



# Microsoft CISO Workshop

## 4a - Threat Protection Strategy (IDENTIFY-PROTECT)

Microsoft Cybersecurity Solutions Group



# Session Outline

## 1. LIFE WITH THE CLOUD (AS SECURITY)

What is security like when fully on the Cloud?

What's gone?

What's new or changed?

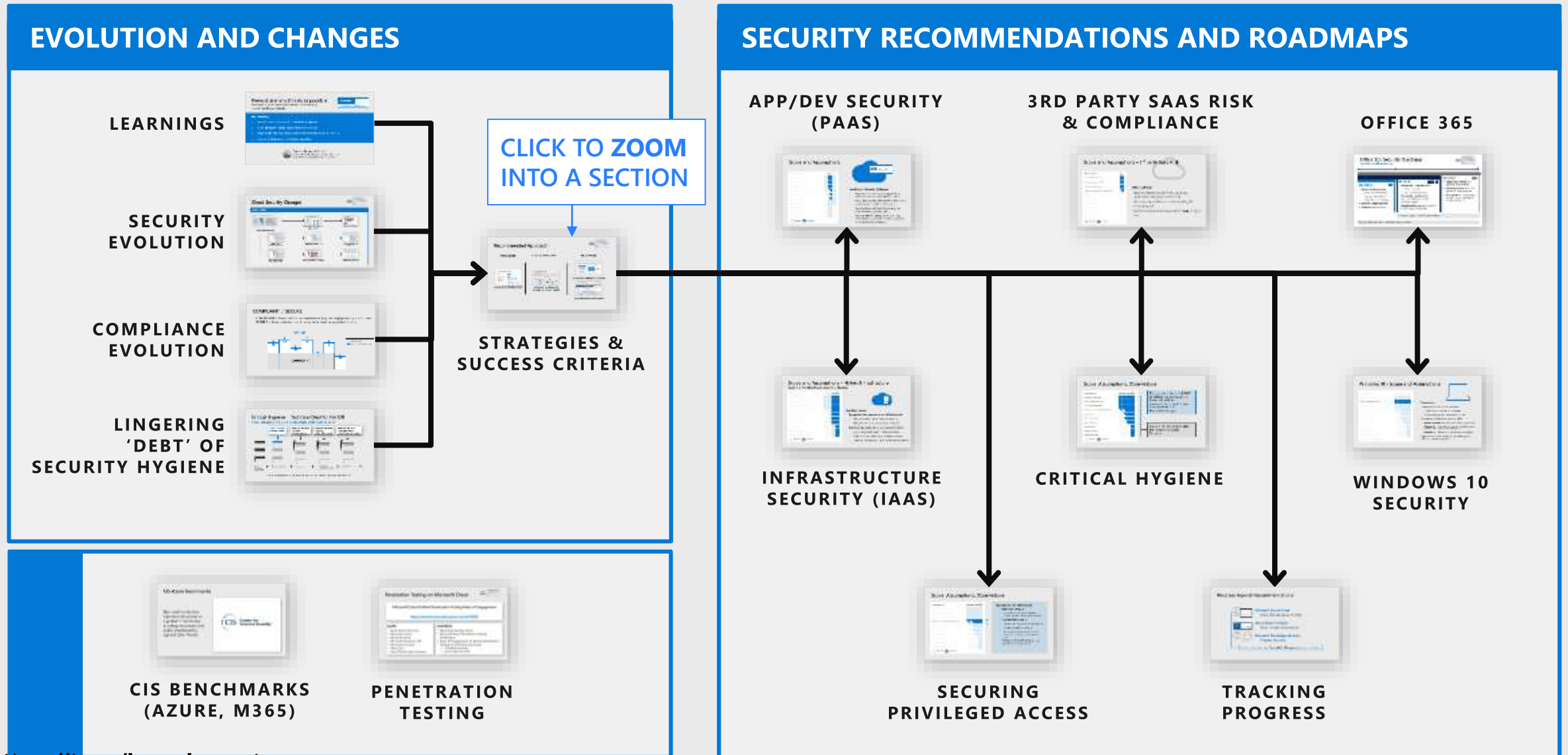


## 2. THE JOURNEY

How do I rapidly protect my cloud assets effectively?

How do I use the cloud to increase my security?

# (A) Threat protection – Identify and Protect



# Prevent as many threats as possible

Prevention raises attacker costs without 24x7 monitoring  
...but it can't block all attacks

Prevention

Detection and Response

## Key Learnings

1. Invest in preventive controls for **each attack phase**
2. Enable **hardware-based assurances** when available
3. Adopt **containment** strategies extensively (network, host, identity, etc.)
4. Integrate **Intelligence** and **Machine Learning**

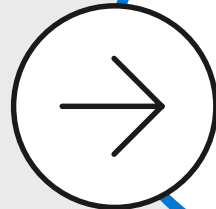


### Security Hygiene is Critical

Vulnerable software and configurations can undermine advanced security capabilities

# Integrate Cloud into a security strategy

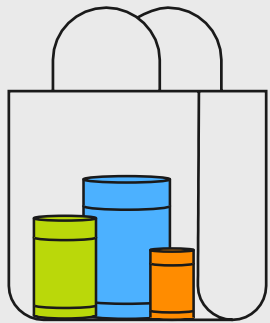
**Secure Platform**  
Protects assets in the cloud



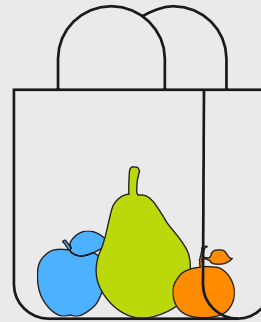
**Security Source**  
Protect assets using the cloud

# Keep everything fresh

As the pace of business, IT, and security changes



**From**  
Major changes  
planned for  
*months or years*



**To**  
Frequent  
adjustments in  
*weeks, days, or hours*

## Digital transformation requires agility from IT and Security

- Rapidly changing business needs
- Rapidly transforming technology (devices, IoT, threat intel, etc.)
- Rapidly changing threats

## Microsoft is investing to help security keep up

Journey **starts** with  
cloud (and integrated  
intelligence/guidance)



Continues with simplifying security tasks:

- **MAINTAIN IP ADDRESSES** (in filtering rules, etc.)
  - **Application Security Groups** abstraction
- **RAPIDLY SPIN UP/DOWN RESOURCES** (Virtual Machines, networks, etc.)
  - **Azure Security Center** – Identify and Correct Security Hygiene Issues
  - **Azure Policy** – Audit and enforce configuration policy
- **UPDATE OPERATING SYSTEM VERSIONS**
  - **Windows as a Service** (WaaS) for Windows 10 and Server 2016
- **DEPLOY AND SECURE OPERATING SYSTEMS** (patch, configuration, etc.)
  - Refactor applications to **Platform as a Service (PaaS)** technology

# Cloud Security Changes

MAIN MENU



## WHAT'S NEW

**Building a resilient cybersecurity program**

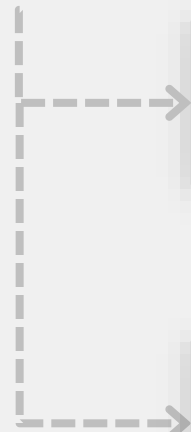
**Evolution of Visibility and Policy Enforcement**

**Security audit changing**

EVOLUTION OF VISIBILITY AND CONTROL

...AND USER CHOICE

### SHARED RESPONSIBILITY



**Security Responsibilities Transfer to Office 365**

OFFICE 365 RESPONSIBILITIES

**Office 365 Threats are different**

THREATS TO OFFICE 365

**Key Change**

"NO FIREWALL" IN OFFICE 365

**Security Responsibilities Transfer to Azure**

INFRASTRUCTURE RESPONSIBILITIES

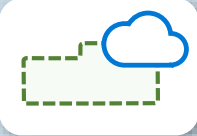
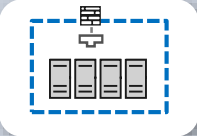
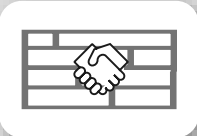
**Azure Threats - Mix of Old & New**

INFRASTRUCTURE THREATS

**Reference Enterprise Design - Azure Network Security**

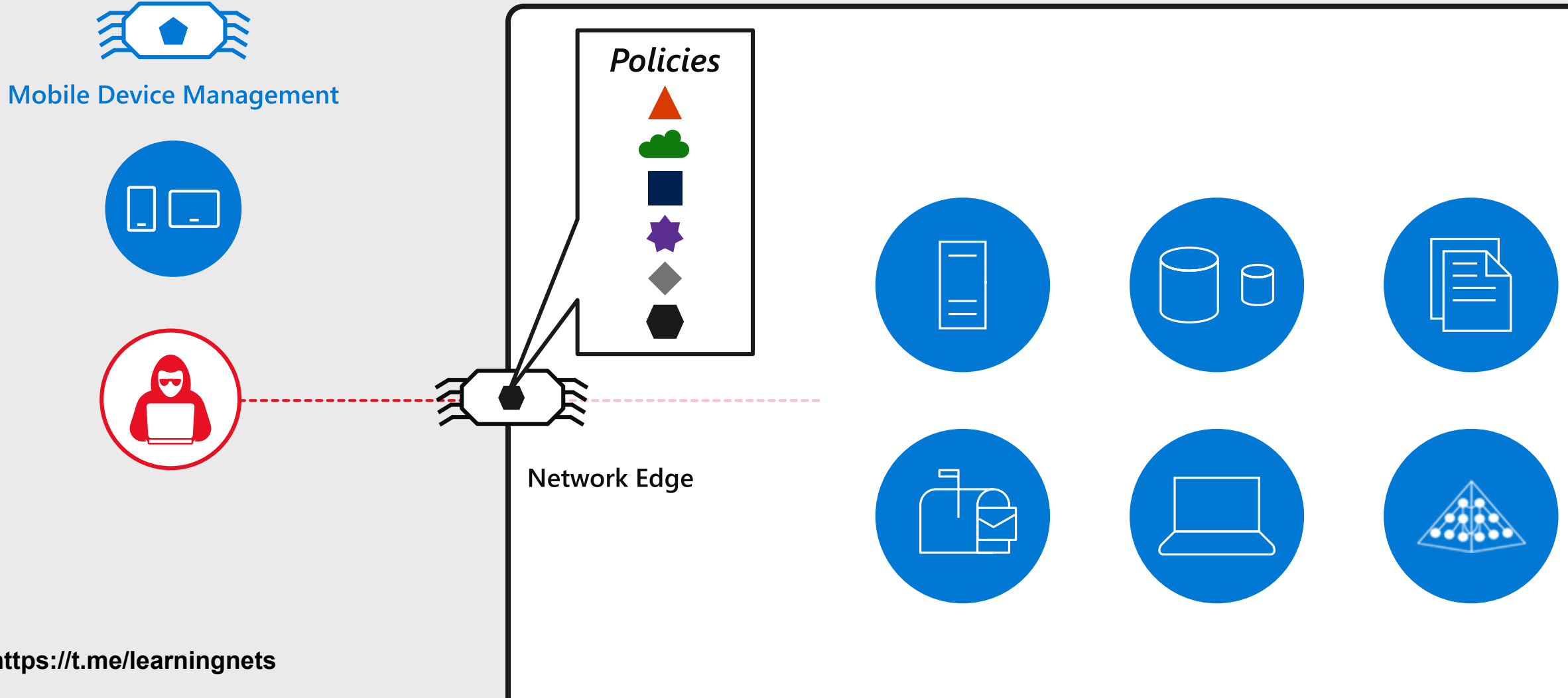
NETWORK SECURITY

# Building a resilient cybersecurity program

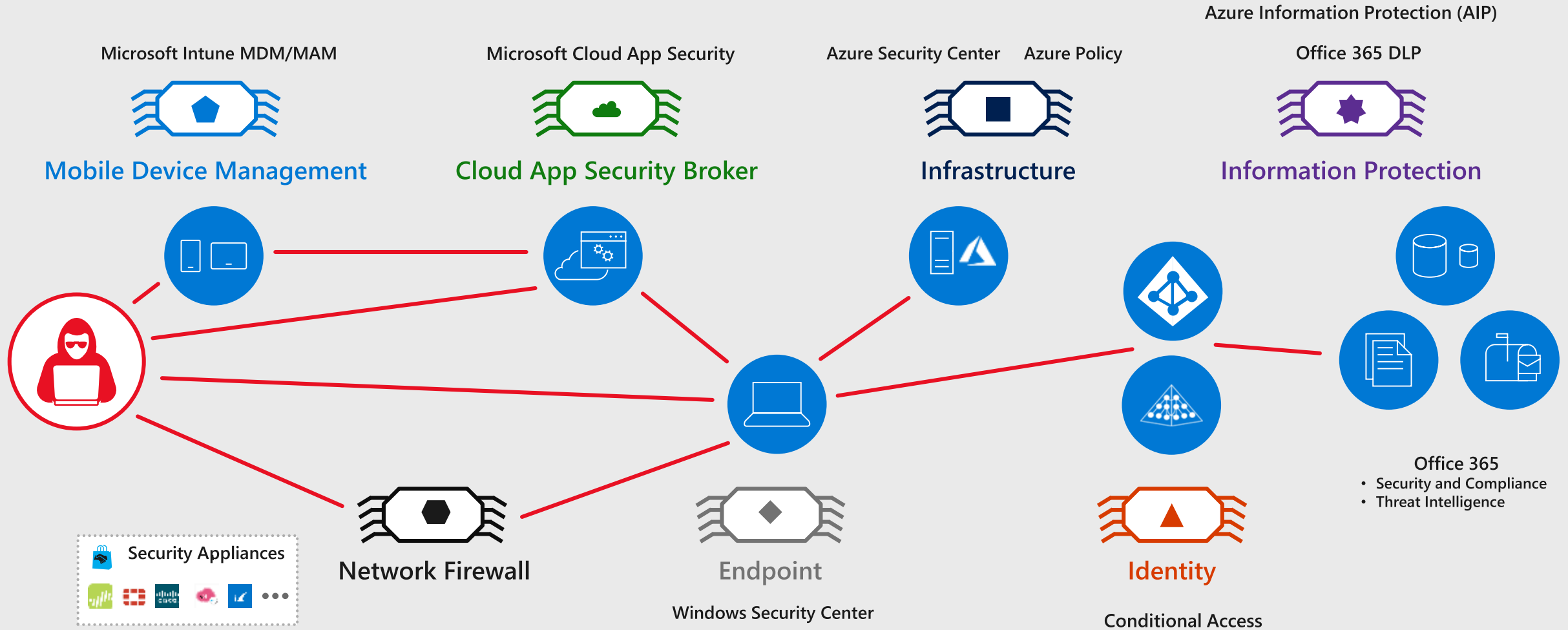
Responsibility	SaaS	PaaS	IaaS	On-prem		
Information and Data	Customer	Customer	Customer	Customer		<b>ALWAYS RETAINED BY CUSTOMER</b> <b>ESTABLISH A MODERN PERIMETER</b>
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer		
Accounts and Identities	Customer	Customer	Customer	Customer		
Identity and directory infrastructure	Customer	Customer	Customer	Customer		<b>VARIES BY SERVICE TYPE</b> <b>MODERNIZE INFRASTRUCTURE SECURITY</b> <b>(SECURITY OF DEVOPS + CLASSIC INFRA)</b>
Applications	Microsoft	Customer	Customer	Customer		
Network Controls	Microsoft	Customer	Customer	Customer		
Operating system	Microsoft	Microsoft	Customer	Customer		
Physical hosts	Microsoft	Microsoft	Microsoft	Customer		<b>TRANSFERS TO CLOUD PROVIDER</b> <b>"TRUST BUT VERIFY" EACH CLOUD PROVIDER</b>
Physical network	Microsoft	Microsoft	Microsoft	Customer		
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer		

