



Microsoft Ignite



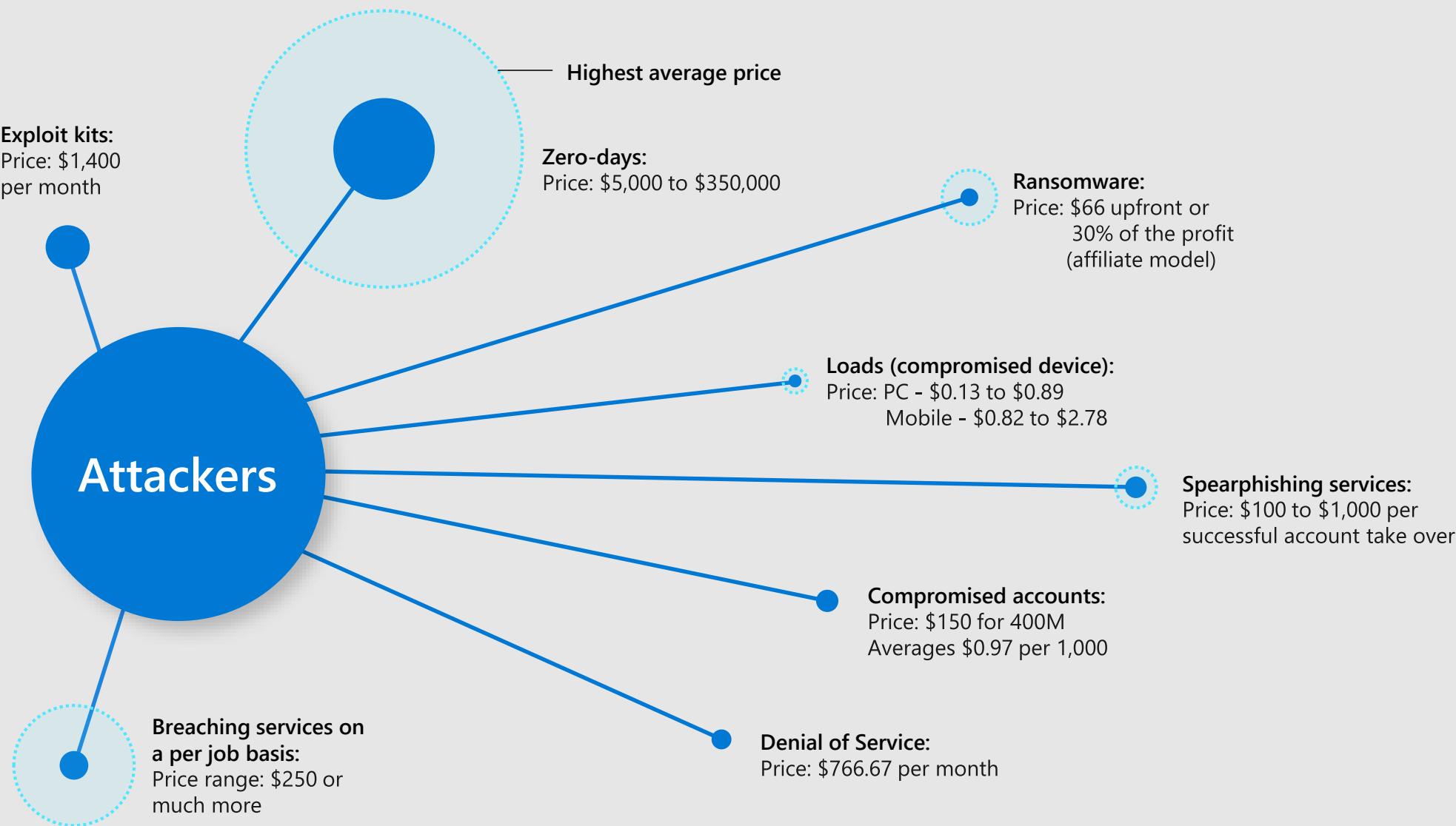
Top 10 Azure Security Best Practices

Mark Simos
Lead Cybersecurity Architect



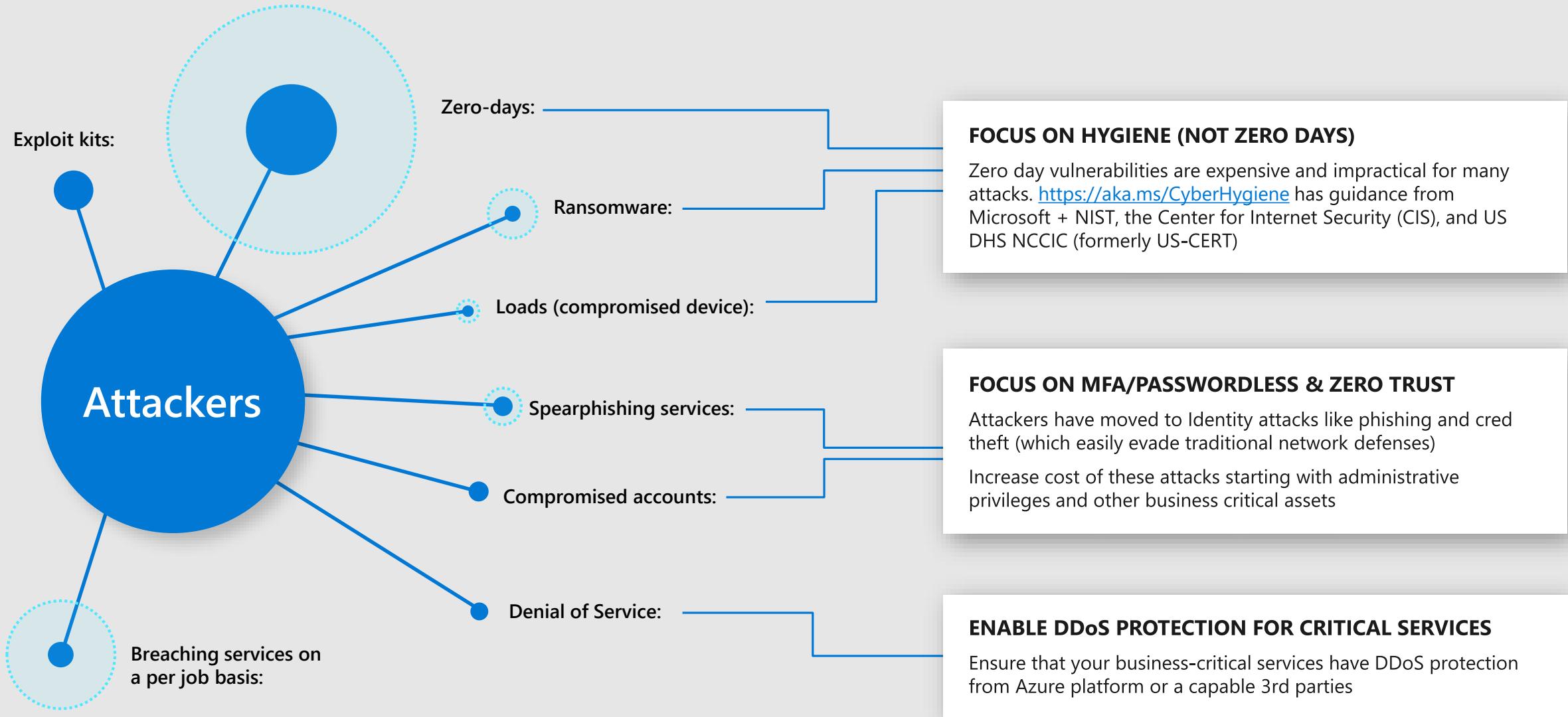
Attack services are cheap

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

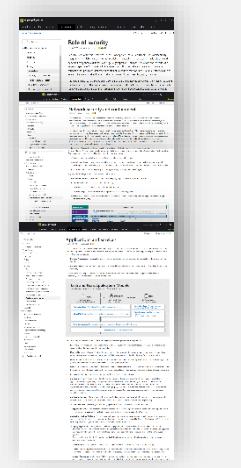
Changes from On-premises Security

Reference Models / Diagrams

Actionable Best Practices (Top 10 is a subset)

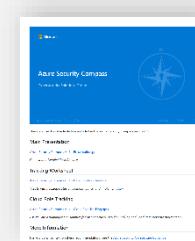
The screenshot displays the Azure Security Compass platform. On the left, the 'Guidance Structure' section shows a hierarchy of security best practices, categorized into 'CRITICAL' and 'GENERAL'. It includes sections for 'Best practices' (Microsoft recommends a single approach) and 'Choices' (Microsoft recommends one or more of several possible approaches). A note at the bottom states: 'Note: These represent Microsoft's default opinion based on our experience and knowledge. Your organization may prioritize risk and mitigations differently based on your unique business needs, business risks, or other factors.' To the right, the 'Executive Summary' provides an overall guidance breakdown. Below these are several 'Extensive Visualizations' such as tracking spreadsheets and dashboards.

Architecture Documentation
