Microsoft

Windows 10 Identity and Security

IT Innovation Series

Agenda

- Device protection
- Threat resistance
- Identity protection
- Information protection
- Breach detection, investigation & response

"CYBER SECURITY IS A **CEO ISSUE**."

-MCKINSEY

$3.0 TRILLION

Impact of lost **productivity and growth**

$3.5 MILLION

Average **cost of a data breach** (15% YoY increase)

$500 MILLION

Corporate **liability** coverage.

CYBER THREATS ARE A **MATERIAL RISK** TO YOUR BUSINESS

Source: McKinsey, Ponemon Institute, Verizon

EVOLUTION OF **ATTACKS**

Mischief

Script Kiddies

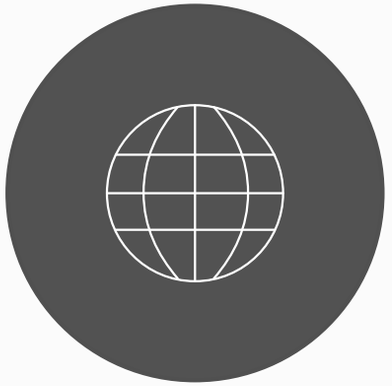
Unsophisticated

Fraud and Theft

Organized Crime

More sophisticated

Damage and Disruption

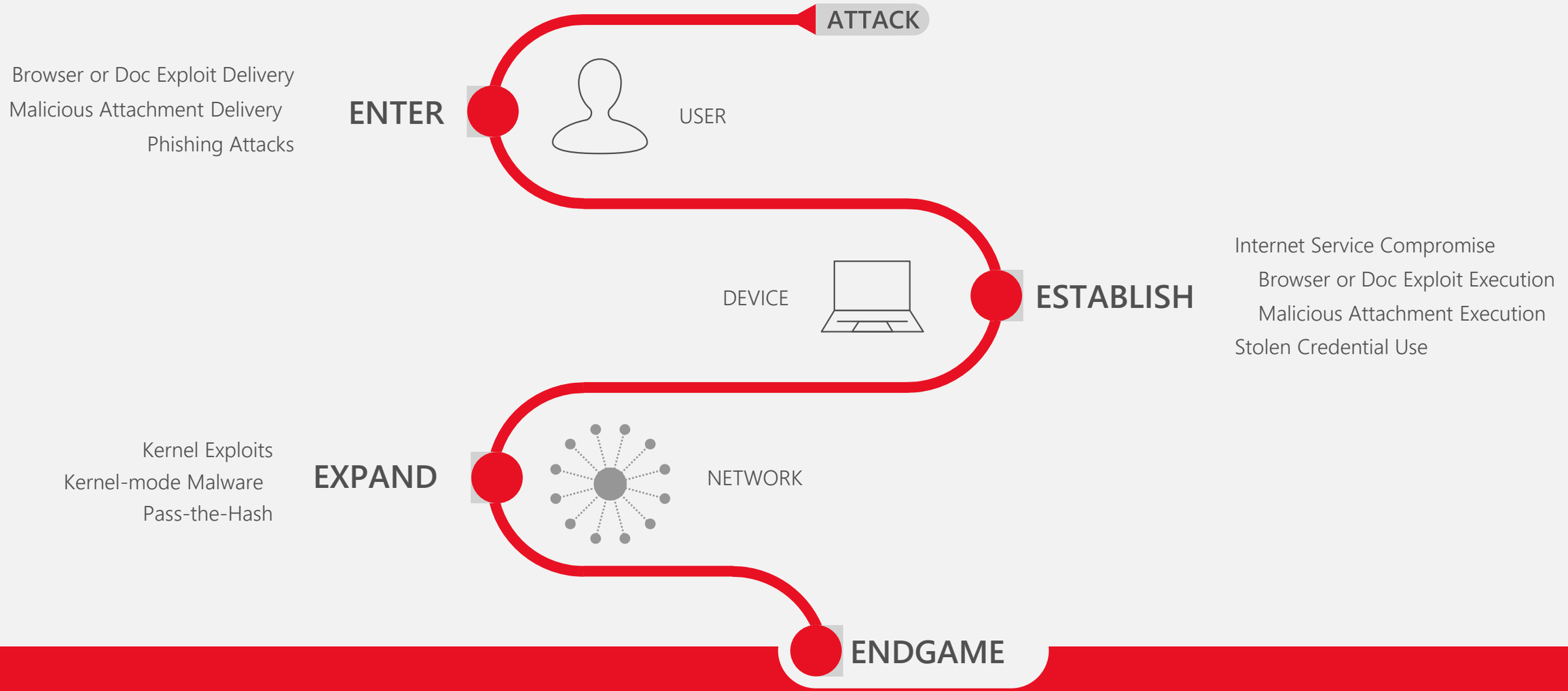


Nations, Terror Groups, Activists

