拒絕成為馬奇諾防線

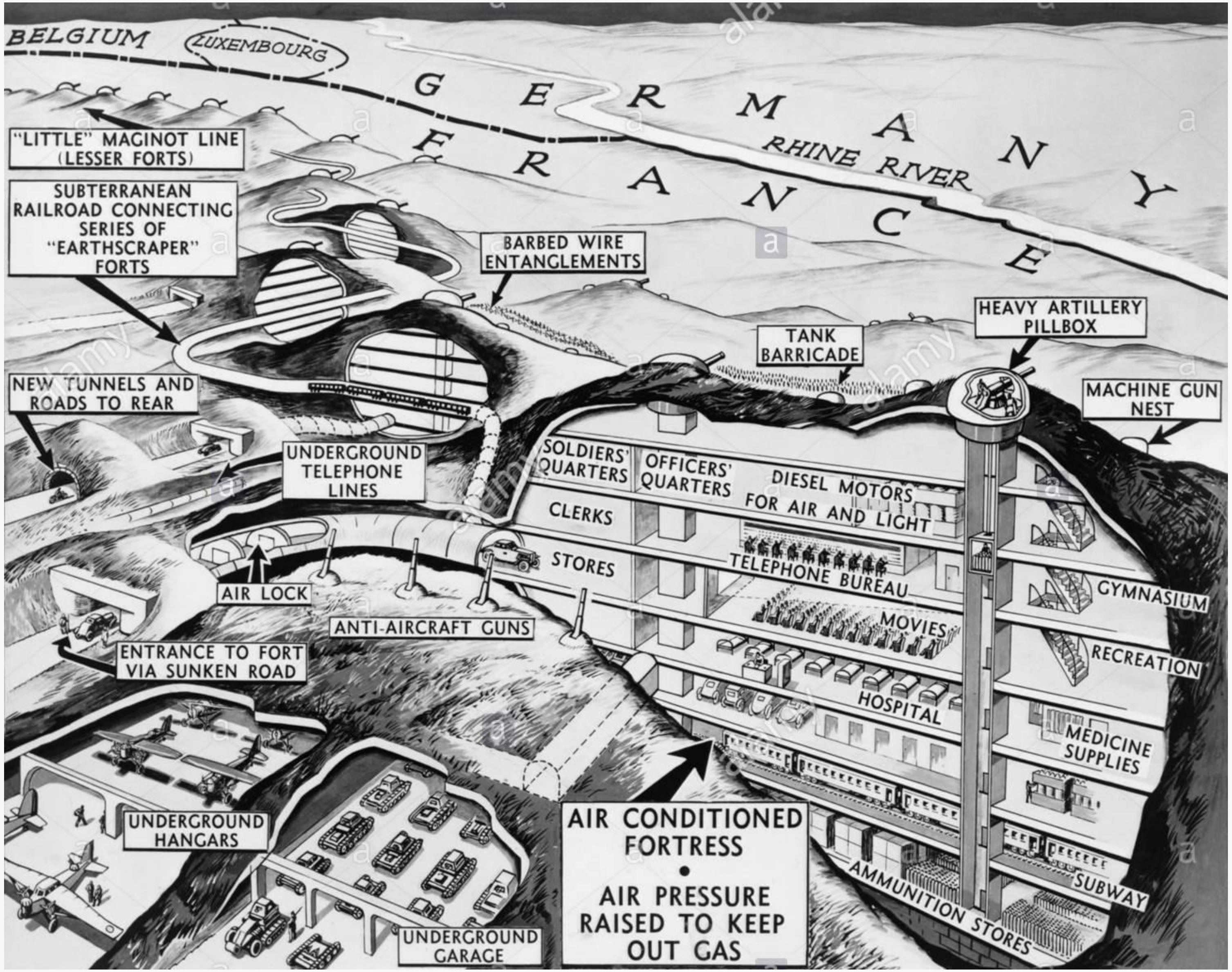
Windows Security Hardening

王偉任 (weithenn.org)

Maginot Line

http://aka.ms/MCRA

馬其諾防線 (Maginot Line)


BELGIUM
LUXEMBOURG
GERMANY
FRANCE
RHINE RIVER
"LITTLE" MAGINOT LINE (LESSER FORTS)
SUBTERRANEAN RAILROAD CONNECTING SERIES OF "EARTHSCRAPER" FORTS
BARBED WIRE ENTANGLEMENTS
HEAVY ARTILLERY PILLBOX
TANK BARRICADE
MACHINE GUN NEST
NEW TUNNELS AND ROADS TO REAR
UNDERGROUND TELEPHONE LINES
SOLDIERS' QUARTERS
OFFICERS' QUARTERS
DIESEL MOTORS FOR AIR AND LIGHT
CLERKS
STORES
TELEPHONE BUREAU
GYMNASIUM
MOVIES
RECREATION
AIR LOCK
ANTI-AIRCRAFT GUNS
ENTRANCE TO FORT VIA SUNKEN ROAD
HOSPITAL
MEDICINE SUPPLIES
UNDERGROUND HANGARS
UNDERGROUND GARAGE
AIR CONDITIONED FORTRESS • AIR PRESSURE RAISED TO KEEP OUT GAS
AMMUNITION STORES
SUBWAY

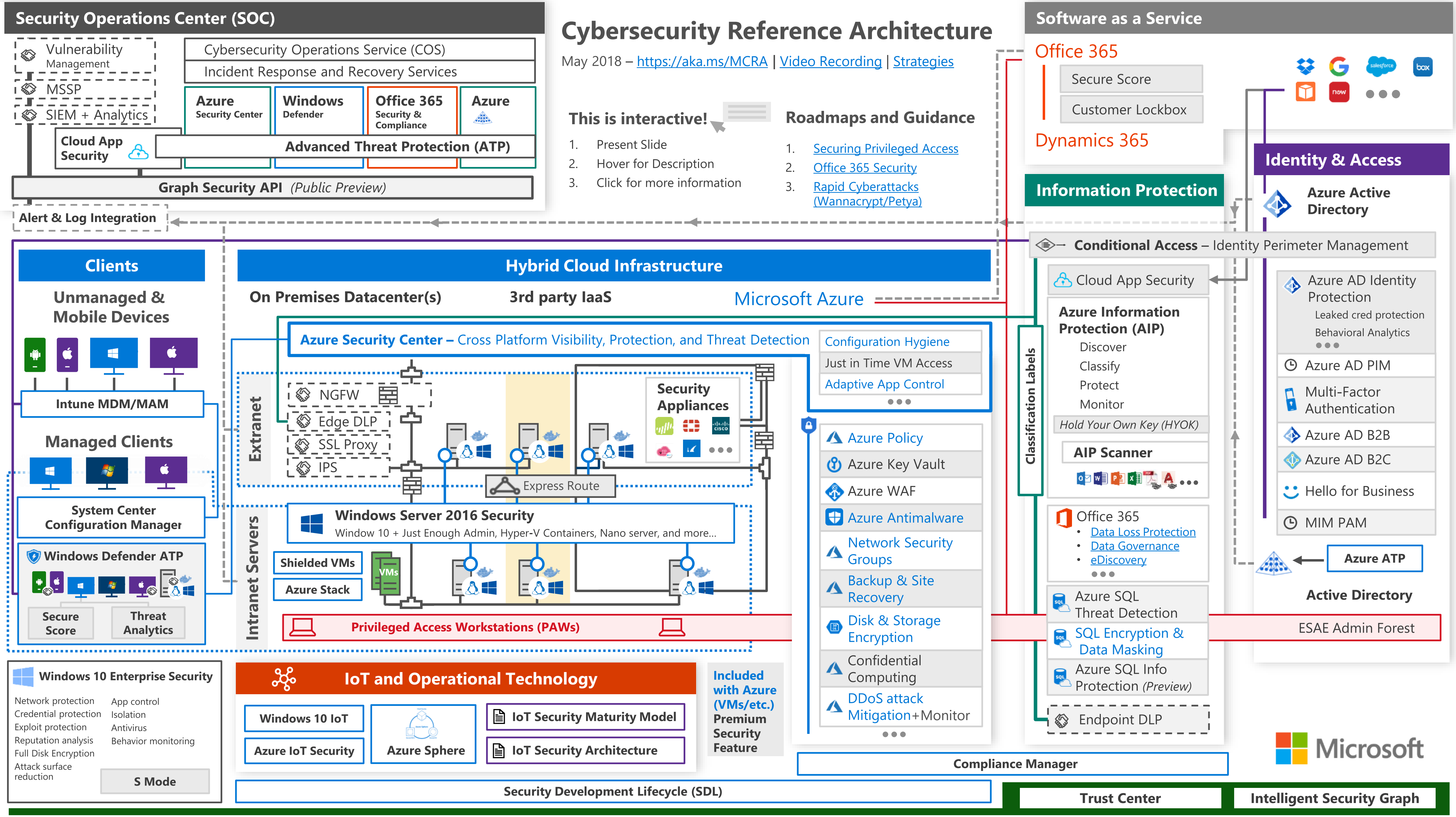
- 全長 700 公里，鋼筋混凝土建造而成，造價 50 億法郎。
- 馬奇諾防線可以防禦多類攻擊，包括空對地轟炸、大口徑火炮轟擊等，其內部擁有各式火炮、壕溝、堡壘、廚房、發電站、醫院、工廠等各類軍事及生活設施，較大的工事中還鋪設有有軌電車的軌道。
- 德軍後來沒有進攻防線正面防區，他們繞道至法國北部。然而由於法比邊界的阿登高地地形崎嶇，不適合德國作戰部隊通過，因此法軍在當地的防禦薄弱，沒有多加防備。**不到一個月後法國投降**。

