Microsoft

Microsoft Ignite

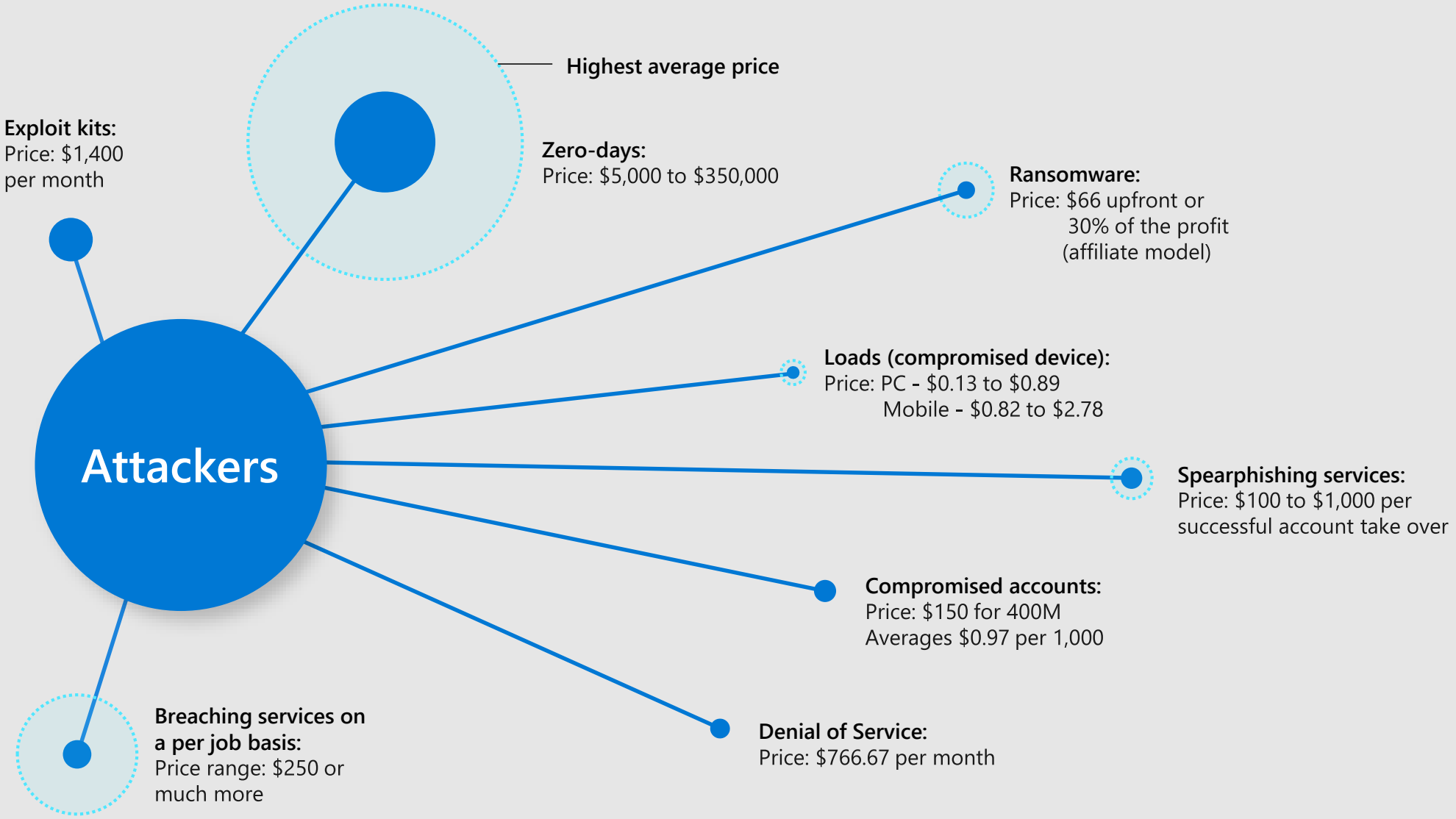
Microsoft

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

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. https://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 Security Compass
- Secure Score

Top 10 Best practices

Calls to Action

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

What is Azure Security compass?

