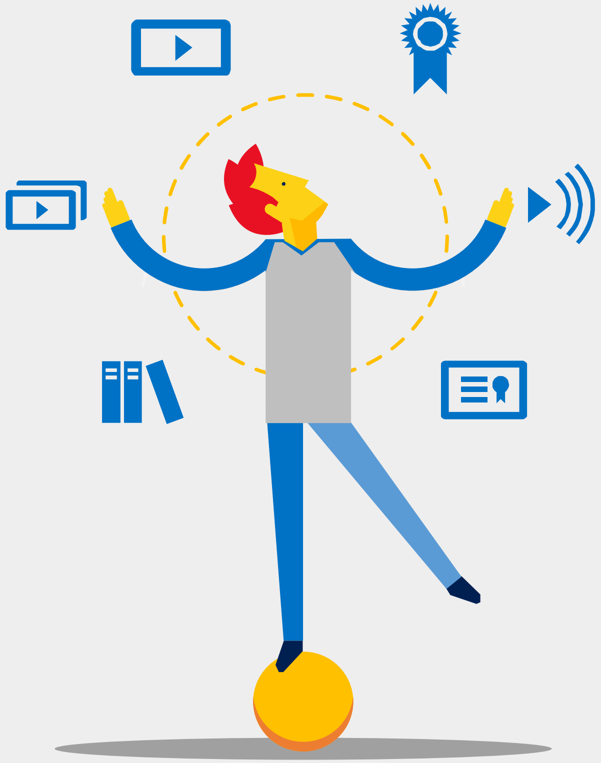
How to Harden Your Enterprise in Today's Threat Landscape

Andrew Idell
Frank Brinkmann

February 1, 2017



Microsoft

Frank Brinkmann

- 19 years with Microsoft and more than 23 years in IT:
  - Director, Cybersecurity Protection Team (CPT), part of the Enterprise Cybersecurity Group. This team develops, pilots, and maintains the cybersecurity consulting offerings that protect our customers' critical assets
  - Frank has worked for Microsoft for more than 19 years, leading growth and innovations across a number of diverse roles in Microsoft, e.g. Development consulting, Enterprise Architect, Project Manager, Service Line & Marketing Lead, Manager Competence Center Modern Datacenter Solutions Germany, and Delivery Manager for EMEA and Asia

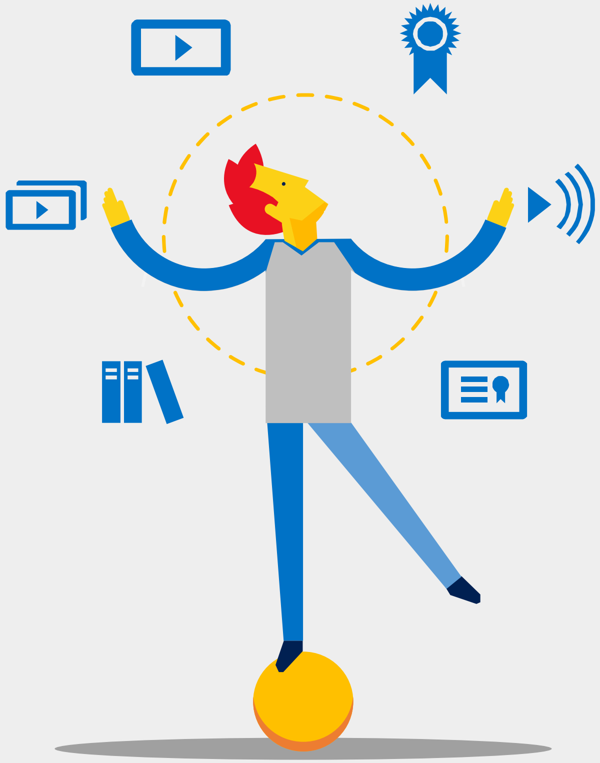
Andrew Idell

- 13 years at Microsoft, 21 years total in IT
  - Cybersecurity Architect – Cybersecurity Protection Team (CPT), part of the Enterprise Cybersecurity Group
  - Holds the CISSP and MCM: Directory Services certifications
  - Andrew's career focused has on Active Directory, PKI, and Windows Security, including work in Corporate IT, as an Microsoft Certified Trainer, and as a consultant at Microsoft Partners. Since joining Microsoft, Andrew has spent time in Product Support, Microsoft Consulting Services in Infrastructure and Cybersecurity, before joining ECG at its beginning in 2015.

Agenda

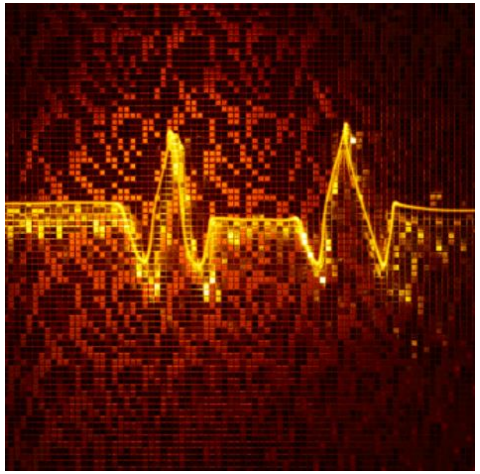
1. The Security Challenge
2. Common Security Misconceptions
3. Addressing the Real Concerns
4. Conclusion and Take-Aways

1. The Security Challenge



Microsoft

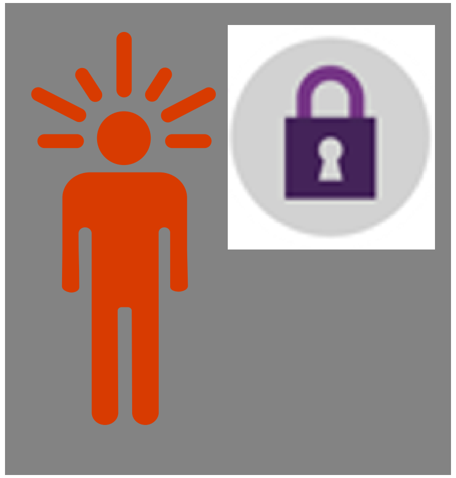
Why is **securing today's datacenter** a challenge?