Microsoft Cybersecurity Reference Architecture

http://aka.ms/MCRA

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies



Security Operations Center (SOC)

Vulnerability Management

MSSP

SIEM + Analytics

Cybersecurity Operations Service (COS)

Incident Response and Recovery Services

Azure Security Center

Windows Defender

Office 365 Security & Compliance

Azure

Cloud App Security

Advanced Threat Protection (ATP)

Graph Security API *(Public Preview)*

Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

•••

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Information Protection

Cloud App Security

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

•••

Classification Labels

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

•••

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection *(Preview)*

Endpoint DLP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Windows Defender ATP

Secure Score

Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

•••

Extranet

NGFW

Edge DLP

SSL Proxy

IPS

Security Appliances

•••

Express Route

Intranet Servers

Windows Server 2016 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

•••

Windows 10 Enterprise Security

Network protection	App control
Credential protection	Isolation
Exploit protection	Antivirus
Reputation analysis	Behavior monitoring
Full Disk Encryption	
Attack surface reduction	

S Mode

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph

Microsoft

Shielded VM

http://aka.ms/shieldedvms

Summary of the high-level **attack types**

Attack applications and infrastructure

1. Compromised privileged accounts
2. Unpatched vulnerabilities
3. Phishing attacks
4. Malware infections

Attack the virtualization fabric itself

5. Compromised fabric exposes guest VMs
6. Easy to modify or copy VM without notice
7. Can’t protect VMs with gates, walls, locks, etc.
8. VMs can’t leverage H/W security (e.g. TPMs)

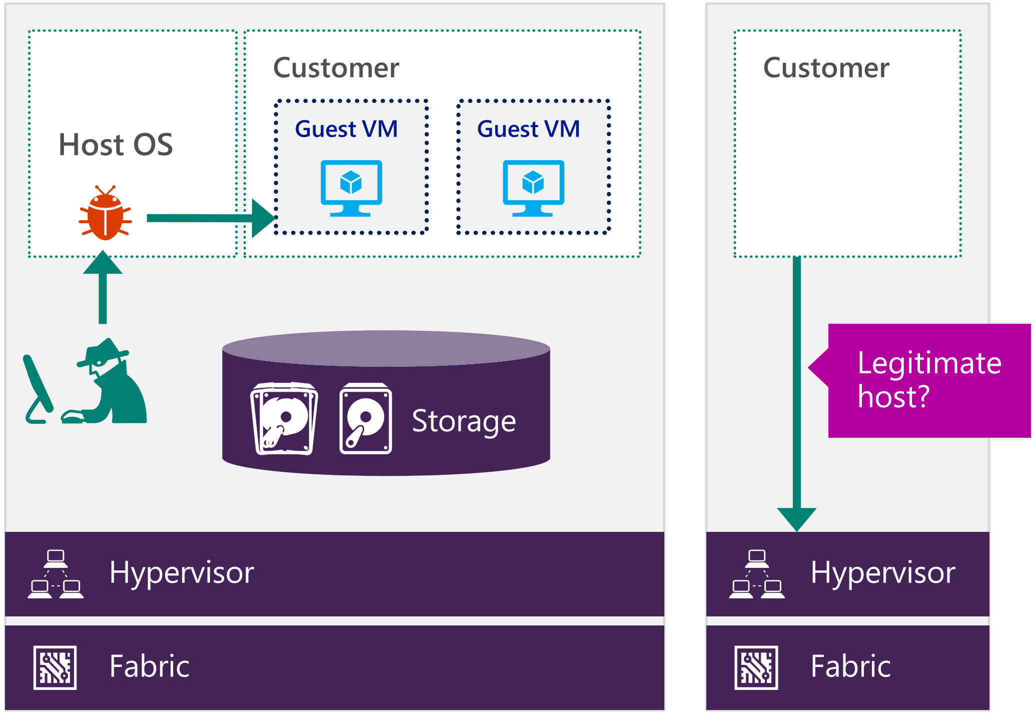
Protect virtual machines

Challenges in protecting high value virtual machines

Any seized or infected host administrators can access guest virtual machines

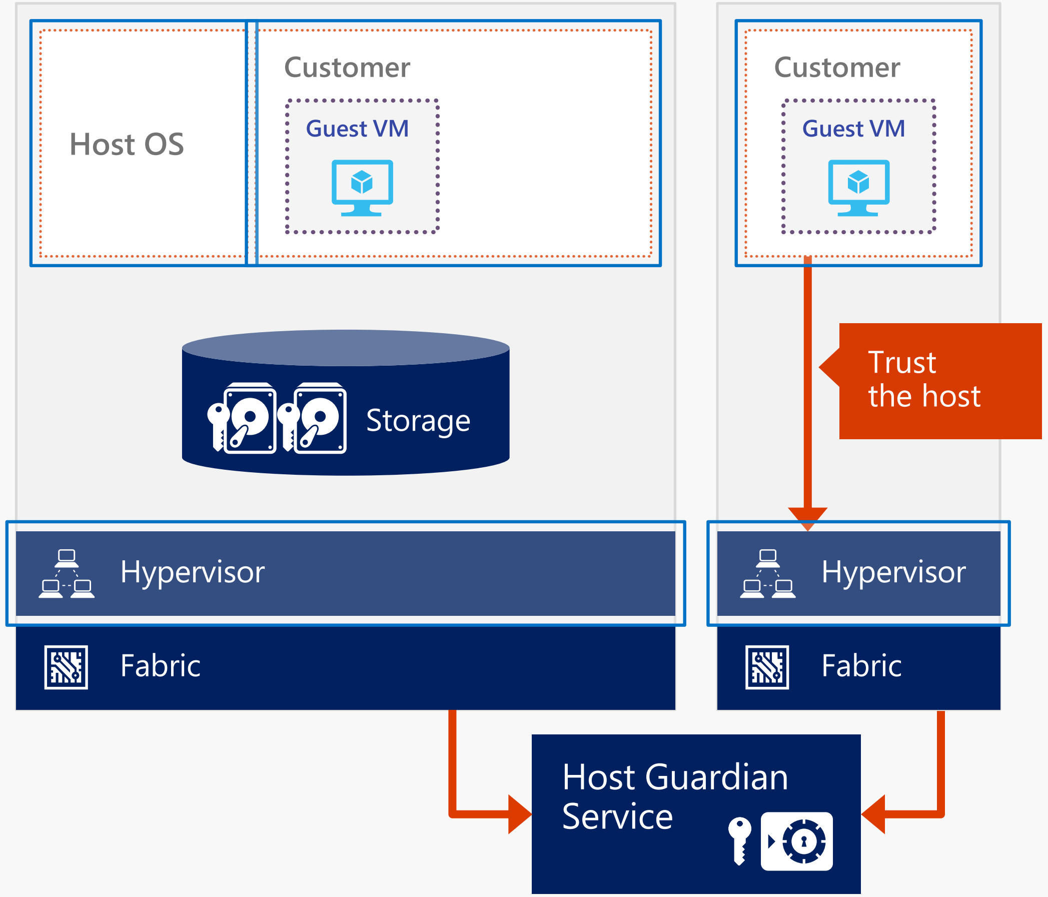
Impossible to identify legitimate hosts without a hardware based verification