aka.ms/AzureSecurityArchitecture

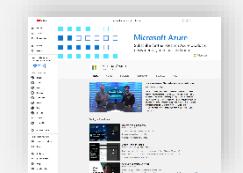


Download Site
aka.ms/AzureSecurityCompass

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



Videos
aka.ms/AzureSecurityCompass-Videos



COMING SOON

Visibility Across Your Estate with Secure Score

The screenshot shows the Microsoft Azure Security Center - Overview page. It features several key metrics and charts:

- Secure score:** 40% (24 of 60)
- Regulatory compliance:**
 - SOC TSP: 0 of 13 passed controls
 - ISO 27001: 0 of 21 passed controls
 - PCI DSS 3.2.1: 3 of 43 passed controls
- Subscription coverage:** 2 Fully covered, 0 Partially covered, 0 Not covered. 457 Covered resources.
- Resource security hygiene:**
 - Recommendations: 53 TOTAL, 29 High Severity, 14 Medium Severity, 10 Low Severity. 278 Unhealthy resources.
 - Resource health by severity:
 - Compute & apps resources: 209
 - Networking resources: 101
 - Data & storage resources: 141
 - Identity & access resources: 5
 - IoT Hubs & resources: 1
- Threat protection:**
 - Security alerts by severity:
 - High Severity: 124
 - Medium Severity: 29
 - Low Severity: 24
 - Security alerts over time: A chart showing alerts per week from 13 Sun to 27 Sun.
 - Attacked resources: 37 Attacked resources.

