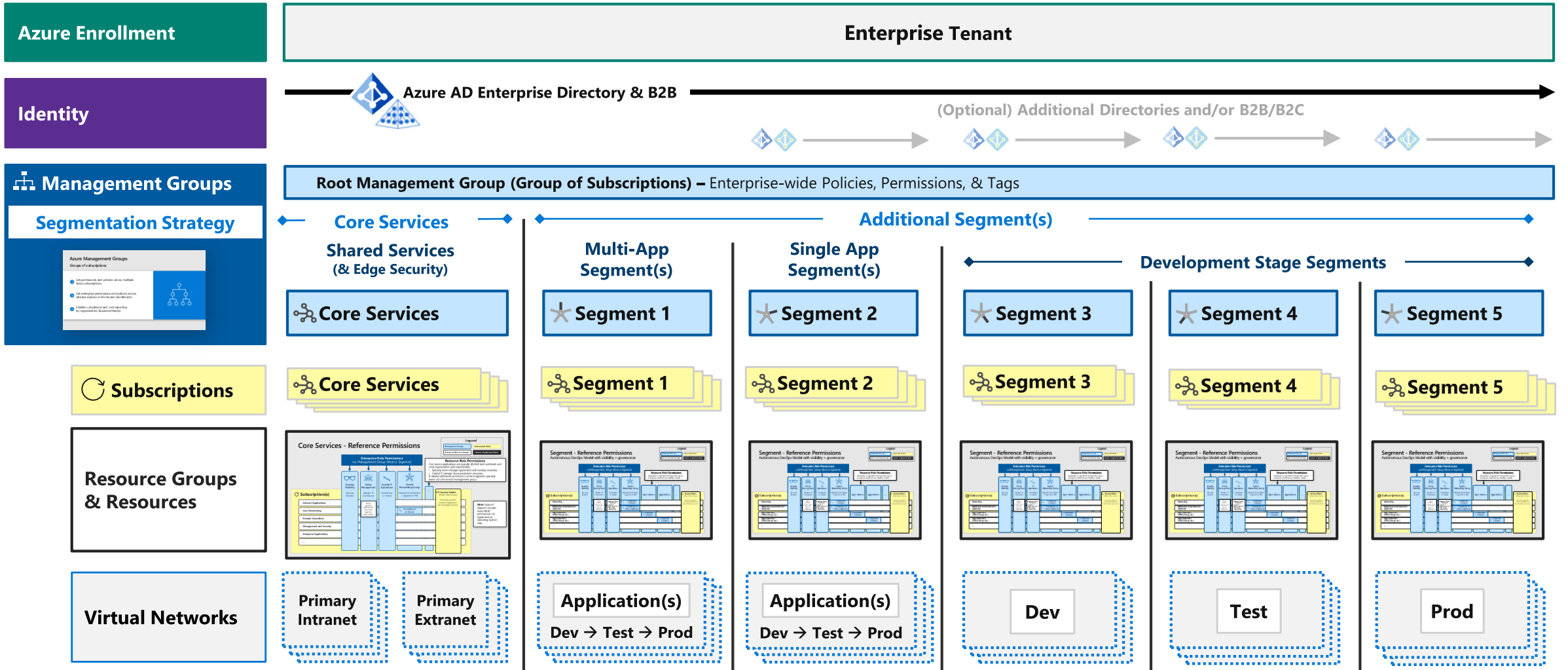
A GOOD SEGMENTATION STRATEGY:

- 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.)