Critical

Complex

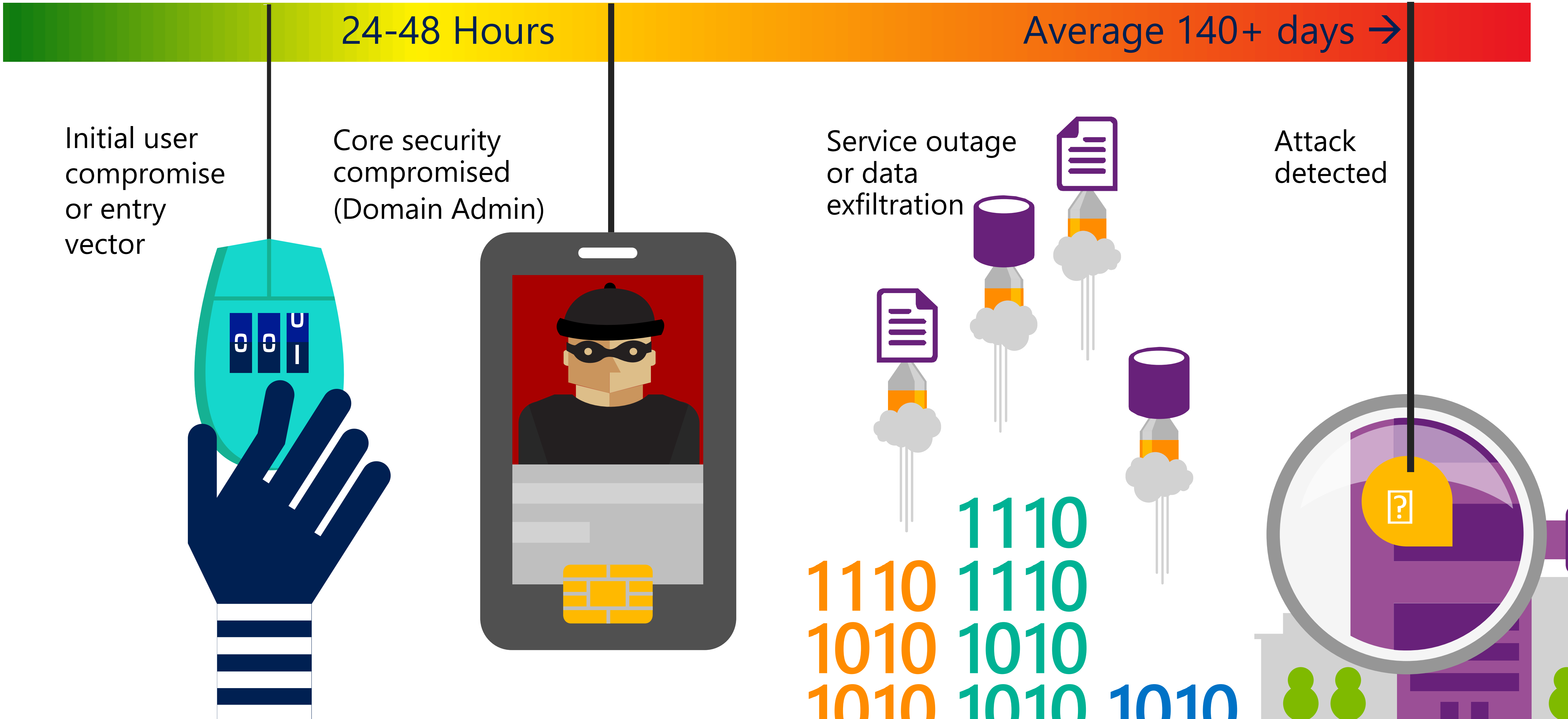
Distributed



Misconceptions

These challenges can leave your business vulnerable

For example: The typical attack timeline & observations



24-48 Hours

Average 140+ days →

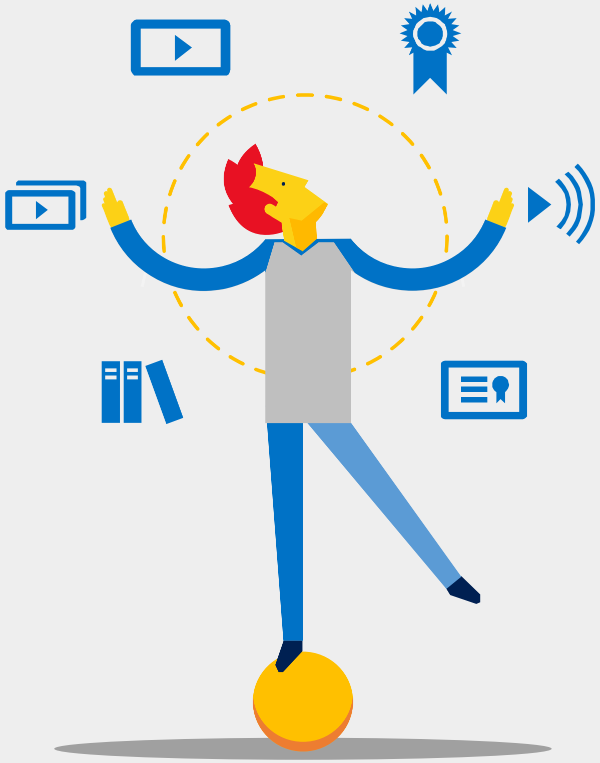
Initial user compromise or entry vector

Core security compromised (Domain Admin)