Microsoft
  Customer

# Evolution of Visibility and Policy Enforcement



# Evolution of Visibility and Policy Enforcement



***Must shift to policy and controls tailored for each asset type***

# Security and IT changing

## SECURITY RISK – ELEVATED TO BUSINESS RISK (ONE OF MANY)



## IT – GOVERNANCE OUTPACED BY CLOUD RELEASE CYCLES

Users bypassing governance to get job done, forcing focus on security and productivity



### Outcomes

Integration with business to put security risk in context

Shadow IT and BYOD programs (discovery, evaluation, integration/transition)

Identity management and security across clouds and devices

# Cloud Changes Security

## DIFFERENT SECURITY MODEL

### SECURITY BENEFITS

- *Secure/consistent platform*
- *Better visibility, control, and threat detection*
- *Less direct responsibility*
- *Automated routine hygiene functions*
- *Easier compliance management/reporting*



### REQUIRES

- *Learn New Platform and Controls*
- *Learn shared responsibility model*
- *Increase Identity & Access hygiene*

## BIG CHANGES

### IDENTITY & ACCESS IS THE FRONT LINE

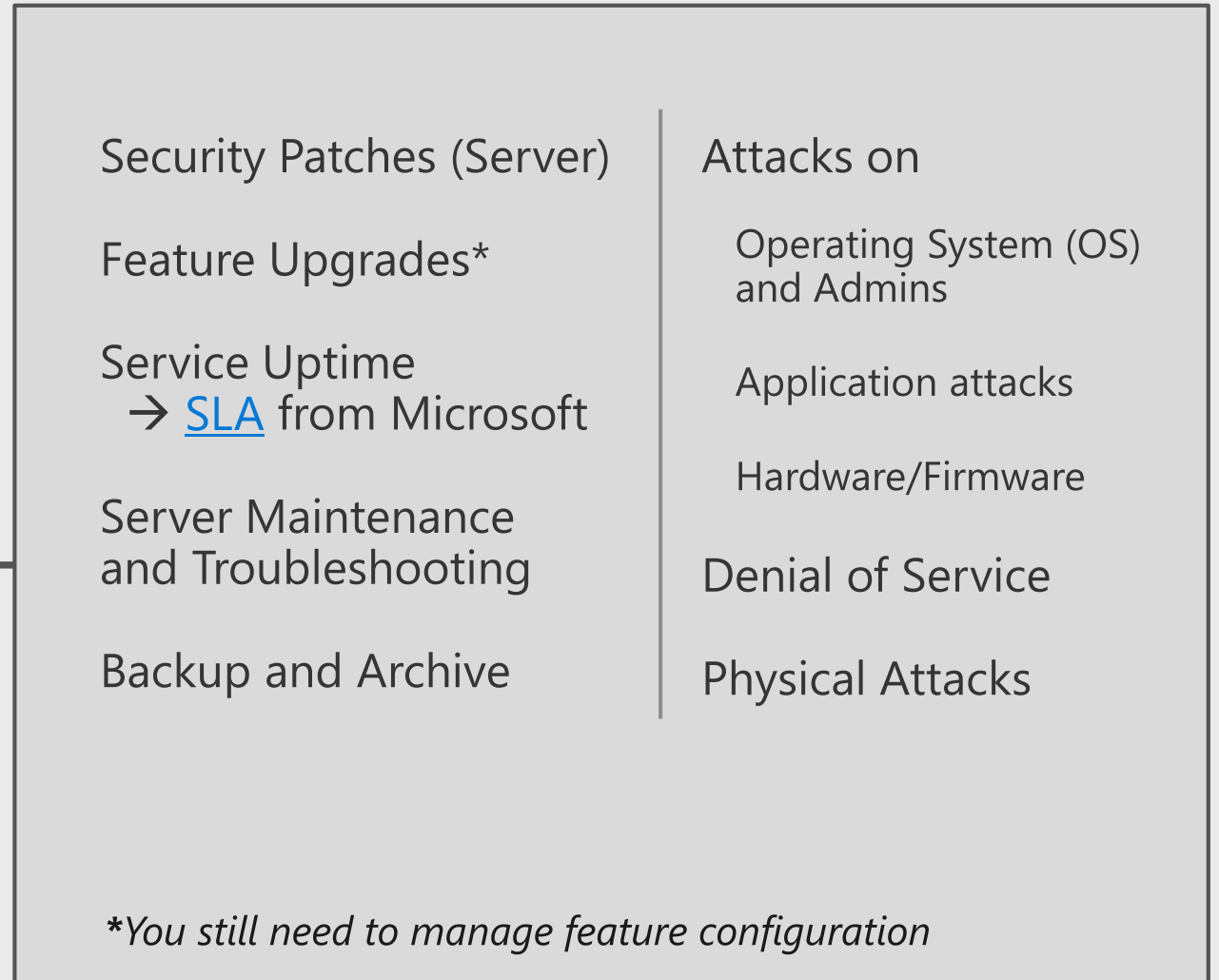
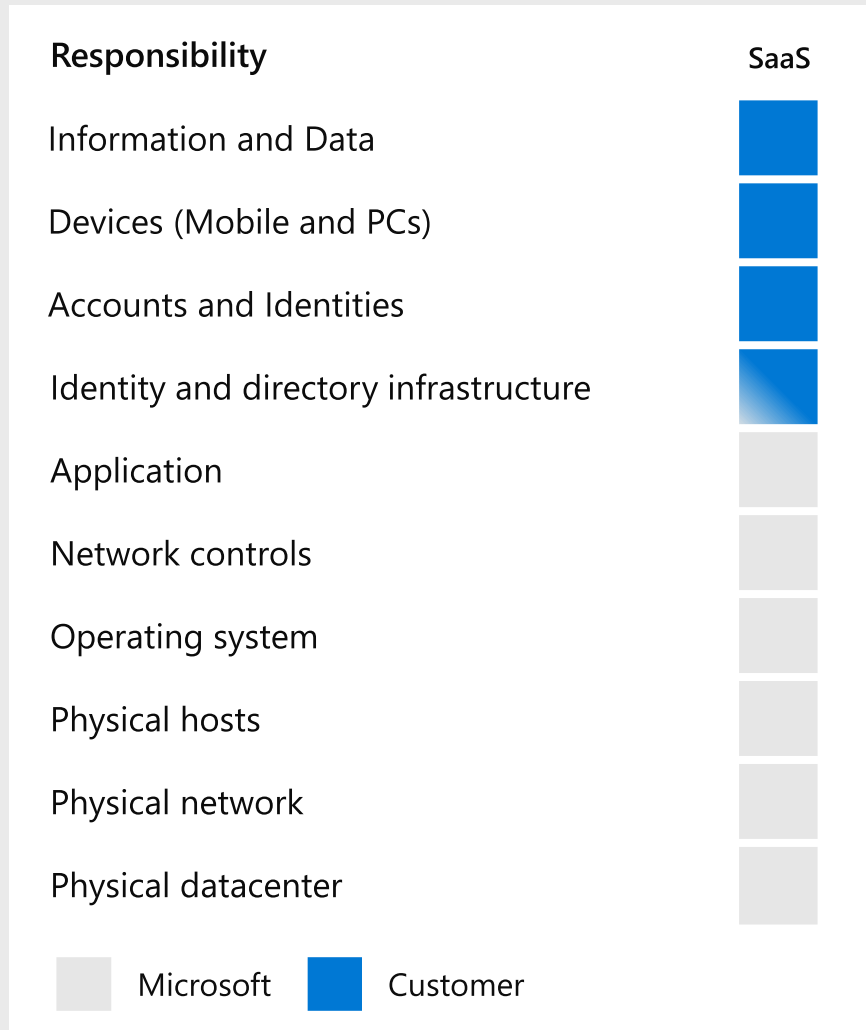
- Primary security perimeter for all workloads
- Firewalls/network still required for legacy workloads



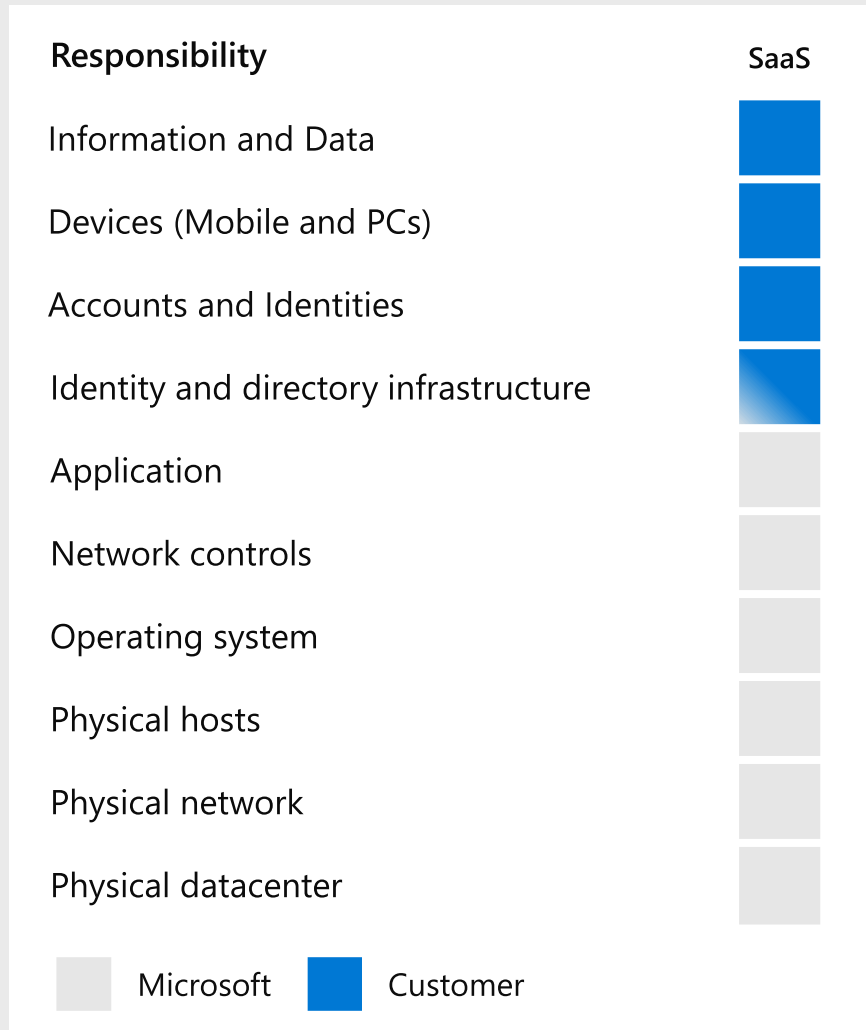
### NO PERMANENT PRIVILEGES

- Just in Time access for all resources
- Used to secure cloud platform and your tenant

# Security Responsibilities Transfer to Office 365



# Office 365 Threats are different



## Notable trends:

### 1. Identity Attacks

- Password spray →
- Brute force
- Password re-use



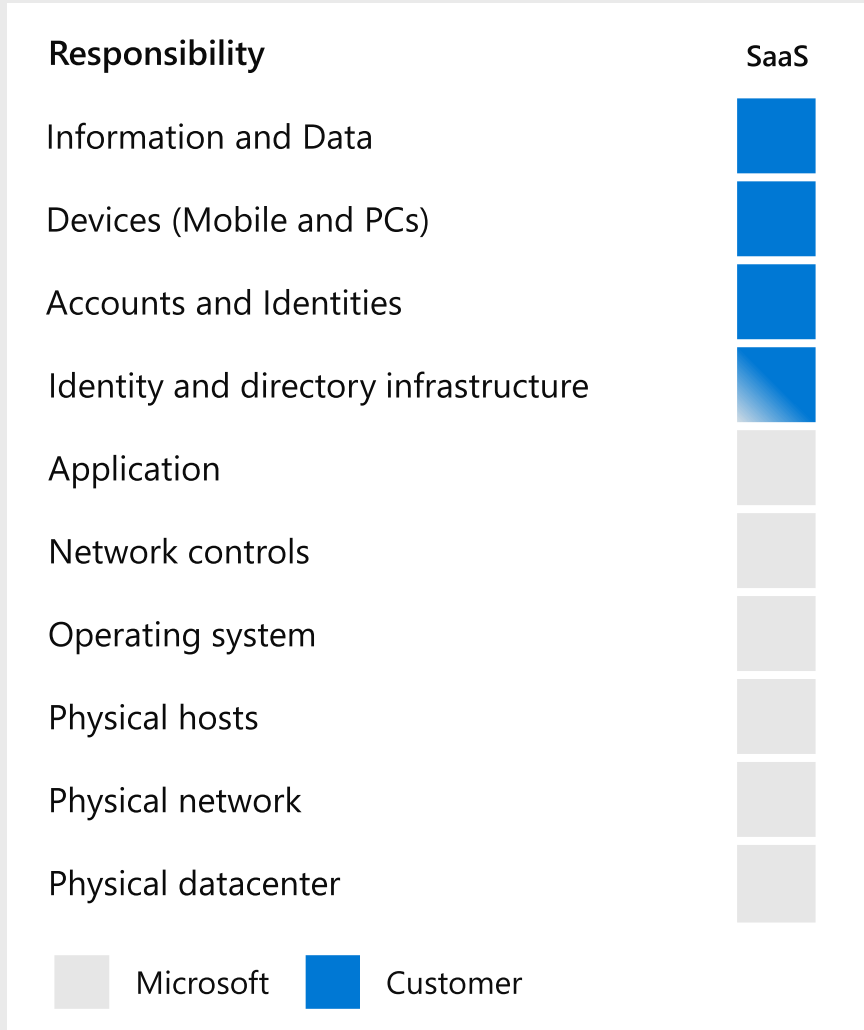
### 2. App/Data Layer Attacks

- Social engineering
- Delegation and forwarding rule attacks
- PowerShell scripts in attacks

### 3. Pivot from On-Premises

For more information, see <https://aka.ms/O365attacks>

# Key Change



## “No Firewall”

Service connected directly to Internet  
(users and **admin interfaces**)

