TRUESEC

INFRASTRUCTURE SUMMIT 2019

Manage your environment – the secure way

GET-EXPERTS

Mikael Nystrom	**Hasain Alshakarti**
@mikael_nystrom	@Alshakarti
Mikael.nystrom@truesec.com	Hasain.Alshakarti@truesec.com
MVP – 15 Years	The “Wolf”
Likes Food, mostly	Halal

Story Time!

The organization that existed until it didn’t

- NTLM Authentication
- If everyone’s a local admin then no one’s a local admin! — Technically correct
- Password resets what are those?
- Azure AD and MFA What’s that?
- Patch Management

Could it been prevented?

10 year old guidelines on how to manage IT would have prevented it

Numbers

45 Minutes

The time it takes for our pen testers to be administrators

80 %

Number of successful attacks done be steeling admin credentials

6 Months

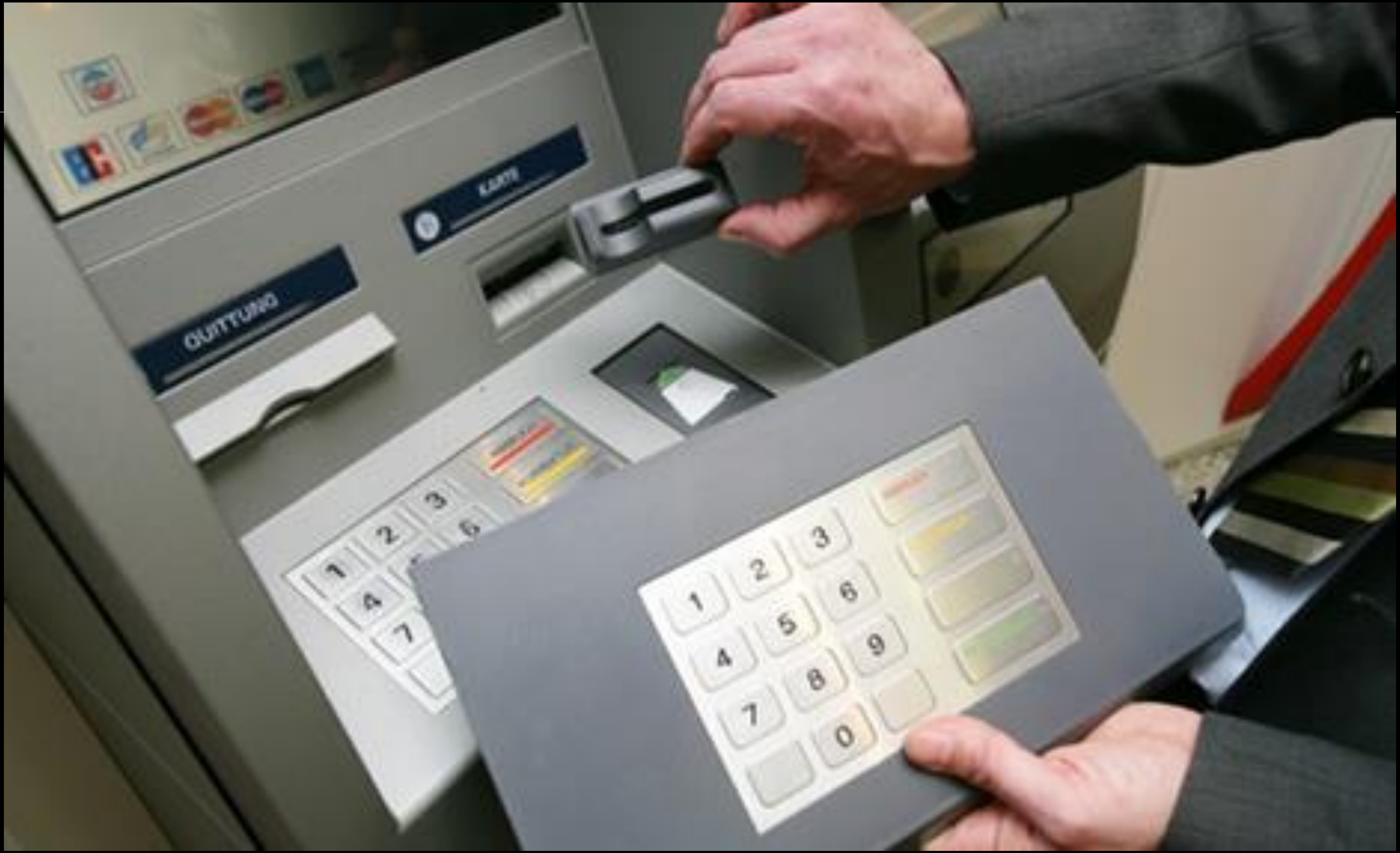
The time between first penetration until detection

Could it been prevented?