NEW (Private Preview) – Percentage based reporting for easier tracking/benchmarking

NEW (Private Preview) – Recommendation Grouping for Clarity (attack vectors/security controls)

Top 10 Best Practices

Focused on Highest Impact
and Rapid Implementation



Best Practices 1 - 5

Operationalize Secure Score	
 SUGGESTED PROCESS OWNERS	
OPERATIONALIZE AZURE SECURE SCORE	 Business Unit  IT Operations Team  IT Infrastructure Team (Hosted below)
<ul style="list-style-type: none"> • What - Align stakeholders to use Secure Score in Azure Security Center to monitor and continuously improve security posture • Why - Properly identifying and mitigating security risks before they can significantly reduce overall risk • How - Set up a target audience (typically IT professionals) and communication plan to engage them - and plan initiatives with specific implementation steps to actually if possible to increase engagement <p>https://docs.microsoft.com/en-us/azure/security-center/secure-score</p>	Monitor Service Score  Business Unit  IT Operations Team  IT Infrastructure Team (Hosted below)
<ul style="list-style-type: none"> • What - Improve the Secure Score • Why - Increase confidence in the security posture of your organization • How - Set up a target audience (typically IT professionals) and communication plan to engage them - and plan initiatives with specific implementation steps to actually if possible to increase engagement <p>https://docs.microsoft.com/en-us/azure/security-center/secure-score</p>	Improve Score Area  Business Unit  IT Operations Team  IT Infrastructure Team (Hosted below)
<ul style="list-style-type: none"> • What - Ensure secure storage of sensitive data • Why - Protect sensitive data from unauthorized access or modification • How - Set up a target audience (typically IT professionals) and communication plan to engage them - and plan initiatives with specific implementation steps to actually if possible to increase engagement <p>https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-service-best-practices</p>	Data & Storage Resources  Business Unit  IT Operations Team  IT Infrastructure Team (Hosted below)
<ul style="list-style-type: none"> • What - Ensure secure management of identities and access • Why - Protect user accounts and sensitive data from unauthorized access • How - Set up a target audience (typically IT professionals) and communication plan to engage them - and plan initiatives with specific implementation steps to actually if possible to increase engagement <p>https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/identity-protection-best-practices</p>	Identity and Access Resources  Business Unit  IT Operations Team  IT Infrastructure Team (Hosted below)
<ul style="list-style-type: none"> • What - Ensure secure networking and connectivity • Why - Protect network traffic and resources from unauthorized access • How - Set up a target audience (typically IT professionals) and communication plan to engage them - and plan initiatives with specific implementation steps to actually if possible to increase engagement <p>https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-best-practices</p>	Networking Resources  Business Unit  IT Operations Team  IT Infrastructure Team (Hosted below)
<ul style="list-style-type: none"> • What - Ensure secure IoT devices and connectivity • Why - Protect IoT devices and data from unauthorized access • How - Set up a target audience (typically IT professionals) and communication plan to engage them - and plan initiatives with specific implementation steps to actually if possible to increase engagement <p>https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-best-practices</p>	IoT Security  Business Unit  IT Operations Team  IT Infrastructure Team (Hosted below)

Operationalize Secure Score for cleaning up risk

2 Administration – Account protection

Critical best practices

PASSWORDLESS OR MULTI-FACTOR AUTHENTICATION FOR AD MINS

What – Request all critical impact address to be passwordless (preferred) or require MFA.

Why – Passwords can prevent account compromise attacks.

How –

- [Passwordless \(Windows Hello\)](#)
- [Multi-factor Authentication](#) (<https://www.microsoft.com/en-us/identity/protect-yourself/multi-factor-authentication>)
- [Multi-step authentication](#) (<https://www.microsoft.com/en-us/identity/protect-yourself/multi-step-authentication>)
- [Do Not Use MFA Solutions](#) (<https://www.microsoft.com/en-us/identity/protect-yourself/do-not-use-mfa-solutions>)

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 –

- [Last in Time](#) – End user access AD RMS or 3rd party software for all critical accounts
- [Break glass](#) – Create a separate, preferred formula for use when立戶室門

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

Key Related Item is to increase administrative workstation security - <http://aka.ms/locadminbestpractices>

Passwordless or MFA for admins

3

Enterprise segmentation & Zero Trust preparation

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

The diagram illustrates the process of aligning segmentation strategy and teams. It starts with a central box labeled "Align segmentation strategy & teams by unifying users, identity, app, etc. into a single enterprise segmentation strategy (as you migrate to Azure)". An arrow points from this box to a circular icon containing a person, representing users. Another arrow points from the same box to a circular icon containing a gear, representing identity. A third arrow points from the same box to a circular icon containing a smartphone, representing apps. Finally, an arrow points from the same box to a circular icon containing a globe, representing the enterprise. The entire process is framed by a large rounded rectangle.