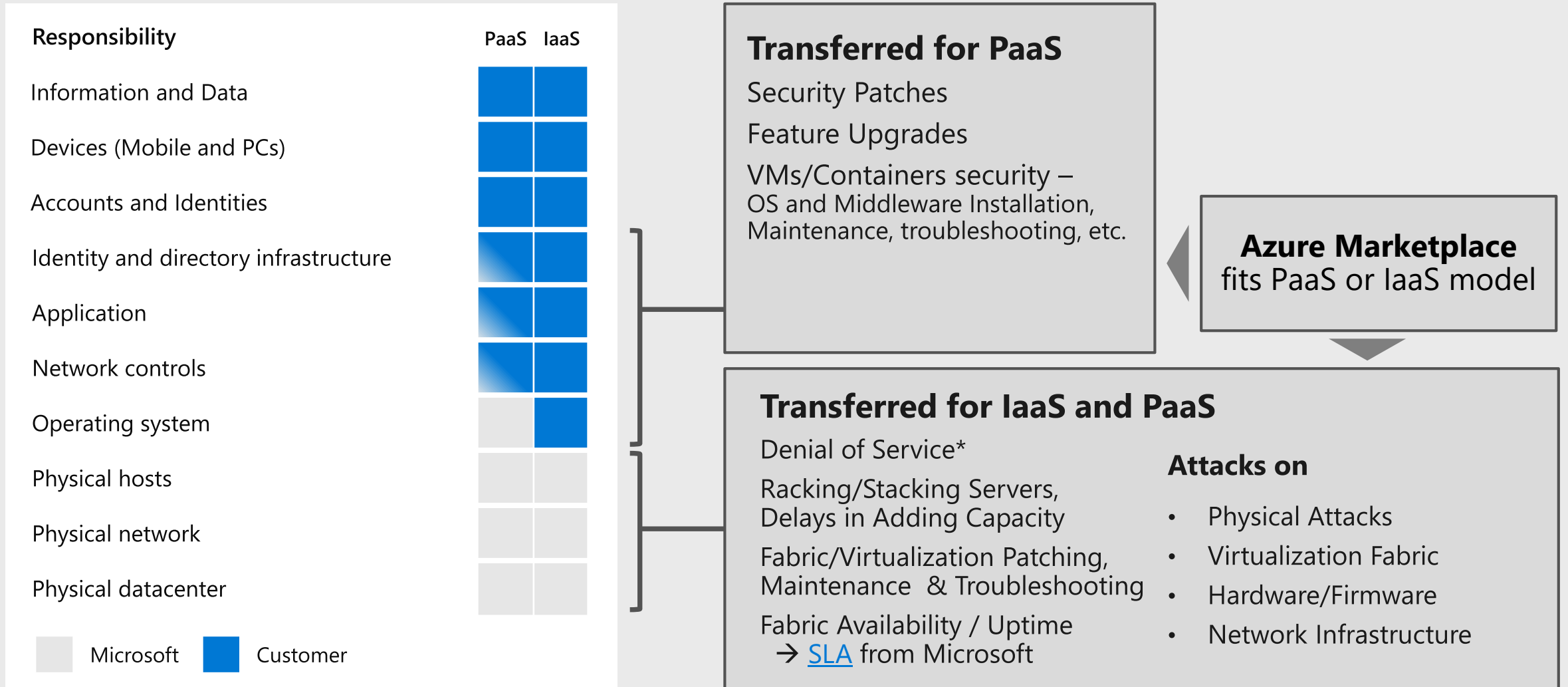
### Implications

#### 1. Authentication Security is Extremely Critical

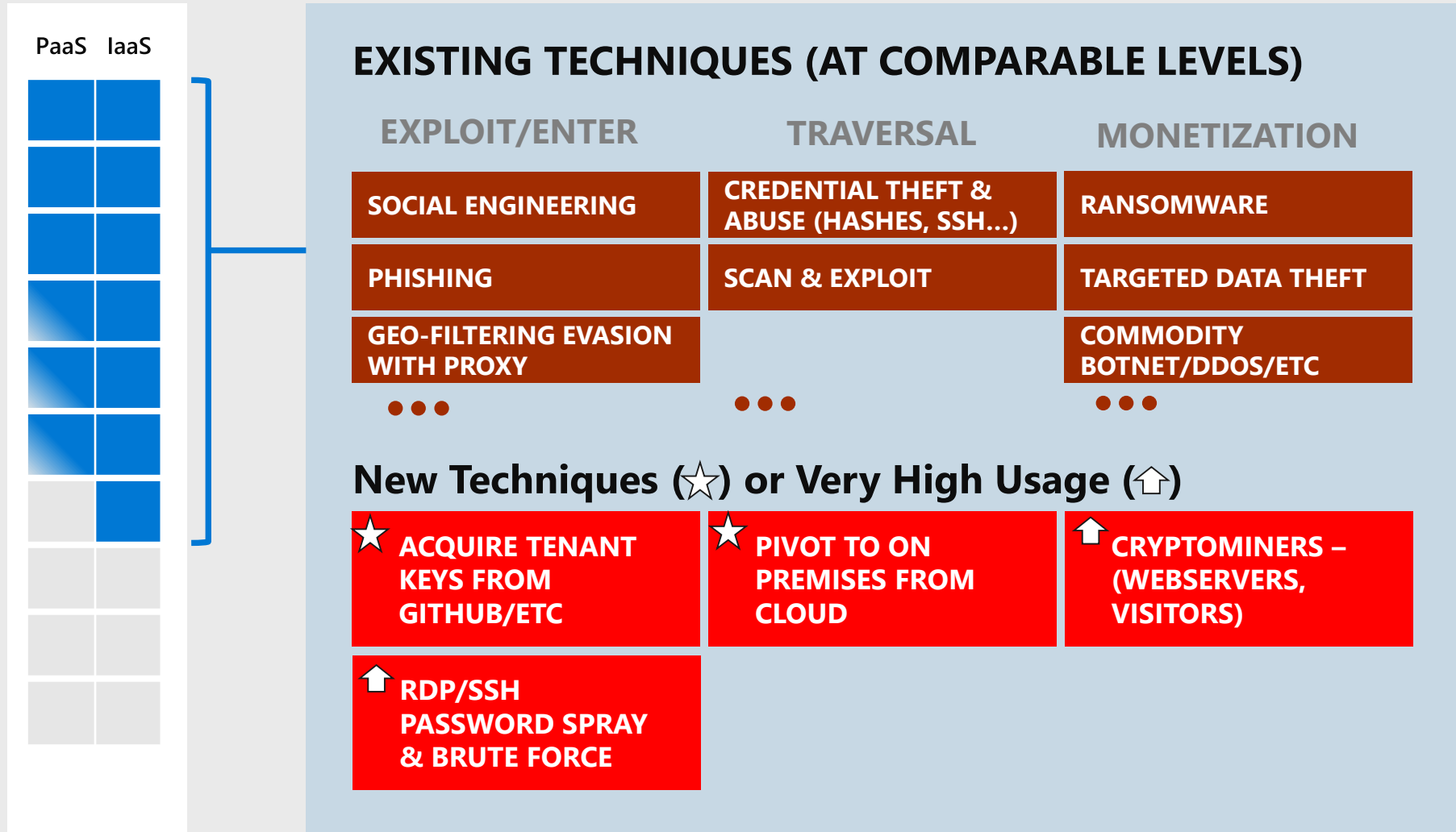
- Multi-factor authentication
- Anomaly detection using
  - User and Entity **Behavior** Analytics (UEBA)
  - **Context** awareness (time, date, geolocation)
- Integrated security **intelligence**

#### 2. Tenant Security Configuration is Critical

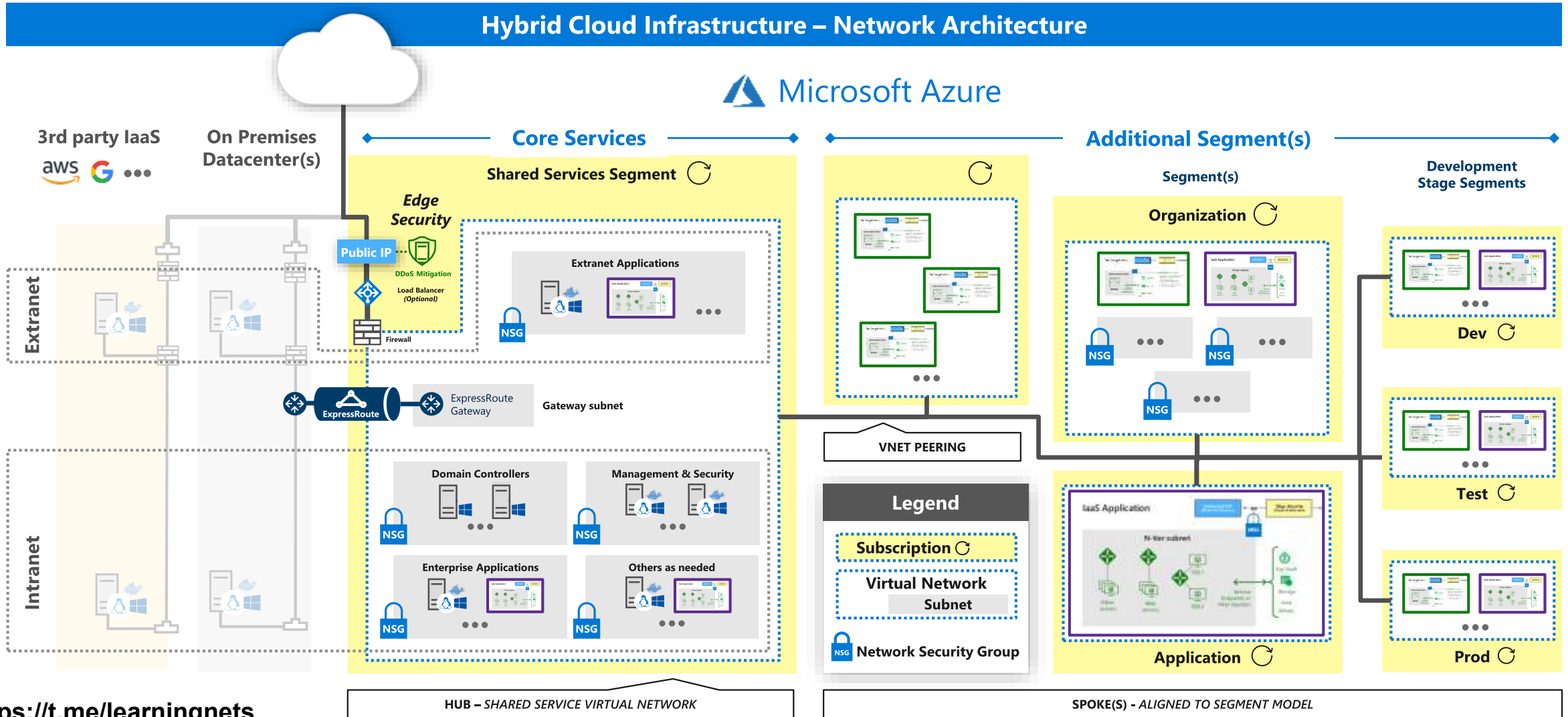
# Security Responsibilities Transfer to Azure



# Azure Threats – Mix of Old & New...



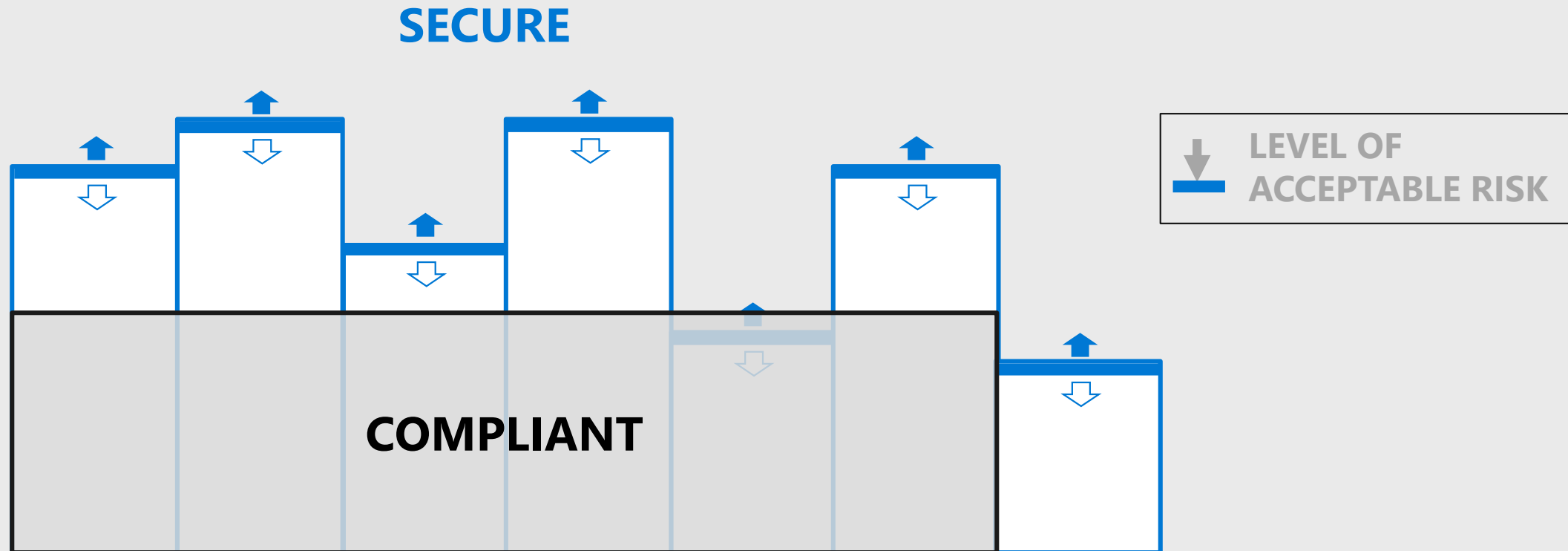
# Reference Enterprise Design - Azure Network Security



# COMPLIANT ≠ SECURE

**COMPLIANT** = Meets minimum requirement (e.g. not negligent) at point in time

**SECURE** = Raises attacker cost to acceptable level for expected attacks



# Security compliance is better in the cloud

Responsibility	SaaS	PaaS	IaaS
Information and Data	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer
Accounts and Identities	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Customer
Applications	Microsoft	Customer	Customer
Network Controls	Microsoft	Customer	Customer
Operating system	Microsoft	Microsoft	Customer
Physical hosts	Microsoft	Microsoft	Microsoft
Physical network	Microsoft	Microsoft	Microsoft
Physical datacenter	Microsoft	Microsoft	Microsoft

Legend:  Microsoft  Customer

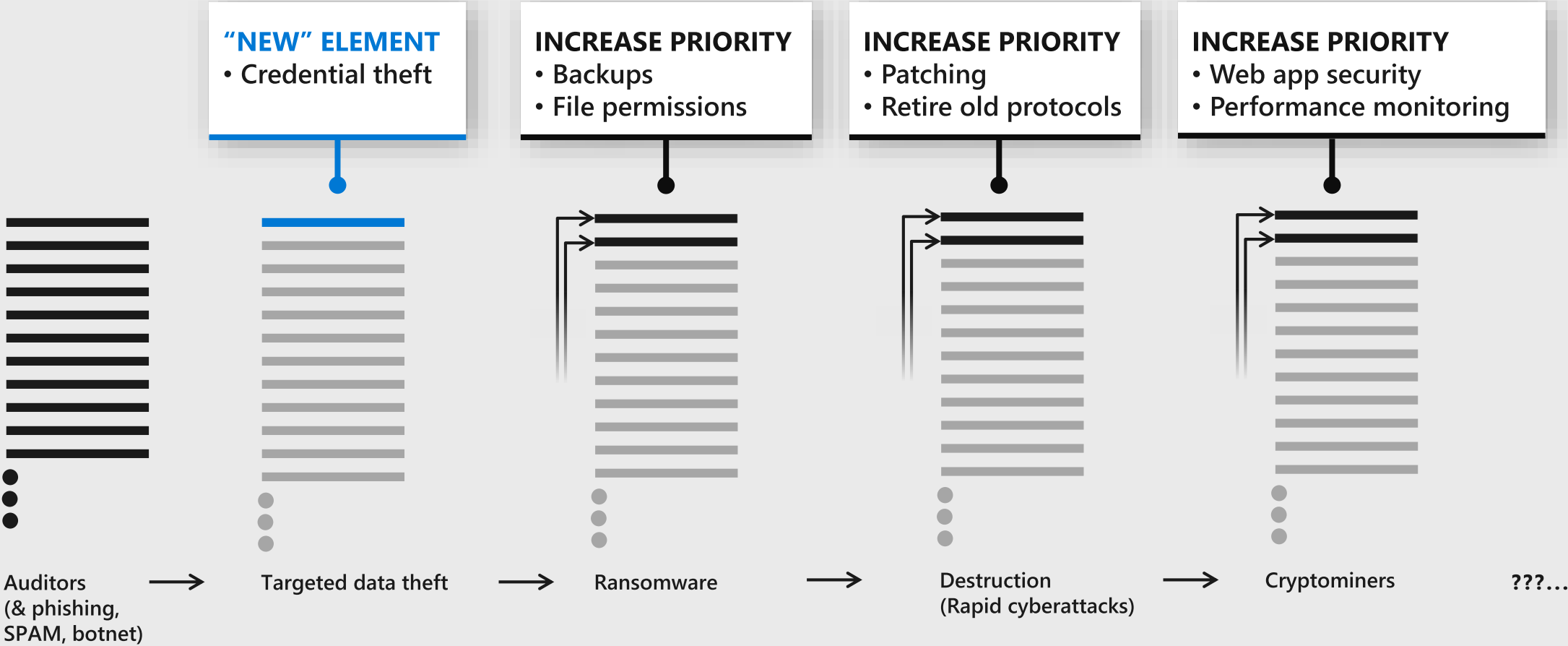
Automated tooling for continuous monitoring and reporting  
(e.g. Microsoft Compliance Manager)