10 year old guidelines on how to manage IT would have prevented it

DEMO SLIDE

Let us do some fun stuff…


QUITTUNG
KARTE
1
2
3
4
5
6
7
8
9
0

Attack services are inexpensive

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

0days price range varies from $5,000 to $350,000

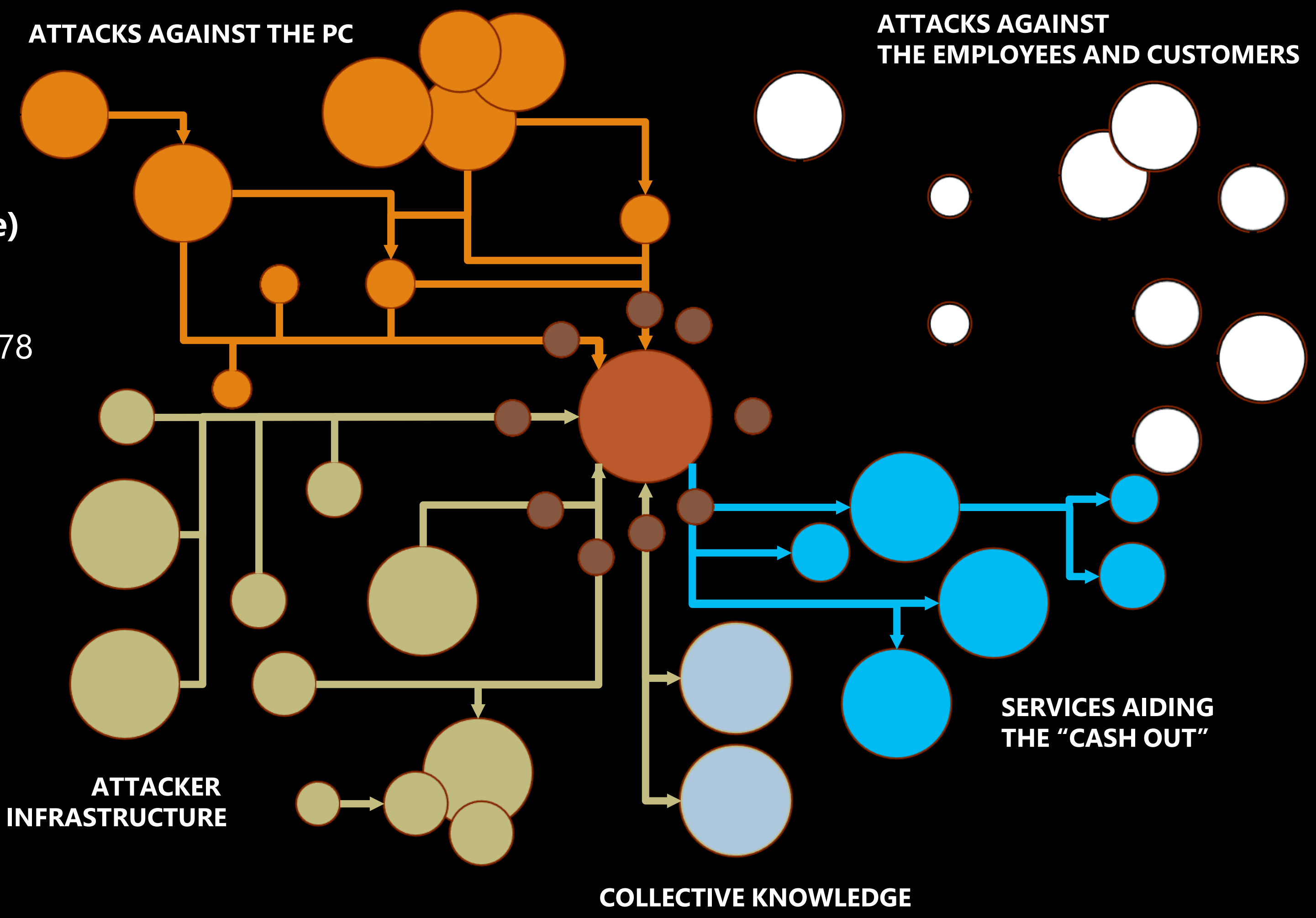
Loads (compromised device) average price ranges

- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices

day: $102.05
week: $327.00
month: $766.67

Proxy services to evade IP geolocation prices vary As low as $100 per week for 100,000 proxies.


ATTACKS AGAINST THE PC
ATTACKS AGAINST THE EMPLOYEES AND CUSTOMERS
ATTACKER INFRASTRUCTURE
SERVICES AIDING THE "CASH OUT"
COLLECTIVE KNOWLEDGE

Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts As low as $150 for 400M. Averages $0.97 per 1k.

Avoiding becoming a story!