Tenants VMs are exposed to storage and network attacks while unencrypted



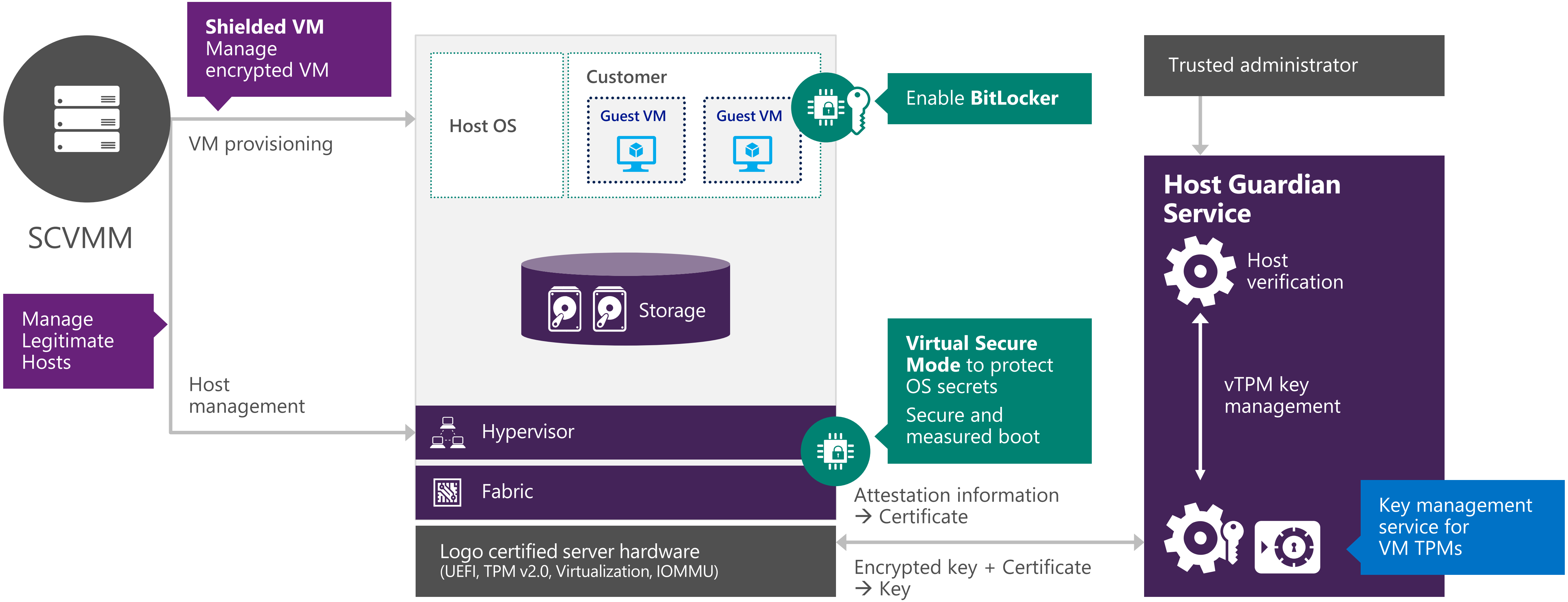
Confidently protect sensitive customer data: Designed for 'zero-trust' environments

Hardware-rooted technologies to separate the guest operating system from host administrators	**Virtual Secure Mode** Process and Memory access protection from the host
Guarded fabric to identify legitimate hosts and certify them to run shielded tenant Generation 2 VMs	**Host Guardian Service** Enabler to run Shielded Virtual Machines on a legitimate host in the fabric
Virtualized trusted platform module (vTPM) support to encrypt virtual machines	**Shielded VM** Bitlocker enabled VM



Protect virtual machines

How it works with Windows Server and System Center



Shielded VM
Manage
encrypted VM

VM provisioning

SCVMM

Manage
Legitimate
Hosts

Host
management

Host OS

Customer

Guest VM

Guest VM

Storage

Hypervisor

Fabric

Logo certified server hardware
(UEFI, TPM v2.0, Virtualization, IOMMU)

Enable **BitLocker**

Virtual Secure Mode to protect OS secrets

Secure and measured boot

Attestation information
→ Certificate

Encrypted key + Certificate
→ Key

Trusted administrator

Host Guardian Service

Host
verification

vTPM key
management

Key management
service for
VM TPMs

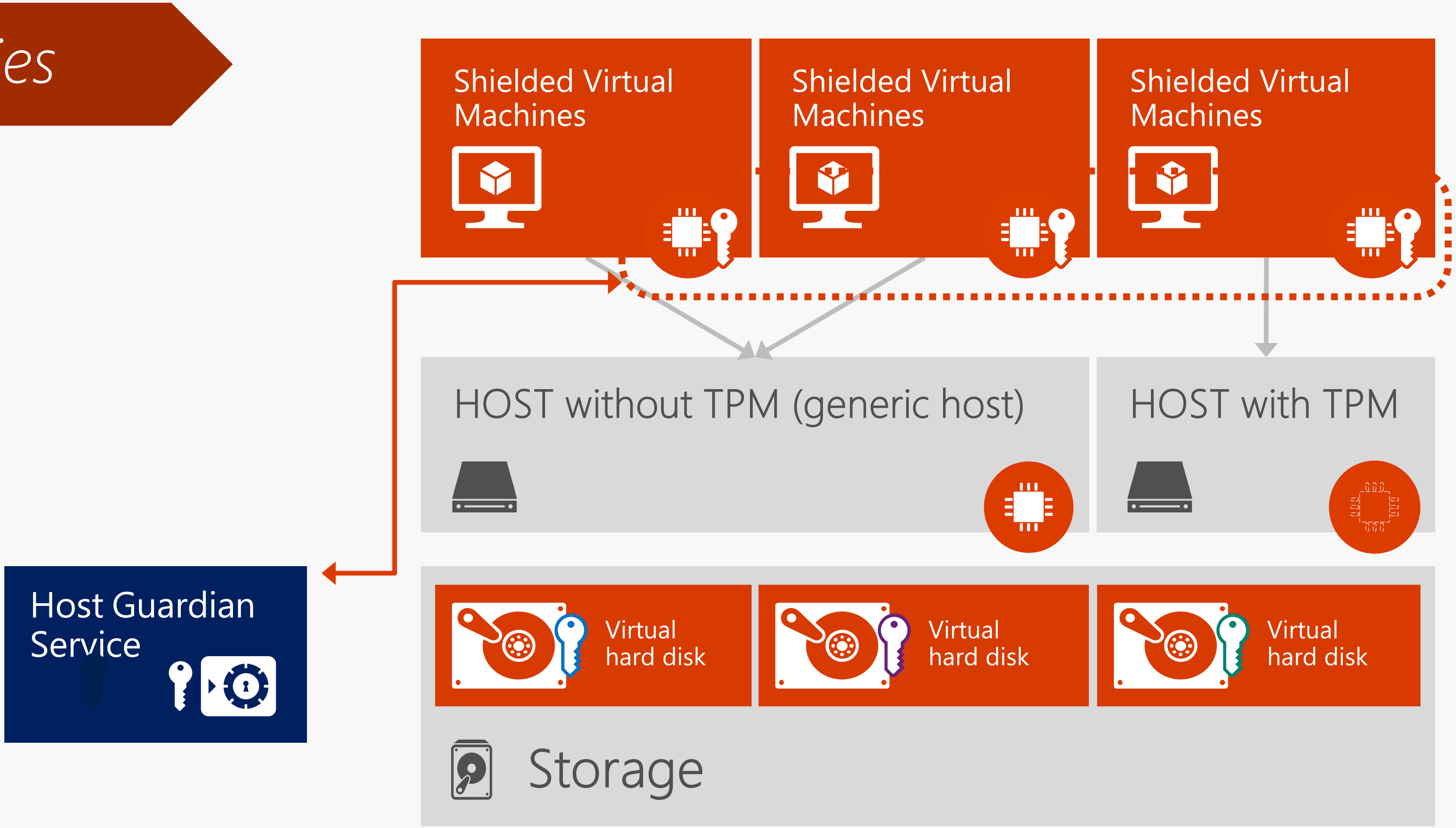
Shielded VMs

Spotlight capabilities

Shielded Virtual Machines can only run in fabrics that are designated as owners of that virtual machine

Shielded Virtual Machines will need to be **encrypted** (by **BitLocker** or other means) in order to ensure that only the designated owners can run this virtual machine

You can **convert** a **running Generation 2 virtual machine** into a Shielded Virtual Machine


Shielded Virtual Machines
Shielded Virtual Machines
Shielded Virtual Machines
HOST without TPM (generic host)
HOST with TPM
Host Guardian Service
Virtual hard disk
Virtual hard disk
Virtual hard disk
Storage

Bare Metal vs. Regular VM vs. **Shielded VM**

Shielded VM

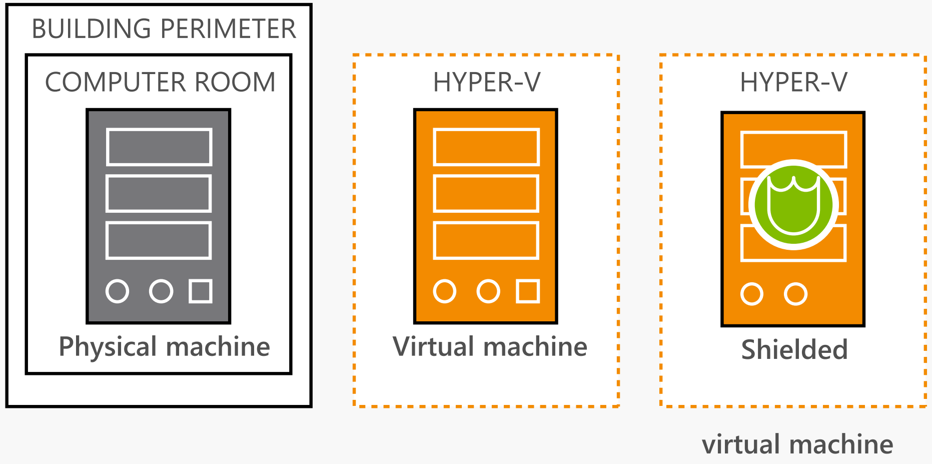
Use BitLocker to encrypt the disk and state of virtual machines protecting secrets from compromised admins & malware