Less responsibility  
(varies by workload)

Utilize Tooling and documentation from cloud provider  
(e.g. Microsoft Trust Center)

# Critical Hygiene = Technical Debt to Pay Off

Cloud can speed this up, but some hard work must be done



New monetization models just reshuffle priorities of same old hygiene debt

# Recommended Approach

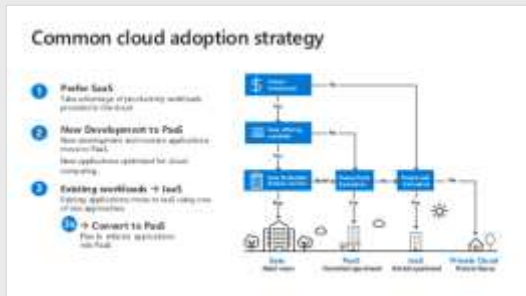
MAIN MENU



## STRATEGIES

## SUCCESS CRITERIA

## RESOURCES



### CLOUD ADOPTION STRATEGIES



### COVERAGE AND BALANCE ACROSS KILL CHAIN + ASSETS



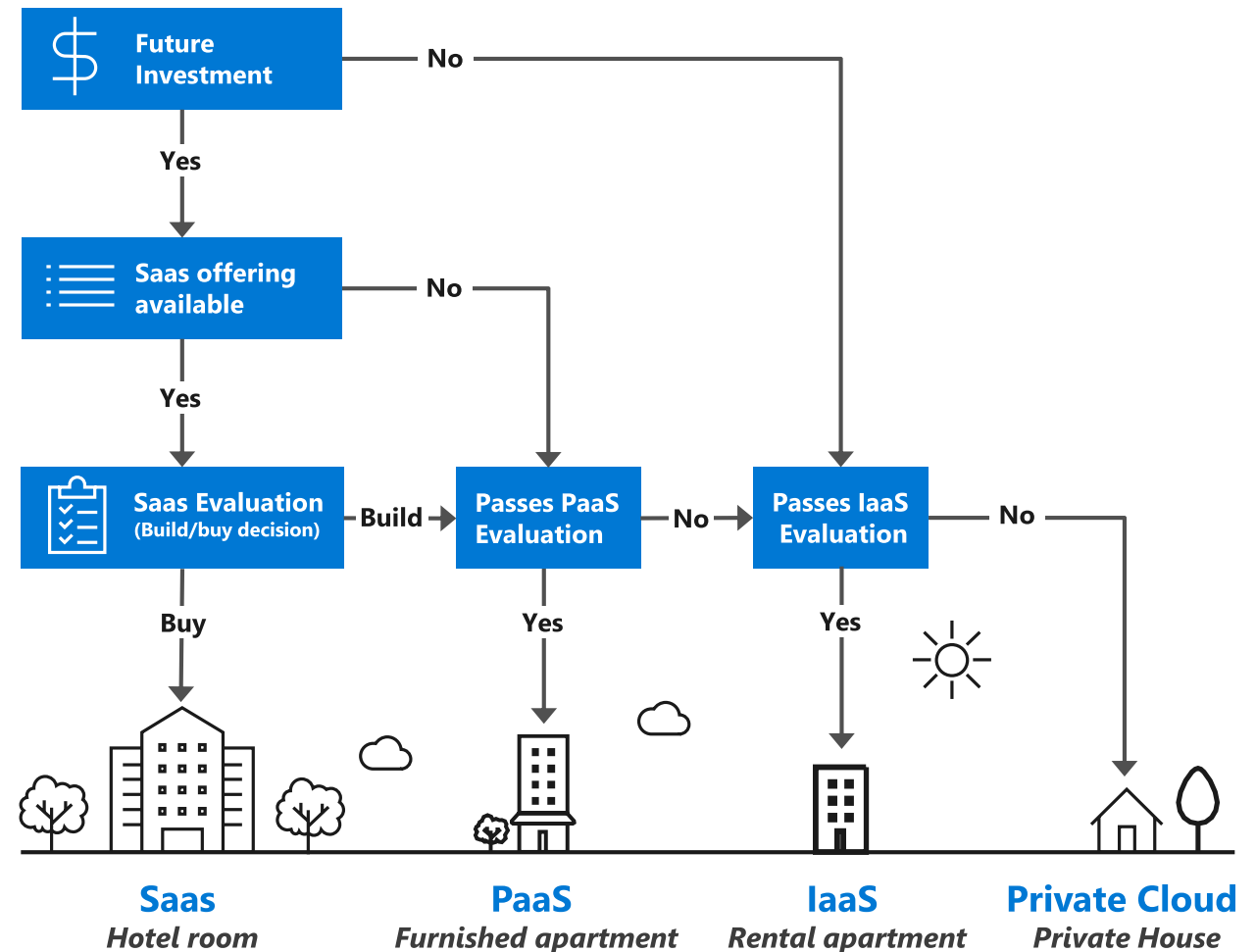
### MICROSOFT LEARNINGS & TOOLING



### RECOMMENDATION ROADMAPS

# Common cloud adoption strategy

- 1 Prefer SaaS**  
Take advantage of productivity workloads provided in the cloud
- 2 New Development to PaaS**  
New development and modern applications move to PaaS.  
New applications optimized for cloud computing.
- 3 Existing workloads → IaaS**  
Existing applications move to IaaS using one of two approaches:
  - 3a → Convert to PaaS**  
Plan to refactor applications into PaaS



# Balanced/Complete coverage

*Assess and prioritize using multiple perspectives*

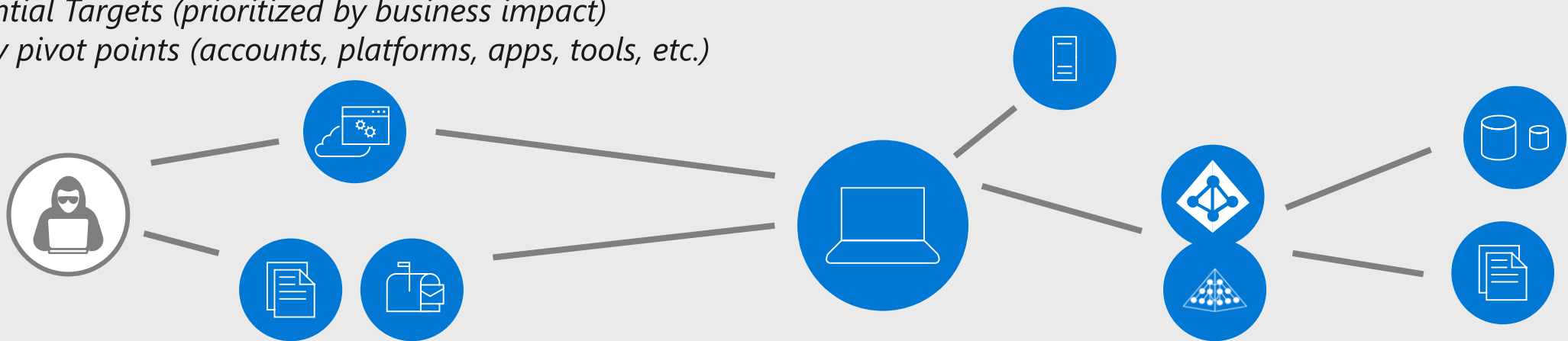
## Across Kill Chains

of Common Attack Profiles: **COMMODITY** | **TARGETED** | **RANSOMWARE** | **RAPID DESTRUCTION** | **COIN MINERS** | **MALWARE-LESS**

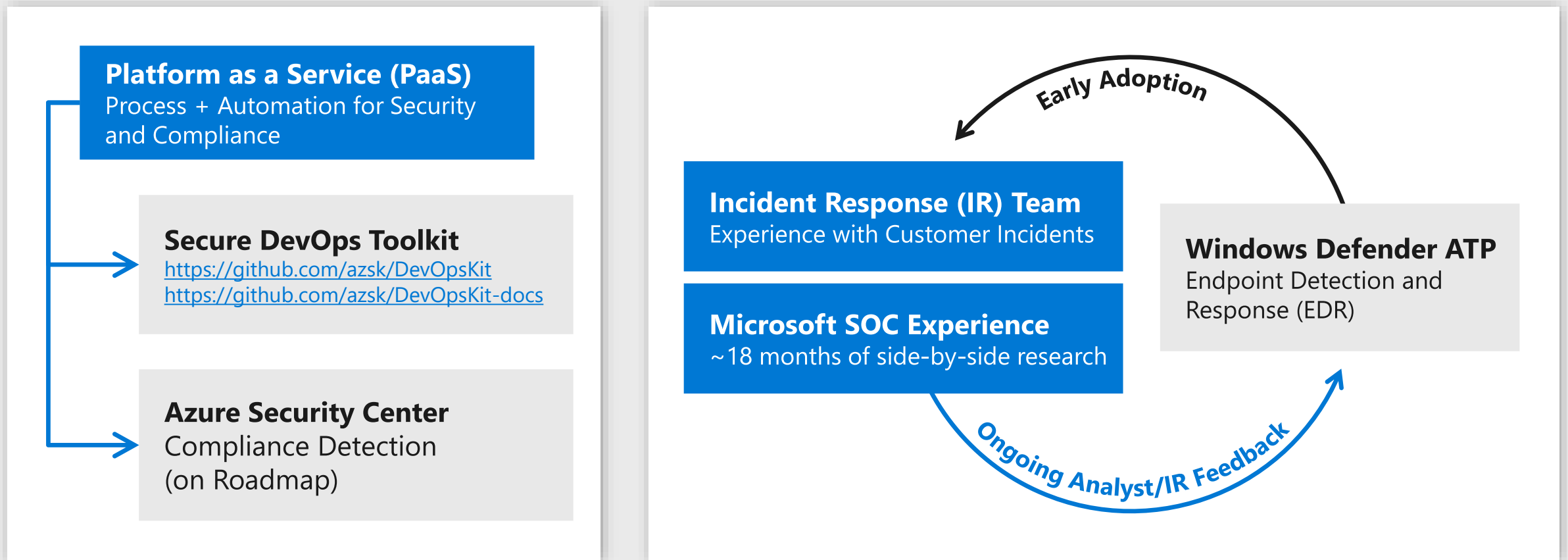


## Across Resources

- *Potential Targets (prioritized by business impact)*
- *Likely pivot points (accounts, platforms, apps, tools, etc.)*



# Inside-Out - Applying Microsoft Learnings (Examples)



# Roadmap Methodology

MAIN  
MENU



## 30 DAYS



**MEANINGFUL POSITIVE IMPACT**  
with zero or minimal:

- Risk of operational downtime
- Learning of new skillsets
- Tooling changes / deployment

## 90 DAYS



**SIGNIFICANT POSITIVE IMPACT**  
with limited investment into

- Operational impact testing
- Learning a new skillset (e.g. threat modeling)
- Detailed tasks such as reviewing code
- Deployment/configuration of tooling

## BEYOND



**SUSTAIN & IMPROVE POSTURE**

Long term investments that provide ongoing meaningful risk mitigation

## RECOMMENDATION ROADMAPS FOR PRIORITY AREAS (IN THIS MODULE)

### OFFICE 365

SECURITY PRIORITIES

### HYBRID INFRASTRUCTURE

INFRA AS A SERVICE (IAAS) + ON-PREMISES

### APPLICATION DEVELOPMENT

FOR PLATFORM AS A SERVICE (PAAS)

### 3RD PARTY SAAS

RISK & COMPLIANCE

### CRITICAL HYGIENE

RANSOMWARE + WANNACRYPT/PETYA

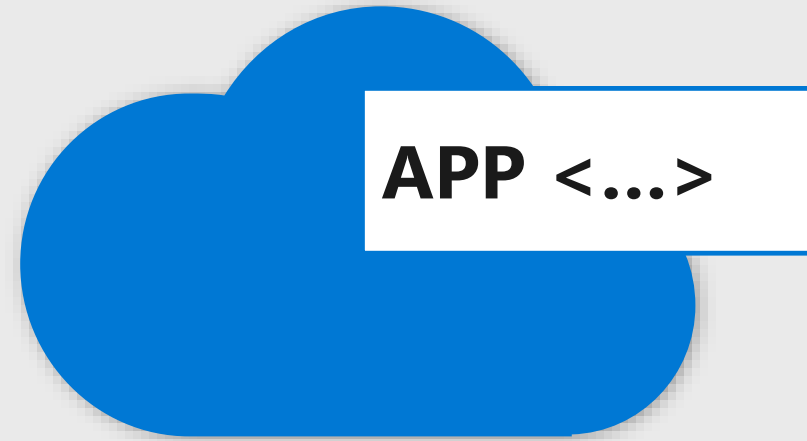
### PRIVILEGED ACCESS

LATERAL TRAVERSAL / PTH / ETC.