Attackers Mindset

Identify High Value Targets

- Fabric components, Domain controllers, Management Servers, jump servers, admin clients …

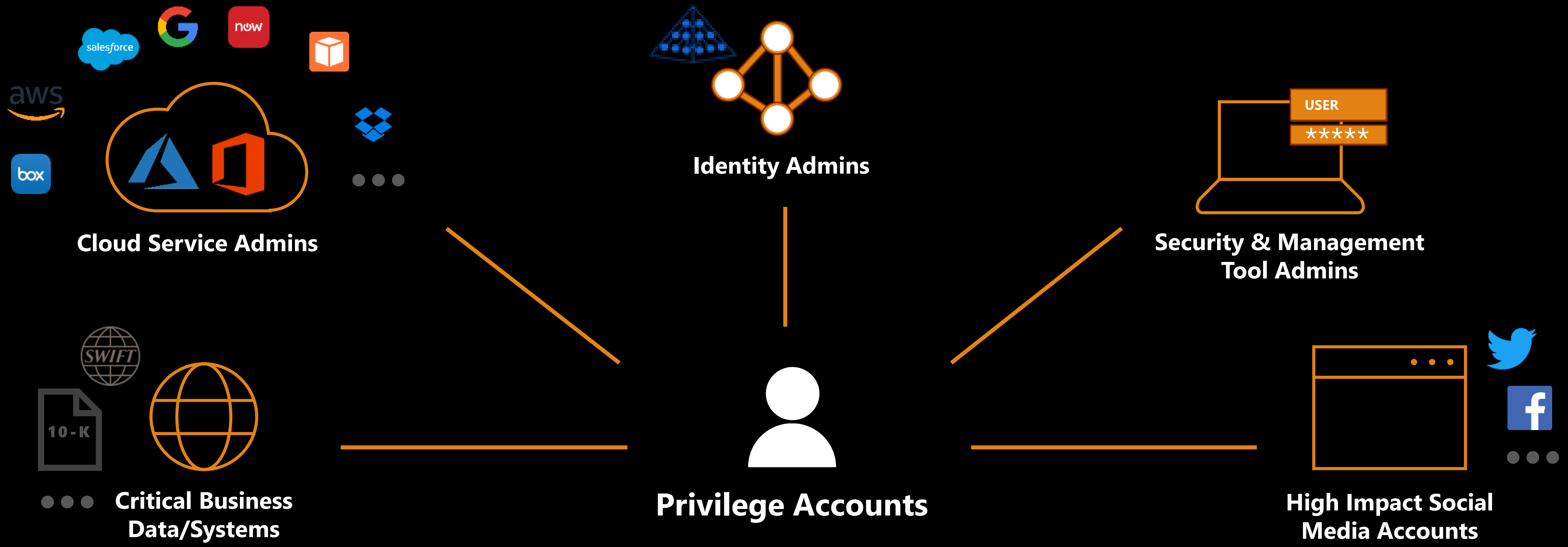
Identify Privileged Accounts

- Who are the administrators on these servers

Gain Access to Admin Credentials

- What can be compromised to get the credentials of a target admin

Privileged Access is more than Administrators



Cloud Service Admins

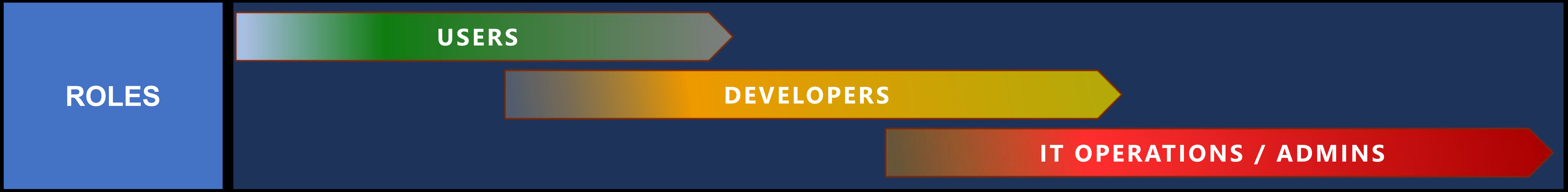
Identity Admins

Security & Management Tool Admins

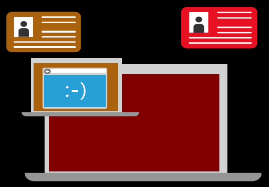
Critical Business Data/Systems

Privilege Accounts

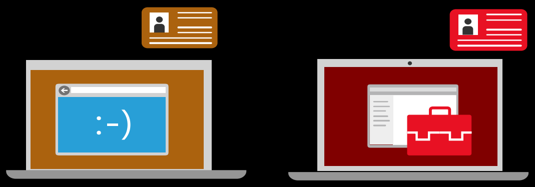
High Impact Social Media Accounts



PROFILES	Low Security Workstation	Enhanced Security Workstation	High Security Workstation	Specialized Workstation	Secured Workstation –aka PAW
SECURITY CONTROLS	•**Productivity Apps** •**Application and browser activity monitored** •**User Managed policies** •**Antivirus**	•*Low Security Plus…* •**Centrally Managed Policies** •**Defender ATP**	•*Enhanced Security Plus…* •**No Local Admin**	•*High Security Plus…* •**Restricted applications** •**Restricted browsing**	•*High Security Plus…* •**No productivity applications** •**Restricted browsing** •**Separate identity**