GRC - Segmentation

Identity

Reference Design - Azure Administration Model

Enterprise segmentation & Zero Trust preparation

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 Synapse Analytics Warehouse
- Azure Storage Accounts
- Azure Cosmos DB
- VM Server running on IaaS VMs
- IoT Devices
- On-premises servers (via Windows Admin Center (WAC))
- Azure App Service
- And more...

As Required, Export or integrate with your SIEM / analytics

```
graph LR; A[As Required, Export or integrate with your SIEM / analytics] --> B[Security Operations - Azure Monitor]
```

The diagram shows a horizontal arrow pointing from the text "As Required, Export or integrate with your SIEM / analytics" to the "Security Operations - Azure Monitor" section. The "Security Operations - Azure Monitor" section is a detailed screenshot of a Microsoft Azure portal page, showing various monitoring dashboards and metrics.

Enable Threat Protection for Azure Resources

5 Applications – Secure DevOps

Critical Best Practice

Follow DevOps Security Guidance

What – Integrate guidance and automation for securing application on the cloud.

Why – Using resources and lessons learned by internal organizations that are already adapting to these changes can accelerate the transition to DevOps. This posture is a security posture with less exposure of effort and resources.

How – Integrate security into the DevOps process by integrating existing guidance such as:

- Microsoft Azure DevSec Toolkit – [https://aka.ms/azuresec](#)
- Organization for Web App Security Project (OWASP) [https://owasp.org/www-project-modern-web-security/MWASP_Folder/Static%20Analysis](#)

Different than Waterfall

Secure Both Dev & Ops

Securing DevOps: Integrate security into the process

Every Sprint

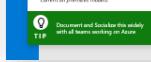
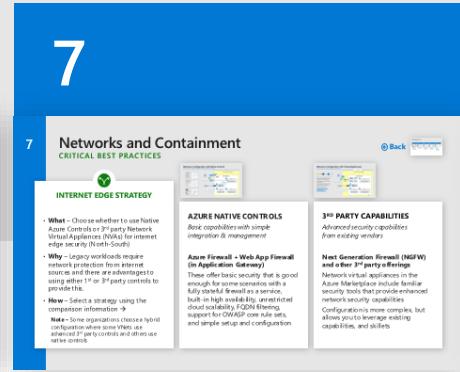
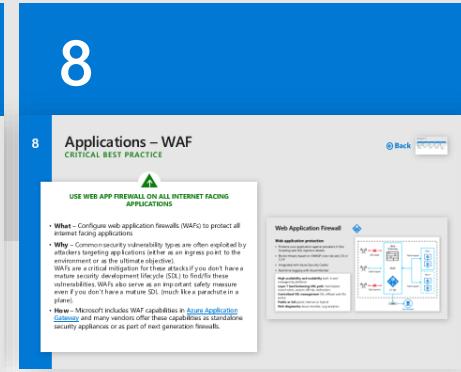
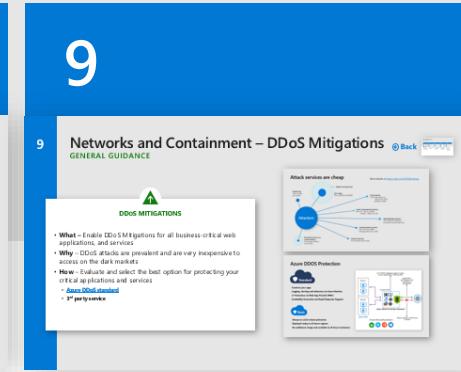
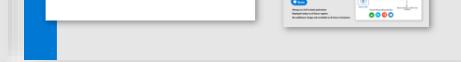
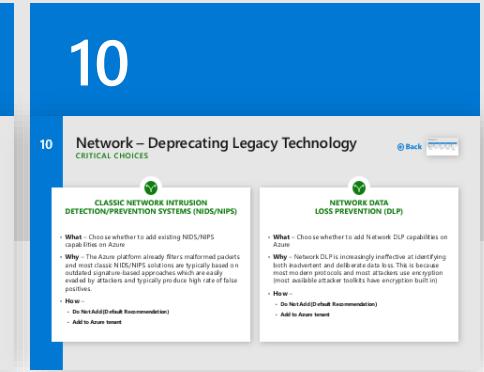
Periodic Actions