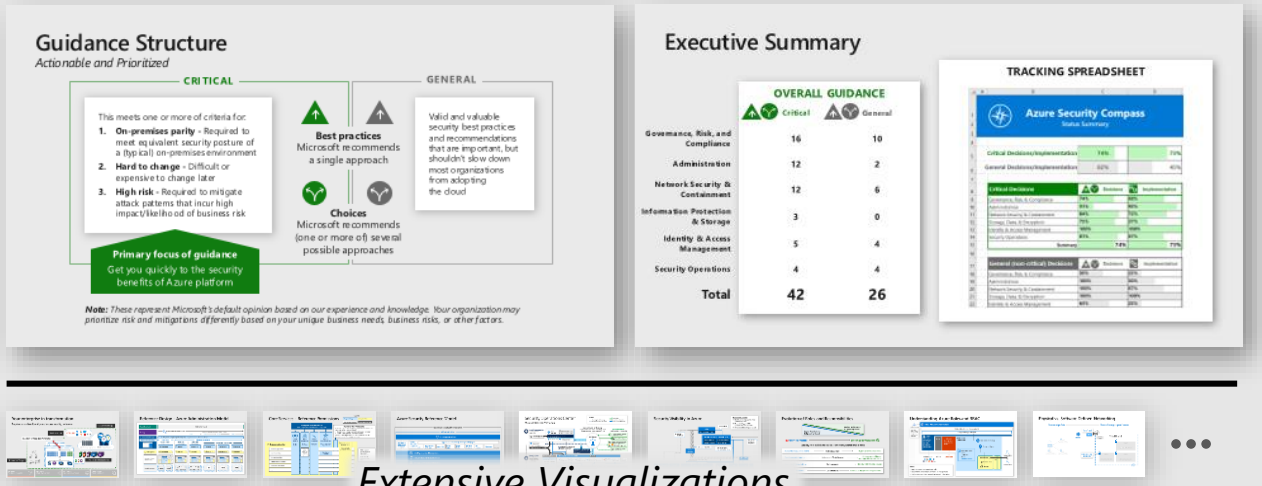
Azure Security Guidance

Strategy Transformation Guidance

Changes from On-premises Security

Reference Models / Diagrams

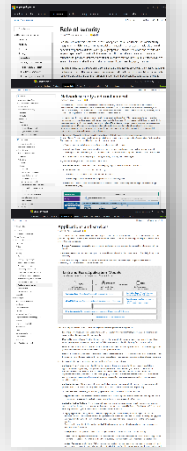
Actionable Best Practices (Top 10 is a subset)