Virtualization



Physical Separation

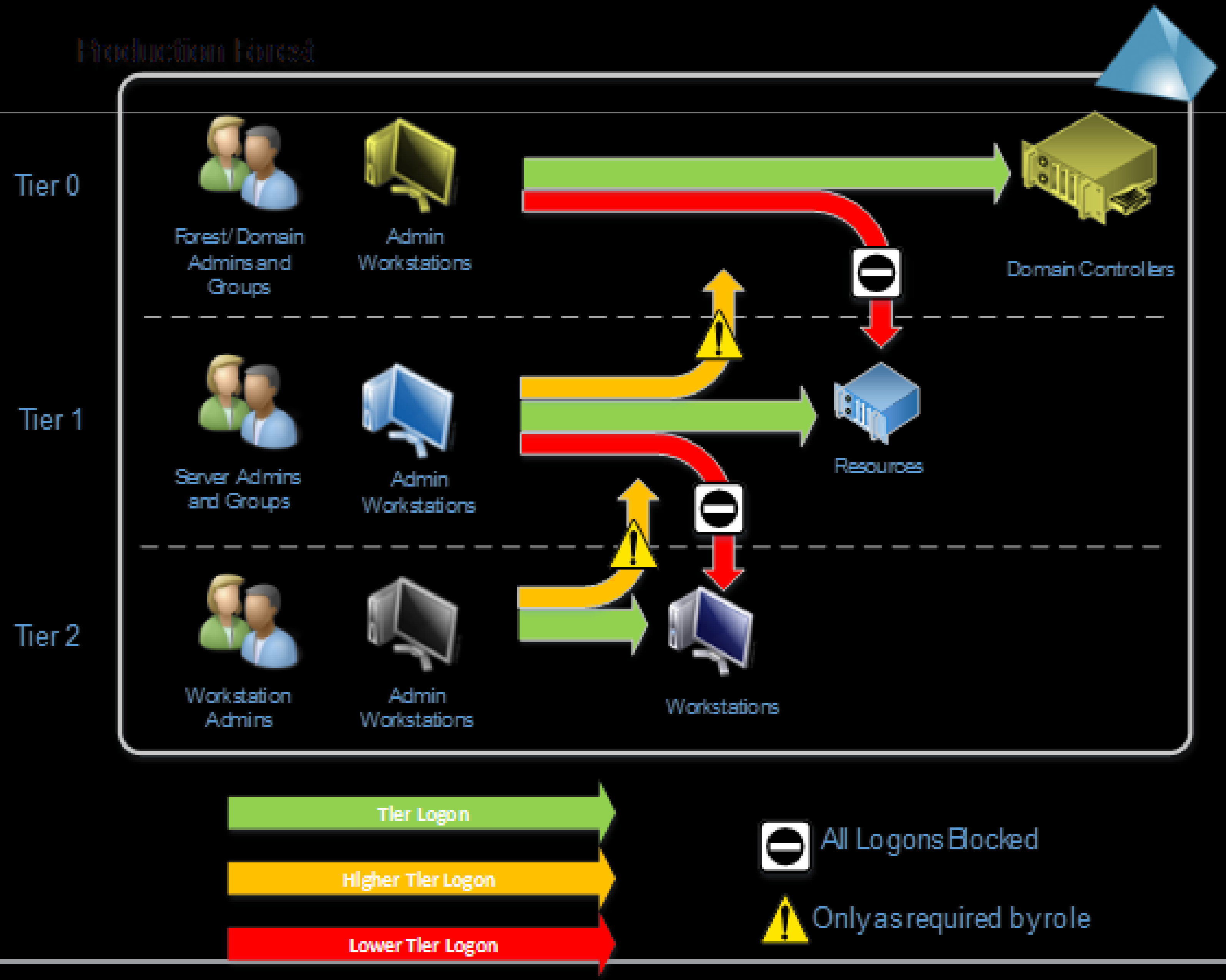
Secure Workstation Documentation

Overview- *http://aka.ms/SWoverview*

Implementation - *http://aka.ms/secureworkstation*

DEMO SLIDE

PAWs, Silo, SSO, Remote Admin



Production Forest

Tier 0

Forest/ Domain Admins and Groups

Admin Workstations