Service outage or data exfiltration

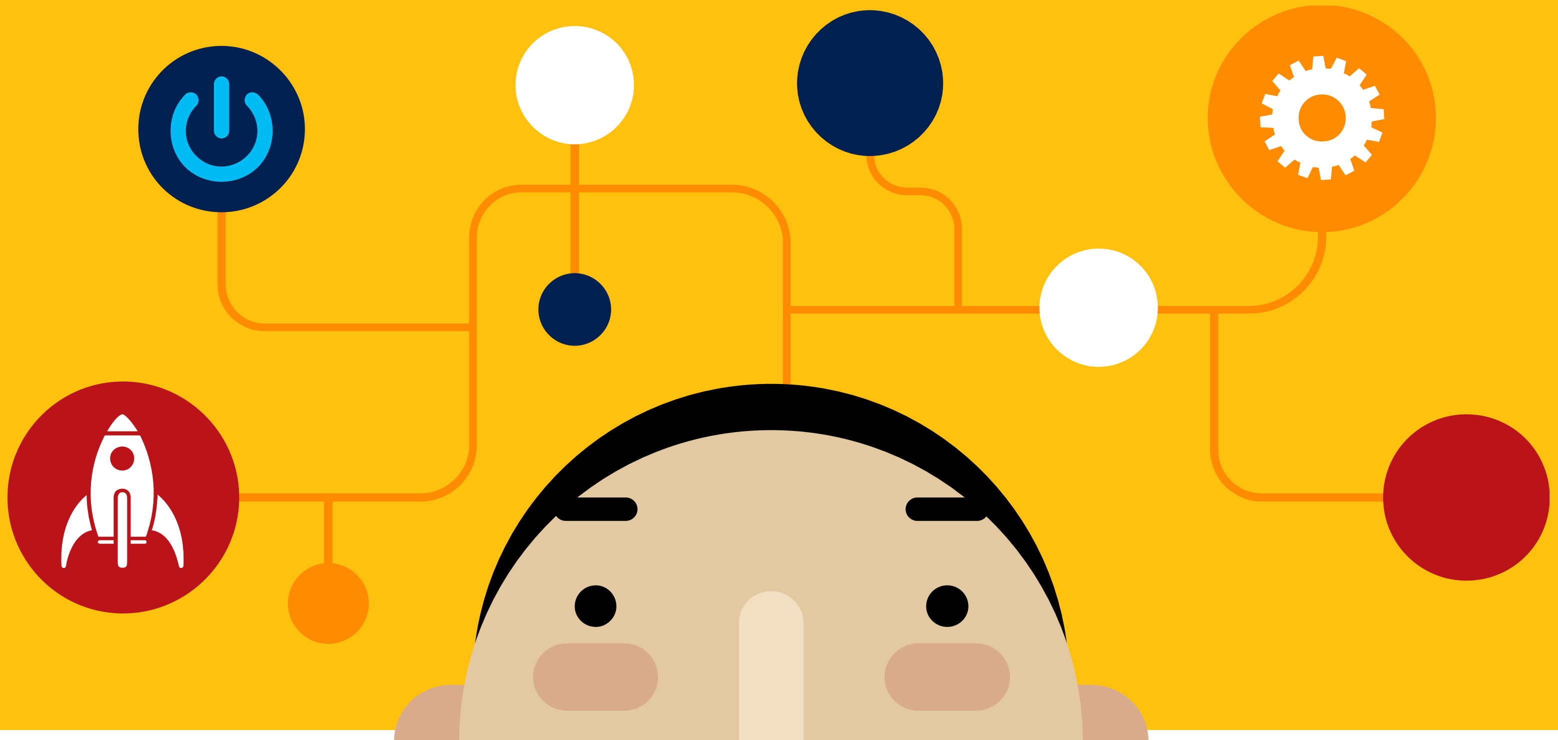
Attack detected

2. Common Security Misconceptions



Microsoft

“My enterprise needs to be very concerned about 0-days.”



Actually…

Not overall, because most companies are compromised by old and unpatched vulnerabilities in software running on top of Windows

“Microsoft's Security Intelligence Report lists the most popular exploits…Most successful exploits are old.”

https://www.microsoft.com/security/sir/default.aspx

“The Verizon Data Breach Report 2016 revealed that out of all detected exploits, **most came from vulnerabilities dating to 2007**. Next was 2011. Vulnerabilities dating to 2003 still account for a large portion of hacks of Microsoft software.“

http://www.infoworld.com/article/3075830/security/zero-days-arent-the-problem-patches-are.html

However, according to the latest SIR, “Over the last six years, it has been observed that if *Microsoft* vulnerabilities are exploited at all, they are most likely to be exploited as zero-day exploits.”

1110
1110 1110
1010 1010
1010 1010 1010

So what should I do?

Step 1: Patch your application layer (Flash, Java, Office, etc.) aggressively as this is how most organizations are compromised today

Step 2: Make sure that you are patching your Operating Systems **within 30 days** of the patch's release

Step 3: Run the latest version of Windows, and turn on the latest protection features that can help stop known *and* unknown malware.

How can Microsoft help me?

VULNERABILITY AND PATCH MANAGEMENT

Option 1: Leverage the public guidance available for System Center Configuration Manager, Intune, and Windows OS Deployment

MALWARE DETECTION

Option 2: If you suspect you have been compromised, engage Premier Support which can arrange for our onsite Incident Response and Tactical Recovery teams.

SECURITY INVESTIGATION AND EVENT MONITORING

Option 3: Microsoft Services has many Consulting and Premier offerings around accelerated Windows OS Deployment, patch management with SCCM or Intune, and Cybersecurity to harden your most critical assets. We also have the Enterprise Threat Detection service to help Detect attacks as they occur and help responders neutralize the threat as soon as possible.

“Will using systems management and security software on my Domain Controllers improve my security?”

Not really…

If the agents are running as System or Administrator, and the administrators of these systems are not properly protected

Why? Any system or user account that can manage a Domain Controller with that level of access is the equivalent of an Enterprise Admin in Active Directory.