### DEVICE SECURITY

WINDOWS 10 + MOBILE

# Scope and Assumptions



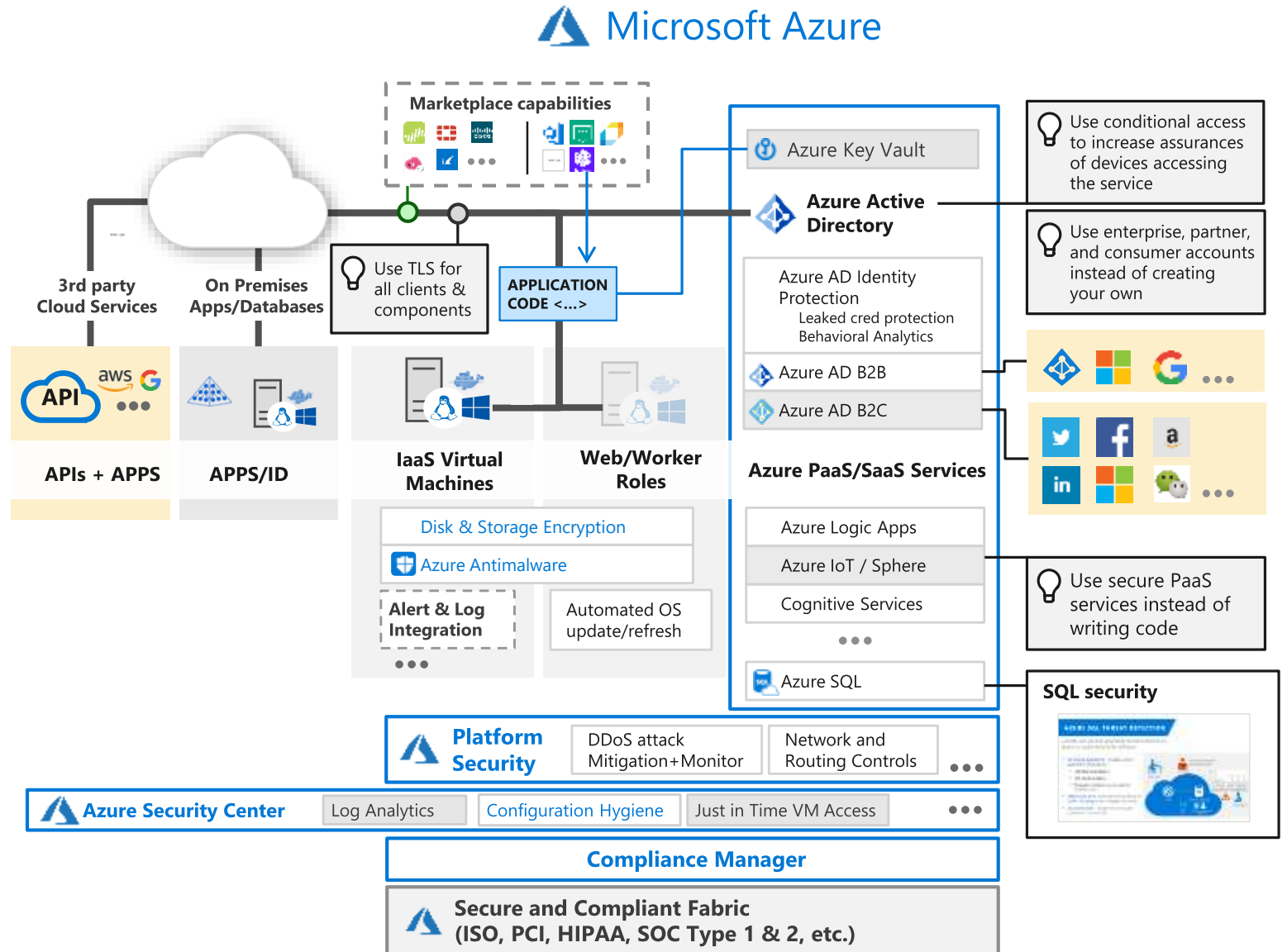
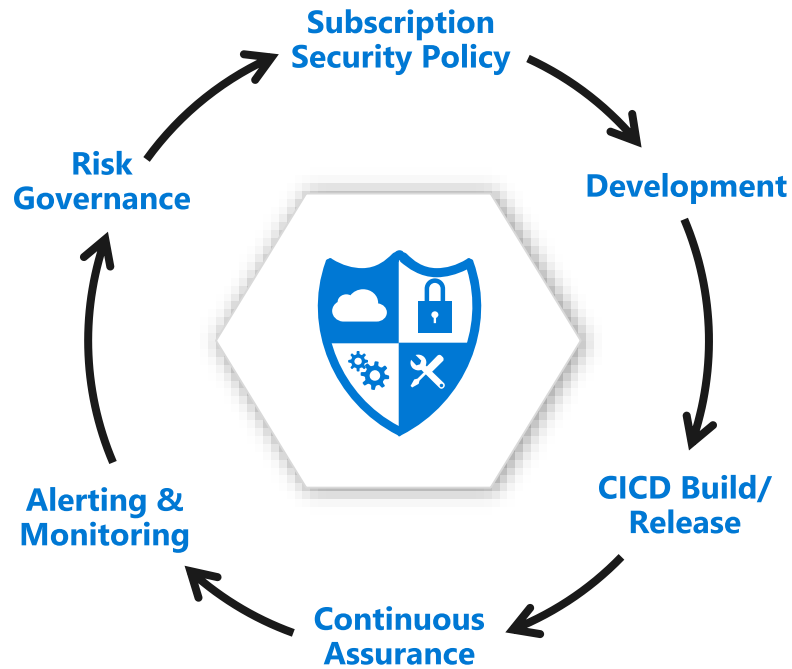
Responsibility	SaaS	PaaS	IaaS
Information and Data	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer
Accounts and Identities	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Customer
Applications	Customer	Customer	Customer
Network Controls	Customer	Customer	Customer
Operating system	Customer	Microsoft	Customer
Physical hosts	Customer	Microsoft	Customer
Physical network	Customer	Microsoft	Customer
Physical datacenter	Customer	Microsoft	Customer

Legend: ■ Microsoft ■ Customer

## Development Security Challenges

- Persistent poor security coding practices (which caused SDL and OWASP to exist)
- Many apps assembled from vulnerable open-source components and frameworks
- Security, Dev, and Ops still on journey to common language/principles
- **Cloud is New to Many** - PaaS (and IaaS) environments unfamiliar to many in security (and continuously changing)

# DevSecOps / PaaS Security Architecture



<https://azsk.azurewebsites.net/>

<https://t.me/learningnets>

# Practical Roadmap for PaaS Security

MAIN  
MENU



## 30 DAYS



1. Enable **Azure Security Center** & **SQL Threat Detection**
2. Mitigate basic coding errors with Web App Firewalls (WAFs) and Web vulnerability scanning
3. Discover and remediate exposed keys with **CredScan**  
<https://secdevtools.azurewebsites.net/helpcredscan.html>
4. Download and review documentation in **Secure DevOps Toolkit**  
<https://azsk.azurewebsites.net/>

## 90 DAYS



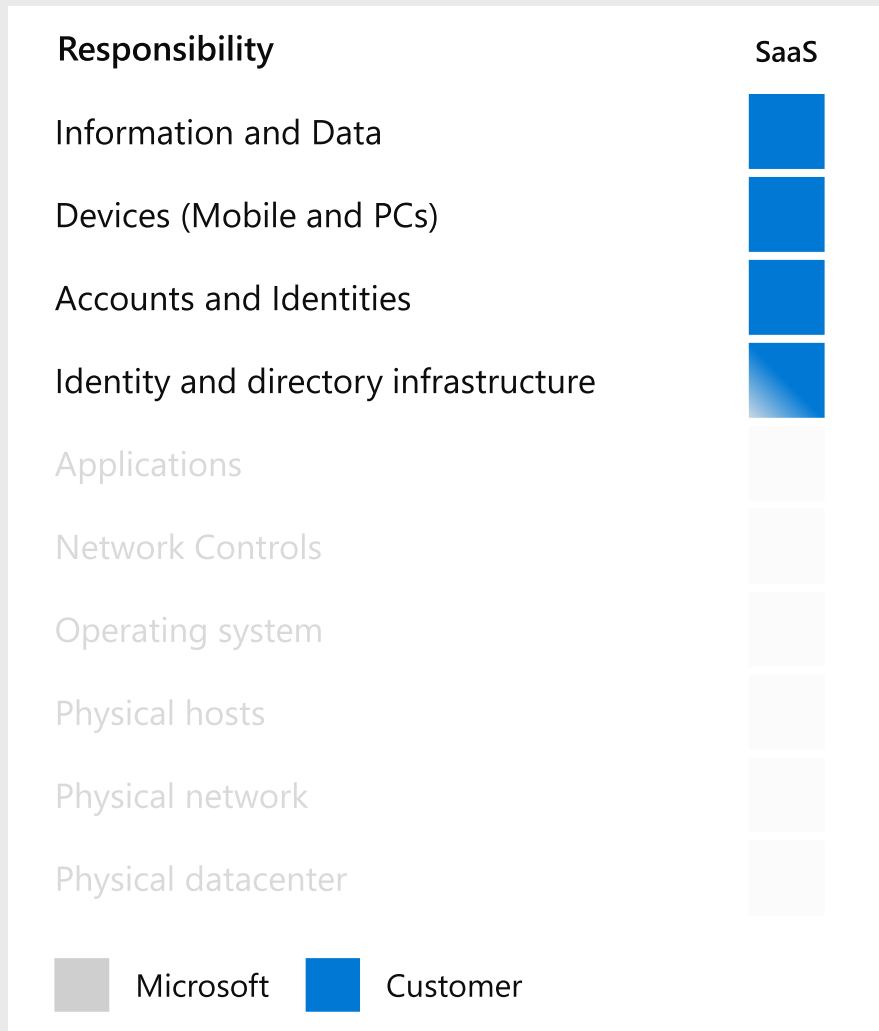
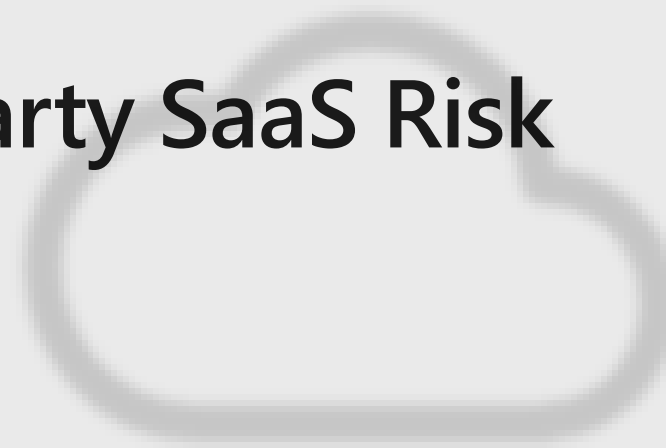
5. Deploy **Secure DevOps Toolkit** automation  
<https://azsk.azurewebsites.net/>
6. Encrypt all network traffic with TLS
7. Validate key & secret management
8. Build **Threat Model** for all critical apps
9. Define **AuthN best practices** for developers (use AAD/established ID providers, Tenant Admin Protections)
10. Validate all inputs and outputs to mitigate attacks like XSS, XSRF, SQL Injection
11. Validate data storage protections
12. Run static and dynamic analysis tools and fix critical bugs

## BEYOND



13. Build **Threat Model** process into new apps and major changes
14. **Cryptographic best practices** – Review code and ensure you are following best practices cryptography
15. **Push Left into CI/CD** with security education programs, enhanced tooling, and support processes for developers
16. Evaluate security of dependencies prior to inclusion (copy/paste 3<sup>rd</sup> party libraries, external module called by app, etc.)

# Scope and Assumptions – 3<sup>rd</sup> party SaaS Risk



## Observations

- 80% of employees admit to using non-approved SaaS apps in their jobs
- Security responsible for understanding & managing risk
- Must meet business requirements **and** mitigate risk

# Roadmap Outcomes

Rapidly discover and manage risk from SaaS applications with Cloud App Security

MAIN  
MENU



## 30 DAY S



### Learn about SaaS Usage & Risk

- **Identify App Usage** with snapshot reports and/or continuous upload
- **Tag apps** as already sanctioned or unsanctioned
- **Review risk scores** of unsanctioned apps to understand the risks
- **Report to stakeholders** on the risks of unsanctioned/risky app usage

## 90 DAYS



### Mitigate risk and Automate

- **User Communications** – Contact users of highly used unsanctioned apps to understand requirements
- **Sanction/Migrate/Acquire**– For highly used unsanctioned apps, choose whether to **sanction**, **migrate** to approved solution, or **acquire** alternate solution.
- **Automate app tagging** where possible using app discovery policies with risk factors/levels

## BEYOND



### Monitor and Refine

- **Monitor usage trends** of unsanctioned apps and the sanctioned alternatives
- **Block access** to unsanctioned apps at firewall/proxy with MCAS block scripts or another control (GPO or MDM policy)
- **Monitor effectiveness** of security policy – Work with users and business leaders on evolving requirements, impact on business

Report risk reduction to stakeholders

Communicate Changes to Affected users

# Office 365 Security Roadmap

<http://aka.ms/o365secroadmap>

MAIN  
MENU



## 30 DAYS



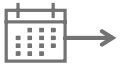
- **Rapid Configuration**
  - Basic admin protections
  - Logging and Analytics
  - Basic Identity Protections
- **Tenant Configuration**
- **Prepare** stakeholders

## 90 DAYS



- **Advanced Protections** for
  - Admin Accounts
  - User Accounts and Data
- **Customize roadmap** for your compliance, threat, and user needs
- **Adapt and implement** default policies and protections

## BEYOND



- **Adjust and refine** key policies and controls
- **Extend protections** to on premises dependencies
- **Integrate** with business and security processes (legal, insider threat, etc.)

Monitor Logs via SIEM (if applicable)

Regularly Review Alerts and Upcoming Updates  
<https://t.me/learningnets>

# 30 DAY Plan



## THREAT PROTECTION

### Admins

- Separate Admin Account
- Enforce MFA for admins
- Highly Secure Productivity Device

Windows 10 guidance <http://aka.ms/HighSecWin10>

### Tenant / All Users

- Enable logging + anomaly detection  
[Logs](#) → [Cloud App Security](#) → [SIEM](#)



## INFORMATION PROTECTION

- Evaluate example Information Protection policies  
<https://aka.ms/O365DataPolicy>
- = Start preparation for action in 90 day plan



## IDENTITY AND ACCESS MANAGEMENT

- [Enable Azure AD Identity protection](#)  
*Ensure passwords hashes are synchronized to Azure AD*
- If Federated, enforce account security (Password length / age / complexity, etc.)
- Evaluate example conditional access policies  
<https://aka.ms/O365IdentityPolicy>



## SECURITY MANAGEMENT

Configure Advanced Threat Protection for Email/Collaboration, Roles, Policies, tenant security settings, and Microsoft Cloud App Security (MCAS) –  
<https://aka.ms/O365TenantSecurity>

Regularly Review Alerts (MCAS, Threat Dashboard) and Upcoming Changes ([Roadmap](#) | [Blog](#) | [YouTube](#) )

# 90 DAY Plan



## THREAT PROTECTION

### Admins

- Privileged Access Workstation <http://aka.ms/cyberpaw>
- Configure Azure AD PIM

### Tenant / All Users

- Configure SIEM to collect *logs* from Identity Federation and Office 365



## INFORMATION PROTECTION

- **Adapt and Implement** Information Protection policies <https://aka.ms/O365DataPolicy>



## IDENTITY AND ACCESS MANAGEMENT

- Enable and Enforce **Multi-factor Authentication** for all users
- **Adapt and Implement** Conditional Access policies <https://aka.ms/O365IdentityPolicy>



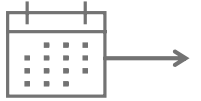
## SECURITY MANAGEMENT

### Plan actions for your unique security needs using:

- **Secure Score** – Identify important actions and low hanging fruit <https://seurescore.microsoft.com>
- **Sharing Risks** – Use MCAS to identify oversharing of sensitive/internal documents
- **Threat Intelligence** – Conduct Attack Simulation + Industry Trends
- **Compliance Status** – Compliance manager (GDPR, NIST 800-171) <https://servicetrust.microsoft.com/ComplianceManager>

Regularly Review Alerts (MCAS, Threat Dashboard, SIEM) and Upcoming Updates

# ...And BEYOND



## THREAT PROTECTION

### Admins

- SPA roadmap for on premises AD  
<http://aka.ms/SPARoadmap>

### Tenant / All Users

- Integrate Microsoft Cloud App Security (MCAS) into
  - Insider threat program
  - Shadow IT GRC risks/program