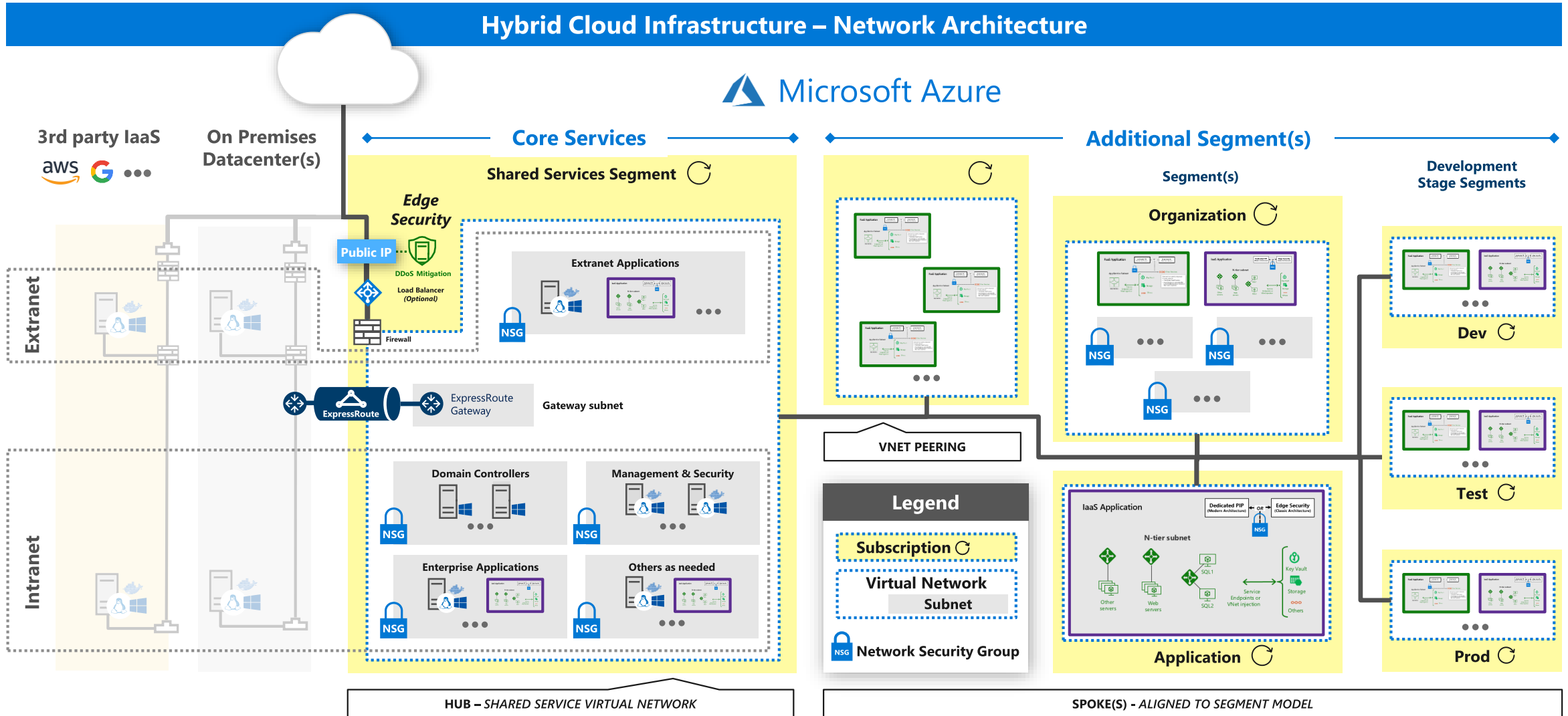
Reference Design - Azure Administration Model



Reference Design - Azure Administration Model



Reference Enterprise Design - Azure Network Security



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 (via Windows Admin Center (WAC))
- Azure App Service
- And more...