Extensive Visualizations

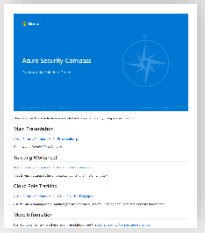
Architecture Documentation

aka.ms/AzureSecurityArchitecture



Download Site

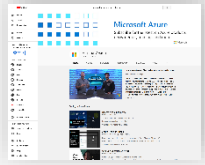
aka.ms/AzureSecurityCompass



- Slides –
- Tracking Spreadsheets
- And more…

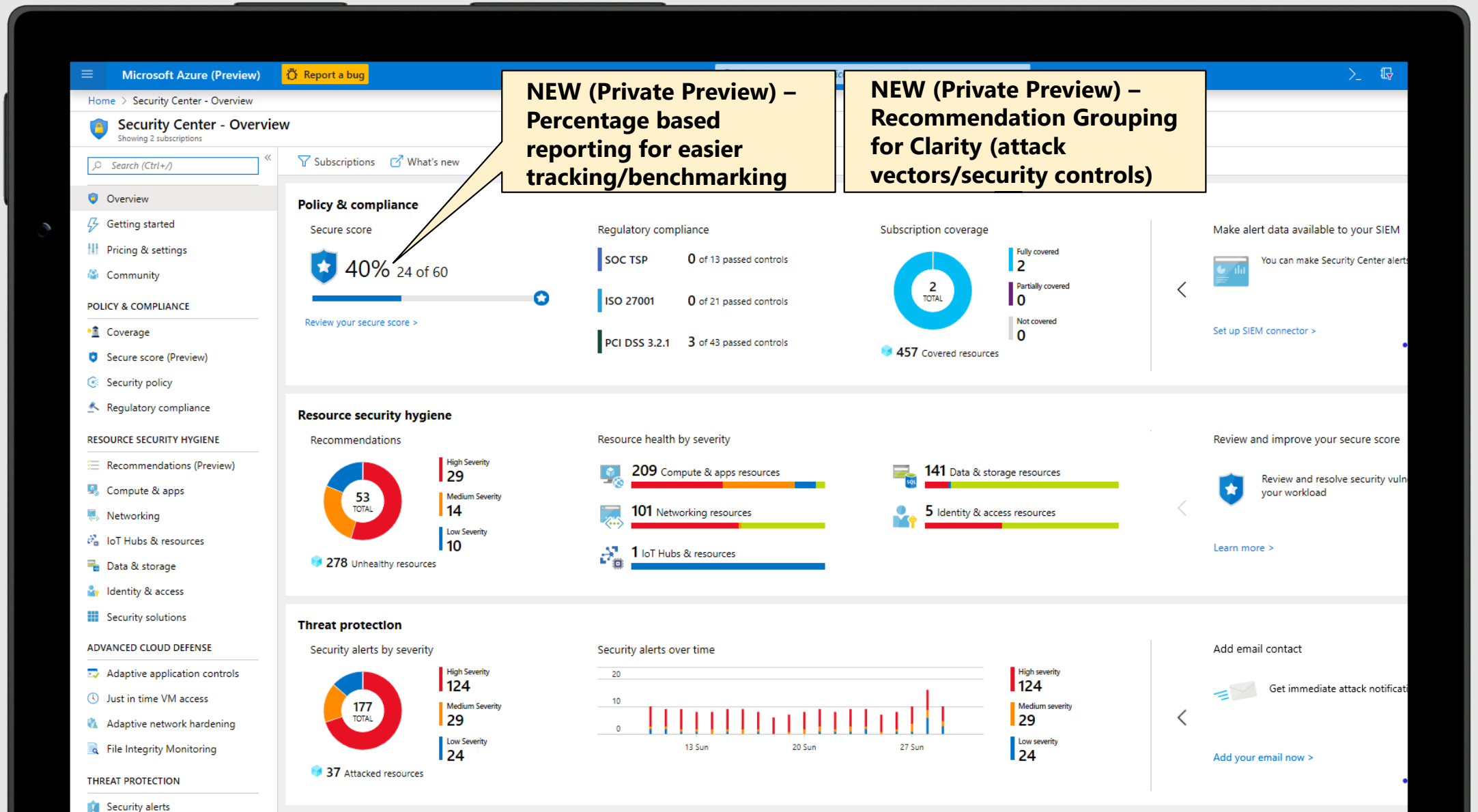
Videos

aka.ms/AzureSecurityCompass-Videos



COMING SOON

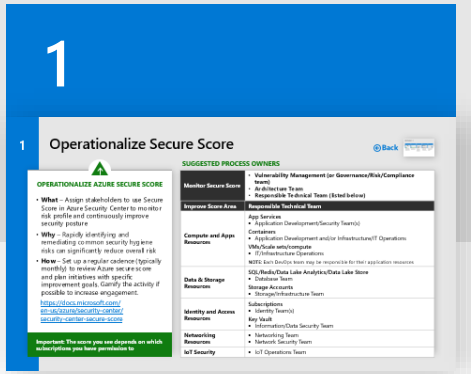
Visibility Across Your Estate with Secure Score



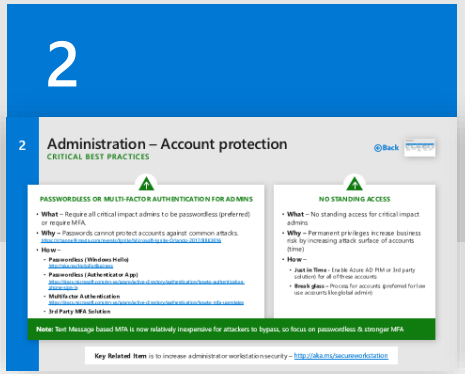
Top 10 Best Practices

Focused on Highest Impact
and Rapid Implementation

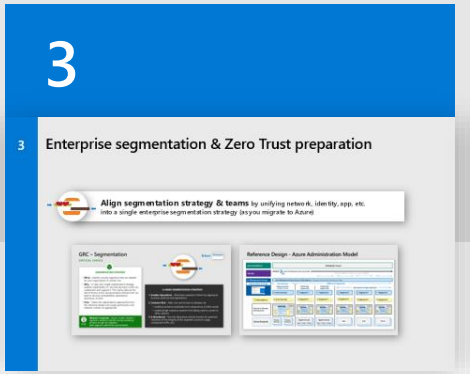
Best Practices 1 - 5



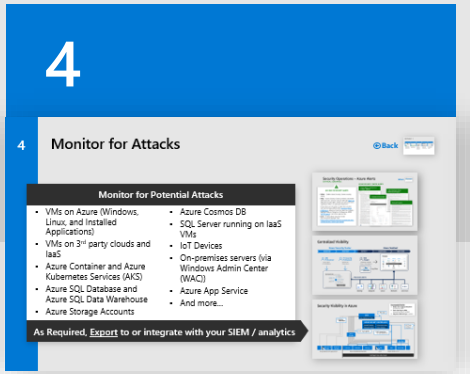
Operationalize Secure Score for cleaning up risk



Passwordless or MFA for admins



Enterprise segmentation & Zero Trust preparation



Enable Threat Protection for Azure Resources

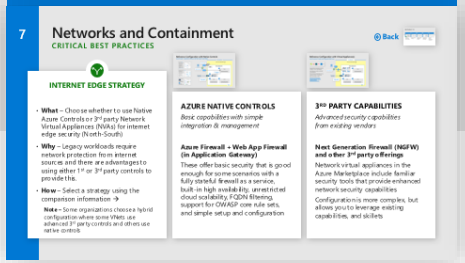
Follow guidance to secure your DevOps

Best Practices 6 - 10

6

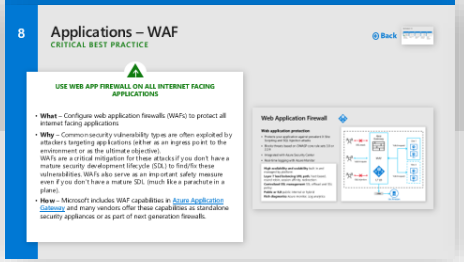
Assign and Publish Roles/ Responsibilities

7



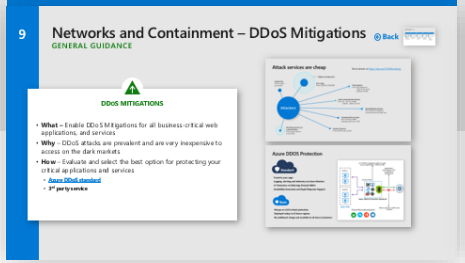
Choose Firewall Strategy

8



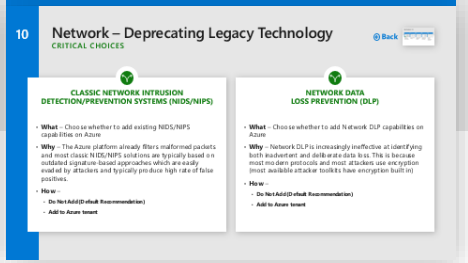
Implement Web Application Firewalls

9



Choose DDoS Mitigation for Critical Apps

10



Consider Retiring Legacy/Classic Technology

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

1 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	• **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