Domain Controllers

Tier 1

Server Admins and Groups

Admin Workstations

Resources

Tier 2

Workstation Admins

Admin Workstations

Workstations

Tier Logon

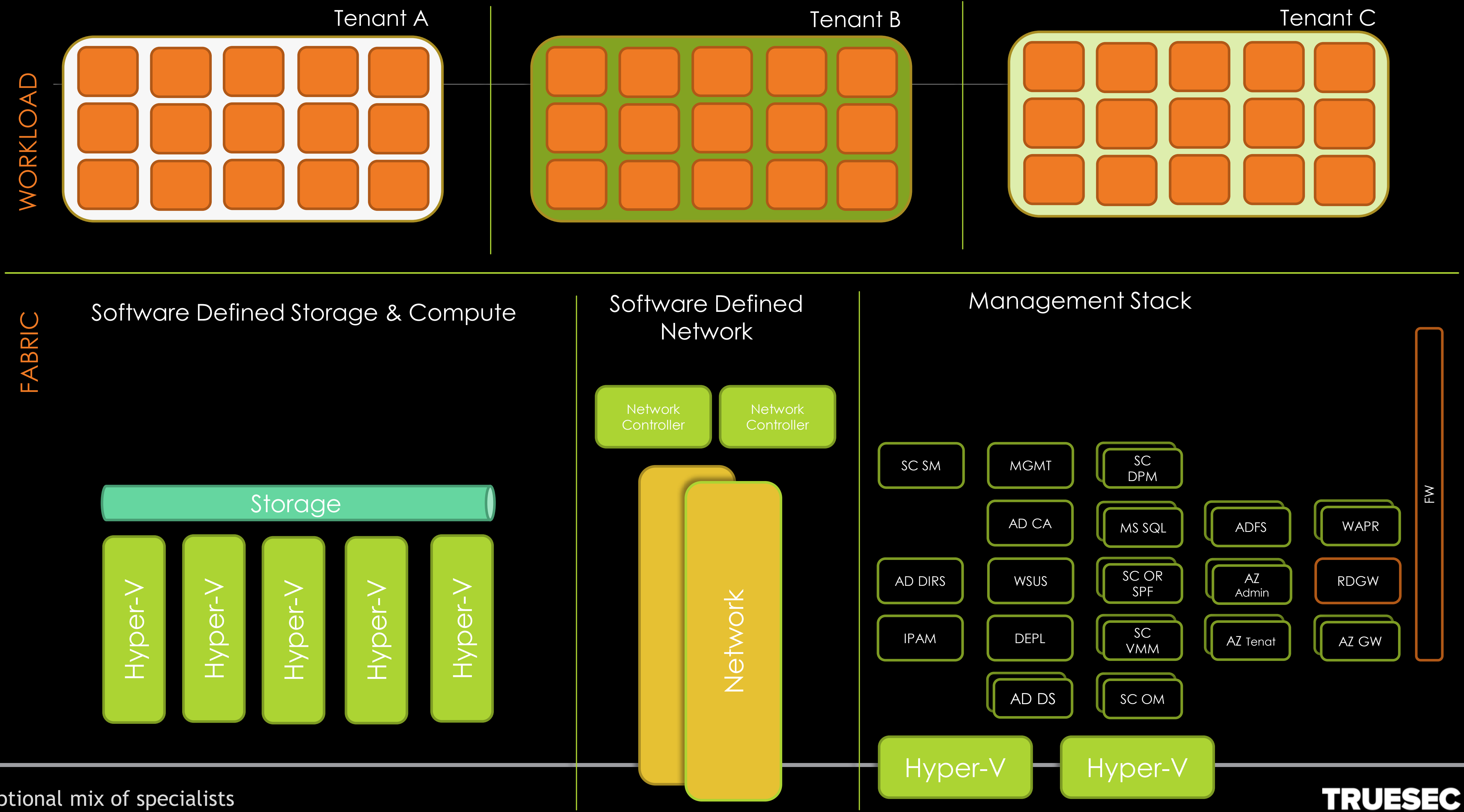
Higher Tier Logon

Lower Tier Logon

⛔ All Logons Blocked

⚠ Only as required by role

Private Cloud (Hyper-Converged)