Vigilance and Response

Integrate Security Natively into Process

**Follow guidance
to secure your
DevOps**

Best Practices 6 - 10

6 GRC – Key Responsible Parties CRITICAL BEST PRACTICES  <p>• What – Designate the parties responsible for specific functions in Azure • Why – Consistency helps avoid confusion that can lead to human and automated errors that create security risks • How – Designate groups to manage specific functions that will be responsible for key controls and functions – This requires that the group can clearly define its current on-premises model </p>	7 Networks and Containment CRITICAL BEST PRACTICES  <p>• What – Identify and implement security zones Configuration and maintenance of Azure Firewall, Network Virtual Appliances (NVA), Network Security Groups (NSG), etc. • Why – Enterprise-wide or local networks and locations • How – Monitor and remediate security incidents in SIEM or source console – Azure AD Identity Protection </p>	8 Applications – WAF CRITICAL BEST PRACTICE  <p>• What – Choose whether to use Native Azure Controls or 3rd party Network Virtual Appliances (NVAs) for internet edge security (Network Edge Strategy) • Why – Legacy webhooks require network providers from email to cloud to support them. Consider the cost of using either 1st or 3rd party controls to protect your application • How – Select a strategy using the comparison information → – Not all organizations require hybrid configurations since there are advanced 3rd party controls and often use native controls </p>	9 Networks and Containment – DDoS Mitigations GENERAL GUIDANCE  <p>• What – Choose whether to add existing NIDS/NIPS capabilities on Azure • Why – DDoS attacks are prevalent and are very inexpensive to launch • How – Evaluate and select the best option for protecting your critical applications and services – 1st party – 3rd party service </p>	10 Network – Deprecating Legacy Technology CRITICAL CHOICES  <p>• What – Choose whether to add Network DLP capabilities on Azure • Why – Network DLP is increasingly ineffective at identifying both exfiltration and data at rest. This is because most data is now stored in the cloud (most available attack tools have encryption built in) • How – – Do Not Add (Default Recommendation) – Add to Azure Tenant  </p>
--	--	---	--	--

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



GRC – Segmentation

CRITICAL CHOICE

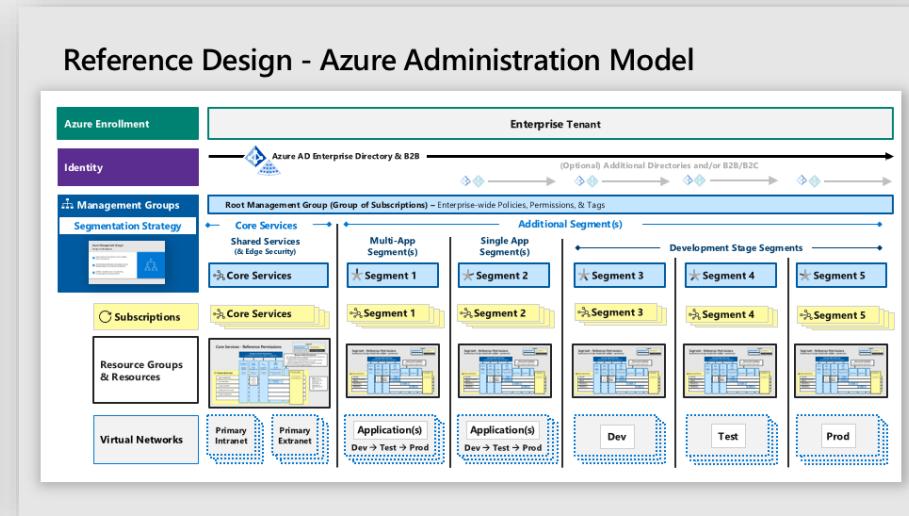
SEGMENTATION STRATEGY

- **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.

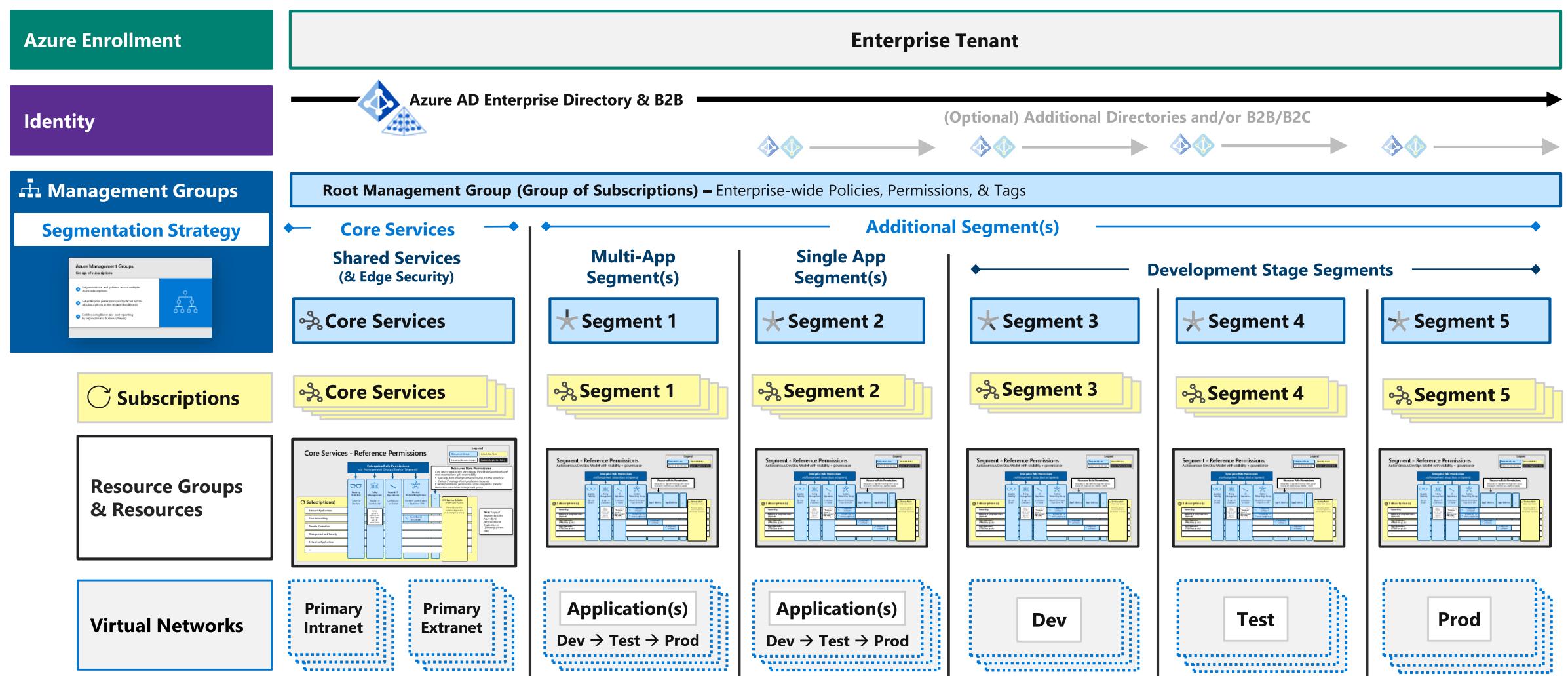
A GOOD SEGMENTATION STRATEGY:

- 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.)

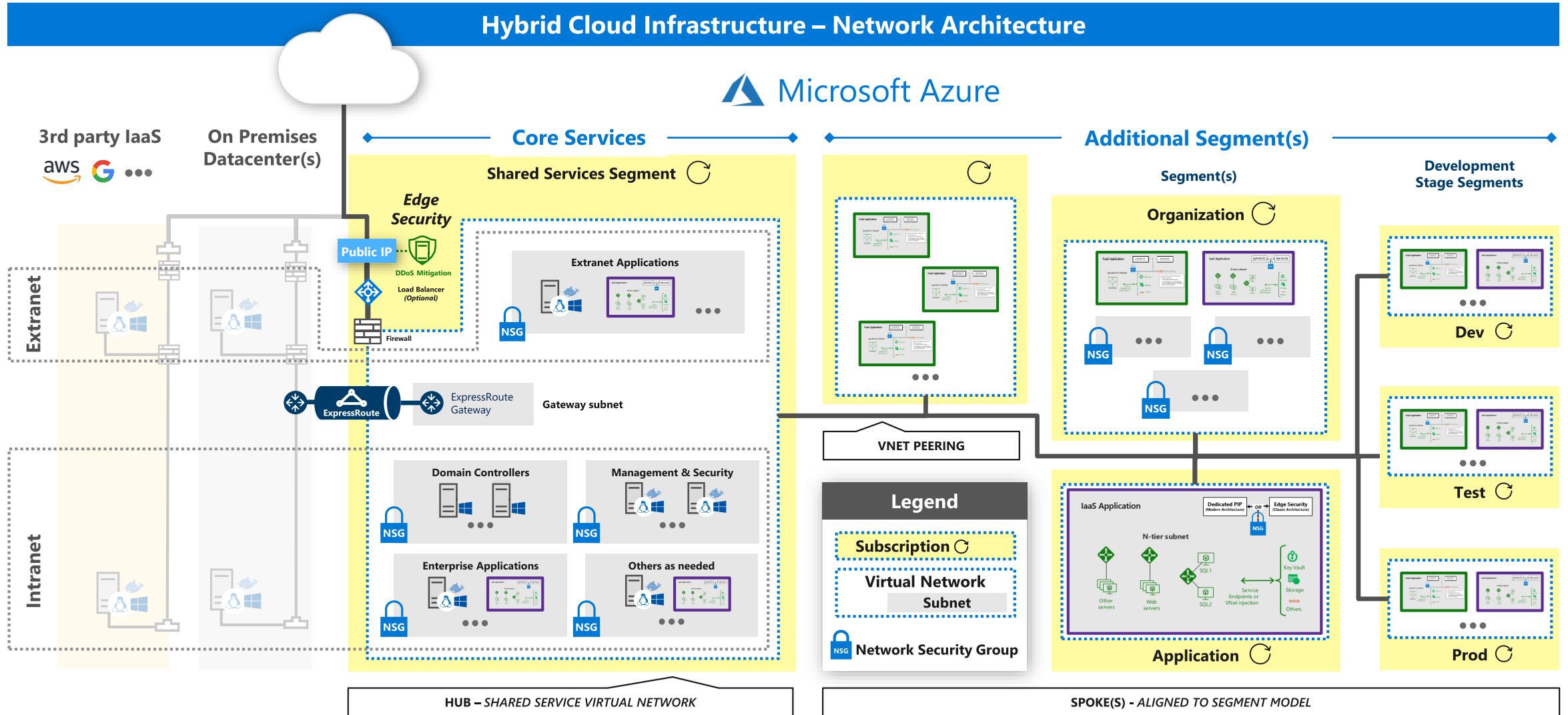
TIP Minimize Complexity - Always consider whether a segment is needed or whether security monitoring provides enough risk mitigation (each segments adds friction and overhead)