How? To answer this, we need to discuss some key security concepts:

- **The Credential Tier Model**
- **Credential Hygiene**

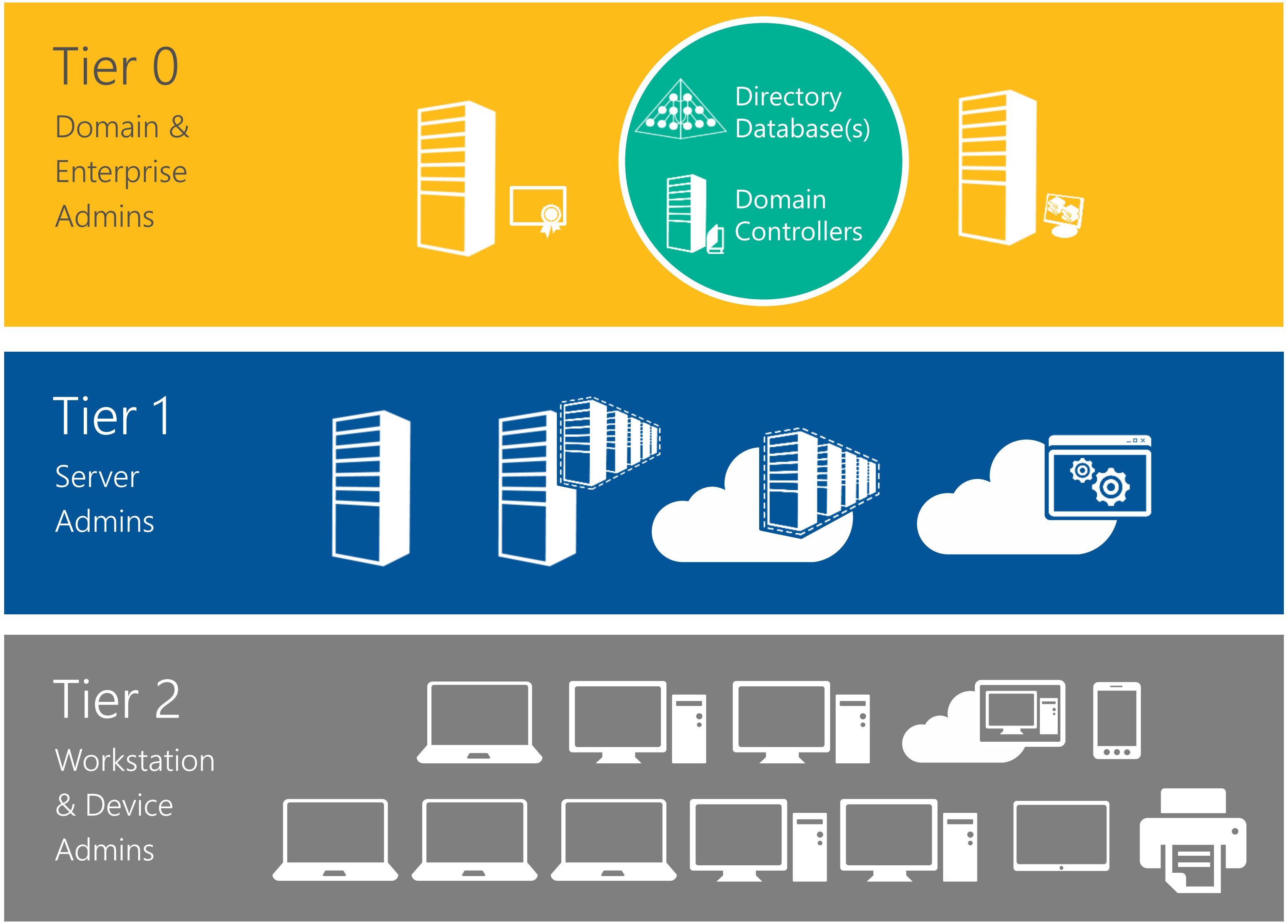
1110
1110 1110
1010 1010
1010 1010 1010

The Credential Tier Model

Rule #1: Credentials from a higher-privileged tier should never be exposed on lower-tier system.

Rule #2: Lower-tier credentials can use services provided by higher-tiers, but not the other way around.

