Microsoft Ignite
Top 10 Azure Security Best Practices

Mark Simos
Lead Cybersecurity Architect
Attack services are cheap

Exploit kits:
Price: $1,400 per month

Zero-days:
Price: $5,000 to $350,000

Ransomware:
Price: $66 upfront or 30% of the profit (affiliate model)

Loads (compromised device):
Price: PC - $0.13 to $0.89
Mobile - $0.82 to $2.78

Spearphishing services:
Price: $100 to $1,000 per successful account take over

Compromised accounts:
Price: $150 for 400M
Averages $0.97 per 1,000

Breaching services on a per job basis:
Price range: $250 or much more

Denial of Service:
Price: $766.67 per month

More details at https://aka.ms/CISOWorkshop
Exploit kits:
Price: $1,400 per month

Attack services are cheap

Ransomware:
Price: $66 upfront or 30% of the profit (affiliate model)

Zero-days:
Price: $5,000 to $350,000

Breaching services on a per job basis:
Price range: $250 or much more

Loads (compromised device):
PC - $0.13 to $0.89
Mobile - $0.82 to $2.78

Spearphishing services:
Price: $100 to $1,000 per successful account takeover

Compromised accounts:

Denial of Service:
Price: $766.67 per month

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

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 credential 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)

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**

**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

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
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
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.


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

**SUGGESTED PROCESS OWNERS**

<table>
<thead>
<tr>
<th>Monitor Secure Score</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Vulnerability Management (or Governance/Risk/Compliance team)</td>
<td></td>
</tr>
<tr>
<td>- Architecture Team</td>
<td></td>
</tr>
<tr>
<td>- Responsible Technical Team (listed below)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Improve Score Area</th>
<th>Responsible Technical Team</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compute and Apps Resources</strong></td>
<td></td>
</tr>
<tr>
<td>- App Services</td>
<td>- Application Development/Security Team(s)</td>
</tr>
<tr>
<td>- Containers</td>
<td>- Application Development and/or Infrastructure/IT Operations</td>
</tr>
<tr>
<td>- VMs/Scale sets/compute</td>
<td>- IT/Infrastructure Operations</td>
</tr>
<tr>
<td><strong>Data &amp; Storage Resources</strong></td>
<td></td>
</tr>
<tr>
<td>- SQL/Redis/Data Lake Analytics/Data Lake Store</td>
<td>- Database Team</td>
</tr>
<tr>
<td>- Storage Accounts</td>
<td>- Storage/Infrastructure Team</td>
</tr>
<tr>
<td><strong>Identity and Access Resources</strong></td>
<td></td>
</tr>
<tr>
<td>- Subscriptions</td>
<td>- Identity Team(s)</td>
</tr>
<tr>
<td>- Key Vault</td>
<td>- Information/Data Security Team</td>
</tr>
<tr>
<td><strong>Networking Resources</strong></td>
<td></td>
</tr>
<tr>
<td>- Networking Team</td>
<td>- Networking Team</td>
</tr>
<tr>
<td>- Network Security Team</td>
<td>- Network Security Team</td>
</tr>
<tr>
<td><strong>IoT Security</strong></td>
<td>- IoT Operations Team</td>
</tr>
</tbody>
</table>

**NOTE**: Each DevOps team may be responsible for their application resources.
Administration – Account protection
CRITICAL BEST PRACTICES

PASSWORDLESS OR MULTI-FACTOR AUTHENTICATION FOR ADMINS

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


- **How** –
  - Passwordless (Windows Hello) http://aka.ms/HelloForBusiness
  - 3rd Party MFA Solution

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

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)

**Key Related Item** is to increase administrator workstation security – http://aka.ms/secureworkstation
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, etc.) to understand and support it. This clarity reduces the number of new initiatives, one-offs, and workarounds that can lead to security vulnerabilities, operational down-time, or both.
- **How** – Select the segmentation approaches from the reference designs and assign permissions and network controls as appropriate.

TIP: Website Complexity: Always consider whether a segment can host a feature, module, or system. Consider the scope of application and business need (which segments A/B test and analyze).

A GOOD SEGMENTATION STRATEGY:

1. **Enables Operations** - Minimizes operational friction by aligning to business priorities and applications.
2. **Contains Risk** - Adds cost and friction to attackers by isolating sensitive workloads, decommissioning other assets - including high exposure systems from being used as a pivot to other systems.
3. **Is Migrated** - Security Operations should monitor for potential violations of high integrity of the segments (account activity, unexpected traffic, etc.)
Reference Design - Azure Administration Model
Monitor for 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

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

Different than Waterfall

Secure Both Dev & Ops

Securing DevOps:
Integrate security into the process

**Every Sprint**
Reduce risk proactively 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 modeling, 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**

**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*

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security</td>
<td>Typically existing network security team</td>
</tr>
<tr>
<td></td>
<td>Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.</td>
</tr>
<tr>
<td>Network Management</td>
<td>Typically existing network operations team</td>
</tr>
<tr>
<td></td>
<td>Enterprise-wide virtual network and subnet allocation</td>
</tr>
<tr>
<td>Server Endpoint Security</td>
<td>Typically IT operations, security, or jointly</td>
</tr>
<tr>
<td></td>
<td>Monitor and remediate server security (patching, configuration, endpoint security, etc.)</td>
</tr>
<tr>
<td>Incident Monitoring and Response</td>
<td>Typically security operations team</td>
</tr>
<tr>
<td></td>
<td>Investigate and remediate security incidents in SIEM or source console:</td>
</tr>
<tr>
<td></td>
<td>• Azure Security Center</td>
</tr>
<tr>
<td></td>
<td>• Azure AD Identity Protection</td>
</tr>
<tr>
<td>Policy Management</td>
<td>Typically GRC team + Architecture</td>
</tr>
<tr>
<td></td>
<td>Set direction for use of Roles Based Access Control (RBAC), Azure Security Center, Administrator protection strategy, and Azure Policy to govern Azure resources</td>
</tr>
<tr>
<td>Identity Security and Standards</td>
<td>Typically Security Team + Identity Team Jointly</td>
</tr>
<tr>
<td></td>
<td>Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards</td>
</tr>
</tbody>
</table>
Networks and Containment
CRITICAL BEST PRACTICES

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

**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.
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

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!