## INFORMATION PROTECTION

- Integrate AIP into insider threat risk strategy
- Refine Information Protection policies
  - Office 365 DLP
  - CASB policies and alerts
  - Data Encryption Solution



## IDENTITY AND ACCESS MANAGEMENT

- Refine policies and operational process
- Integrate alerts on user behavior in with insider threat program (from Azure AD Identity Protection or other capability)



## SECURITY MANAGEMENT

- **Secure Score** – Continue Planning Next Actions
- **eDiscovery** – Integrate into legal and threat response processes

Regularly Review Alerts and Upcoming Updates

# Scope and Assumptions – Hybrid Infrastructure

## *Securing Workloads on Legacy Architecture*

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	Customer	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and Identities	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Customer	Customer
Applications	Customer	Customer	Customer	Customer
Network Controls	Customer	Customer	Customer	Customer
Operating system	Customer	Customer	Customer	Customer
Physical hosts	Customer	Customer	Microsoft	Customer
Physical network	Customer	Customer	Microsoft	Customer
Physical datacenter	Customer	Customer	Microsoft	Customer

Microsoft
  Customer



### Key Observations

#### **Enterprise infrastructure is (or will be) hybrid**

- Difficult to resist value & security of cloud
- Difficult to retire all on-premises hardware

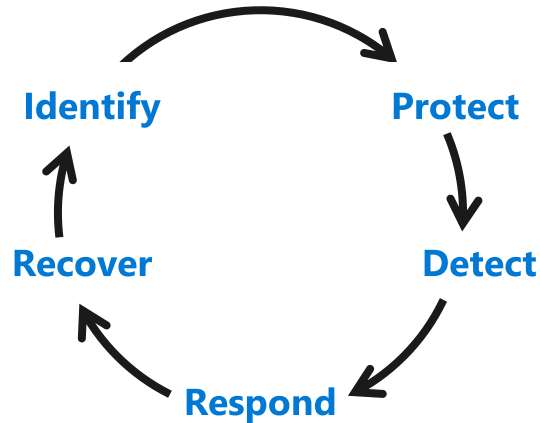
#### **IaaS security similar to on-premises, but better**

- Legacy workloads require network controls
- Cloud platform makes security hygiene easier
- Cloud vastly improves threat detection & response

# Roadmap to a secure modern infrastructure

## First 30 Days

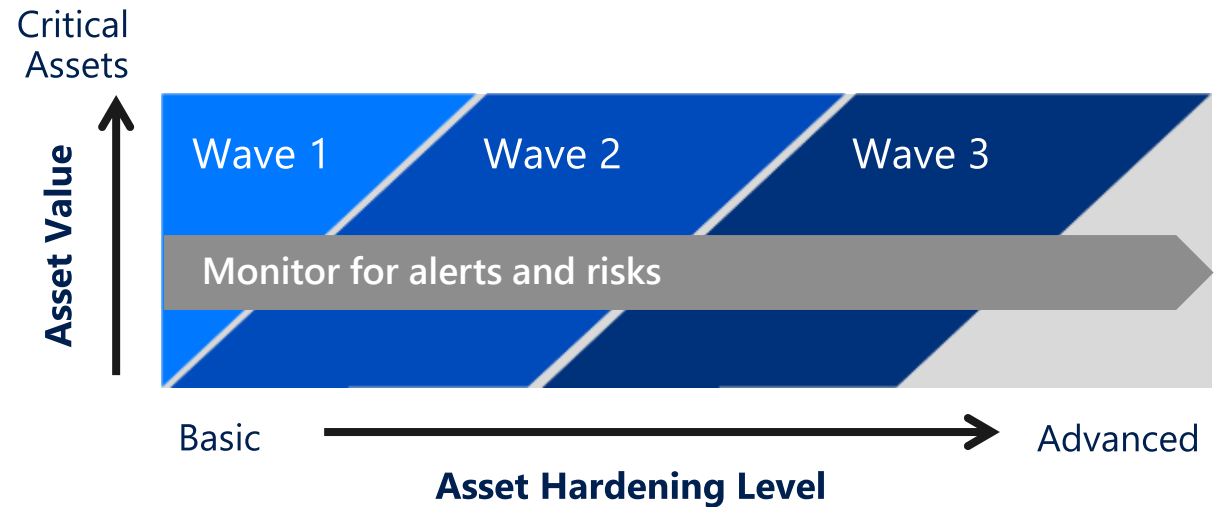
*Quick wins*



- Identification of Assets
- Establish critical protections, monitoring
- Establish response processes

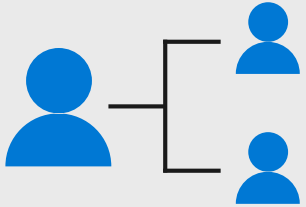
## Day 31 and Beyond

*Prioritized infrastructure handling*



- Categorize Systems
- Harden assets in waves
- Monitor datacenter resources for attacks and vulnerabilities

# Measuring and Planning - A-H/N Approach



## Admin

Isolate Administrative Interfaces from Risk, enforce Role Based Access Control (RBAC) for all layers of access:

- Tenant
- Identity
- Storage & Network
- OS, Apps, Containers
- PaaS Service Configuration



## Host

Harden Hosts against compromise including IaaS VMs, On-Premises VMs, and physical servers

Addresses many aspects of platform security:

- Security Monitoring
- Configuration baselines
- Security updates
- AV & Security Tooling



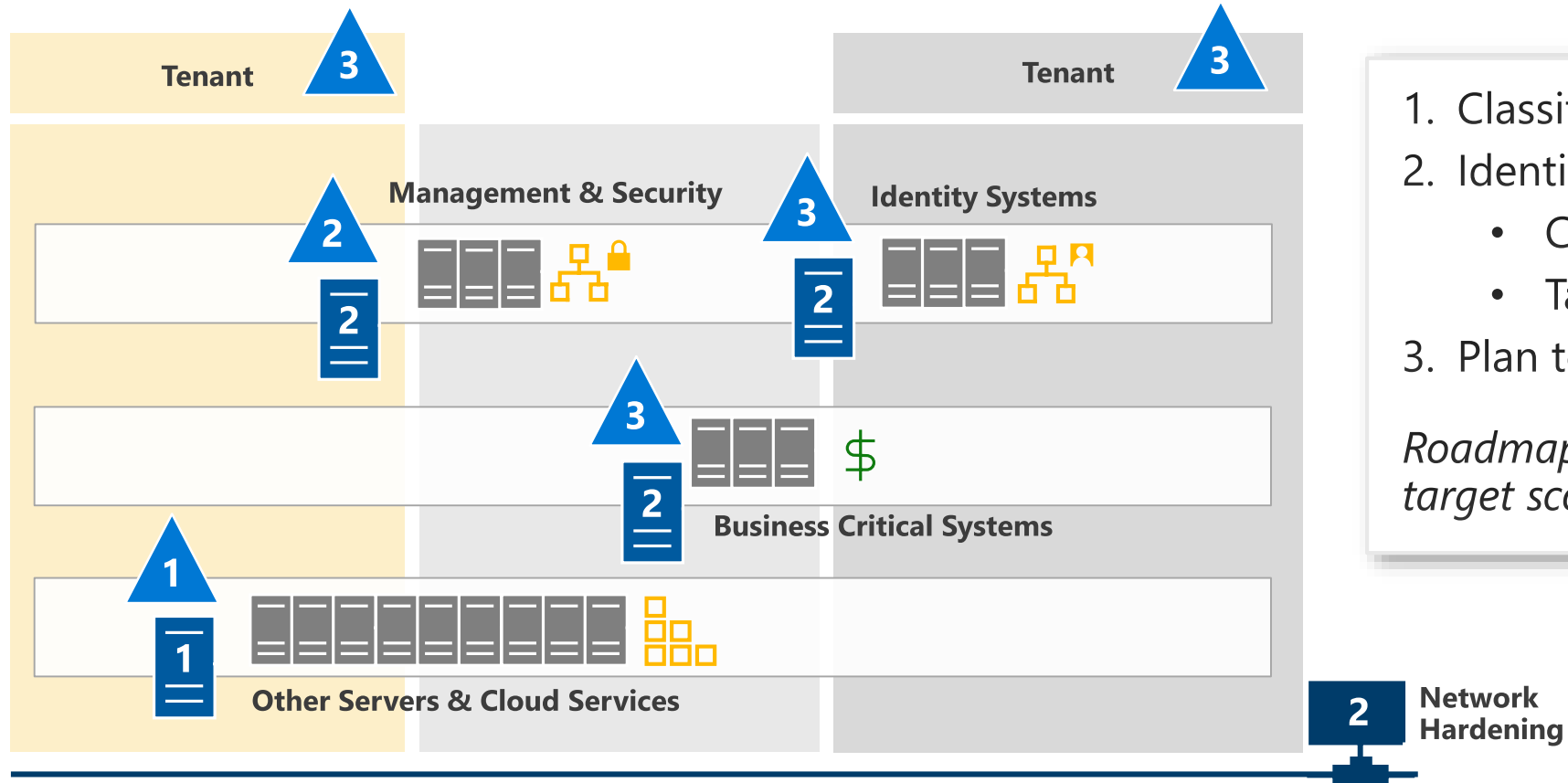
## Network

Implement network defenses

Addresses **network protections** including

- Security Monitoring
- Device security updates
- Device configuration & Password Management
- **Thoughtful** network segmentation

# Use A-H/N scoring to measure and improve security



1. Classify your assets
2. Identify **A-H/N** scores
  - Current Score
  - Target Score
3. Plan to fill gaps

*Roadmap contains default target scores and schedule*

# A Admin isolation

-

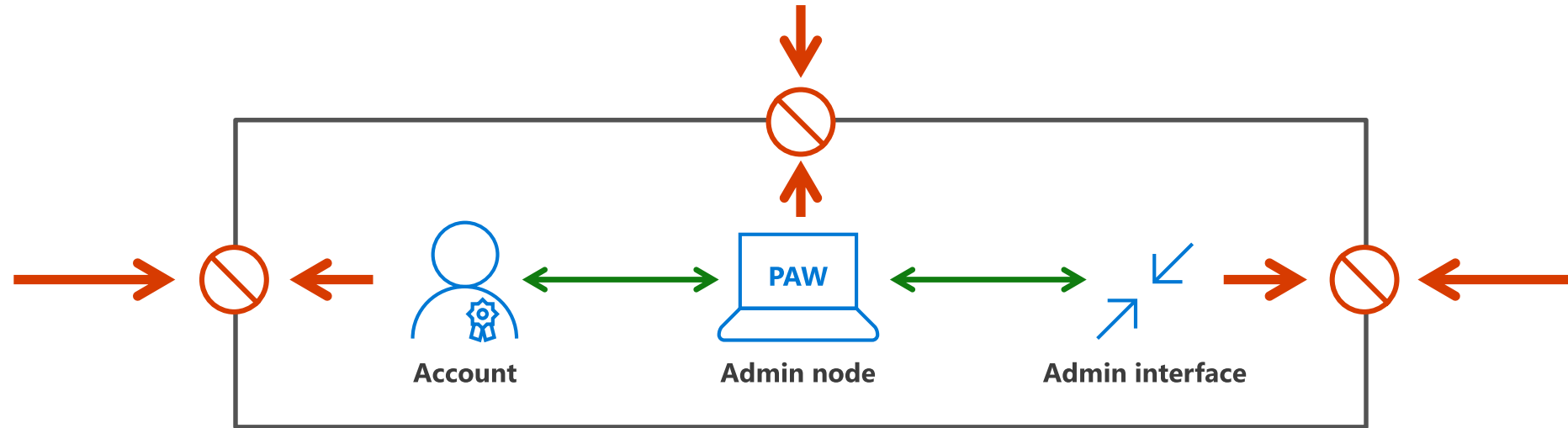
# H Host hardening

/

# N Network isolation

# Isolate Administrative Interfaces

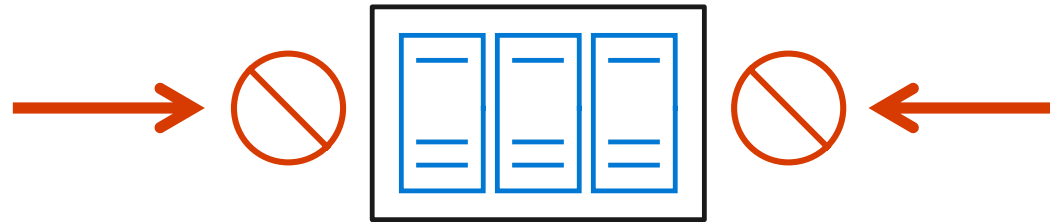
*Protect and Monitor all administrative interfaces for servers/services*



1 Basic	2 Intermediate	3 Advanced
Service Defense	Per-Role Defense	Specialized / Advanced Hardening
<ul style="list-style-type: none"><li>• Reduce admin quantity &amp; eliminate shared accounts</li><li>• Enable logging &amp; analytics</li><li>• Strong AuthN + Device Security</li><li>• Enable built-in PIM (as available)</li></ul>	<ul style="list-style-type: none"><li>• Role Based Access Control</li><li>• PAW + PAM for all admin roles</li><li>• Restrict Tier 0 account exposure</li><li>• Randomize local passwords</li></ul>	<ul style="list-style-type: none"><li>• Service account hardening/restrictions</li><li>• Reduce and Restrict Administration rights on server hosts</li></ul>

# Host Hardening

Reduce the attack surface of servers and services



**1 Basic**

Host Hardening

- Basic patch management
- Disk/Volume encryption
- Antivirus + Endpoint Detection & Response (EDR)
- Host firewall
- Whitelisting applications (*Azure Windows Hosts*)

**2 Intermediate**

Platform Hardening

- OS Configuration Baseline
- Enable logging Monitor with SIEM/Analytics
- Full patch compliance
- Restrict remote credential exposure
- Firmware security (updates + remote access) (*physical hosts*)

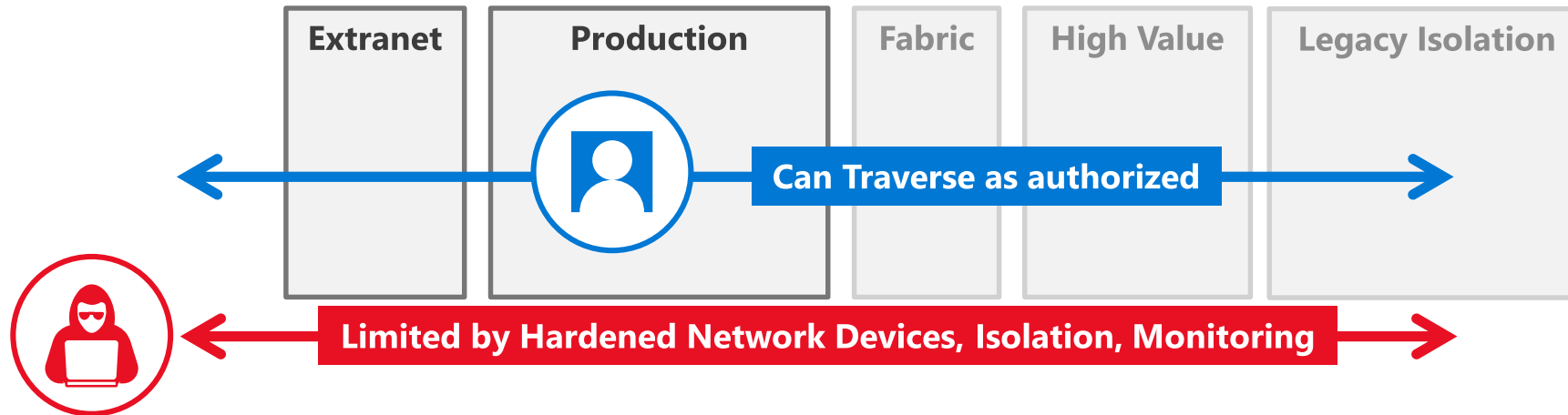
**3 Advanced**

Workload Hardening

- Whitelisting Applications (All)
- Code signing for Critical Apps
- Crashdump + in memory process analysis
- Automated Investigation and Response

# Network Isolation

*Increase the cost and difficulty for an attacker to traverse your environment*



**1 Basic**

Network  
Perimeter Segmentation

- Filter inbound traffic from Internet → Extranet → Intranet
- Next Generation Firewall / Web Application Firewalls (WAFs)
- DNS hygiene and monitoring
- Strong password for network devices

**2 Intermediate**

Network  
Access Segmentation

- Just in time management port access
- Filter outbound access for servers
- Unique and segmented passwords for network devices
- Network Device patching and configuration hygiene

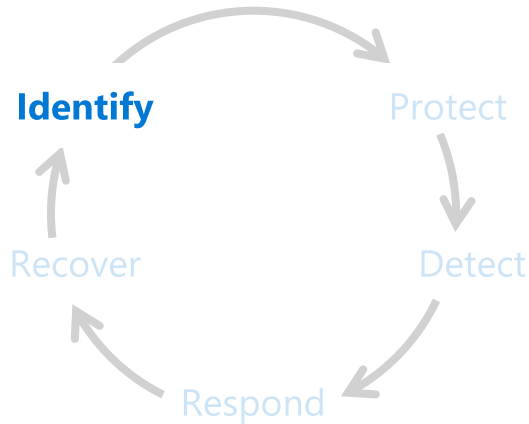
**3 Advanced**

Network  
Flow Segmentation

- Monitor network flow
- Encrypt all workload traffic
- PIM for network device management
- Advanced micro-segmentation and workload isolation
- Retire insecure management protocols

# First 30 Days (1-3)

## Quick wins



- Identification of Assets
- Establish critical protections & monitoring
- Establish response processes

## 1. Identify Management & Security Systems (e.g. Tier 0)

(systems, administrative roles, admin count, etc.)