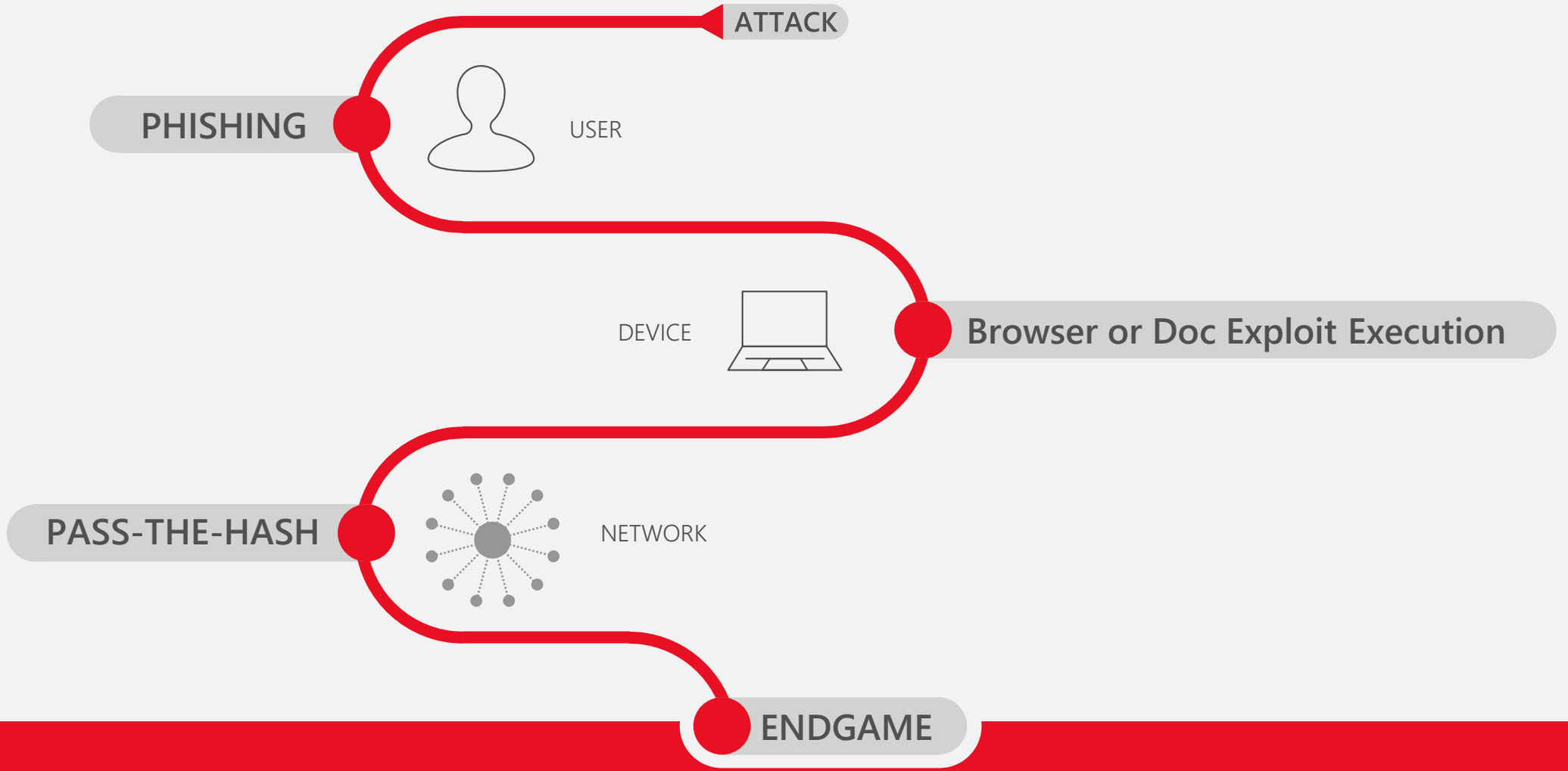
Very sophisticated and well resourced

RANSOMWARE

ANATOMY OF AN **ATTACK**

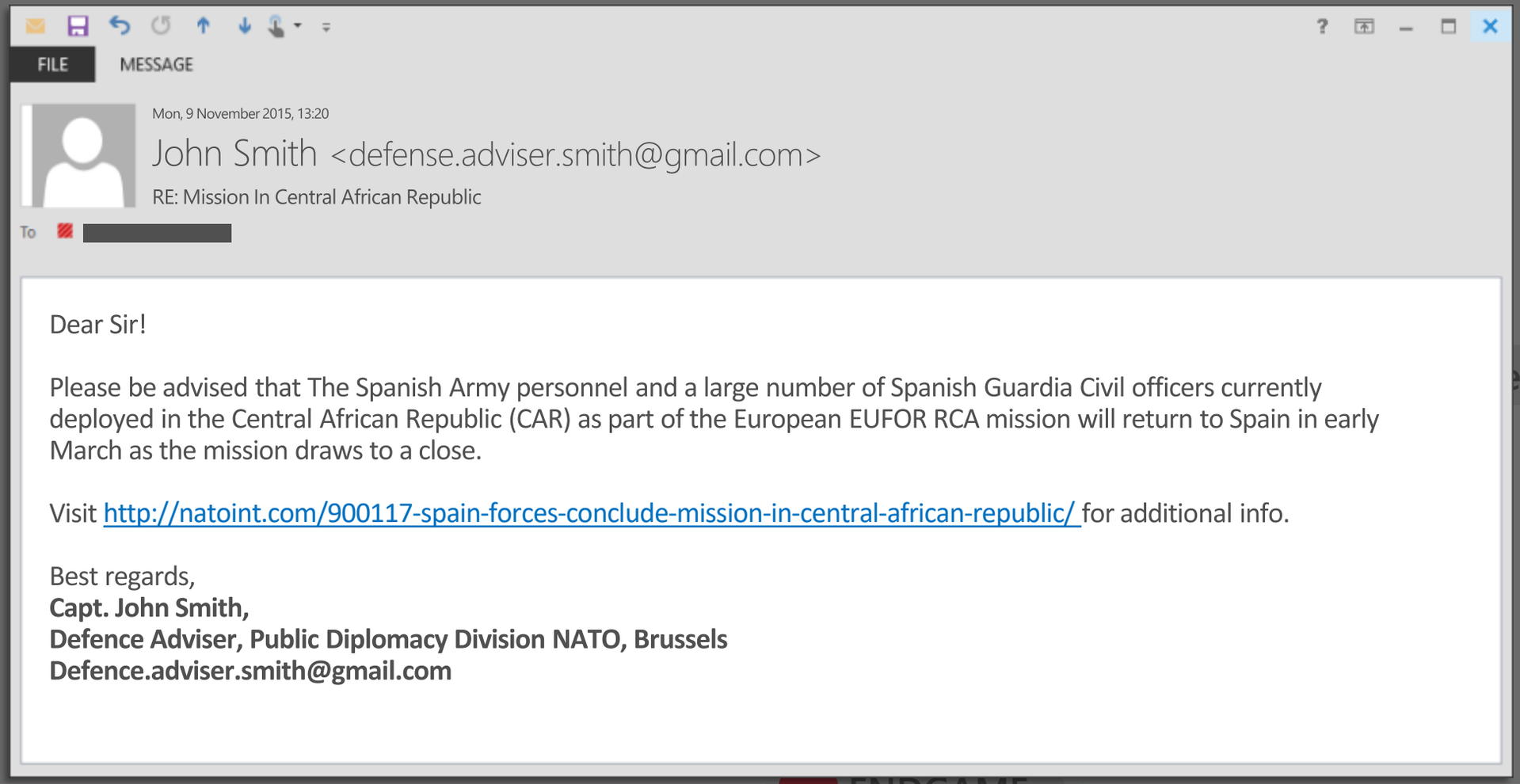


ANATOMY OF AN **ATTACK: STRONTIUM**



Theft of sensitive information, disruption of government.

ANATOMY OF AN **ATTACK: STRONTIUM**



FILE MESSAGE

Mon, 9 November 2015, 13:20

John Smith <defense.adviser.smith@gmail.com>

RE: Mission In Central African Republic

To [redacted]

Dear Sir!

Please be advised that The Spanish Army personnel and a large number of Spanish Guardia Civil officers currently deployed in the Central African Republic (CAR) as part of the European EUFOR RCA mission will return to Spain in early March as the mission draws to a close.

Visit http://natoint.com/900117-spain-forces-conclude-mission-in-central-african-republic/ for additional info.