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

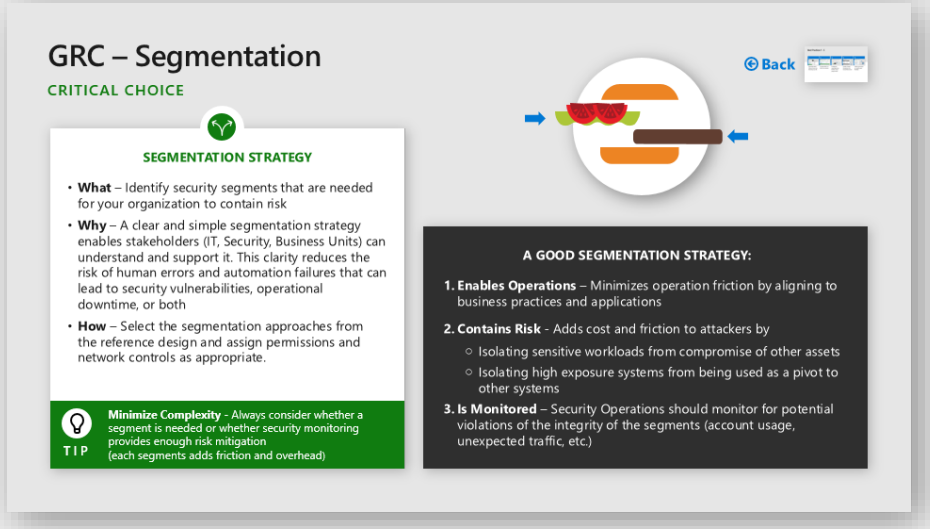
- **What** – No standing access for critical impact admins
- **Why –** Permanent privileges increase business risk by increasing attack surface of accounts (time)
- **How** –
  - **Just in Time -** Enable Azure AD PIM or 3rd party solution) for all of these accounts
  - **Break glass –** Process for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

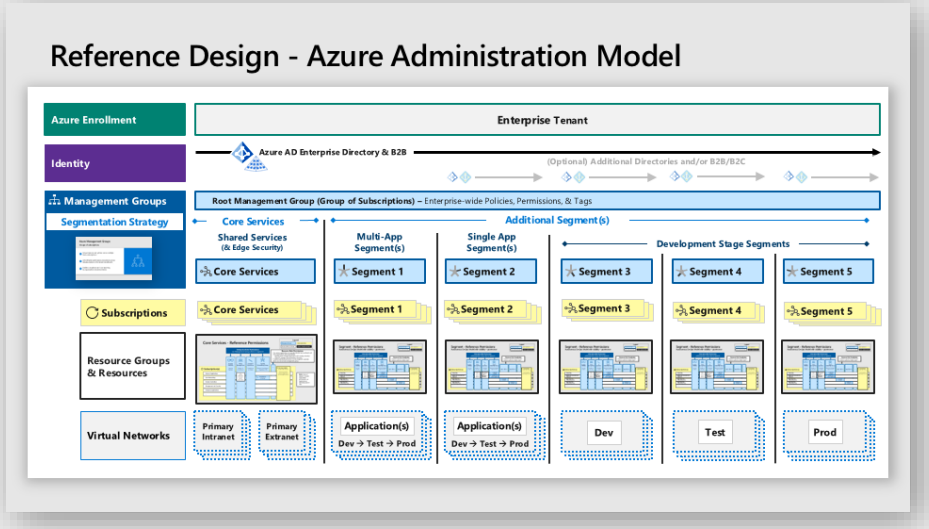
Note: Text Message based MFA is now relatively inexpensive for attackers to bypass, so focus on passwordless & stronger MFA