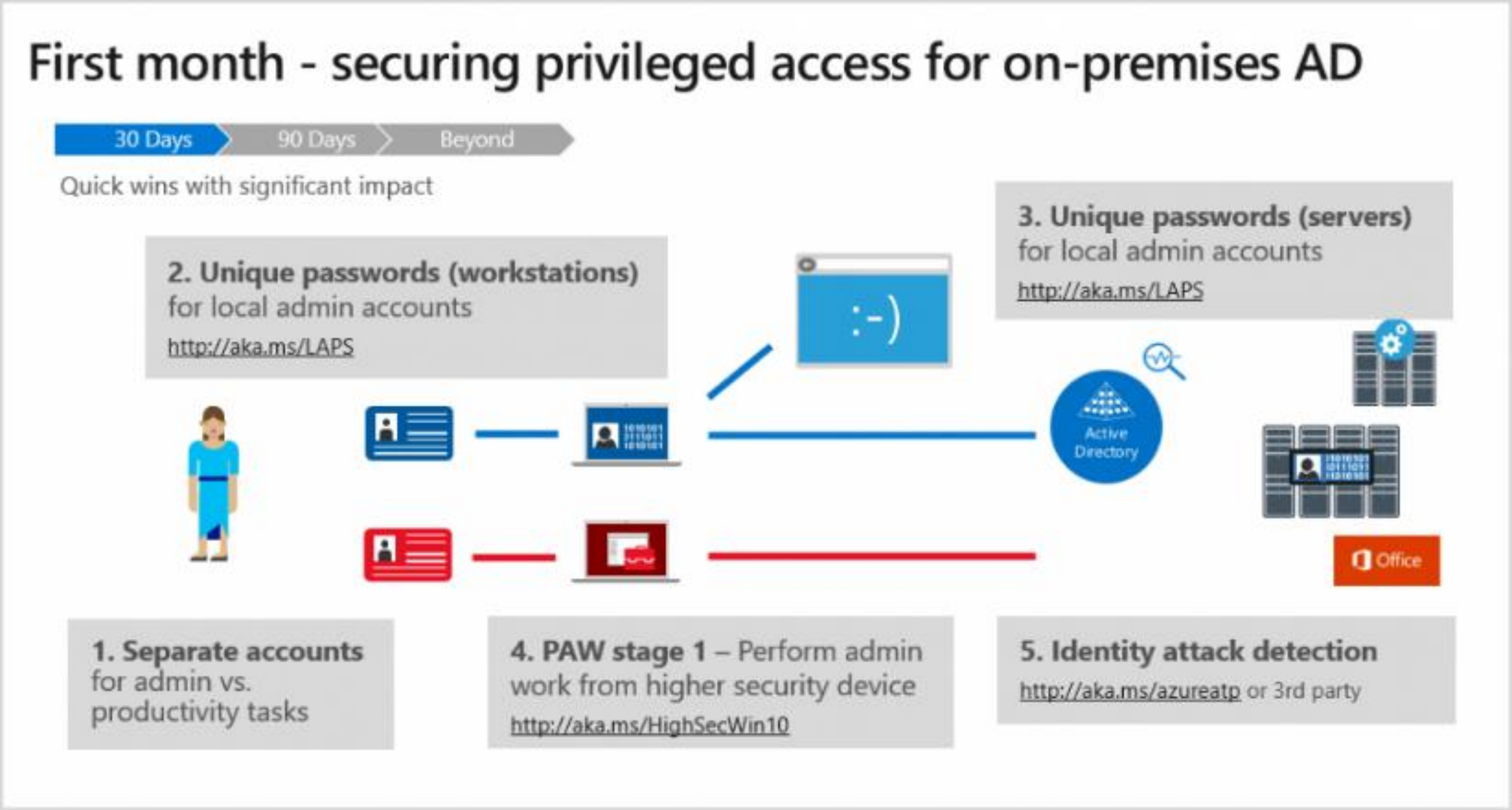
Server Management

Remote server support

- Primary (tool) - Remote tools using network logons (PS Remoting, RPC, WMI)
- Primary (interactive) - Logon using a local account password set by LAPS
- Secondary (interactive) RDP (RemoteGuard / RestrictedAdmin) from PAW
- Forbidden - Standard RDP with domain account
- Forbidden - Using domain accounts while in the session

“Physical” server support

- Primary - Log on using a local account password set by LAPS
- Forbidden - Logon with a domain account
- Forbidden - Using domain accounts while in the session



First month - securing privileged access for on-premises AD

30 Days | 90 Days | Beyond

Quick wins with significant impact

2. Unique passwords (workstations) for local admin accounts
http://aka.ms/LAPS

3. Unique passwords (servers) for local admin accounts
http://aka.ms/LAPS

1. Separate accounts for admin vs. productivity tasks

4. PAW stage 1 – Perform admin work from higher security device
http://aka.ms/HighSecWin10

5. Identity attack detection
http://aka.ms/azureatp or 3rd party

https://www.microsoft.com/security/blog/2018/11/29/secure-your-privileged-administrative-accounts-with-a-phased-roadmap/