Best regards,
Capt. John Smith,
Defence Adviser, Public Diplomacy Division NATO, Brussels
Defence.adviser.smith@gmail.com

ecution

ENDGAME

Theft of sensitive information, disruption of government.

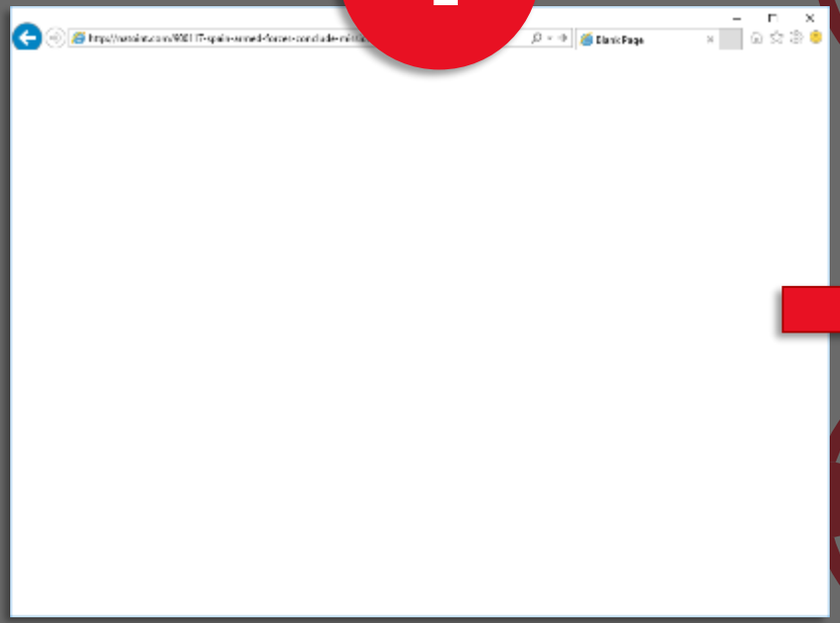
Total Elapsed Time: 00:00.1

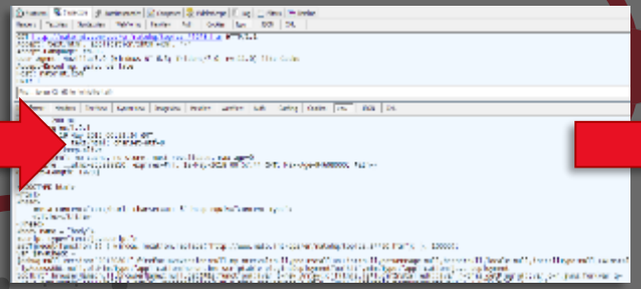
ATTACK

1 PHISHING

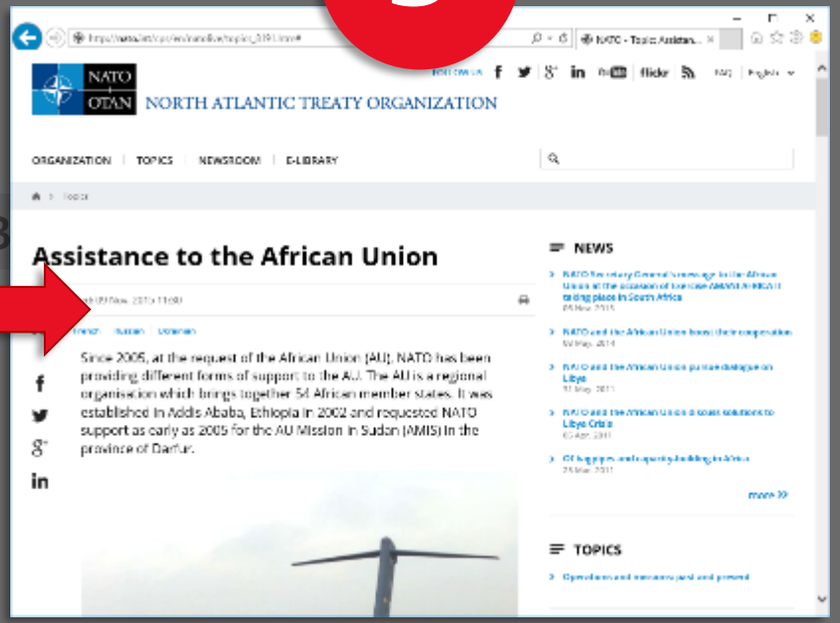
2

3





Exploit runs



Land on exploit page

Redirected to legitimate page

ENDGAME

Theft of sensitive information, disruption of government.

THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND

PRE-BREACH → POST-BREACH

Device protection

Device integrity

Device control

Threat resistance

SmartScreen

Windows Firewall

Microsoft Edge

Device Guard

Windows Defender

Identity protection

Windows Hello :)