Host Guardian Service

Attests to host health releasing the keys required to boot or migrate a Shielded VM only to healthy hosts

Generation 2 VM

Supports virtualized equivalents of hardware security technologies (e.g. TPMs) enabling BitLocker encryption for Shielded VMs



	Physical machine	Virtual machine	Shielded virtual machine
Server Administrator	✓	✓	✗*
Storage administrator	✗	✓	✗
Network administrator	✗	✓	✗
Backup operator	✗	✓	✗
Virtualization-host administrator	✗	✓	✗
Virtual machine administrator	✗	✓	✓

*Configuration dependent

Shielded VMs: **a few Spotlights**

Generation 2 VMs only

Leveraging virtual EFI, Secure boot, virtual TPM

Hyper-V Host: Windows Server 2016

Guarded host requires Windows Server 2016 Datacenter edition

Shielded Guest VM OS support

Windows 8 / Windows Server 2012 or newer

vTPM not tied to physical TPM

Permits VM mobility, e.g. Live Migration

Guarded Fabric: **Attestation Modes**

Admin-trusted

Simplified Setup/Configuration

- Setup an Active Directory trust + register group
- Authorize a Hyper-V host to run shielded VMs by adding it to the Active Directory group

Leveraging Existing H/W

- H/W needs to support Hyper-V on Windows Server 2016

Weaker levels of assurance

- Fabric-admin is trusted
- No hardware-rooted trust or measured-boot
- No enforced code-integrity

INITIAL ADOPTION SIMPLIFIER

TPM-trusted ★

Complex setup/configuration

- Register each Hyper-V host's TPM (EKpub) with the guardian service
- Baseline CI policy for each different hardware SKU
- Optional: Deploy HSM and use HSM-backed certificates

Specific host hardware required

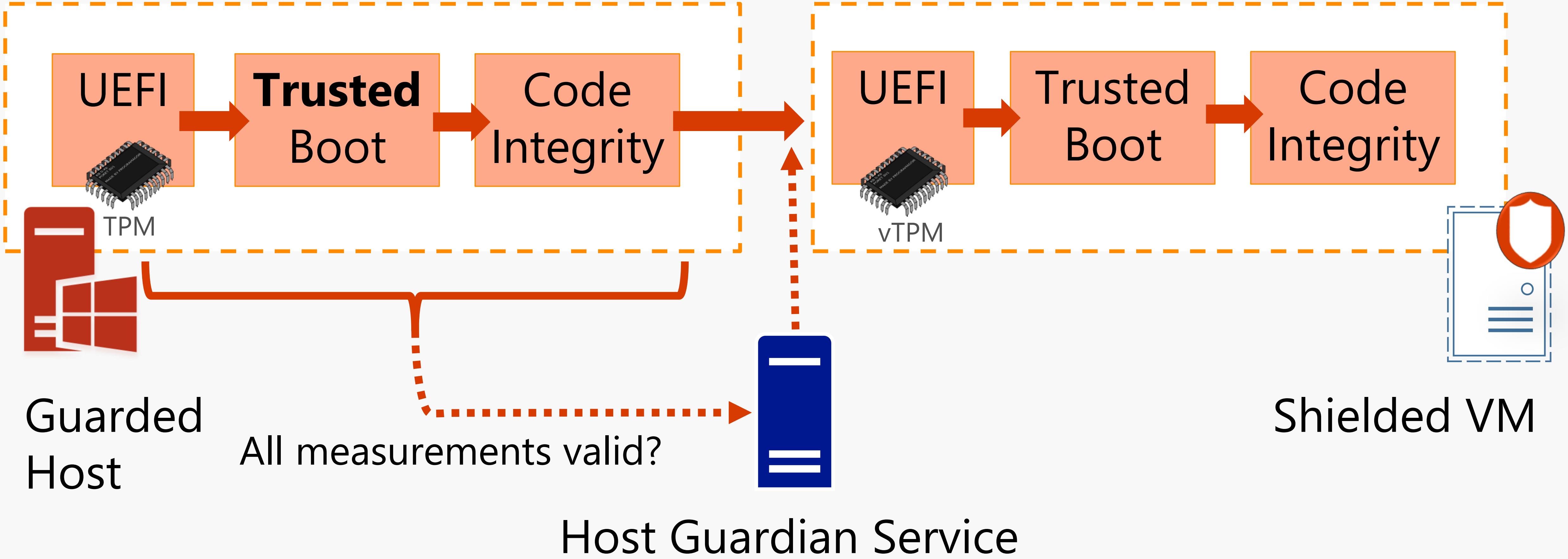
- Needs to support TPM v2.0 and UEFI 2.3.1

Highest levels of assurance

- Fabric-admin untrusted
- Trust rooted in hardware
- Compliance with code-integrity policy required for key-release (attestation)

RECOMMENDED STEADY-STATE

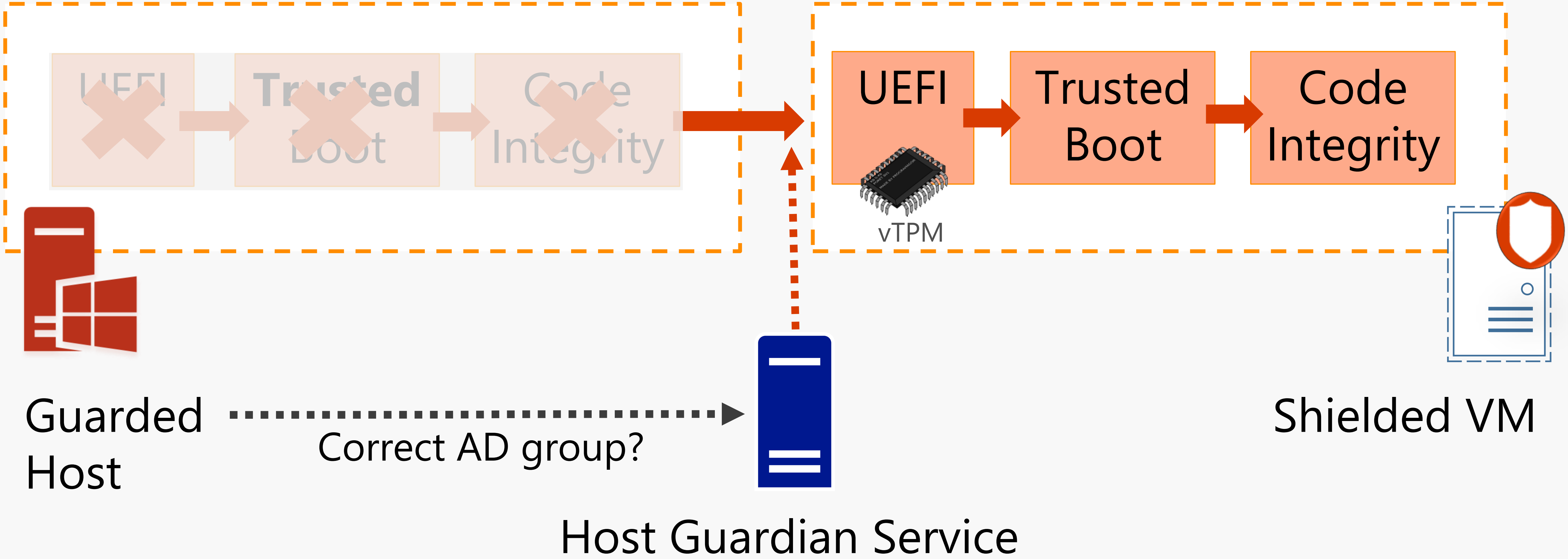
Trust chain: **TPM-trusted attestation**



Attestation: validates the health of the host (boot and CI measurements)

Requires: UEFI 2.3.1 and TPM 2.0 for guarded hosts

Trust chain: **admin-trusted attestation**



Attestation: no boot measurements or code-integrity policies are taken into account

Shielded VMs: **two modes of shielding**

Shielded

- OS disk encrypted, Live Migration traffic encrypted, use vTPMs to seal keys, VMconsole connections blocked, PowerShell Direct blocked, integration components blocked, VM runs as protected process (light)
- Common use-case: *public cloud, private cloud requiring segregation of admin duties*

Encryption Supported

- OS disk encrypted, Live Migration traffic encrypted, use vTPMs to seal keys
  - VMconsole connections permitted
  - PowerShell Direct permitted
- Common use-case: *compliance, private cloud with trusted admins, etc.*

NOTE: *a VM's shielding type is dictated/configured by the Shielding Data from which the shielded VM is born*

Demo

Regular VM (Non-Shielded VM)