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

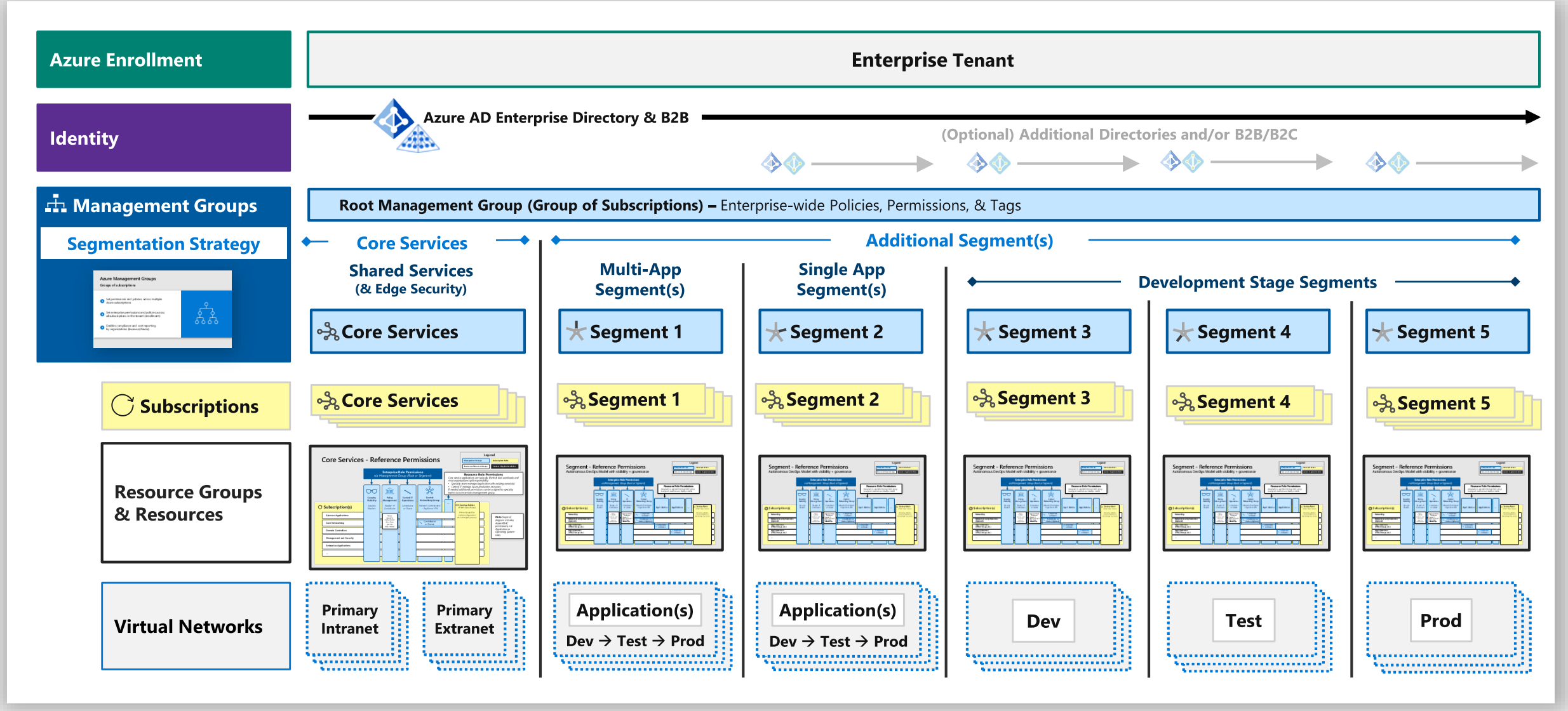
3 Enterprise segmentation & Zero Trust preparation