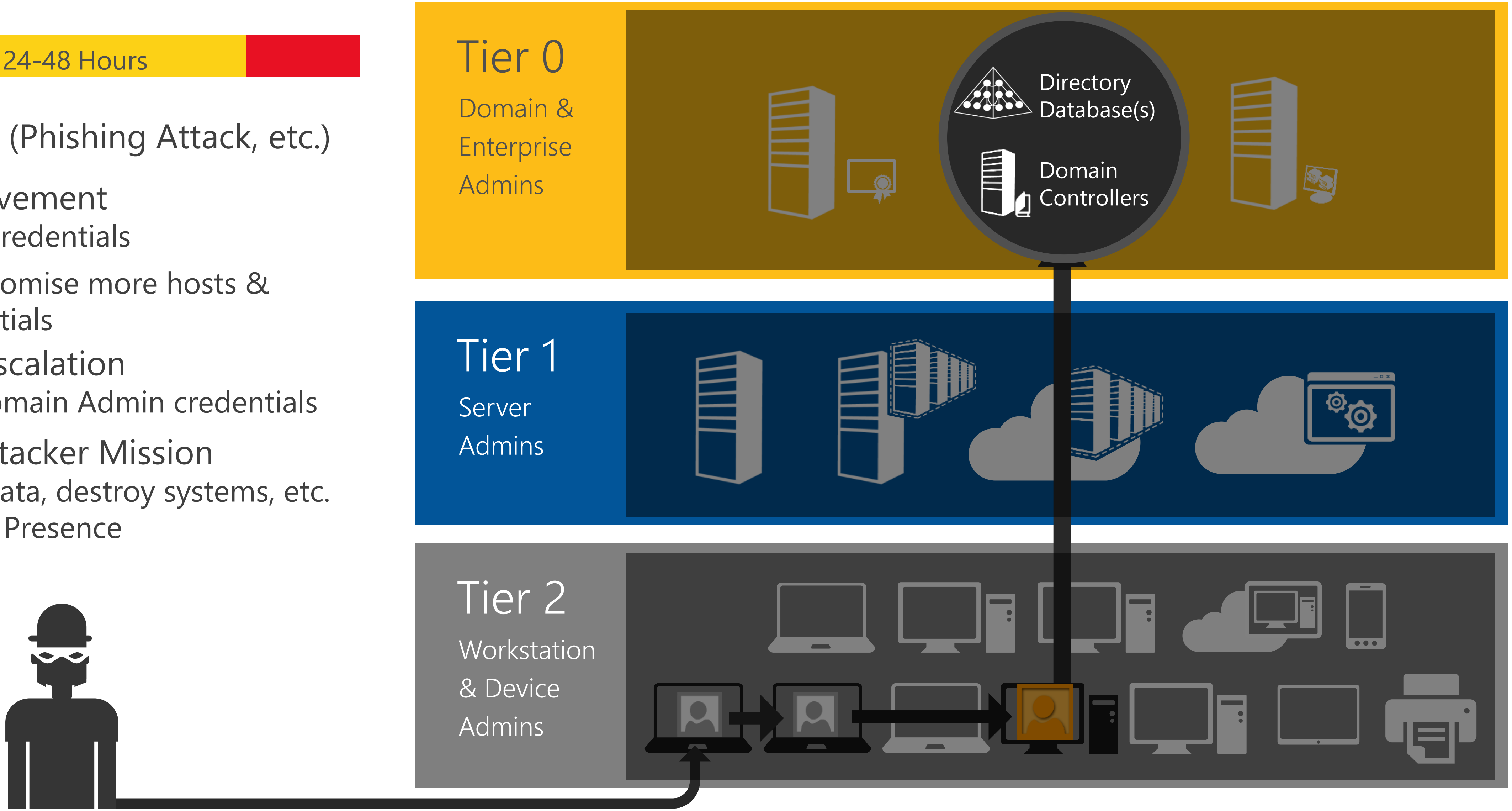
Rule #3: Any system or user account that can manage a higher tier is also a member of that tier, whether you intended it to be or not.



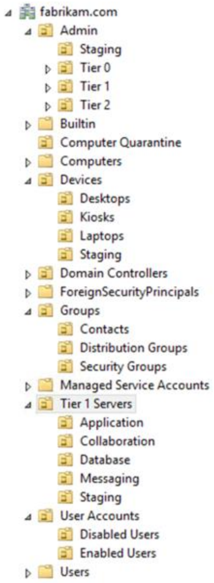
When those rules aren't followed: a typical attack chain

Compromise of privileged access to the whole business

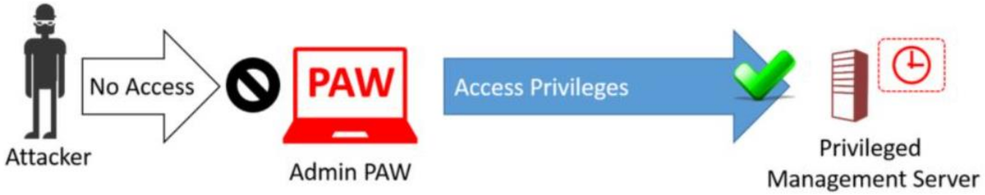
1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Steal Credentials
   b. Compromise more hosts & credentials
3. Privilege Escalation
   a. Get Domain Admin credentials
4. Execute Attacker Mission
   a. Steal data, destroy systems, etc.
   b. Persist Presence



So what should I do?



```
fabrikam.com
  Admin
    Staging
    Tier 0
    Tier 1
    Tier 2
  Builtin
  Computer Quarantine
  Computers
  Devices
    Desktops
    Kiosks
    Laptops
    Staging
  Domain Controllers
  ForeignSecurityPrincipals
  Groups
    Contacts
    Distribution Groups
    Security Groups
  Managed Service Accounts
  Tier 1 Servers
    Application
    Collaboration
    Database
    Messaging
    Staging
  User Accounts
    Disabled Users
    Enabled Users
  Users
```



Step 1: Deploy a Tier model-based OU structure inside your Active Directory, and start enforcing the rules and concepts as part of your daily system administration practices.

Step 2: Protect and isolate your administrator's credentials by using dedicated Privileged Access Workstations (or PAWs) aligned to each Tier.

Step 3: Evaluate and trim as many agents from your Domain Controllers as possible. This reduces the often unintended scope and size of Tier 0.

For software agents still needed on your DCs, such as System Center, Advanced Threat Analytics, or Anti-virus, deploy a dedicated instance just for them.

And make sure those admins use a PAW!