Demo

Shielded VM

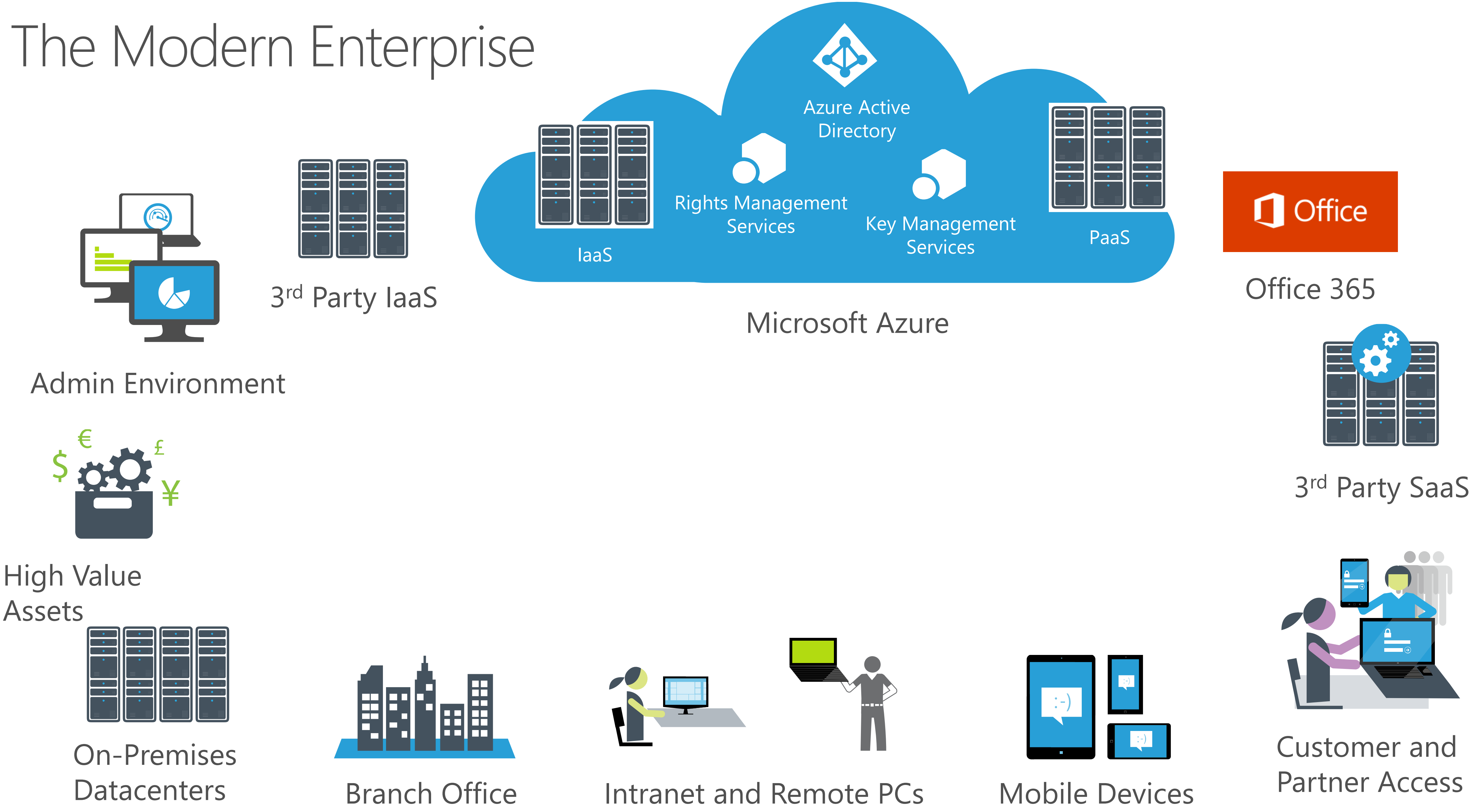
Hyper-V Shielded VM: **Compliance Mapping**

	ISO 27001: 2013	PCI DSS 3.2	FedRAMP; NIST 800-53 Revision 4
Enforcing Separation of Duties	A.6.1.2– Segregation of duties	6.4.2 – Separation of duties between test and production environments	AC-5 – Separation of Duties
Implementation of Least Privilege Access and Partitioning Tenant Functionality	A.9.2.3 – Management of privileged access rights A.12.1.4 – Separation of development, testing, and operational environments	6.4.1 – Test and Production Environment Separation 7.2 – User access control on need-to-know basis 7.2.3 – Default "deny-all" setting	AC-6 – Least Privilege AC-6 (10) – Prohibit Non-Privileged Users from Executing Privileged Functions SC-2 – Application Partitioning
Protecting Information Stored in Shared Resources	None	8.7 – Restricted access to databases containing cardholder data	SC-4 – Information in Shared Resources
Protection of Data at Rest	A.8.2.3 – Media Access	3.4 – Verifying stored PAN is unreadable 3.4.1 – Disk encryption usage and access control 6.5.3 – Insecure cryptographic storage	SC-28 – Protection of Information at Rest SC-28(1) – Protection of Information at Rest
Security Function Verification and Integrity Monitoring	None	11.5 – Change-detection mechanism deployment	SI-6 – Security Function Verification SI-7 – Software, Firmware, and Information Integrity

Credential Guard

http://aka.ms/privsec

The Modern Enterprise



Azure Active Directory

Rights Management Services

Key Management Services

IaaS

PaaS

Microsoft Azure

Office

Office 365

3rd Party IaaS

Admin Environment

3rd Party SaaS

High Value Assets

On-Premises Datacenters

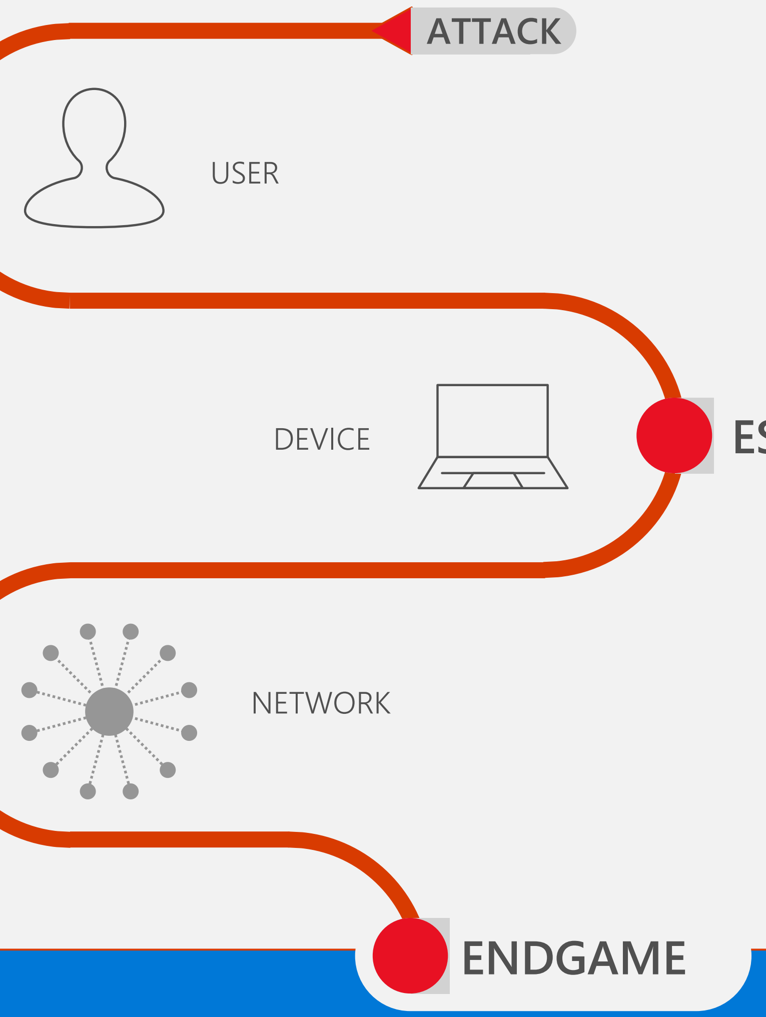
Branch Office

Intranet and Remote PCs

Mobile Devices

Customer and Partner Access

Anatomy of an **attack**



ATTACK

Browser or Doc Exploit Delivery
Malicious Attachment Delivery
Phishing Attacks

ENTER

USER

DEVICE

ESTABLISH

Internet Service Compromise
Browser or Doc Exploit Execution
Malicious Attachment Execution
Stolen Credential Use

Kernel Exploits
Kernel-mode Malware
Pass-the-Hash

EXPAND

NETWORK

ENDGAME

BUSINESS DISRUPTION | **LOST PRODUCTIVITY** | **DATA THEFT** | **ESPIONAGE, LOSS OF IP** | **RANSOM**

What do most attacks have **in-common?**

- Phishing attacks
- Stolen credentials
- Pass-the-hash (PtH) attacks
- Insider attacks
- Fabric attacks