Reference Design - Azure Administration Model



Reference Enterprise Design - Azure Network Security



Monitor for Attacks

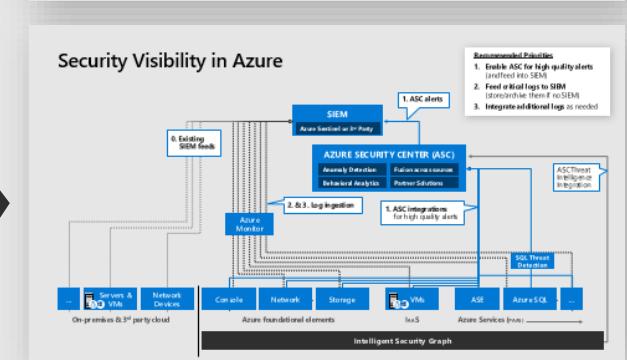
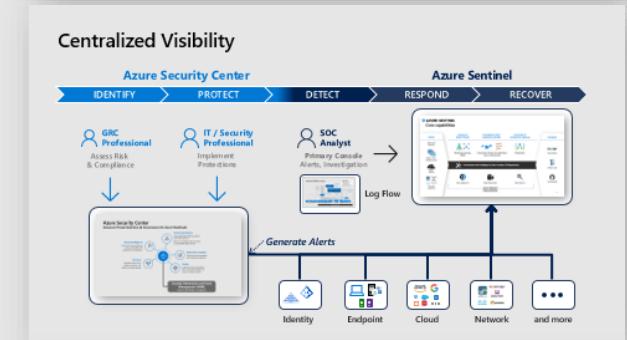
Back



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

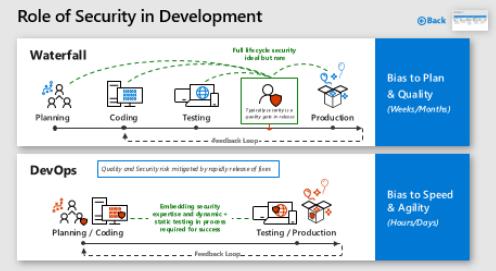
Back



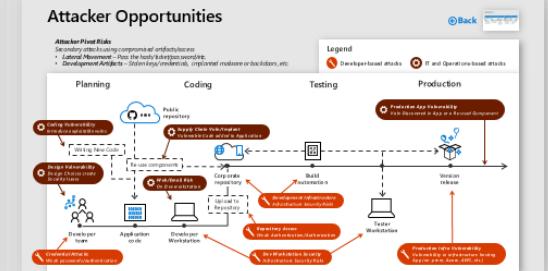
FOLLOW DEVOPS SECURITY GUIDANCE

- **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



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

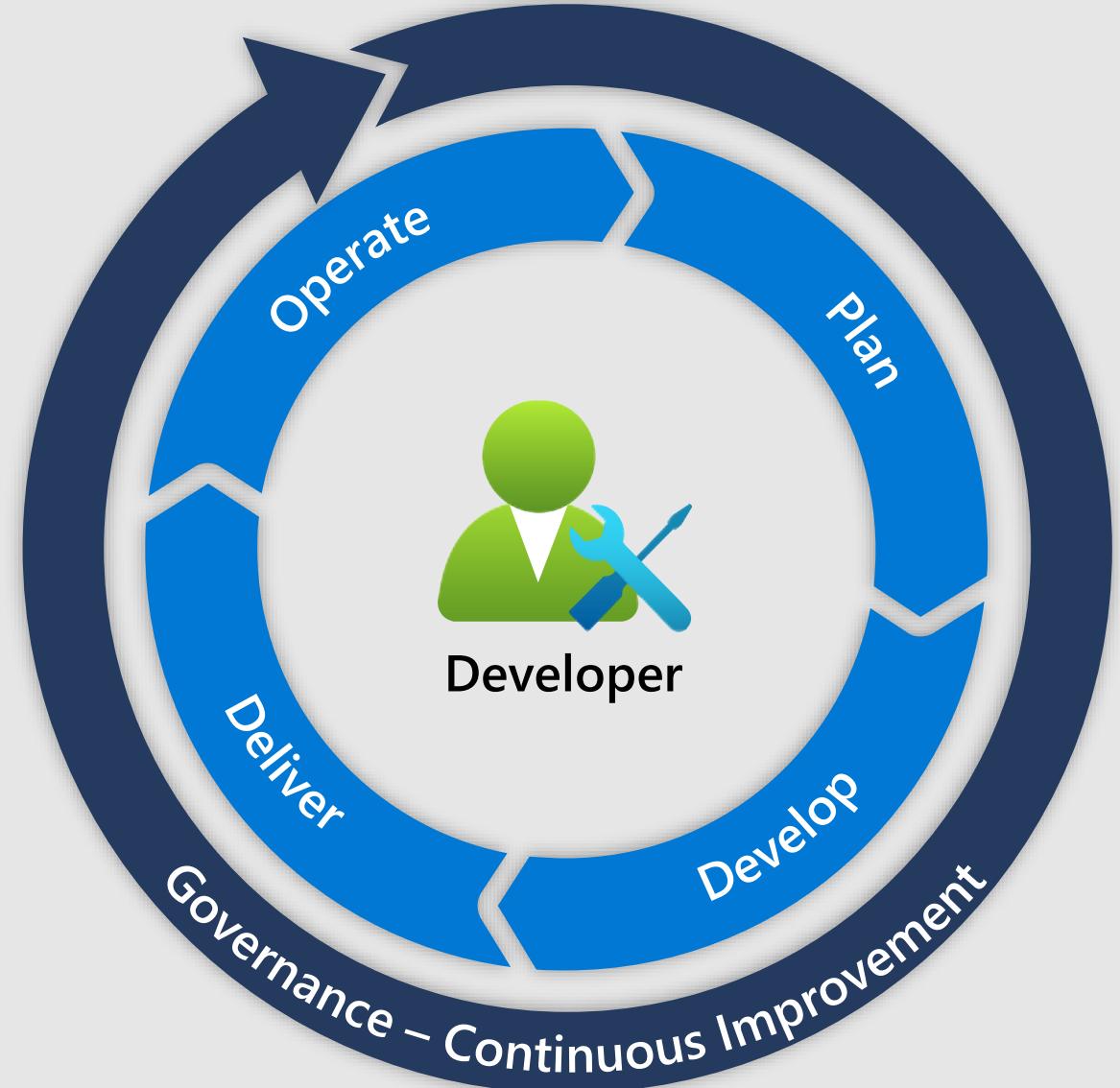
Reduce risk natively in Continuous Integration / Continuous Delivery (CI/CD) with real-time developer guidance, build checks, and more