Credential Guard

Information protection

BitLocker and BitLocker to Go

Windows Information Protection

Breach detection investigation & response

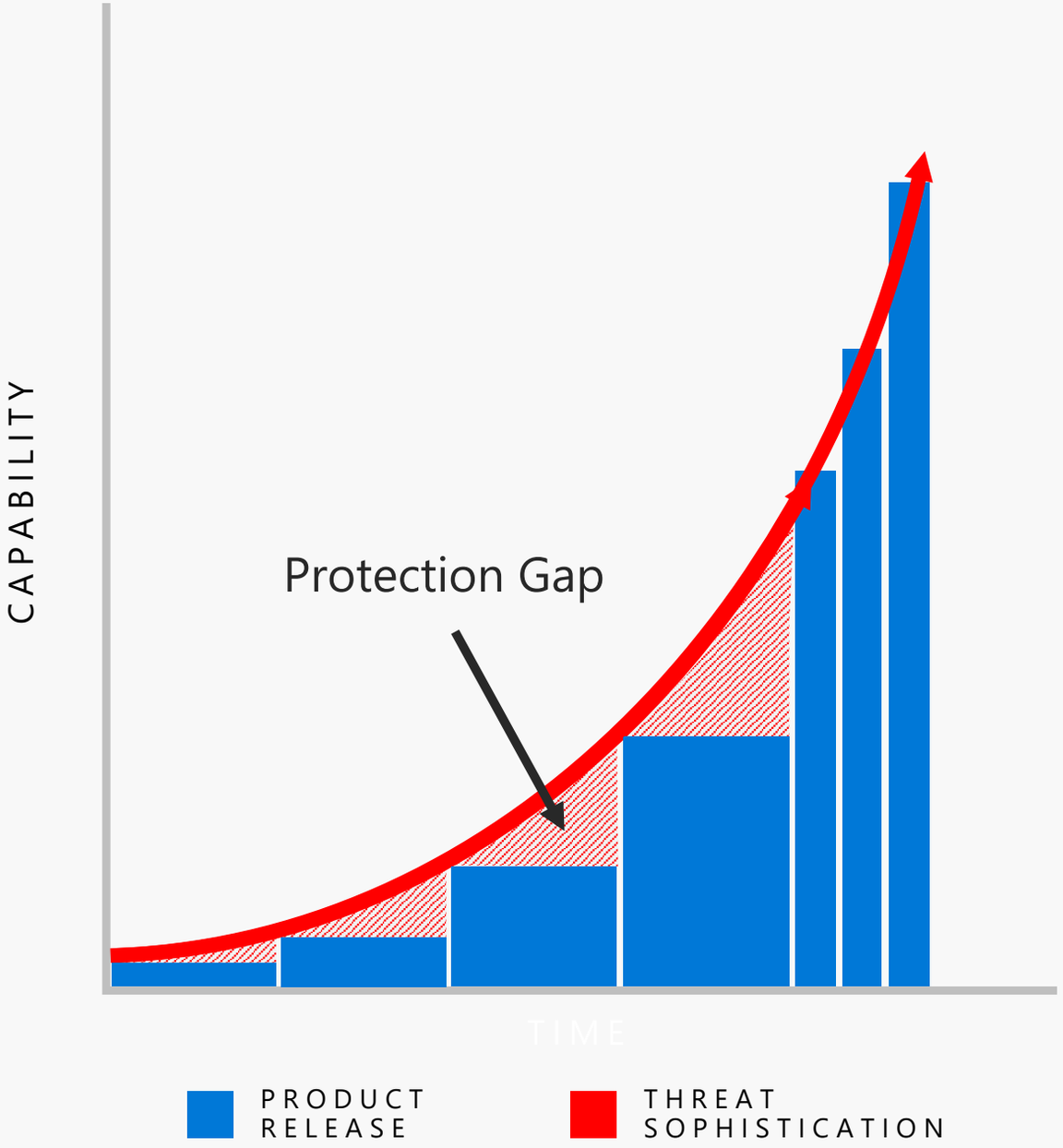
Conditional Access

Windows Defender ATP

Threat protection with Windows and Software as a Services

Attackers take advantage of periods between releases

Disrupt and out innovate our adversaries by design



Windows 7 Security features

Windows Update

Trusted Platform Module

Windows Firewall

SmartScreen

BitLocker Admin and Monitoring

BitLocker

BitLocker to Go

Device protection

Threat resistance

Identity protection

Information protection

Breach detection investigation & response

PRE-BREACH

POST-BREACH

Windows 10 Security on Legacy or Modern Devices

(Upgraded from Windows 7 or 32-bit Windows 8)

Device protection

- Windows Trusted Boot
- Windows Update
- Trusted Platform Module

Threat resistance

- Microsoft Edge
- Windows Defender
- Windows Firewall
- SmartScreen

Identity protection

- Windows Hello Companion Devices
- Windows Hello

Information protection

- Windows Information Protection
- BitLocker Admin and Monitoring
- BitLocker
- BitLocker to Go

Breach detection investigation & response

- Windows Defender Advanced Threat Protection

PRE-BREACH → POST-BREACH

Windows 10 Security on Modern Devices

(Fresh Install or upgraded from 64-bit Windows 8)

Virtualization Based Security

UEFI Secure Boot

Windows Trusted Boot

Windows Update

Trusted Platform Module

Device Guard

Microsoft Edge Barcelona

Microsoft Edge

Windows Defender

Windows Firewall

SmartScreen

Credential Guard

Windows Hello Companion Devices

Windows Hello

Device Encryption

Windows Information Protection

BitLocker Admin and Monitoring

BitLocker

BitLocker to Go

Security Management[2]

Conditional Access

Windows Defender Advanced Threat Protection

Device protection

Threat resistance

Identity protection

Information protection

Breach detection investigation & response

PRE-BREACH

POST-BREACH

THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND

PRE-BREACH → POST-BREACH

Device protection

Device integrity

Device control

Threat resistance

SmartScreen

Windows Firewall

Microsoft Edge

Device Guard

Windows Defender

Identity protection

Windows Hello :)