Central risk: **Administrator privileges**

Administrative Privileges

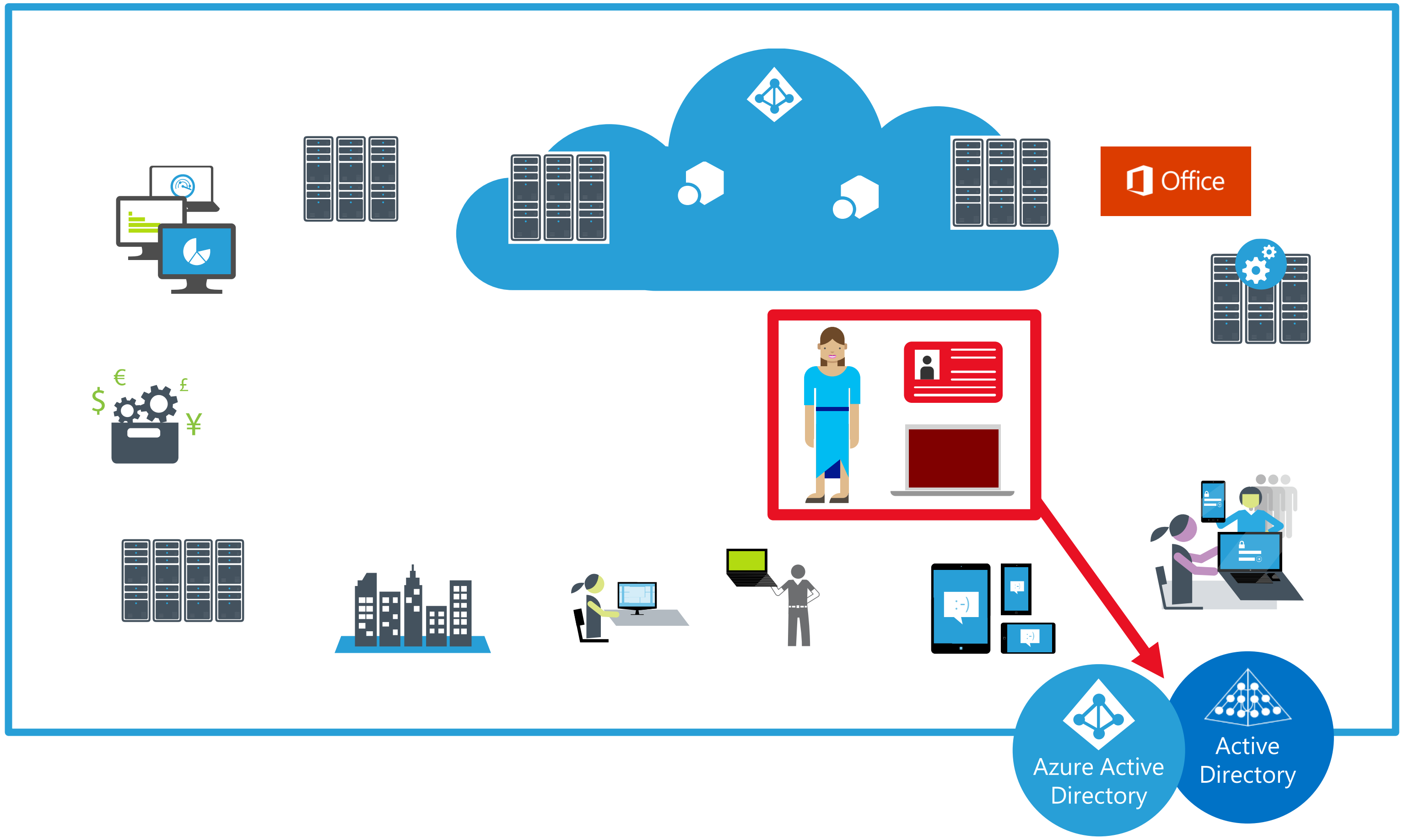
Most attack-types seek out & exploit privileged accounts

These privileged accounts have the keys to the kingdom; we gave them those keys decades ago

But now, those administrators’ privileges are being compromised through social engineering, bribery, coercion, private initiatives, etc.

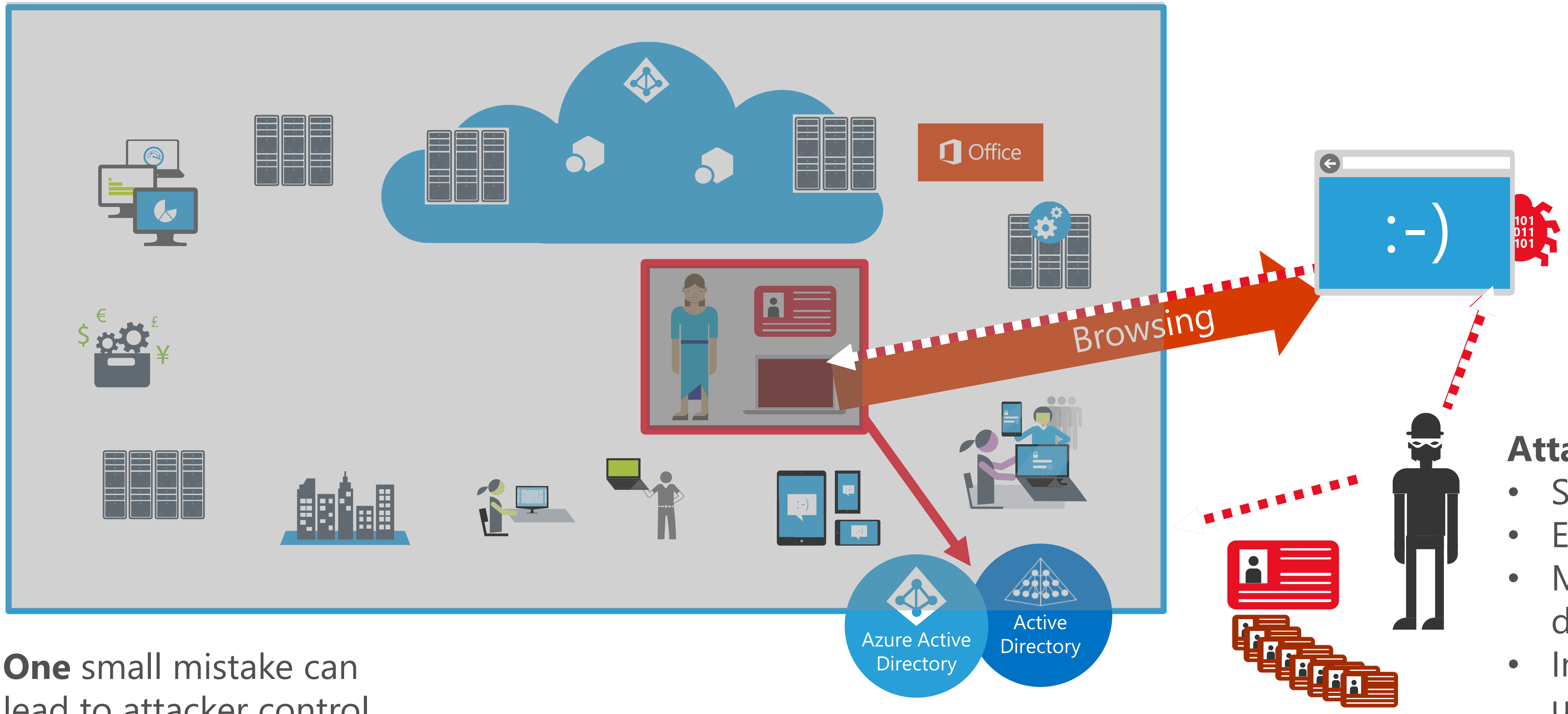
Identity is the new security "perimeter"