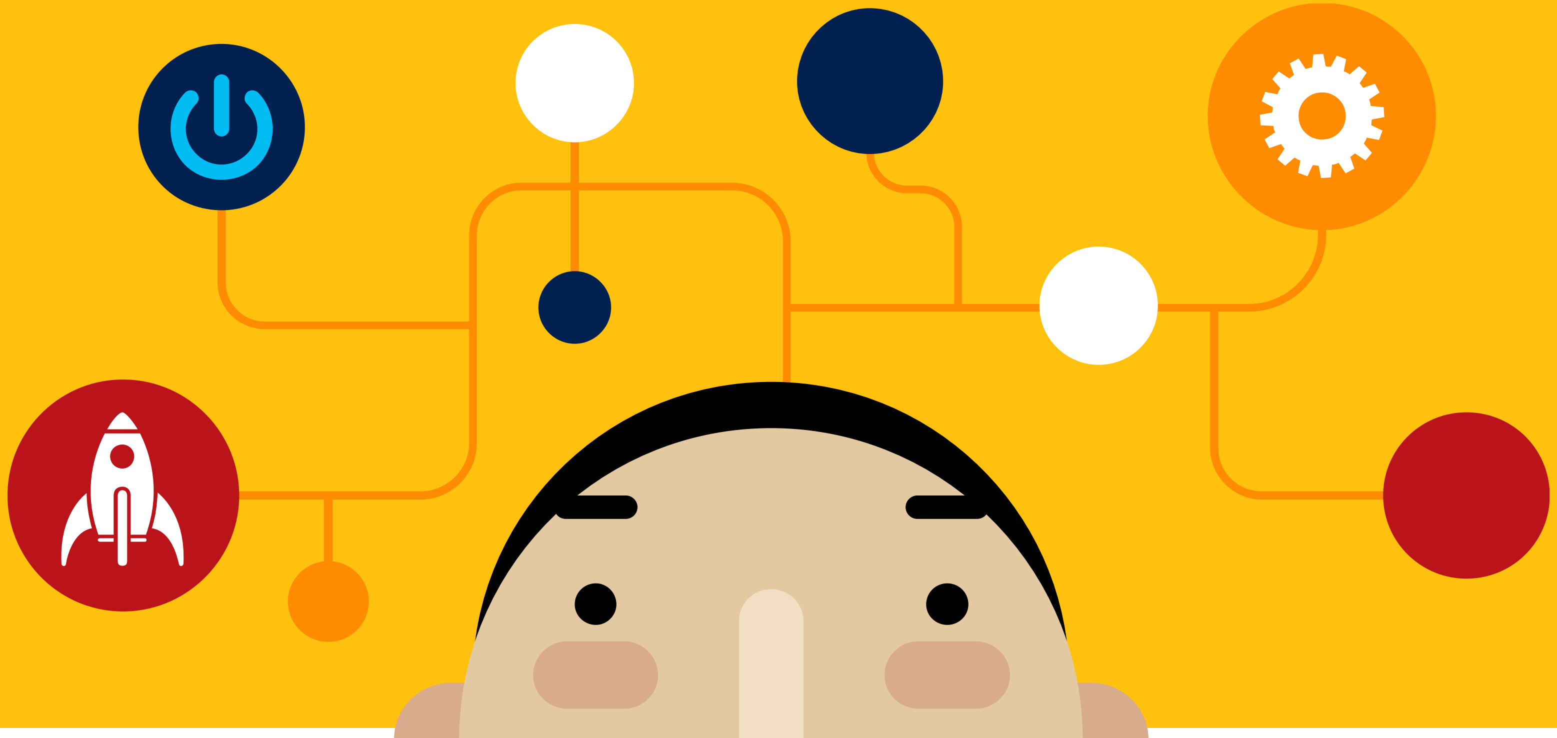
How can Microsoft help me?

Option 1: Leverage the public guidance at http://aka.ms/cyberpaw on how to create and protect your admin workstations. For more information on the Credential Tier Model, check out http://aka.ms/tiermodel.

Option 2: Microsoft Services can help accelerate your adoption of PAWs, identify and reduce upstream risks to Active Directory, and implement the Credential Tier Model in your organization with the following offerings:

- Privileged Access Workstation (PAW) and the Enhanced Security Administrative Environment (ESAE)
- Active Directory Hardening (ADH)
- Advanced Threat Analytics Implementation Services (ATA-IS)

“Using jump servers and multi-factor authentication protect my administrators”



Not really…

If the system used to log in with multi-factor authentication to your jump servers is compromised.

Why? An everyday workstation with unrestricted Internet access, email and LOB applications is much more likely to be compromised, because often these systems have not had (or cannot have) many of the latest protections applied to them to prevent compromise.

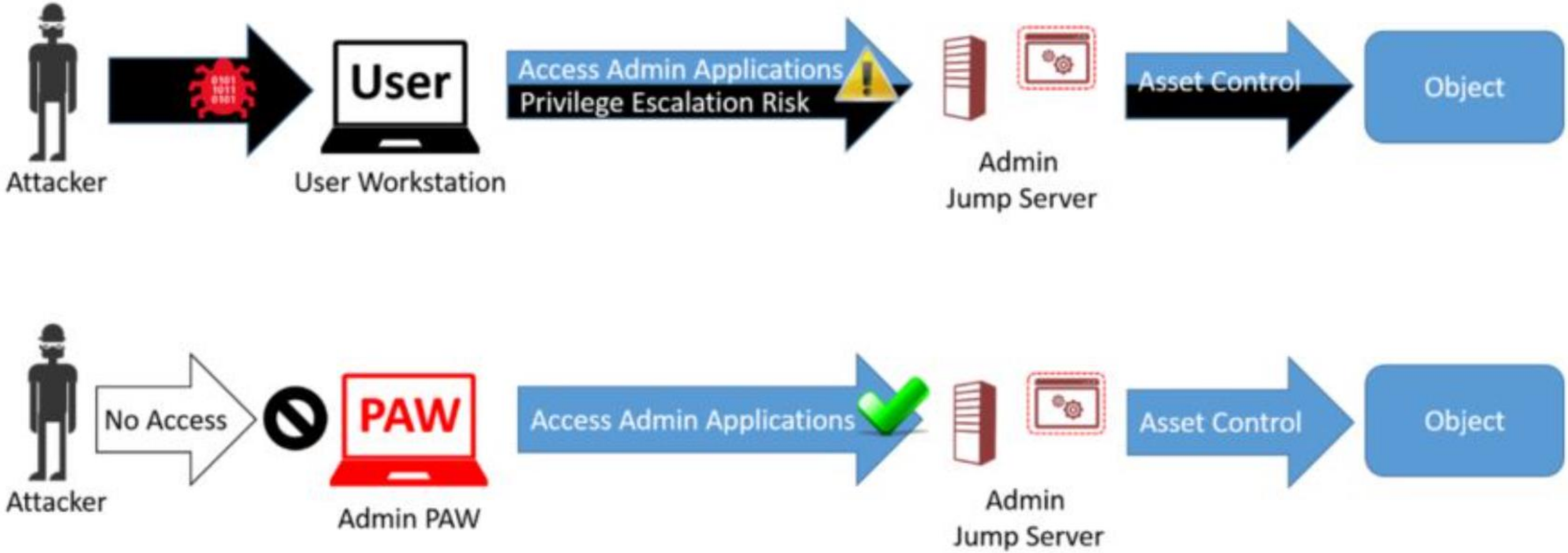
Also, unless this workstation was built from an OS image based on the **clean-source principle**, it is at high risk to have been compromised even at the moment of installation.