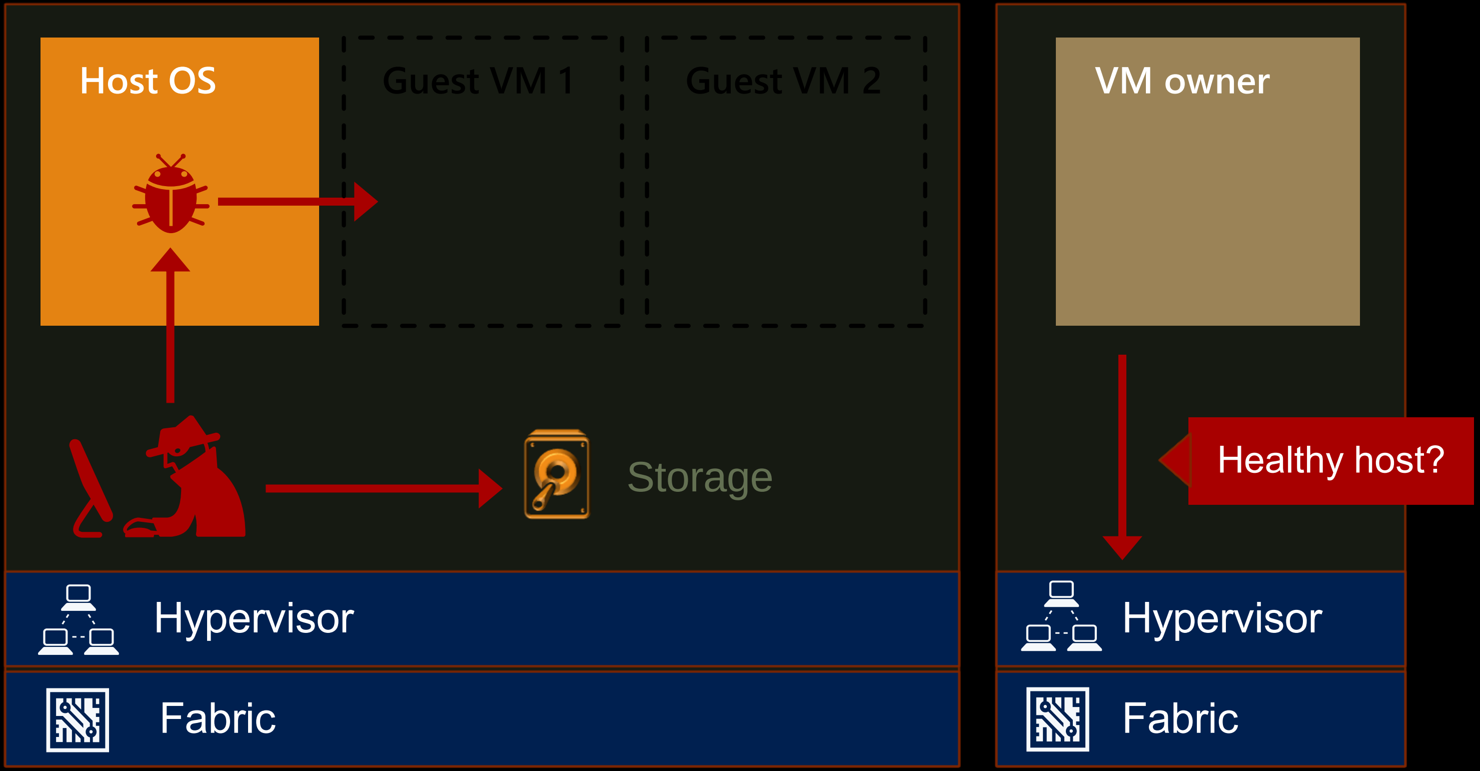
“Attackers” target virtual machines

Compromised or malicious fabric admin can access guest VM’s

Health of hosts not taken into account before starting VMs

Tenant VMs are exposed to storage and network attacks

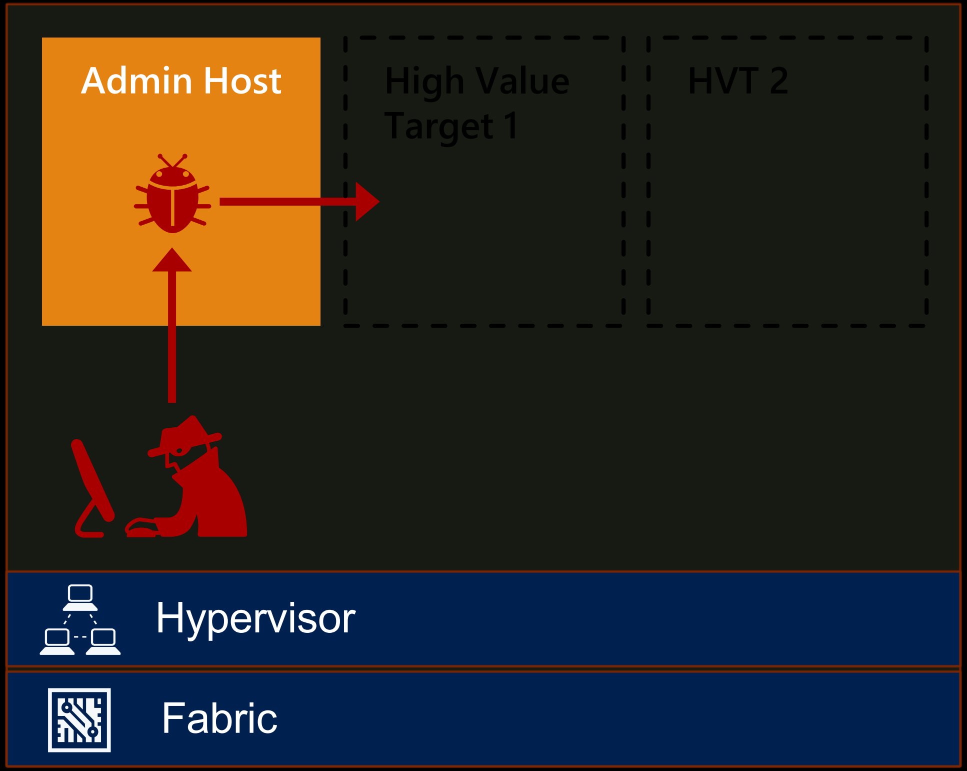
Virtual machines can’t take advantage of hardware-based security such as Trusted Platform Modules (TPMs)



“Attackers” target privileged accounts

Hosts that are expected to use high-value accounts:

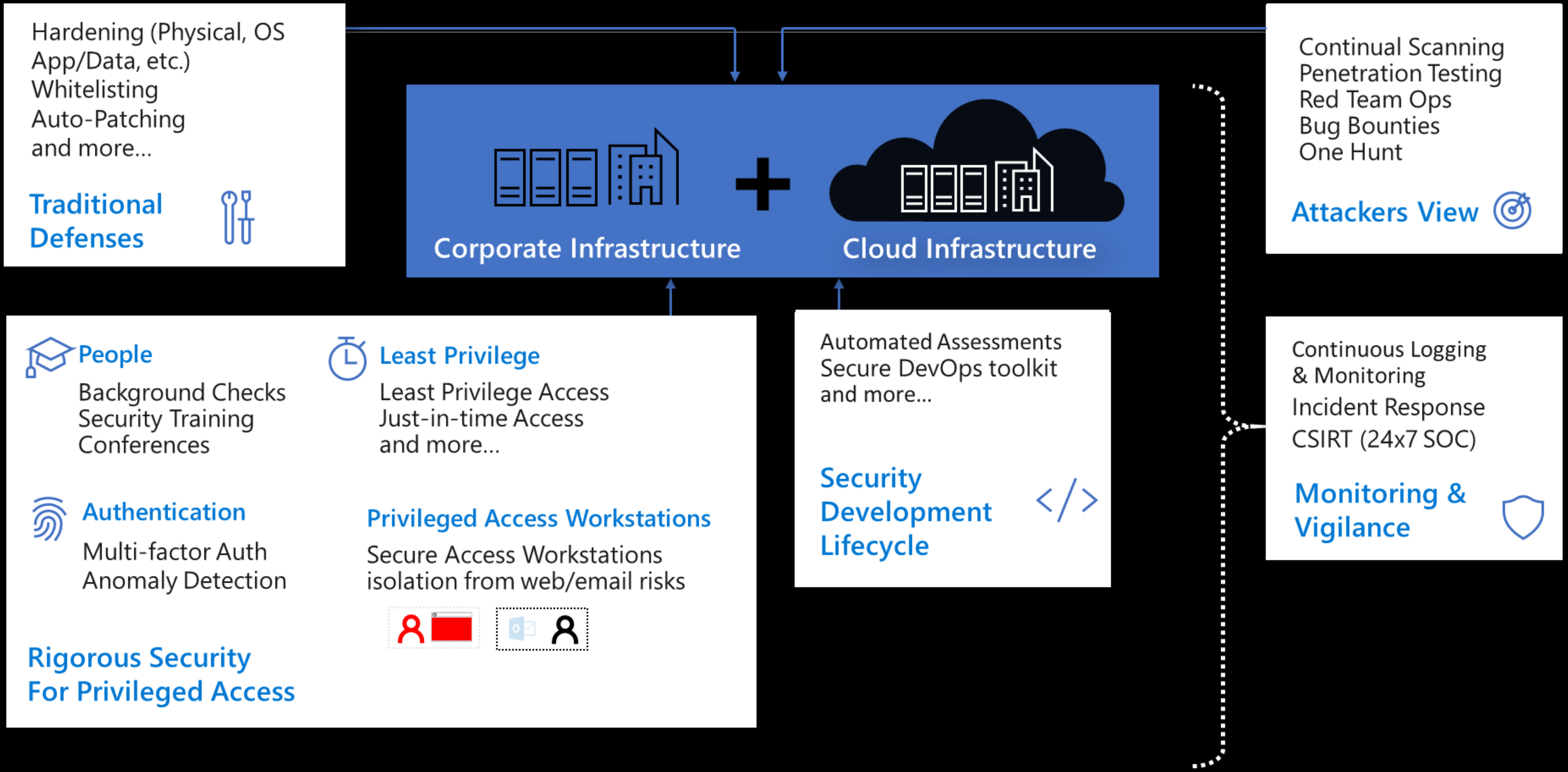
- Computers used for administration
- Computers used for support, such as help desk
- System management servers



DEMO SLIDE

Host Guardian Services and Shielded VM's

Microsoft protecting Microsoft



Hardening (Physical, OS App/Data, etc.)
Whitelisting
Auto-Patching
and more…

Traditional Defenses

Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties
One Hunt

Attackers View

People

Background Checks
Security Training
Conferences

Least Privilege

Least Privilege Access
Just-in-time Access
and more…

Authentication

Multi-factor Auth
Anomaly Detection

Privileged Access Workstations

Secure Access Workstations
isolation from web/email risks

Rigorous Security For Privileged Access

Automated Assessments
Secure DevOps toolkit
and more…

Security Development Lifecycle

Continuous Logging & Monitoring
Incident Response
CSIRT (24x7 SOC)

Monitoring & Vigilance

Transforming from Legacy to Cloud

Risk

Patching Sandboxing

Segmentation

Scanning

Encryption Secure Development Lifecycle

Forensics Threat Protection

Logging & Analytics Orchestration & Automation SIEM

WAFs Vulnerability Management Firewalls TLS

Information Protection Threat Intelligence

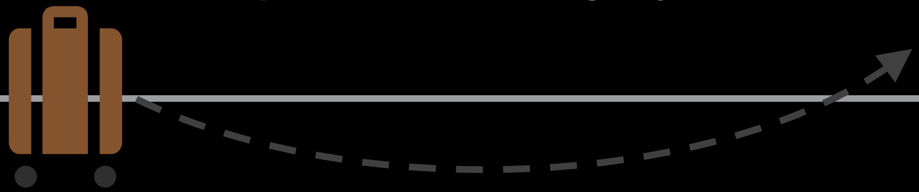
Architectures change, but principles & outcomes remain the same

Roles, responsibilities, and skillsets will evolve

Controls, tools, and processes will evolve

Same	Changed	New

Note: Legacy ‘technical debt’ persists with legacy workloads/applications in IaaS



Summery

YOU NEED TO CHANGE.

YOU NEED TO LEARN NEW WAYS.

YOU NEED ANOTHER TOOLS.