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

← Back



Security Operations – Azure Alerts

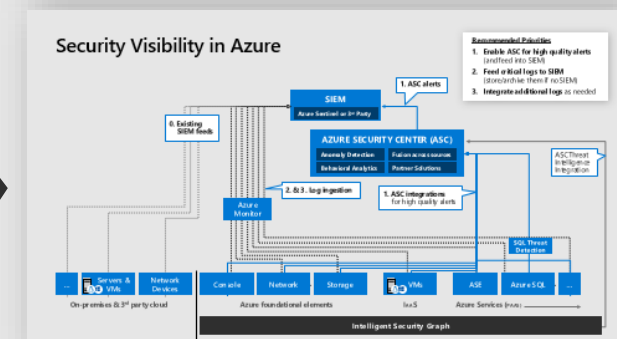
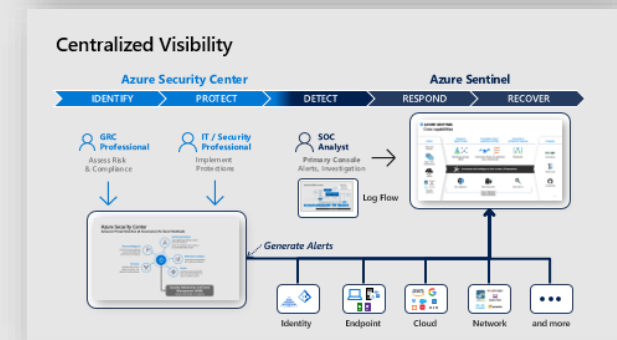
CRITICAL GUIDANCE

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 Microsofts [advanced threat protection](#), advanced machine learning, industry leading Incident Detection & Response (IDR), [MITRE reports](#), 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 (MBA)
- SQL Database & Data Warehouse Analysis
- Contextual Information
- Network Analysis



Applications – Secure DevOps

CRITICAL BEST PRACTICE

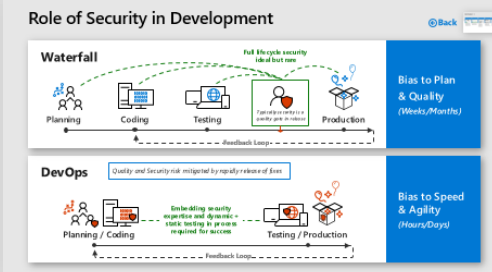
[← Back](#)



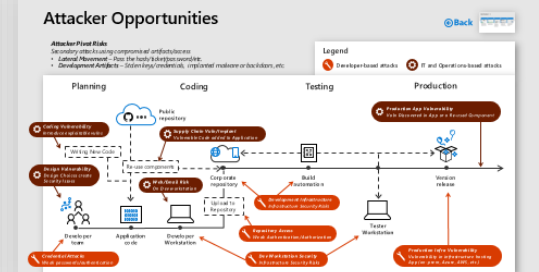
FOLLOW DEVOPS SECURITY GUIDANCE

- **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

Different than Waterfall



Secure Both Dev & Ops



Securing DevOps: Integrate security into the process

Every Sprint

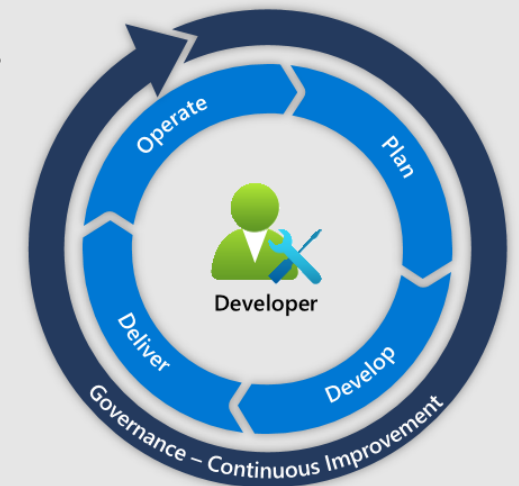
Reduce risk natively in Continuous Integration / Continuous Delivery (CI/CD) with real-time developer guidance, build checks, and more

Periodic Actions

Regular risk reduction and governance activities like Threat modelling, Training, etc.