- ✓ Tenant Administration
- ✓ Configuration Management
- ✓ Deployment Systems
- ✓ Monitoring
- ✓ Security scanning
- ✓ Backups
- ✓ Firewall | IDS/IPS
- ✓ Vulnerability scanning

## 2. Build Inventory of servers

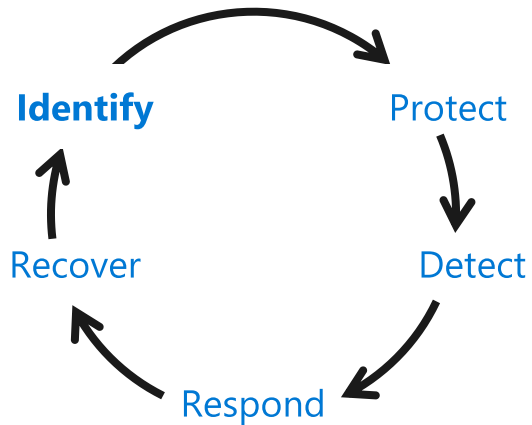
- Azure - 100% Using [Azure Security Center](#)
- On-Premises & 3<sup>rd</sup> Party Cloud - 80% using tools or manual processes

## 3. Identify Internet Facing Servers

- Azure - 100% identified and remediated) with [Azure Security Center Alerts](#)
- On-Premises & 3<sup>rd</sup> Party Cloud - 80% using tools or manual processes

# First 30 Days (4-6)

## Quick wins



- Identification of Assets
- Establish critical protections & monitoring
- Establish response processes

## 4. Essential Security for Azure Tenant Administration

- Dedicated Admin account with no email/browsing allowed
- Reduce Tenant Administrator Count
  - Global Admins – 2 people max or identify specific justification for why each admin can't use a delegated role (for 3+ admins)
- Enforce MFA and Just in Time Privileges

## 5. Establish Critical Security Monitoring

- Azure - 100% Coverage using Azure Security Center (Standard)
- On-Premises & 3<sup>rd</sup> Party Cloud VMs – Azure Security Center or SIEM
- All – Monitor for identity attacks on admins (Azure ATP or 3<sup>rd</sup> party)

## 6. Build/Update Response and Recovery Processes

Establish or validate written guidance on how to investigate, classify, and recover from server/datacenter incidents

- Response and Recovery Framework
- Technical Instructions for Recovering Accounts, Hosts, Devices

# Beyond the quick wins

MAIN MENU



		60 days	90 days	120 days	180 days	6 months +
<b>Critical assets</b>	Management + security Identity systems Business critical systems					
	Servers and cloud services	N/A	N/A			
	Network hardening	N/A				

Monitor Logs via SIEM/ASC + Lateral movement paths via Azure ATP



Amin isolation



Host hardening



Network isolation

# Scope, Assumptions, Observations

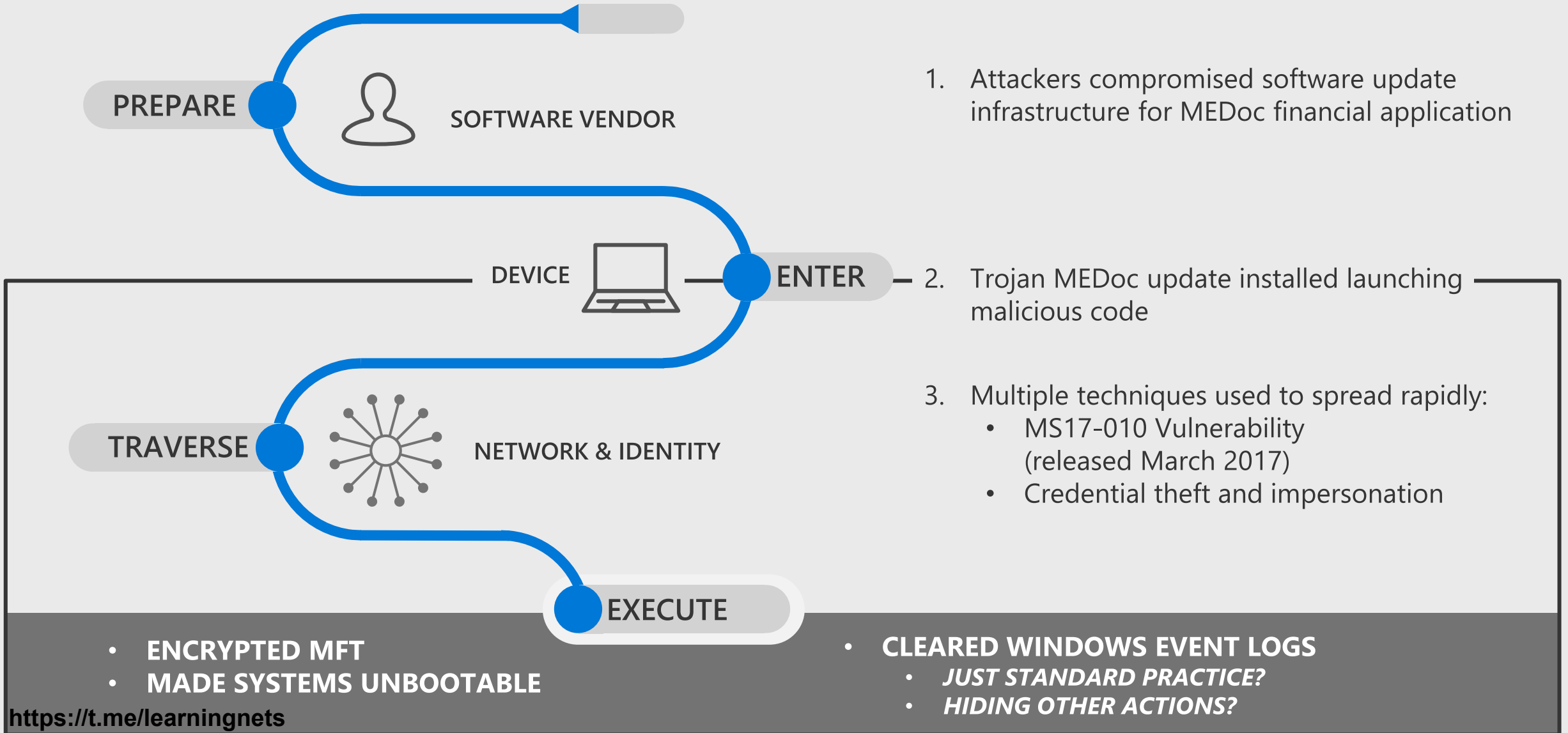
Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	Customer	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and Identities	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Microsoft	Microsoft	Customer	Customer
Applications	Microsoft	Microsoft	Customer	Customer
Network Controls	Microsoft	Microsoft	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

Legend:  Microsoft  Customer

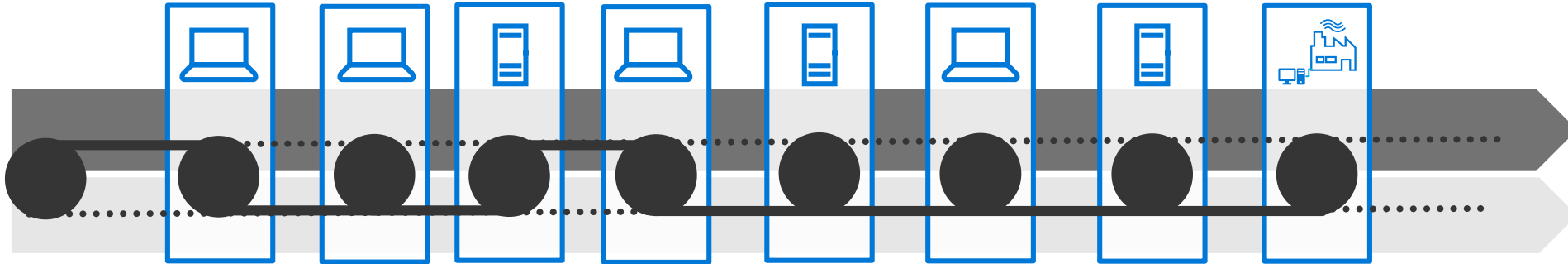
Paying down "technical debt" of critical hygiene leads to lower risk and less vulnerability to 'new' attack combinations like Petya/Wannacrypt

Cloud Provider Responsible for Hygiene of Cloud Services

# Anatomy of a Petya Attack



# Critical Element: Multi-Channel Propagation



## MITIGATING ONE VECTOR ISN'T ENOUGH

Most of Petya propagations were from impersonation "channel"  
97% patched was not enough to stop the spread



## DUAL BENEFITS OF INVESTMENTS






Credential theft, patch, and other investments also mitigate targeted attacks

# Petya - Massive Technical and Business Impact

## *Rapid Destruction at Global Organizations*

### Example of Technical Impact

(Anonymous)

	<b>GEOGRAPHIES</b>	All
	<b>DURATION</b>	~60 minutes
	<b>IMPACTED COMPUTERS</b>	<b>62,000 computers</b>  12,000 servers  50,000 workstations

### Publicly Reported Losses

(By Different Organizations)

**\$200** Million

**\$300** Million

**\$310** Million

# Summary of Key Recommendations

MAIN  
MENU



Measures that directly impact the known attack playbook

<https://aka.ms/rapidattack>

## Quick wins: 0-30 Days

DIRECT ATTACK MITIGATION  
RAPID ENABLEMENT

- 1 Create **destruction-resistant backups** of your critical systems and data
- 2 Immediately deploy **critical security updates** for OS, browser, & email
- 3 **Isolate (or retire) computers** that cannot be updated and patched
- 4 Implement **advanced e-mail and browser protections**
- 5 Enable host anti-malware and network defenses to get near-**realtime blocking responses from cloud** (if available in your solution)
- 6 Implement **unique local administrator passwords** on all systems
- 7 Separate and protect **privileged accounts**

## Less than 90 Days

DIRECT ATTACK MITIGATION  
LONGER ENABLEMENT

- 1 **Validate** your backups using standard restore procedures and tools
- 2 **Discover and reduce** broad permissions on file repositories
- 3 Rapidly deploy all **critical security updates**
- 4 **Disable unneeded** legacy protocols
- 5 **Stay current** – Run only current versions of operating systems and apps

## Next Quarter + Beyond

<https://t.me/learningnets>

# Windows 10 - Scope and Assumptions



Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	Microsoft	Microsoft	Microsoft	Microsoft
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and Identities	Microsoft	Microsoft	Microsoft	Microsoft
Identity and directory infrastructure	Microsoft	Microsoft	Microsoft	Microsoft
Applications	Microsoft	Microsoft	Microsoft	Microsoft
Network Controls	Microsoft	Microsoft	Microsoft	Microsoft
Operating system	Microsoft	Microsoft	Microsoft	Microsoft
Physical hosts	Microsoft	Microsoft	Microsoft	Microsoft
Physical network	Microsoft	Microsoft	Microsoft	Microsoft
Physical datacenter	Microsoft	Microsoft	Microsoft	Microsoft

Legend:  Microsoft  Customer

## Observations

- Client devices are on the front line
  - Target of many single stage attack patterns
  - Entry point for many multi-stage attack patterns
- Fundamental Windows Security Shift
  - **Previous Versions** - advanced security from 3<sup>rd</sup> party tools
  - **Windows 10** – Native advanced security capabilities built in (EDR, Exploit Mitigations, Whitelisting etc.)
  - **Windows 10** – Windows as a Service (WaaS) for updates
- Application compatibility is top challenge to security feature adoption

# Practical Roadmap for Windows 10 Security

Enabling Advanced Threat Protection (ATP) capabilities

MAIN  
MENU



## 30 DAYS



### Enable Critical Capabilities

#### Protect

- **Antimalware** ([Defender](#) with [cloud-delivered protection](#) or 3<sup>rd</sup> party)
- [Credential Guard](#)
- [SmartScreen](#) (+ [Chrome plug-in](#))

#### Identify/Detect/Respond

- **Patching** – view status in [Secure Score](#)
- **Endpoint Detection & Response** (EDR) ([Defender ATP](#) or 3<sup>rd</sup> party)
- **Exploit Guard 1** ([Audit Mode](#))

## 90 DAYS



### Enable Next Critical Capabilities

- **Patching** - Apply critical security updates 99%+ of computers within 4 days (Operating System, Email, browser)
- **Random Local Passwords** - Deploy [Local Administrator Password Solution \(LAPS\)](#)
- Enable [Application Guard](#)
- **Exploit Guard 2** – [Deploy Enforcement](#) in a pilot (using audit mode data)
- **Windows Hello for Business** – [Plan and deploy](#) production pilot

## BEYOND



- Deploy [Security Baseline](#) configurations (Pilot → Production)
- Remove **local admin rights** from standard users
- Deploy [Application Whitelisting](#)
- **Exploit Guard 3** – [Deploy Enforcement](#) to all production workstations
- **Reduce critical attack surface** - Unsupported applications + Apps requiring vulnerable middleware
- **Stay Current** - Ensure processes support deploying new versions (usually every 6 months)

Plan and execute **Secure Score** recommendations - <https://aka.ms/WindowsSecureScore>