Active Directory and Administrators control all the assets



Identity is the new security "perimeter" under attack

Active Directory and Administrators control all the assets



One small mistake can lead to attacker control

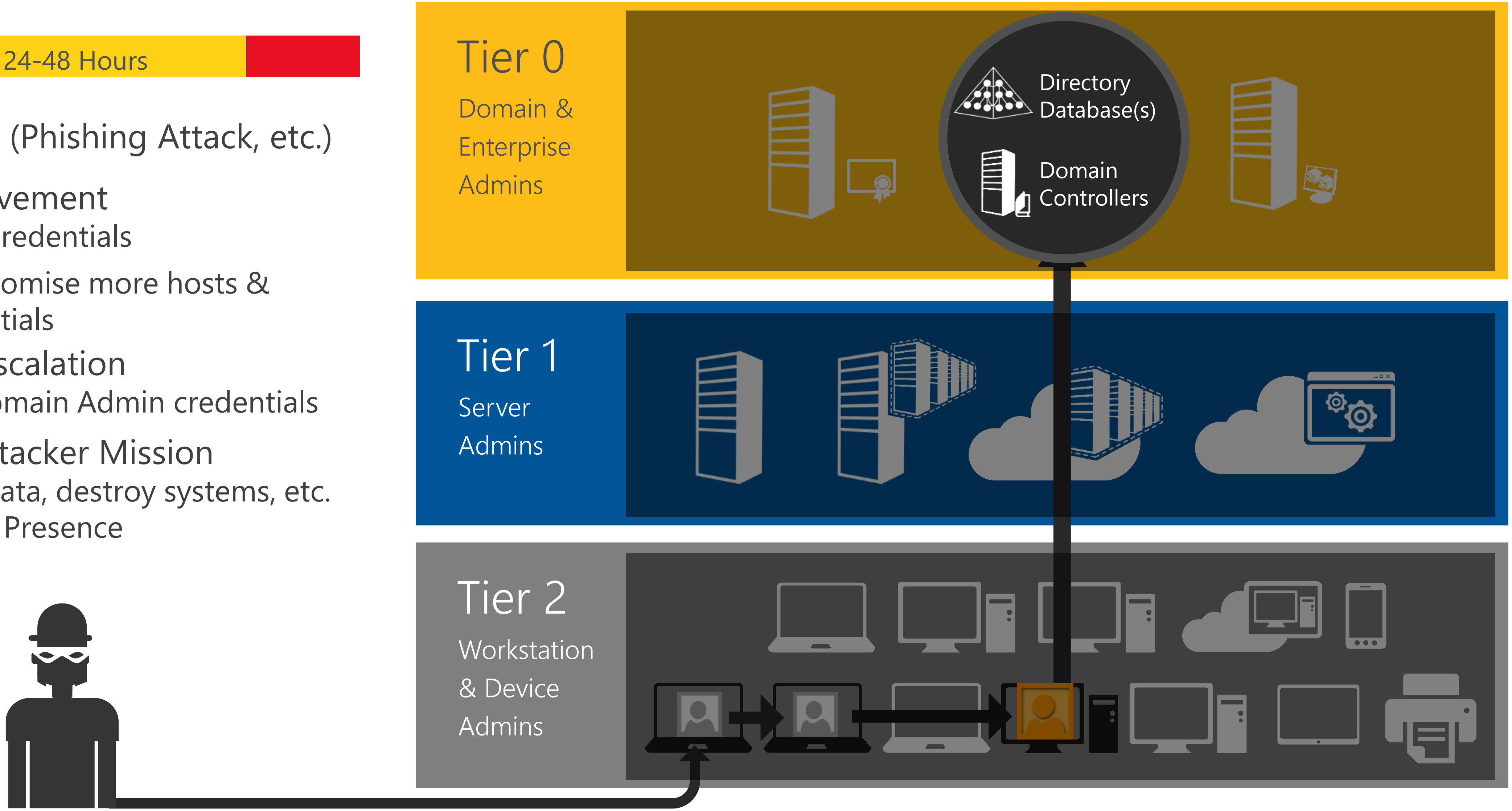
Attackers Can

- Steal any data
- Encrypt any data
- Modify documents
- Impersonate users
- Disrupt business operations

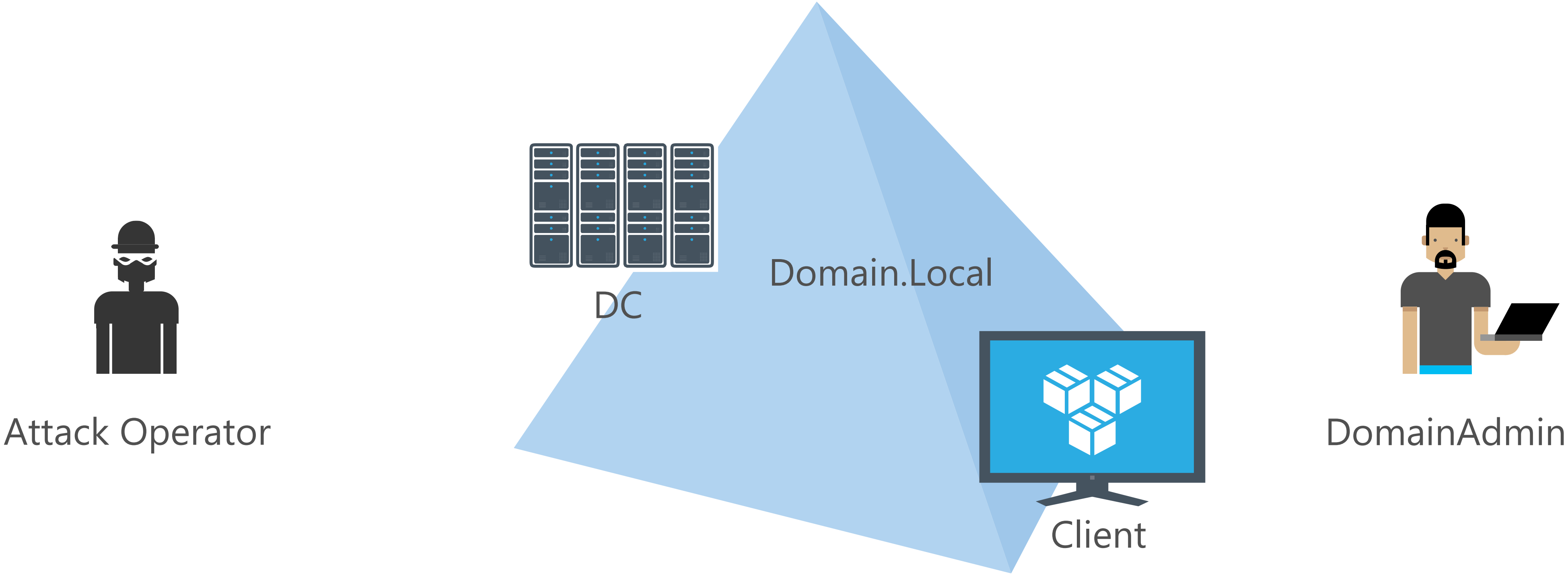
Phase 1 Critical Mitigations: Typical Attack Chain

Compromises privileged access

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



Phase 1 Critical Mitigations: Credential Theft Demonstration



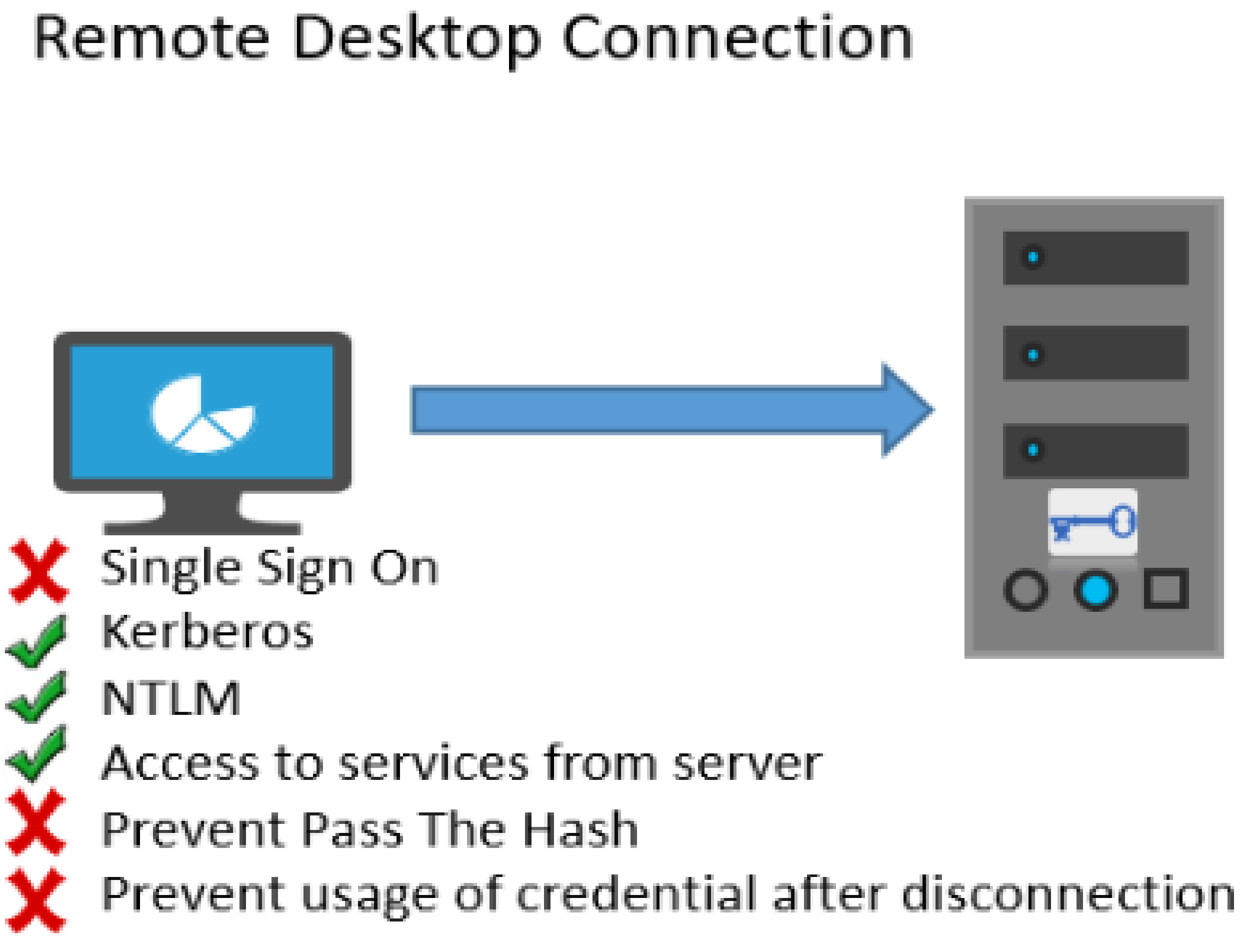
Demo

Without Credential Guard (Win 7 & Win 10)