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

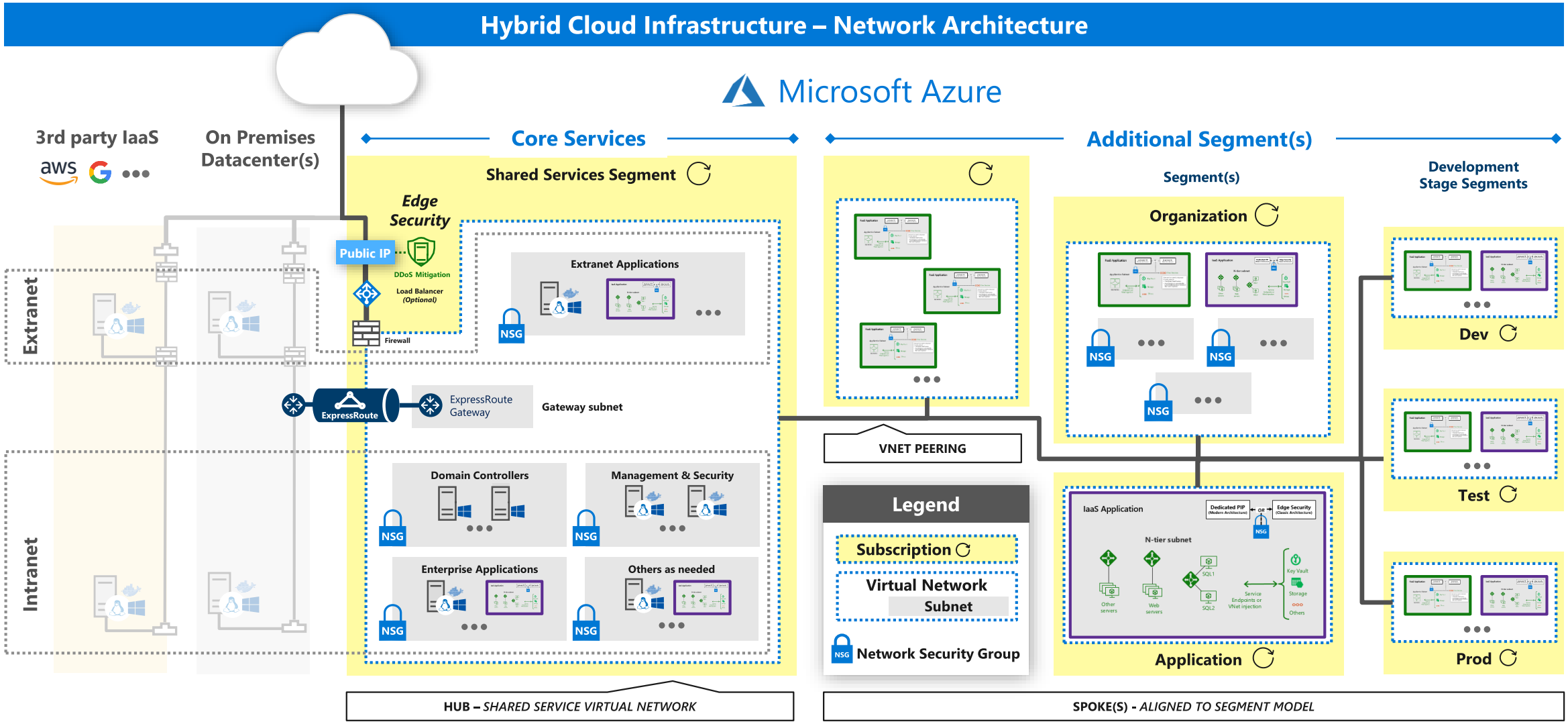




Reference Design - Azure Administration Model

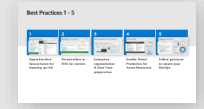


Reference Enterprise Design - Azure Network Security



4 Monitor for Attacks

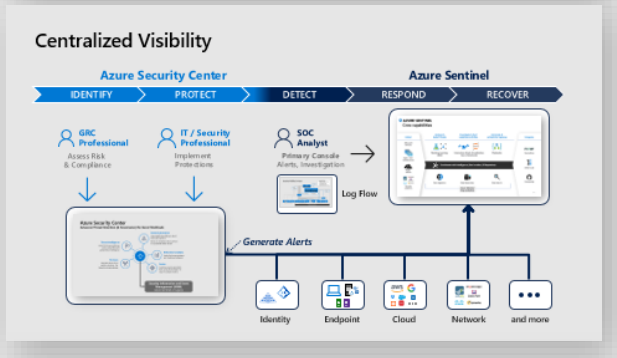
Back

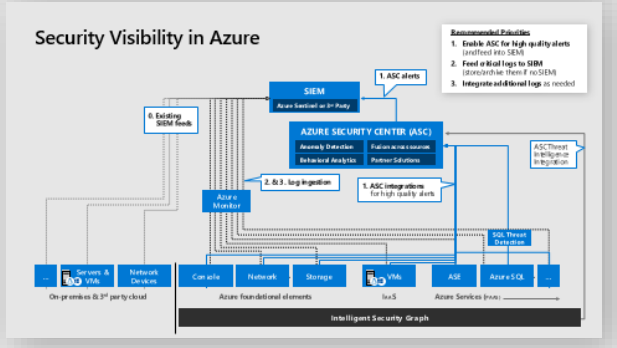


Monitor for Potential Attacks

- 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





Applications – Secure DevOps

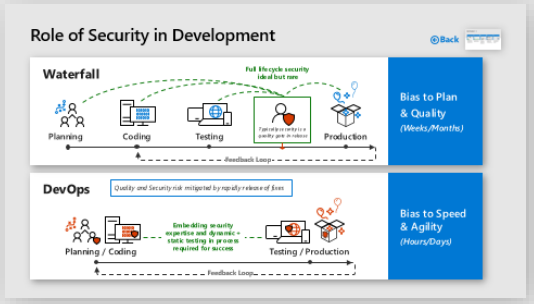
CRITICAL BEST PRACTICE

Back

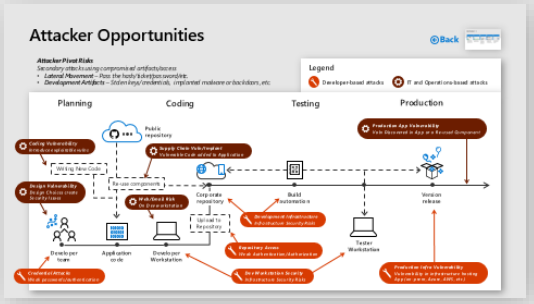
FOLLOW DEVOPS SECURITY GUIDANCE

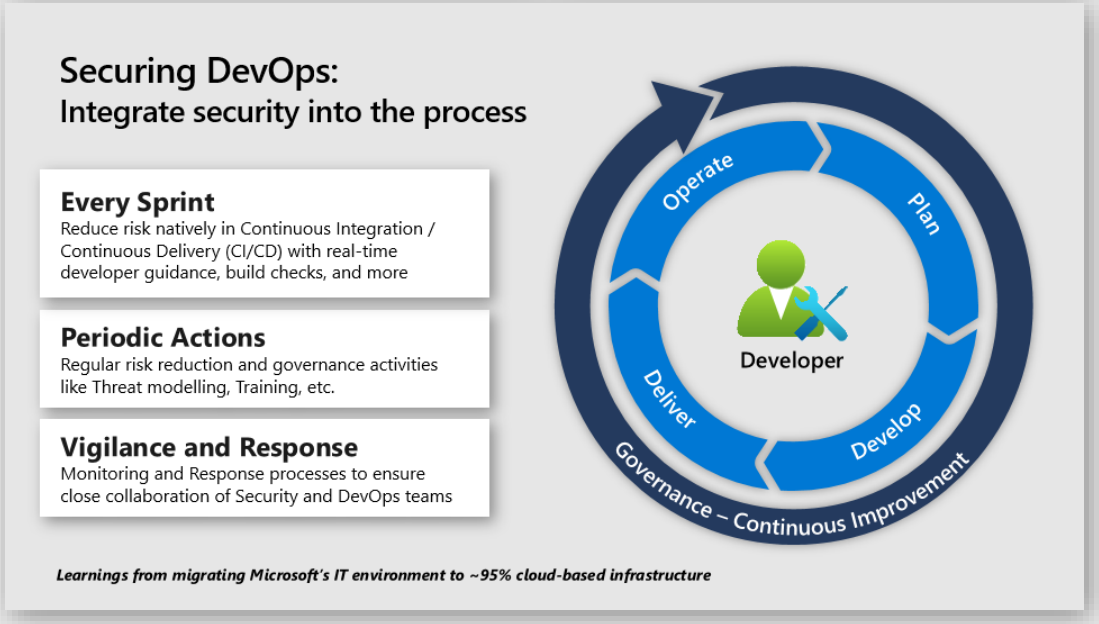
- **What –** Integrate guidance and automation for securing applications on the cloud
- **Why** – Using resources and lessons learned by external organizations that are early adopters of these models can accelerate the improvement of an organization's security posture with less expenditure of effort 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