Don't new OS features like Credential Guard, Device Guard and Defender ATP mitigate these threats? While a Windows 10 system deployed with the latest protections raises the bar immensely with these powerful protection and detection systems, removing unrestricted Internet access, email, and blocking all inbound traffic with a host-based firewall are needed **in addition to all of the above** to mitigate the primary ways customers are compromised.

1110
1110 1110
1010 1010
1010 1010 1010

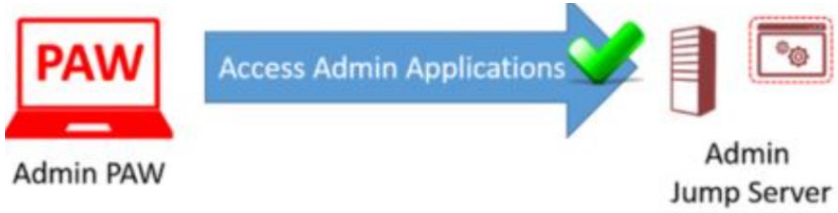
And what about multi-factor authentication like Smart Cards and Windows Hello for Business?
Smart Cards, Windows Hello for Business, and other MFA technologies are designed for one purpose:
To ensure you are in fact who you claim to be in as rigorous as way as possible.
However, they are not mitigations for Credential Theft or malware that might be able to impersonate you once you have logged in.

Why the starting point has to be clean:



So what should I do?

Step 1: Protect and isolate your administrator's credentials by using dedicated Privileged Access Workstations (or PAWs) aligned to each Tier. Follow the clean-source principle for the OS and all software that will be installed on your admin workstations.



Step 2: Deploy the hardening features on your PAWs that may not have yet been implemented enterprise-wide, such as Credential Guard, Device Guard and Hello, as well as blocking inbound traffic, limiting Internet access to Cloud management sites, and removing email access.

Step 3: You don't need to eliminate your jump servers, just access them from your PAWs and harden them in many of the same ways:

- Limit Internet access / remove email
- Use Server 2016 so you can turn on Credential Guard, Device Guard, etc.
- Use RestrictedAdminMode or Remote Credential Guard to protect your administrators' credentials while on the jump server

How can Microsoft help me?

Option 1: Leverage the public guidance at http://aka.ms/cyberpaw on how to create and protect your admin workstations. For more information on the clean-source principle, check out http://aka.ms/cleansource.

Option 2: Microsoft Enterprise Services can help accelerate your adoption of PAWs, to include implementation of both the security features and automation of the clean-source principle, with the following offerings:

- Privileged Access Workstation (PAW)
- The Enhanced Security Administrative Environment (ESAE)
- Active Directory Hardening (ADH)

"Using virtualization and shared infrastructure in my Private Cloud reduces complexity, thereby increasing security"

Not really…

Unless the virtual machines can be isolated from the virtualization admins, and their storage encrypted with a key inaccessible by any storage administrators.

Why? Having a Private Cloud that provides Infrastructure-as-a-Service to your internal customers **is a must** in today’s IT datacenter. However, certain systems like Domain Controllers need special care and protection when virtualized.

What is the issue? On most virtualization platforms, having local administrator or root privileges gives you access to the data stored inside them. If the virtualization host uses a shared storage system, such as a SAN, you have another problem as any account used to administrate that storage also has access to the data inside these virtual machines (or VMs).

1110
1110 1110
1010 1010
1010 1010 1010

Why are Domain Controllers special? Having access to the storage of a Domain Controller gives that user access to the Active Directory database. This is a violation of the Credential Tier Model if that user isn’t already an Enterprise Admin, because anyone with access to the database file could abuse it to take over Active Directory.

So what should I do?

Option 1: Use dedicated virtualization hosts and storage for your Domain Controllers and High Value Assets. If shared storage is required, be sure to protect it by using Bitlocker or other full-volume encryption software.

Option 2: Deploy Windows Server 2016 for your Hyper-V hosts, Shield your VMs and deploy the Host Guardian Service role.

How can Microsoft help me?

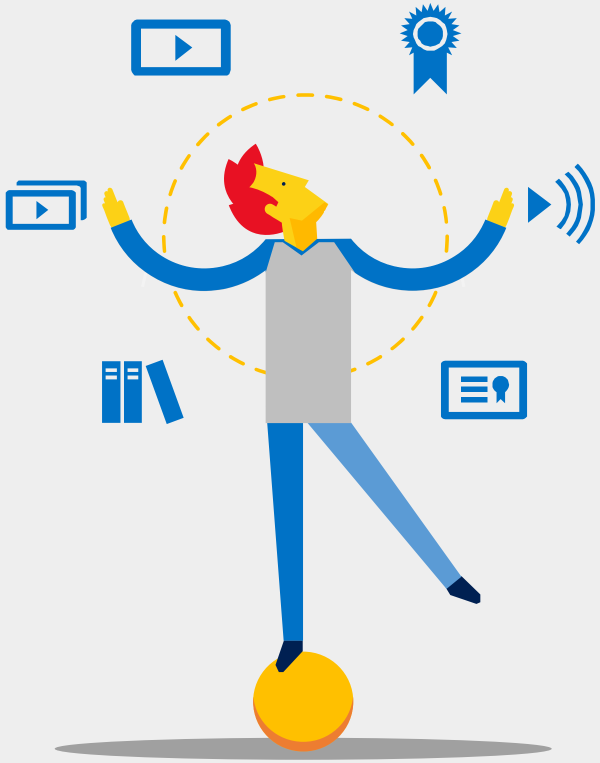
Option 1: Leverage the public guidance at the link below on how to deploy the Host Guardian Service and Shielded VMs on Windows Server 2016:

https://blogs.technet.microsoft.com/datacentersecurity/2016/03/16/windows-server-2016-and-host-guardian-service-for-shielded-vms/