Demo

Windows 10 with Credential Guard

Remote Desktop Connection



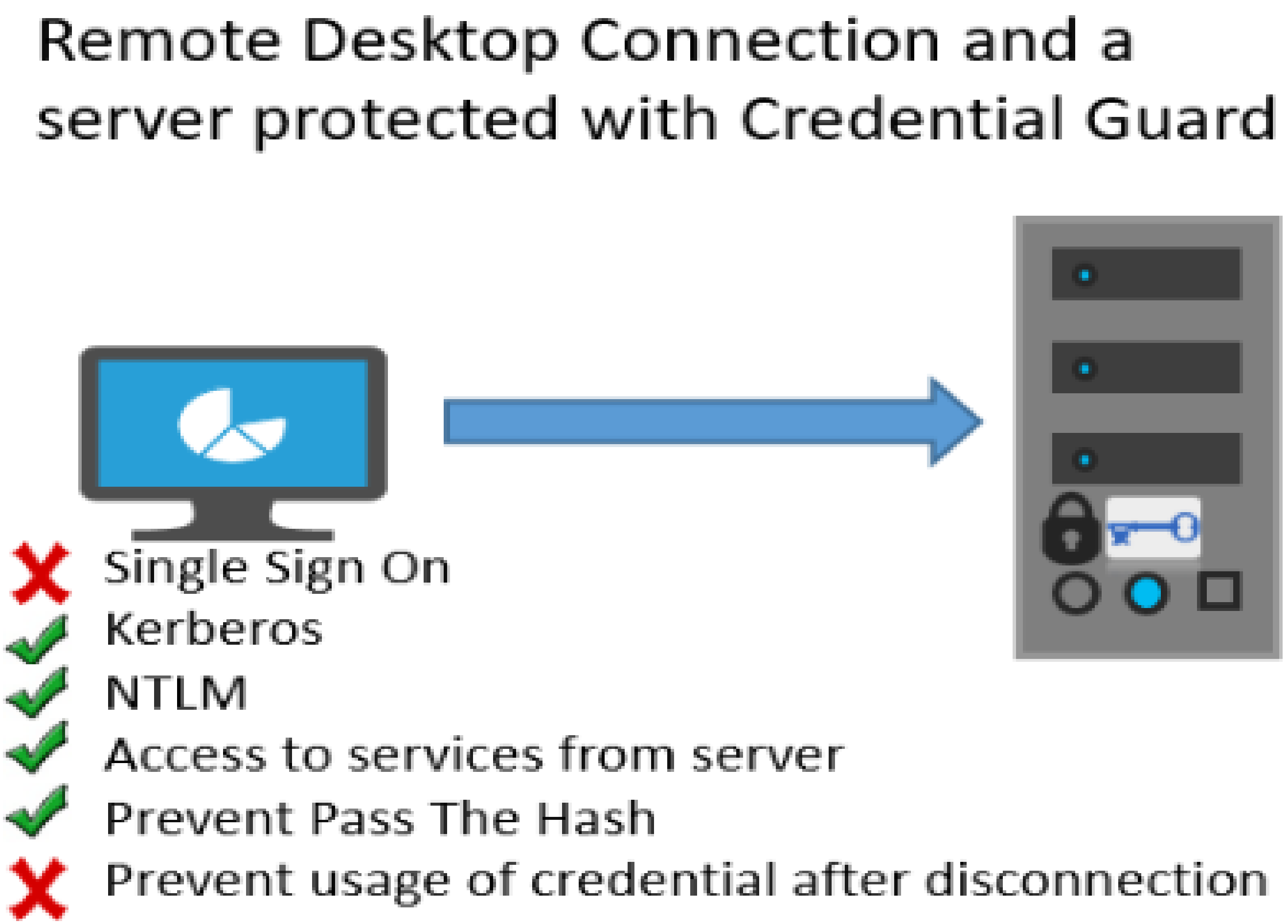
Remote Desktop Connection

- ✗ Single Sign On
- ✓ Kerberos
- ✓ NTLM
- ✓ Access to services from server
- ✗ Prevent Pass The Hash
- ✗ Prevent usage of credential after disconnection

Demo

Standard Remote Desktop Connection

RDP Server with Credential Guard



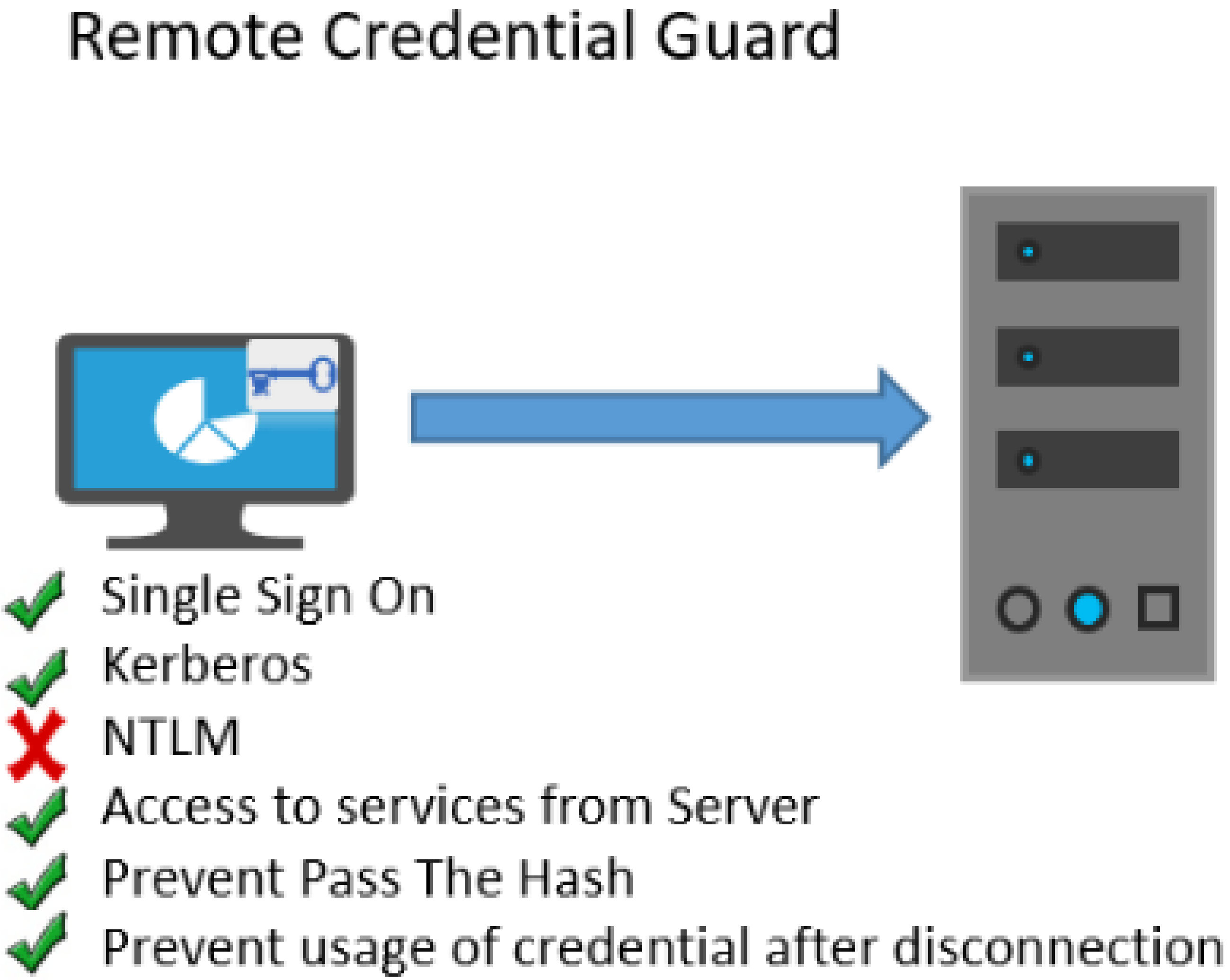
Remote Desktop Connection and a server protected with Credential Guard

- ✗ Single Sign On
- ✓ Kerberos
- ✓ NTLM
- ✓ Access to services from server
- ✓ Prevent Pass The Hash
- ✗ Prevent usage of credential after disconnection

Demo

RDP Server with Credential Guard

RDP Client with Remote Credential Guard



Remote Credential Guard

- ✓ Single Sign On
- ✓ Kerberos
- ✗ NTLM
- ✓ Access to services from Server
- ✓ Prevent Pass The Hash
- ✓ Prevent usage of credential after disconnection

Demo

RDP Client with Remote Credential Guard

Q&A

Thanks you!