Credential Guard

Information protection

BitLocker and BitLocker to Go

Windows Information Protection

Breach detection investigation & response

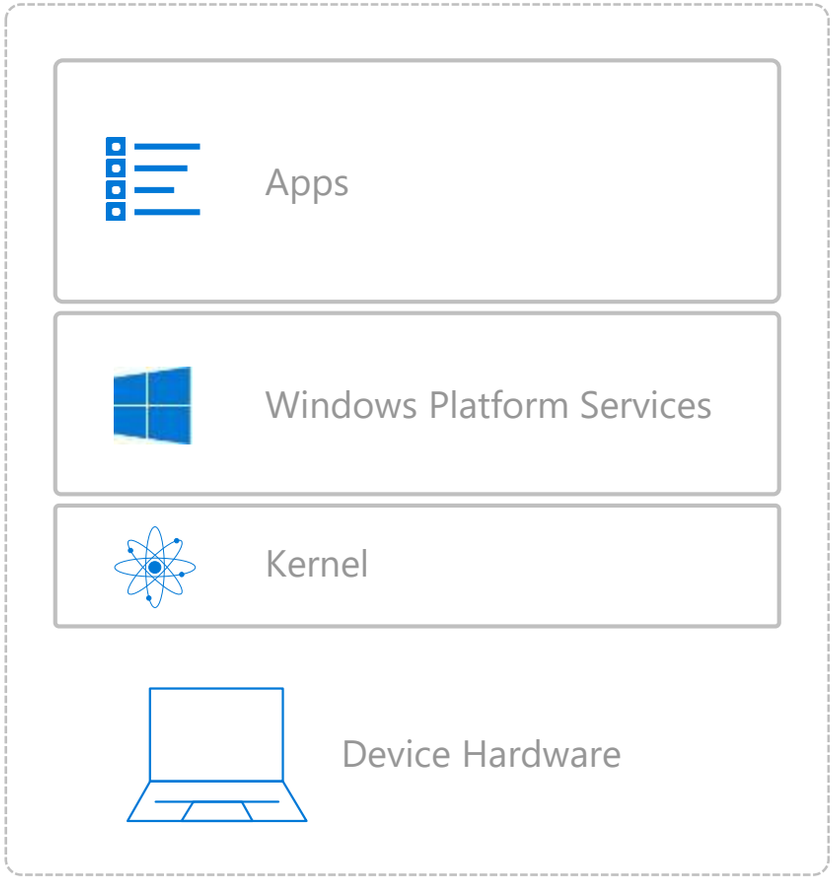
Conditional Access

Windows Defender ATP

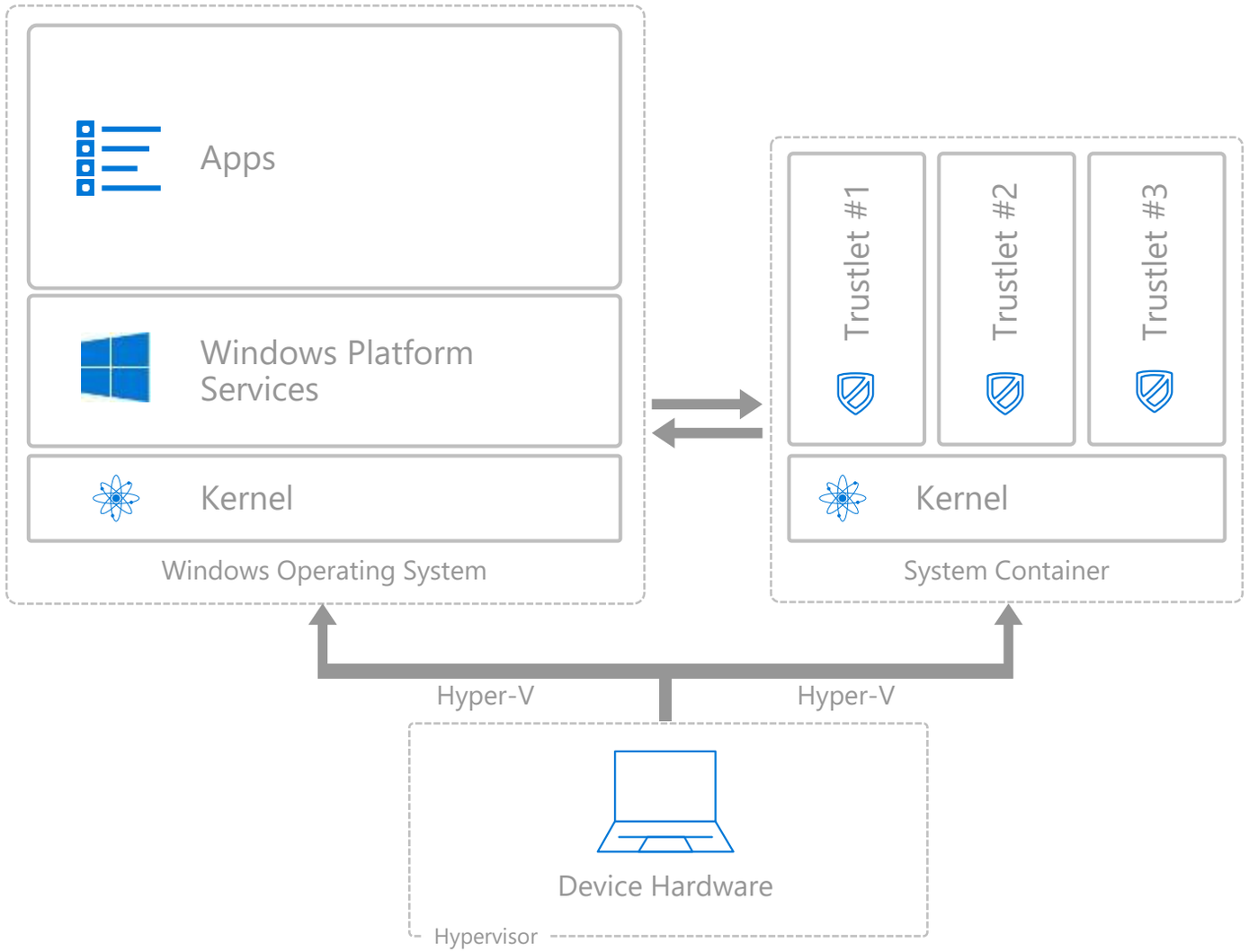
DEVICE PROTECTION

SECURE ROOTS OF TRUST

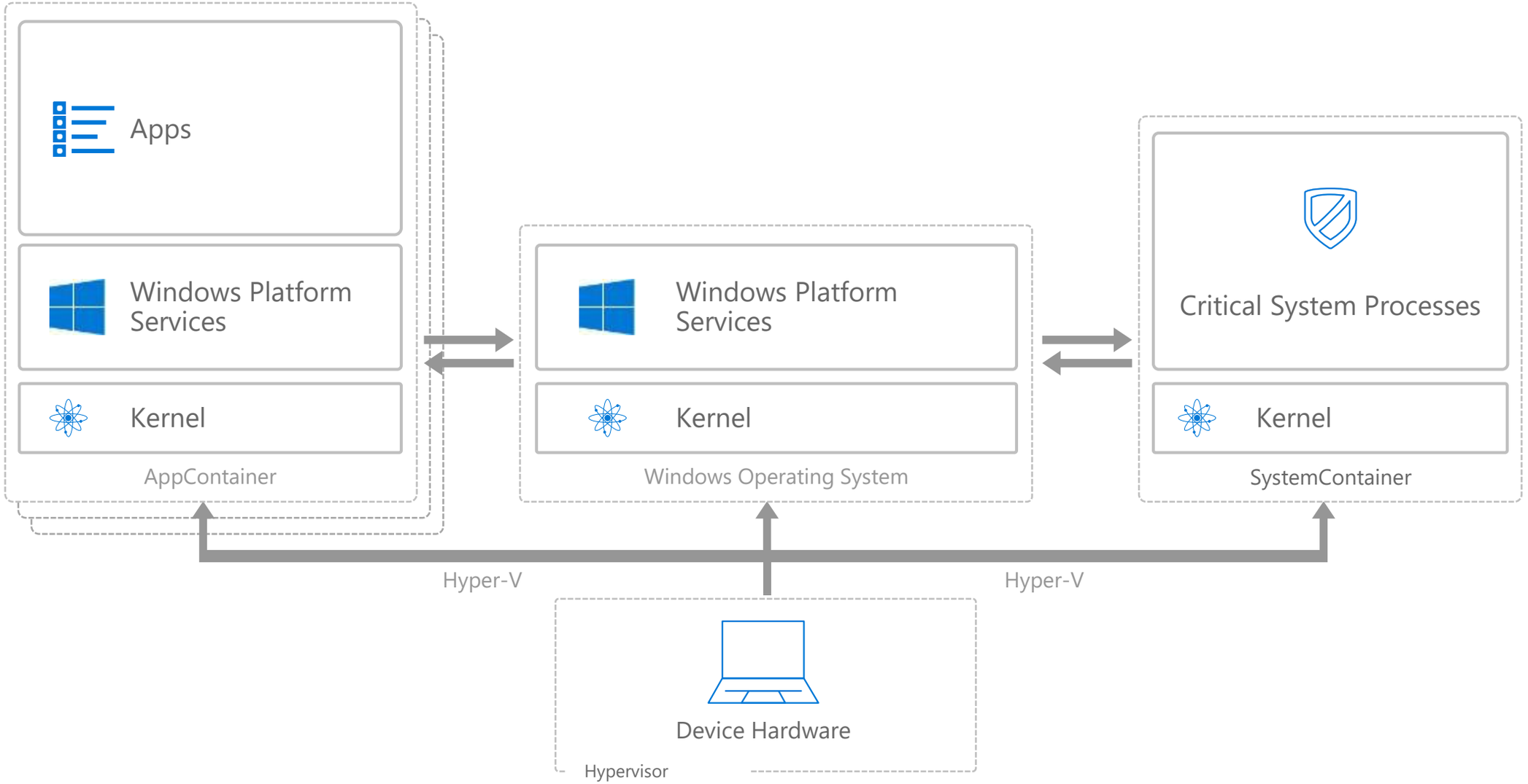
TRADITIONAL PLATFORM STACK



VIRTUALIZATION BASED SECURITY WINDOWS 10



VIRTUALIZATION BASED SECURITY THE FUTURE



THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND

PRE-BREACH → POST-BREACH

Device protection

Device integrity

Device control

Threat resistance

SmartScreen

Windows Firewall

Microsoft Edge

Device Guard

Windows Defender

Identity protection

Windows Hello :)

Credential Guard

Information protection

BitLocker and BitLocker to Go

Windows Information Protection

Breach detection investigation & response

Conditional Access

Windows Defender ATP

TRADITIONAL **APPROACH**

Type of threats to consider and mitigate

Device Tampering	Vulnerabilities	Malware	Phishing

COMPREHENSIVE **THREAT RESISTENCE**

Office ATP

SmartScreen

Windows Firewall

External

Internal

Microsoft Edge

Windows Defender

Device Guard

Windows 10

PROTECT FROM THE EDGE

Protect devices before they encounter threats

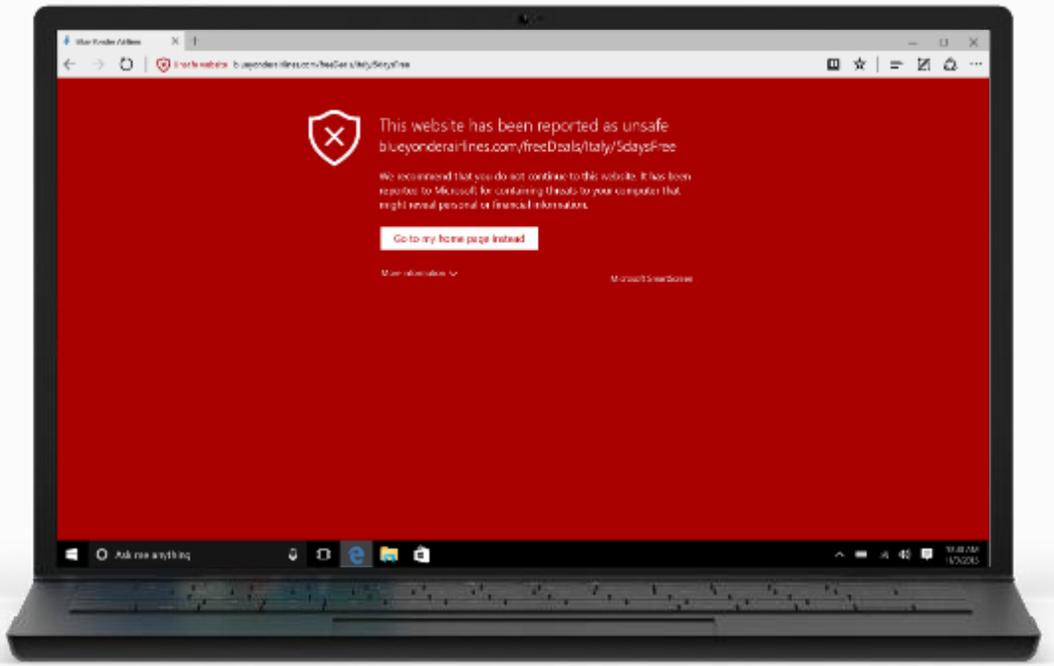
PROACTIVE THREAT IDENTIFICATION AND **PROTECTION**

Microsoft SmartScreen

- Phishing and malware filtering technology for Microsoft Edge and Internet Explorer 11 in Windows 10.
- Provides protection from drive-by attacks.
- Cloud service is continuously updated, nothing for you to deploy.

Exchange Online Advanced Threat Protection