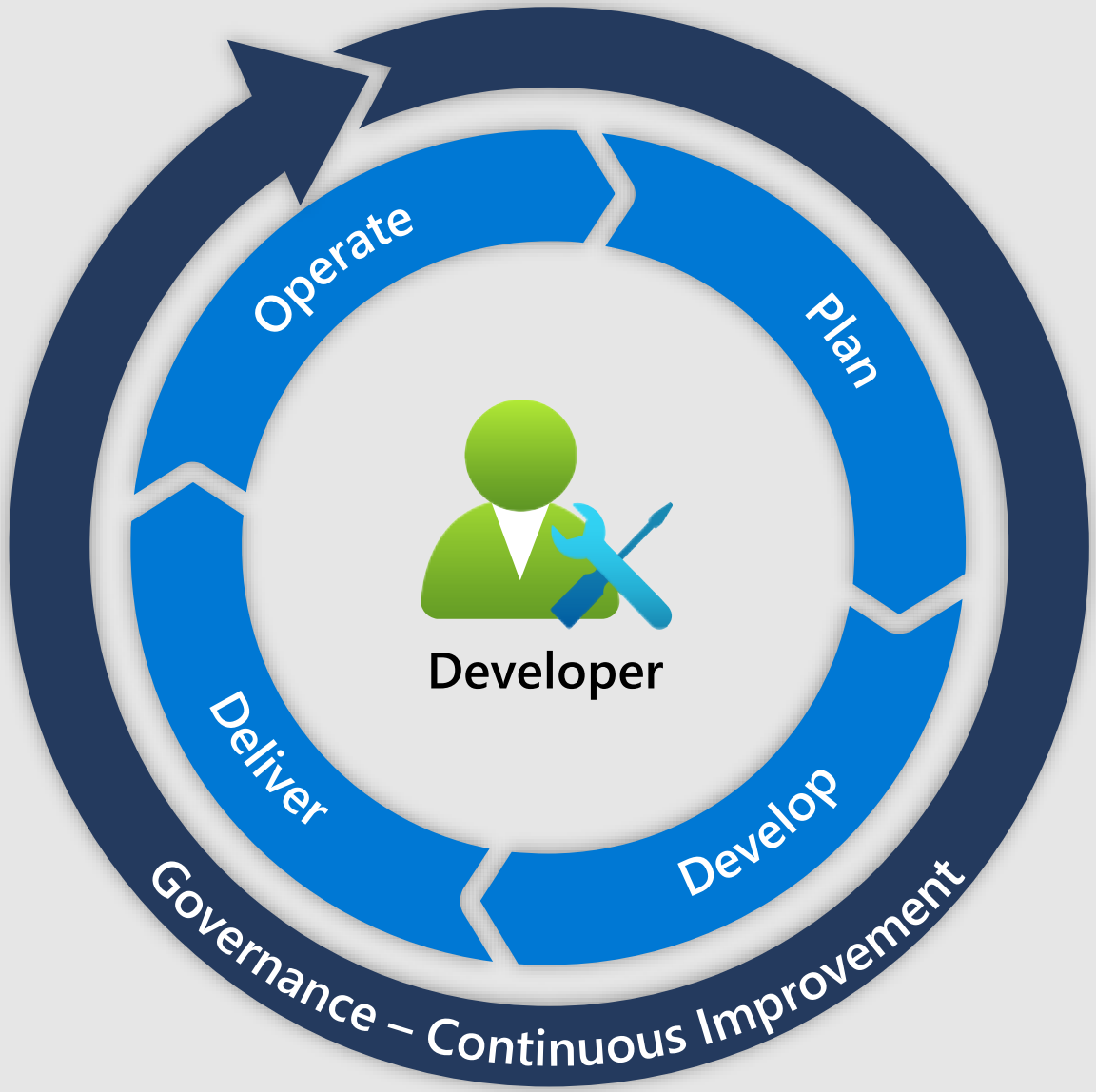
Integrate Security Natively into Process