Vigilance and Response

Monitoring and Response processes to ensure close collaboration of Security and DevOps teams



Learnings from migrating Microsoft's IT environment to ~95% cloud-based infrastructure

Integrate Security Natively into Process

Securing DevOps: Integrate security into the process

Every Sprint

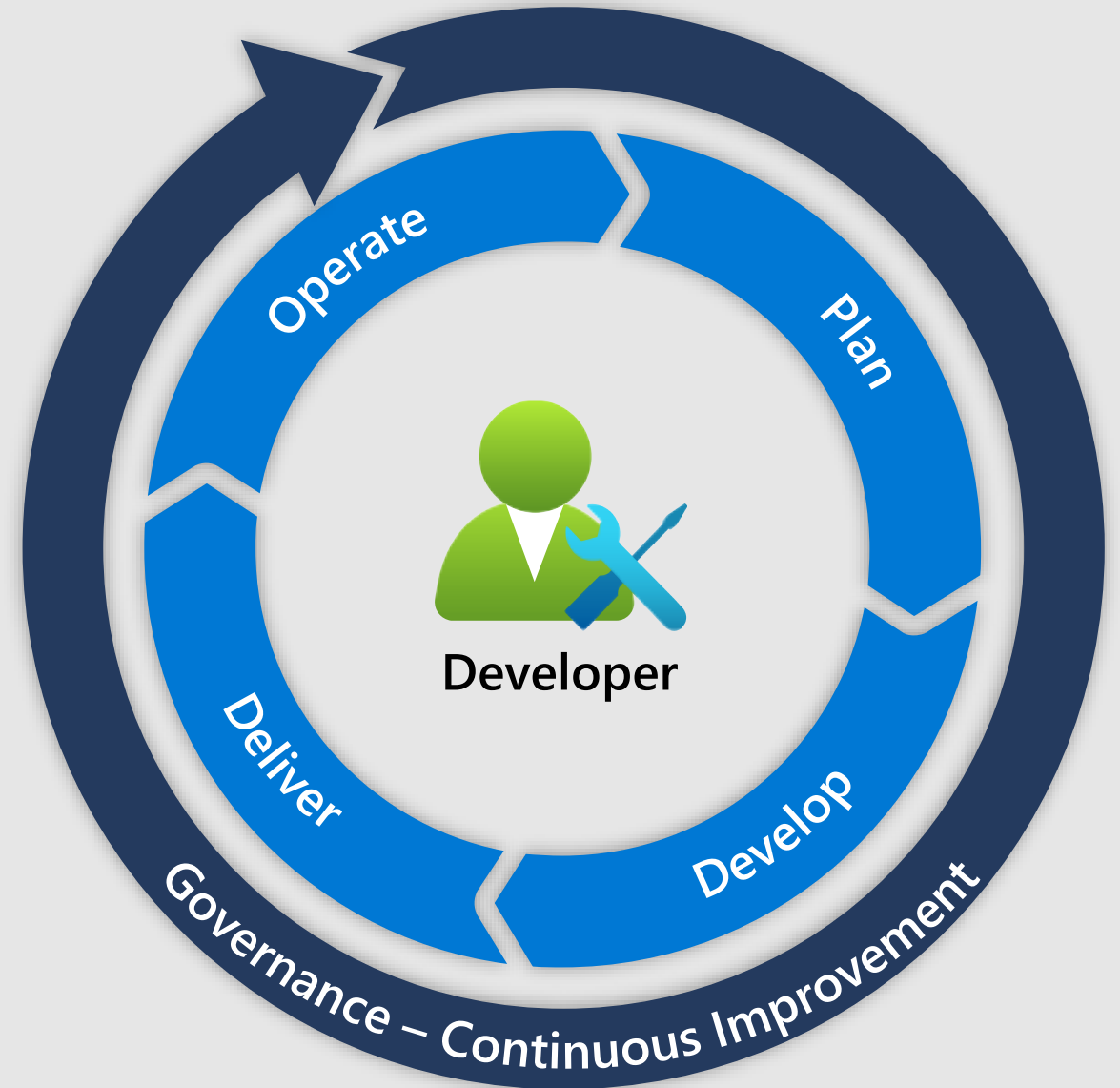
Reduce risk natively in Continuous Integration / Continuous Delivery (CI/CD) with real-time developer guidance, build checks, and more

Periodic Actions

Regular risk reduction and governance activities like Threat modelling, Training, etc.