- Cloud-based email filtering service helps protect against unknown malware and viruses.
- URL trace technology examines potentially harmful links.



Windows 10

PROTECT FROM WITHIN

Operating system used defense in depth to address threats that get inside the perimeter

MICROSOFT EDGE: DESIGNED FOR **SECURE BROWSING**

Microsoft Edge is the most secure browser Microsoft has ever shipped

Objective

Keep our customers safe when browsing the web

Strategy

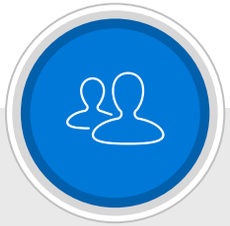
Make it difficult and costly for attackers to find and exploit vulnerabilities in Microsoft Edge

Tactics

- Eliminate vulnerabilities before attackers can find them
- Break exploitation techniques used by attackers
- Contain the damage when vulnerabilities are discovered
- Prevent navigation to known exploit sites

MICROSOFT EDGE: **BUILDING A SAFER BROWSER**

Fundamentally improve security and enable users to confidently experience the web when using Windows 10



DEFEND USERS

Identify and block known trickery and fraud

Defend against malicious web sites and downloads
(SmartScreen)

Stronger, and more convenient, credentials that attackers cannot steal
(Microsoft Passport and Windows Hello)

Supporting new web security standards to block common attacks and prevent impersonation
(Cert. Reputation, EdgeHTML, W3C Content Security Policy, HTTP Strict Transport Security)

DEFEND THE BROWSER

New model for safer browser extensions, extended defenses against memory corruption

Microsoft Edge is an app, sandboxed by default
(Universal Windows Platform)

Memory randomization space increased dramatically
(Windows Address Space Layout Randomization on 64-bit systems)