# Scope, Assumptions, Observations

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	Microsoft	Microsoft	Microsoft	Microsoft
Devices (Mobile and PCs)	Microsoft	Microsoft	Microsoft	Microsoft
Accounts and Identities	Microsoft	Microsoft	Microsoft	Microsoft
Identity and directory infrastructure	Customer	Customer	Customer	Customer
Applications	Microsoft	Microsoft	Microsoft	Microsoft
Network Controls	Microsoft	Microsoft	Microsoft	Microsoft
Operating system	Microsoft	Microsoft	Microsoft	Microsoft
Physical hosts	Microsoft	Microsoft	Microsoft	Microsoft
Physical network	Microsoft	Microsoft	Microsoft	Microsoft
Physical datacenter	Microsoft	Microsoft	Microsoft	Microsoft

Legend:  Microsoft  Customer

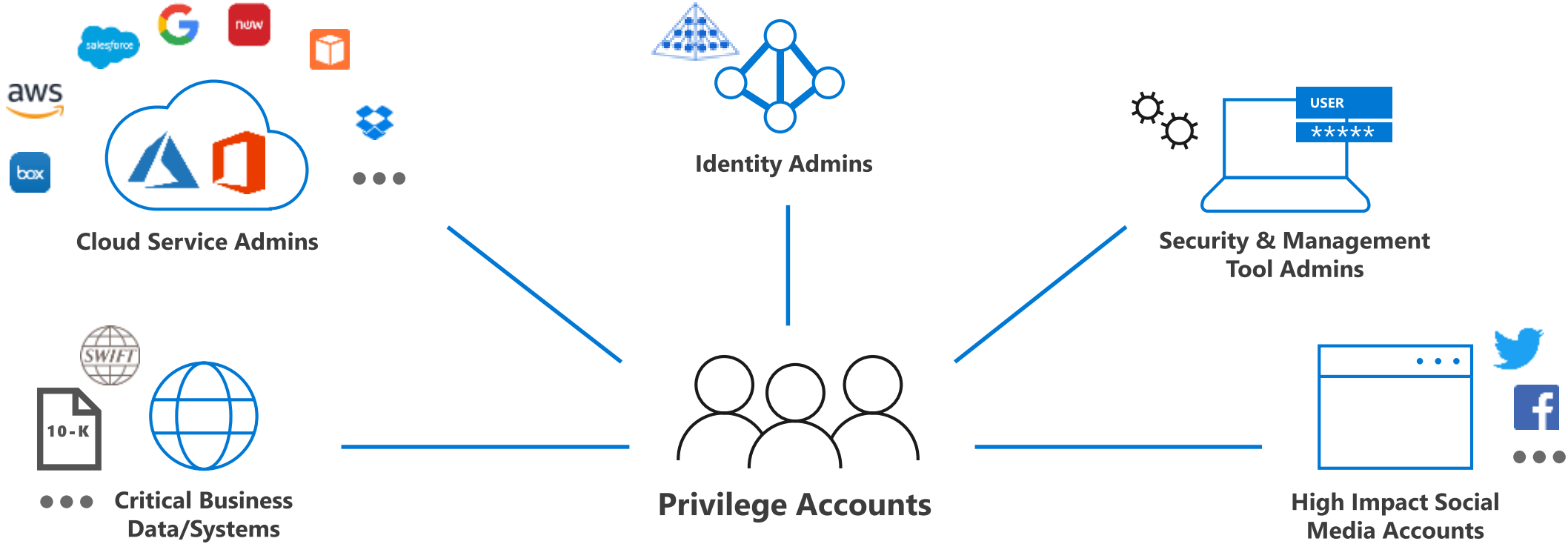


## Assumptions and Observations

- **High Business Impact**
  - Privileged access provides attacker control of many critical systems at once
- **Cloud has higher security**
  - Rigorous security practices from day one
  - Stringent regulatory oversight
  - Key investments (no standing access, admin workstations, physical security, etc.)
- **On Premises Active Directory** is a key dependency for many systems

# Privileged Access is more than Administrators

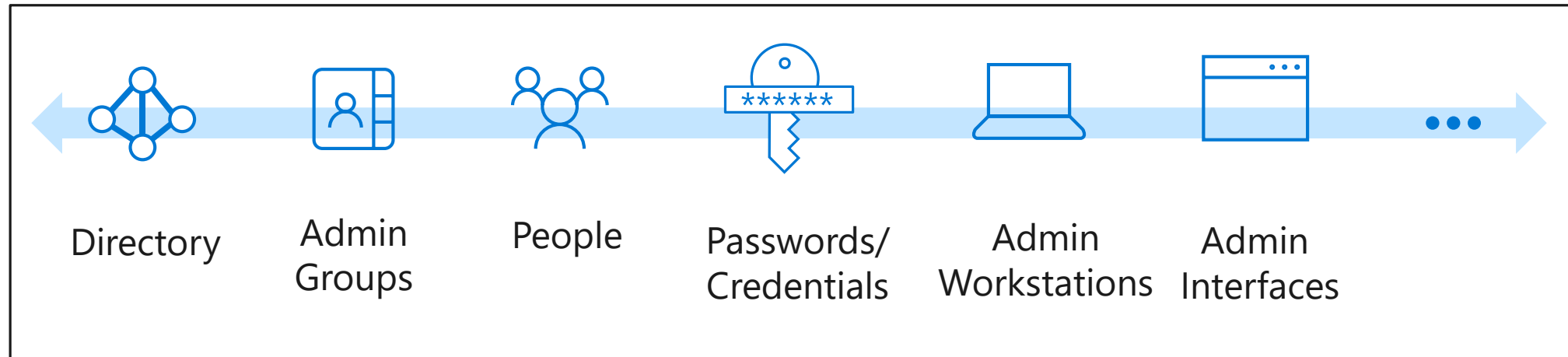
*Protect high impact accounts/roles*



# Securing Privileged Access

## More than just vaulting admin passwords

Protect all parts of the privileged lifecycle



# Securing Privileged Access

## 1. Strengthen Authentication

- Passwordless, MFA, Leaked credential detection, etc.

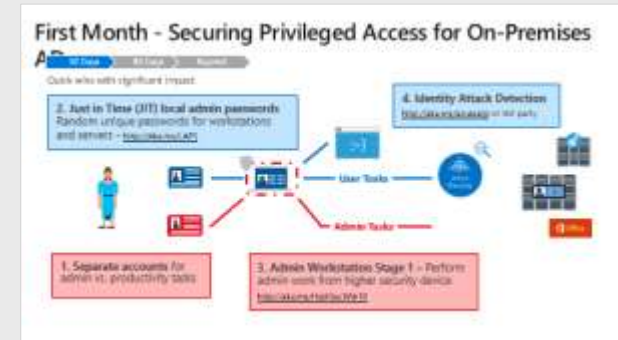
## 2. Reduce Attack surface

- Remove legacy/insecure protocols
- Remove duplicate/weak passwords
- Reduce dependencies

## 3. Increased Monitoring and Detection

## 4. Automate Threat Response

## 5. Ensure Usability for Administrators



**ON-PREMISES AD**

[AKA.MS/SECURITYSTEPS](https://aka.ms/securitysteps)

**AZURE AD**

# First Month - Securing Privileged Access for On-Premises



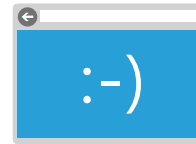
Quick wins with significant impact

## 2. Just in Time (JIT) local admin passwords

Random unique passwords for workstations and servers - <http://Aka.ms/LAPS>

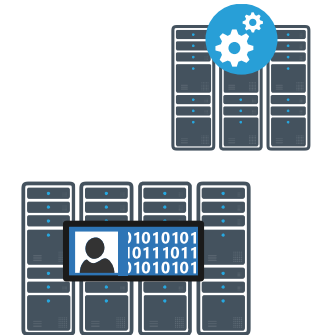
## 4. Identity Attack Detection

<http://aka.ms/azureatp> or 3rd party



User Tasks

Admin Tasks



1. Separate accounts for admin vs. productivity tasks

3. Admin Workstation Stage 1 – Perform admin work from higher security device

<http://aka.ms/HighSecWin10>

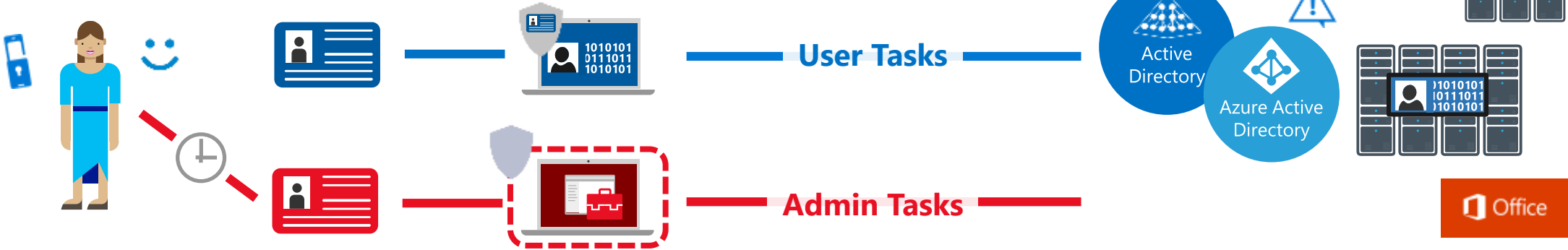
# First Quarter - Securing Privileged Access for On-Premises AD

30 Days → 90 Days → Beyond  
Key protections that provide significant mitigation

**4. Enable Credential Guard** on Windows 10 user workstations  
<http://aka.ms/credguard>

**5. Leaked Credentials 1** - Detect risk by synchronizing user password hashes to Azure AD & reviewing reports  
<https://aka.ms/hashsync> | <https://aka.ms/LeakedCreds>

**6. Lateral Movement Vulnerability Detection**  
<http://aka.ms/LateralMovementRisk>



**1. Require Windows Hello for business / MFA** for admin accounts  
<http://aka.ms/HelloForBusiness>

**2. Admin Workstation Stage 2 –** Require Privileged Access Workstations for AD admins  
*Phase 1 Instructions of* <http://aka.ms/CyberPAW>

**3. Just in Time Privileges** using privileged access management (PAM) solution  
<http://aka.ms/PAM> or 3<sup>rd</sup> party

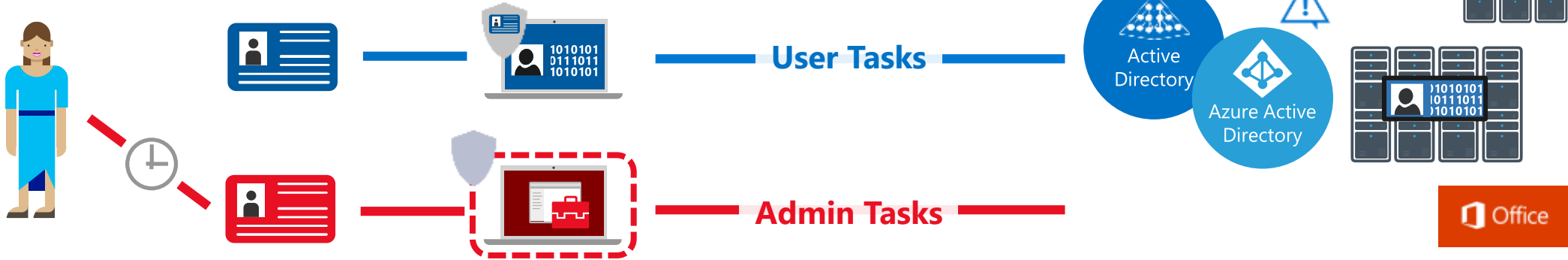
# Beyond - Securing Privileged Access for On-Premises AD



Proactively increase security posture

**1. Review Role Based Access Control (RBAC) model to reduce risk from tier combinations**  
<https://aka.ms/TierModel>

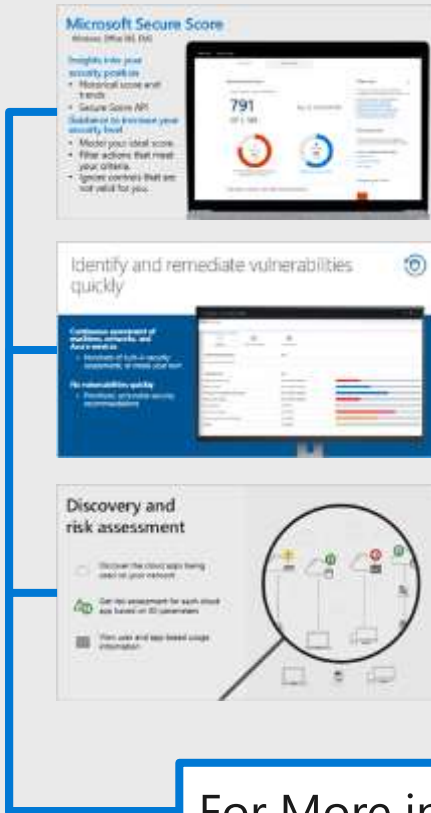
**4. Leaked Credentials 2 - Force Reset of passwords using conditional access and self-service password reset**  
<https://aka.ms/CAPolicy> | <https://aka.ms/selfservicepasswordreset>



**2. Lower attack surface of Domain, DCs, ADFS, and Connect**  
<http://aka.ms/HardenAD>

**3. Integrate Logs with SIEM**  
<https://aka.ms/SIEM-AD>

# Progress Against Recommendations



## Microsoft Secure Score

Office 365, Windows 10, EMS

## Azure Security Center

Cloud Hybrid Infrastructure

## Microsoft Cloud App Security

3<sup>rd</sup> party SaaS risk

For More information, See **Vulnerability Management** Section in Module 2

# CIS Azure Benchmarks

Non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.



# Microsoft and CIS Partnership

## Goal

Simplify and drive consistency in our customers' efforts to securely deploy workloads to Azure

## Benefits

CIS brings independence and consensus driven approach

Benchmarks informed by Microsoft's experience & best practices



# CIS Benchmarks


MAIN  
MENU



- Azure
  - <https://azure.microsoft.com/en-us/resources/cis-microsoft-azure-foundations-security-benchmark/>
- Microsoft 365
  - <https://cloudblogs.microsoft.com/microsoftsecure/2019/01/10/best-practices-for-securely-using-microsoft-365-the-cis-microsoft-365-foundations-benchmark-now-available/>

What are CIS Benchmarks?

- Consensus Based Best Practices
- Over 100 benchmarks covering 14 technology groups
- Examples:
  - Ensure Multi-factor Auth is Enabled
  - Ensure SSH access is restricted
  - Ensure that 'Data disks' are encrypted



What's inside a CIS benchmark?

- What it applies to...
- What to do...
- Why to do it...
- How to audit...
- How to fix...



CIS Implementation Levels

**Level 1** – Recommended, minimum security settings

- Should be configured on all systems
- Should cause little or no interruption of service or reduced functionality

**Level 2** – Recommended for highly secure environments

- Could result in some reduced functionality

# Penetration Testing on Microsoft Cloud

MAIN  
MENU



## Microsoft Cloud Unified Penetration Testing Rules of Engagement

<https://technet.microsoft.com/en-us/mt784683>

### SCOPE

- Azure Active Directory
- Microsoft Intune
- Microsoft Azure
- Microsoft Dynamics 365
- Microsoft Account
- Office 365
- Visual Studio Team Services

### CONTENTS

- Reporting Security Issues
- Microsoft Azure Penetration Testing Notification
- Rules Of Engagement To Perform Penetration Testing On The Microsoft Cloud
  - Prohibited activities
  - Encouraged Activities