Option 2: Microsoft Services can help accelerate your adoption of HGS and Shielded VMs with the following offerings:

- Deploying Host Guardian Service
- HGS + the Enhanced Security Administration Environment (ESAE)

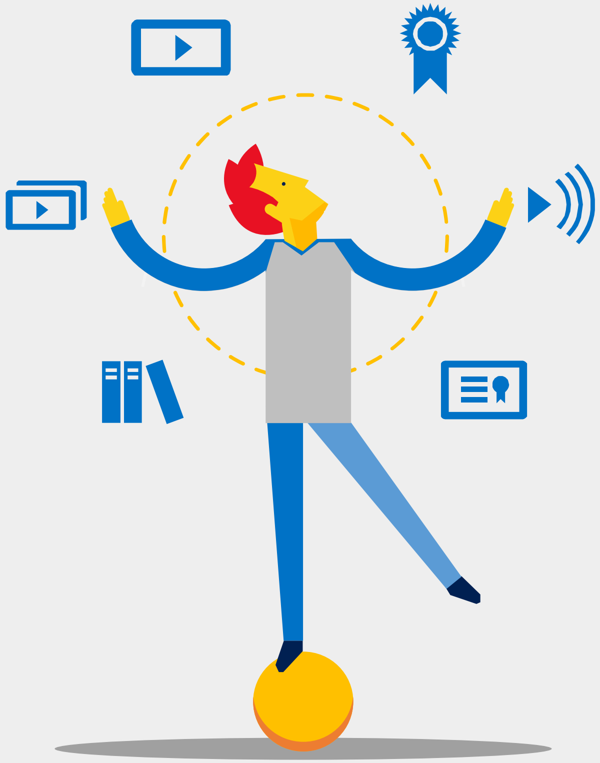
3. Addressing the Real Concerns



Every misconception is based on a legitimate concern

Security Need or Concern	Solutions	Microsoft Services Offerings
Protecting Administrators and their Credentials	• Use hardened, dedicated workstations for administrative tasks • Deploy a separate, hardened forest for your admin users and workstations	• Privileged Access Workstation (PAW) • Enhanced SecurityAdministrative Environment (ESAE)
Hardening Tier0 Servers	• Remove upstream risks • Deploy Shielded VMs and the Host Guardian Service • Deploying official Windows Security Templates to DCs and other Tier 0 servers	• Active Directory Hardening (ADH) • HGS for Guarded Fabric and Shielded VMs • Offline Assessment for Active Directory Services (OAADS)
Hardening Active Directory	• Reducing membership in Tier 0 groups • Deploying official Windows Security Templates • Implementing an OU and policy structure that enforces the Tier Model	• Active Directory Hardening (ADH) • Offline Assessment for Active Directory Services (OAADS)
Detecting and Responding to Attacks	• Deploying a detection solution that leverages machine learning to reduce the “noise” and false positives • Operations ManagementSuite, Advanced Threat Analytics or Windows Defender ATP	• Enterprise Threat Detection (ETD) • Advanced Threat Analytics Implementation Services (ATA-IS)

4. Conclusion/Take-Aways



Microsoft

Key Take-Aways

Common security misconceptions are a reflection of genuine security concerns.

They often are correct in their intentions, but sometimes need additional components to address the underlying concerns.

Microsoft has public guidance for solutions to address these concerns.

Microsoft has a large amount of content to help IT implement these solutions in-house.

Microsoft Services can help accelerate the adoption of these solutions in your enterprise.

But if you need help, we a Services portfolio to help you get there!

Reference Links

Privileged Access Workstation: http://aka.ms/cyberpaw

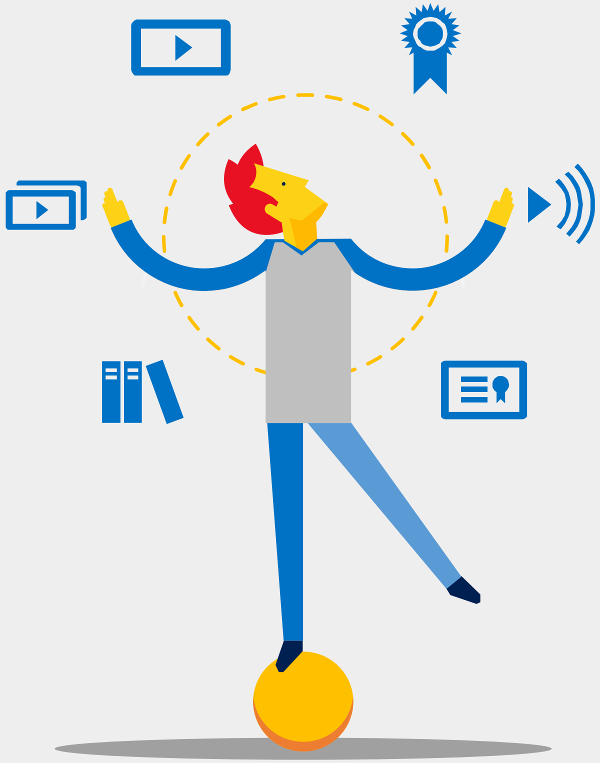
The Credential Tier Model: http://aka.ms/tiermodel

The clean-source principle: http://aka.ms/cleansource

The Ten Immutable Laws of Security Administration:
https://technet.microsoft.com/en-us/library/cc722488.aspx

Sticking with Well-Known and Proven Solutions:
https://blogs.technet.microsoft.com/fdcc/2010/10/06/sticking-with-well-known-and-proven-solutions/

Responding to IT Security Incidents:
https://technet.microsoft.com/en-us/library/cc700825.aspx



Microsoft

Microsoft