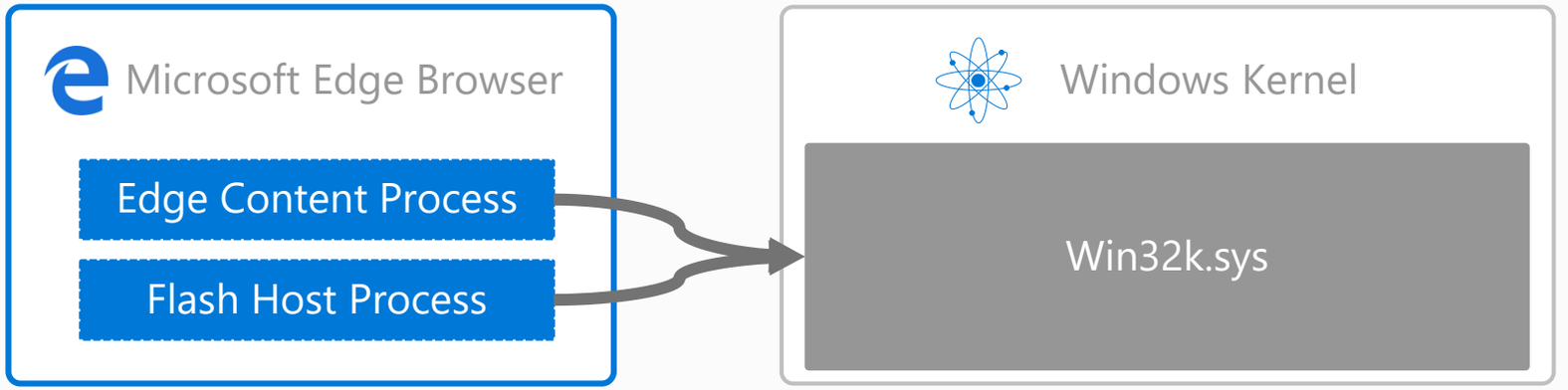
Automate memory cleanup, even if program does not
(MemGC)

Dev tools to make it significantly more difficult to take over an application
(Control Flow Guard)

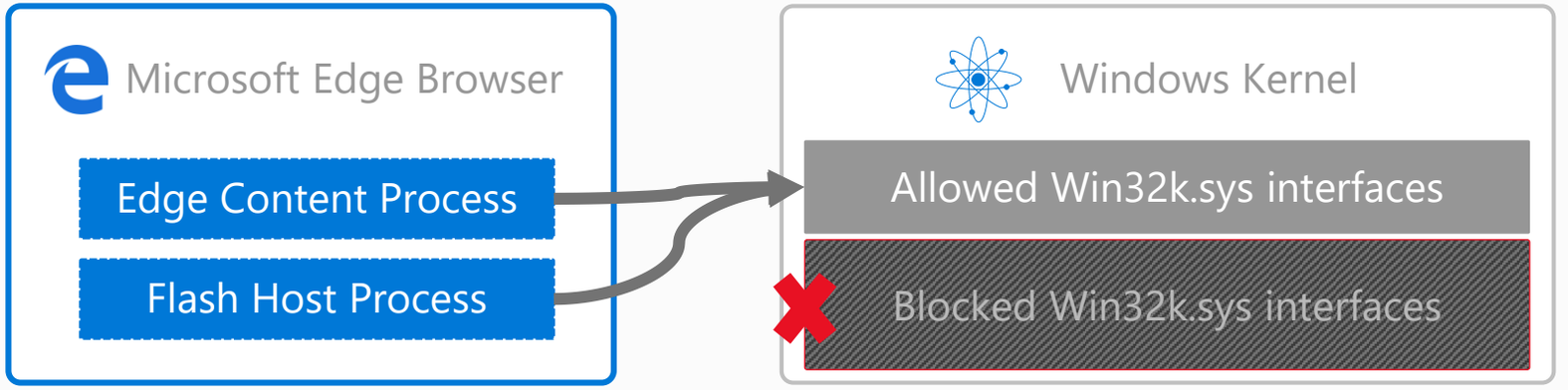
MICROSOFT EDGE **SECURITY IMPROVEMENTS**

- Microsoft Edge and Flash no longer have full access to win32k.sys—API calls are filtered
- Only 40% of interfaces are available to Flash and Edge reducing attack surface
- Flash player moves into its own AppContainer
- Working directly with Adobe to harden Flash player to be resistant to vulnerability exploits

Before – Full access to Win32.sys



Today – 60% less surface area of attack on a highly targeted library



MICROSOFT EDGE

Hardware based isolation enables the most secure browsing experience

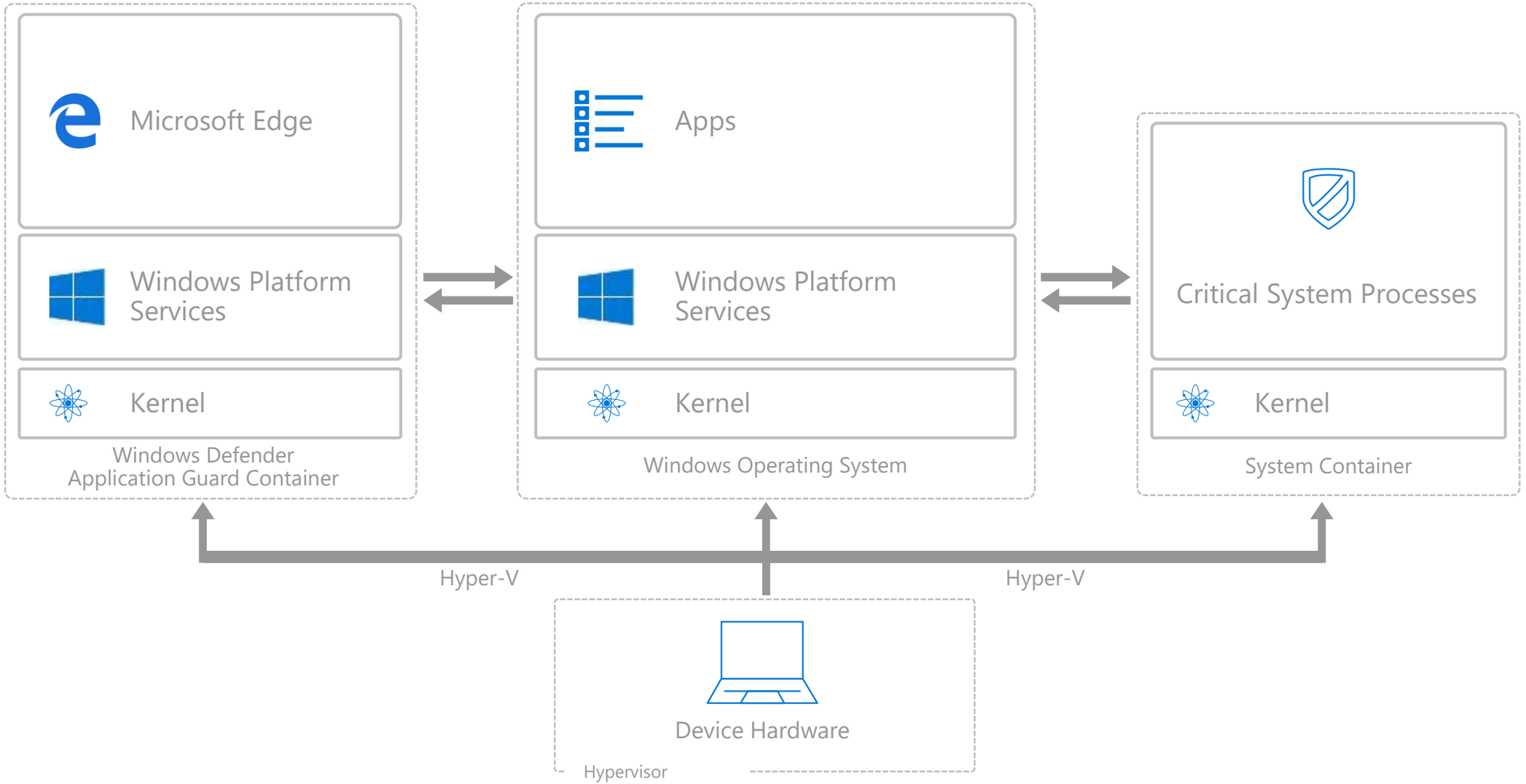
Windows Defender Application Guard protects the device from advanced attacks launched against Microsoft Edge