Vigilance and Response

Monitoring and Response processes to ensure close collaboration of Security and DevOps teams



Learnings from migrating Microsoft's IT environment to ~95% cloud-based infrastructure

GRC – Key Responsible Parties

CRITICAL BEST PRACTICES

[← Back](#)



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"> • Azure Security Center • Azure AD Identity Protection
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

Networks and Containment

CRITICAL BEST PRACTICES

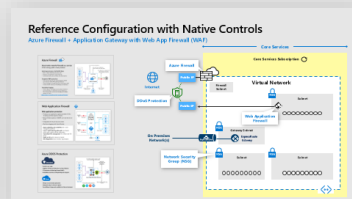
[← Back](#)



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

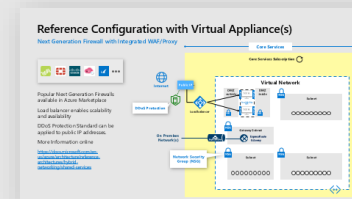


AZURE NATIVE CONTROLS

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



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

Applications – WAF

CRITICAL BEST PRACTICE

← Back



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.

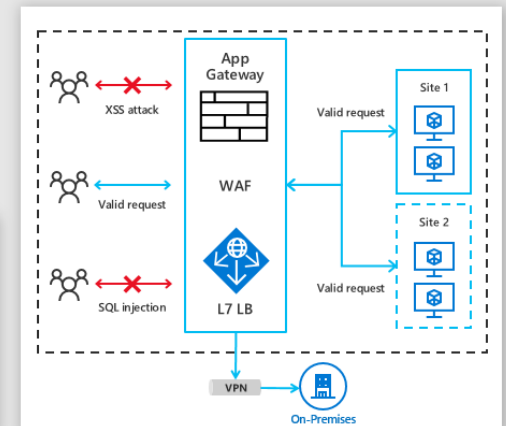
Web Application Firewall



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



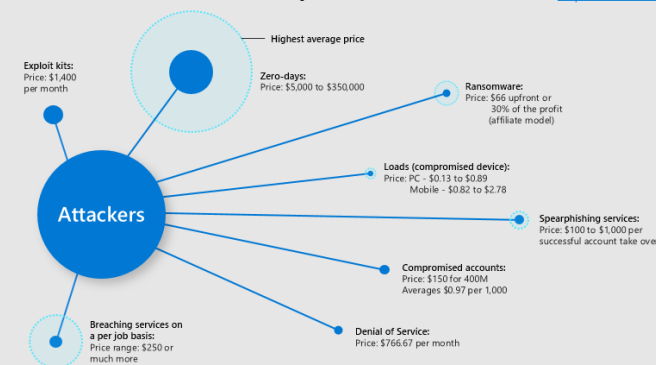


DDoS MITIGATIONS

- **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

Attack services are cheap

More details at <https://aka.ms/CISOWorkshop>



Azure DDoS Protection



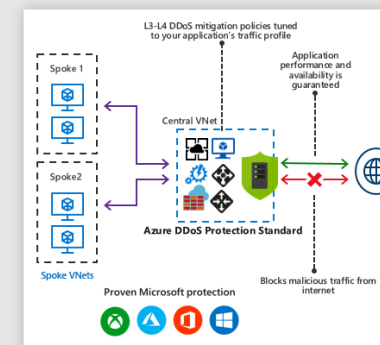
Standard

Tuned to your apps
Logging, alerting and telemetry via Azure Monitor
L7 Protection via Web App Firewall (WAF)
Availability Guarantee and Rapid Response Support



Basic

Always on L3/L4 attack protection
Deployed today in all Azure regions
No additional charge and available to all Azure Customers



Network – Deprecating Legacy Technology

CRITICAL CHOICES

[← Back](#)



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**



Thank you!