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

Back

CRITICAL BEST PRACTICES

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

Networks and Containment

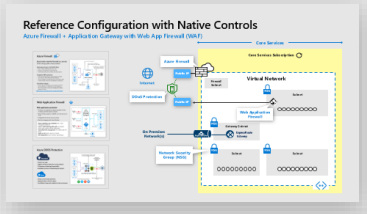
CRITICAL BEST PRACTICES

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

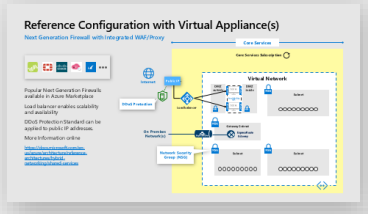


AZURE NATIVE CONTROLS

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 skillets

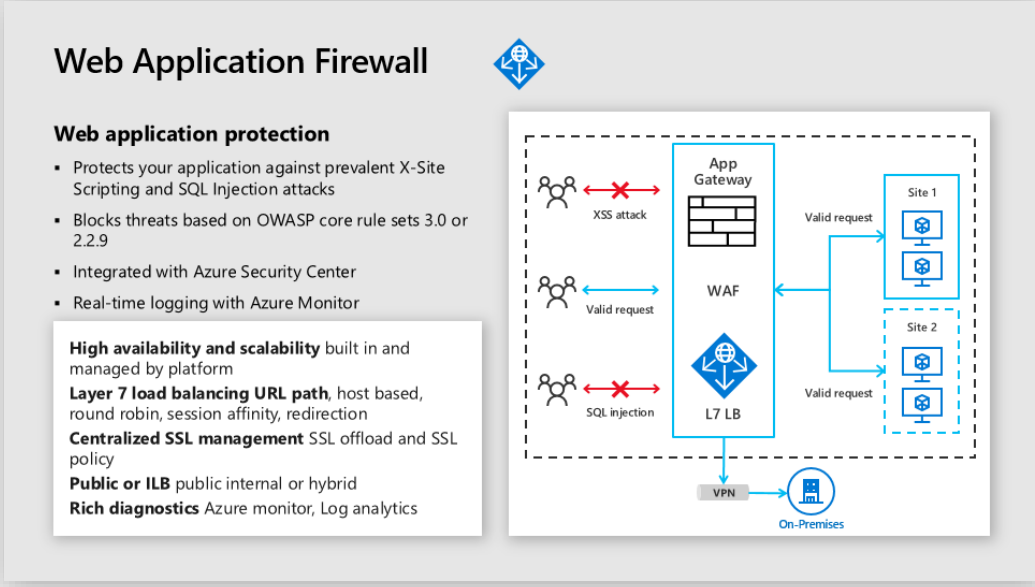
Applications – WAF

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.



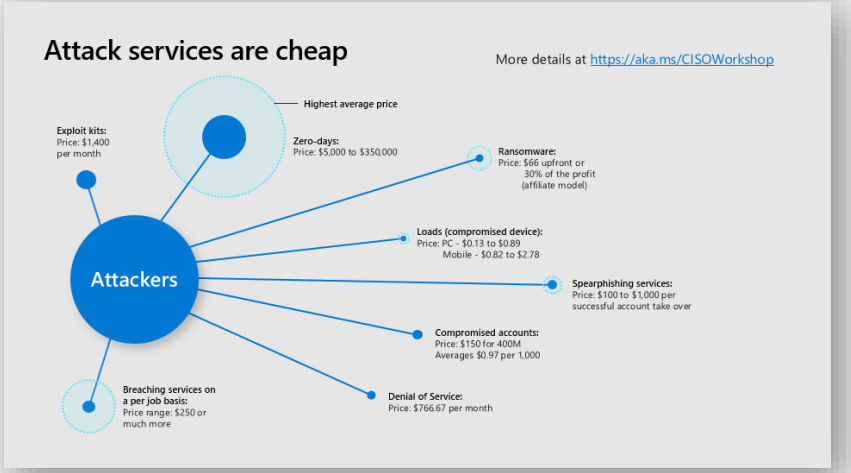
Networks and Containment – DDoS Mitigations

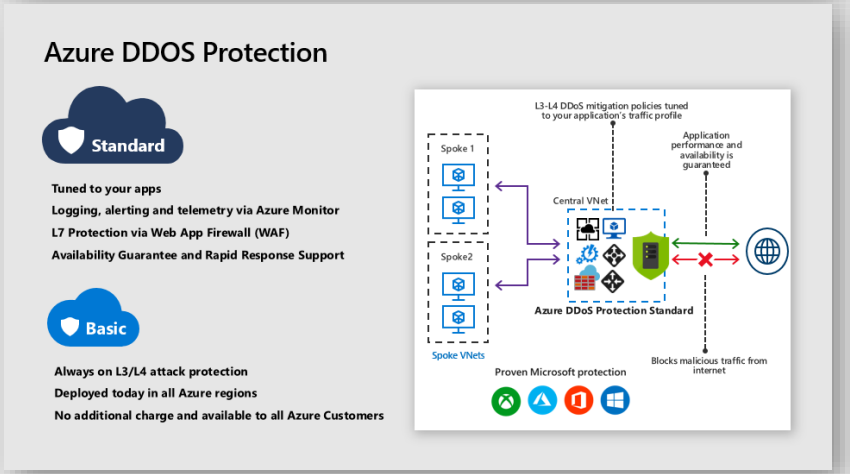
GENERAL GUIDANCE

Back

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**





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**

Microsoft

Thank you!