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

Networks and Containment

CRITICAL BEST PRACTICES

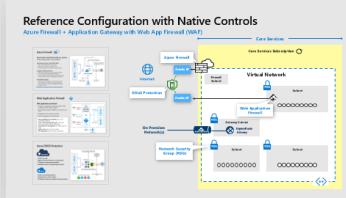
[Back](#)



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

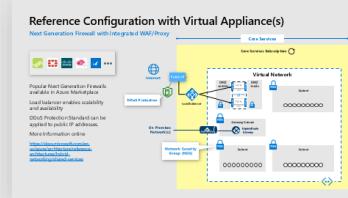


AZURE NATIVE CONTROLS

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

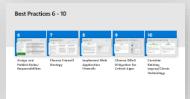
Network virtual appliances in the Azure Marketplace include familiar security tools that provide enhanced network security capabilities

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

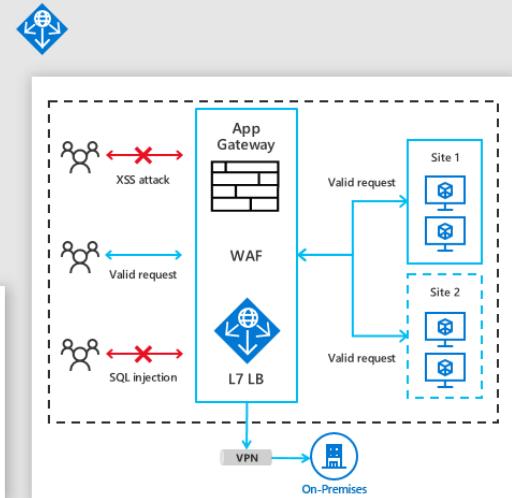
- What** – Configure web application firewalls (WAFs) to protect all internet facing applications
- Why** – Common security vulnerability types are often exploited by attackers targeting applications (either as an ingress point to the environment or as the ultimate objective).
WAFs are a critical mitigation 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.

Web Application Firewall

Web application protection

- Protects your application against prevalent XSS 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



Networks and Containment – DDoS Mitigations

[Back](#)



GENERAL GUIDANCE

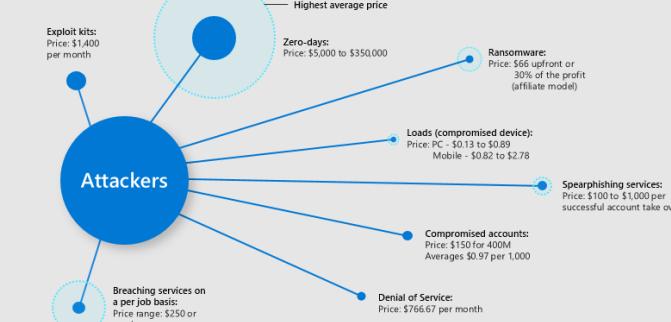


DDoS MITIGATIONS

- **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>



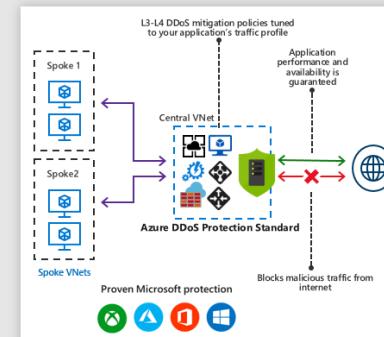
Azure DDOS Protection



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



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!