Malware and vulnerability exploits targeting the browser, including zero days, are unable to impact the operating system, apps, data and network

Application Guard uses virtualization based security to hardware isolate to isolate Microsoft Edge and any browsing activity away from the rest of the system

Closing Microsoft Edge wipes all traces of attacks that may been encountered while online

HARDWARE ISOLATION WITH
WINDOWS DEFENDER APPLICATION GUARD



Demo
Windows Defender Application Guard

TODAY'S CHALLENGE:

Trusted by default
until defined as threat

APPS

Detection based
methods **alone** can't
keep up

YOUR SECURITY DEPENDS ON A PLATFORM WHERE:

APPS MUST EARN TRUST BEFORE USE

Windows 10

NEXT GENERATION APP CONTROL

Secure your devices with Device Guard

DEVICE **GUARD**

Hardware Rooted App Control

Windows desktop can be locked down to only run trusted apps, just like many mobile OS's (e.g.: Windows Phone)

Untrusted apps and executables, such as malware, are unable to run

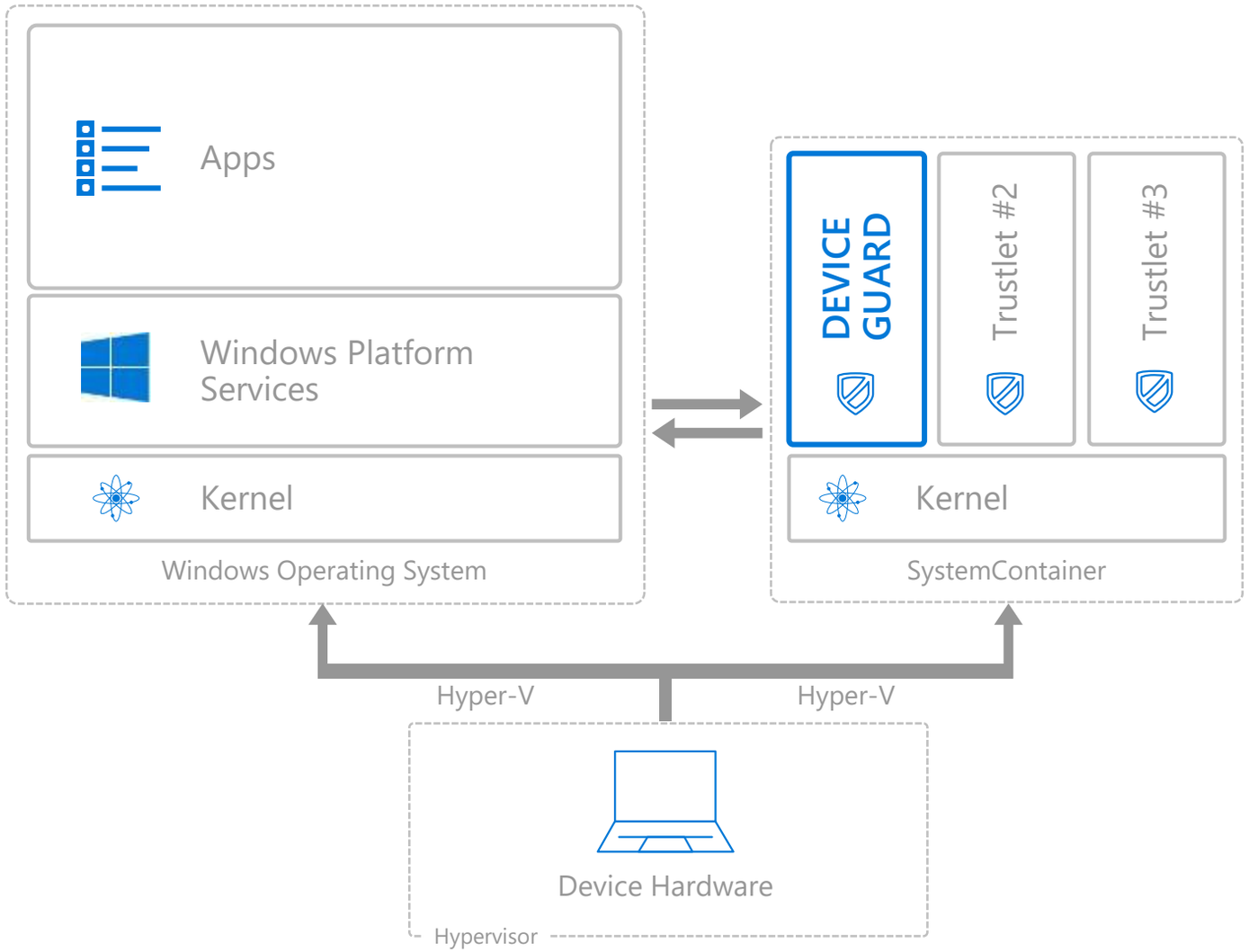
Signed policy secures configuration from tampering

Protects system core (kernel mode) and drivers from zero days and vulnerabilities

Requires Windows 8 certified or greater hardware with VT-X and VT-D

DEVICE GUARD IN VBS ENVIRONMENT

DECISIVE MITIGATION



Demo
Device Guard

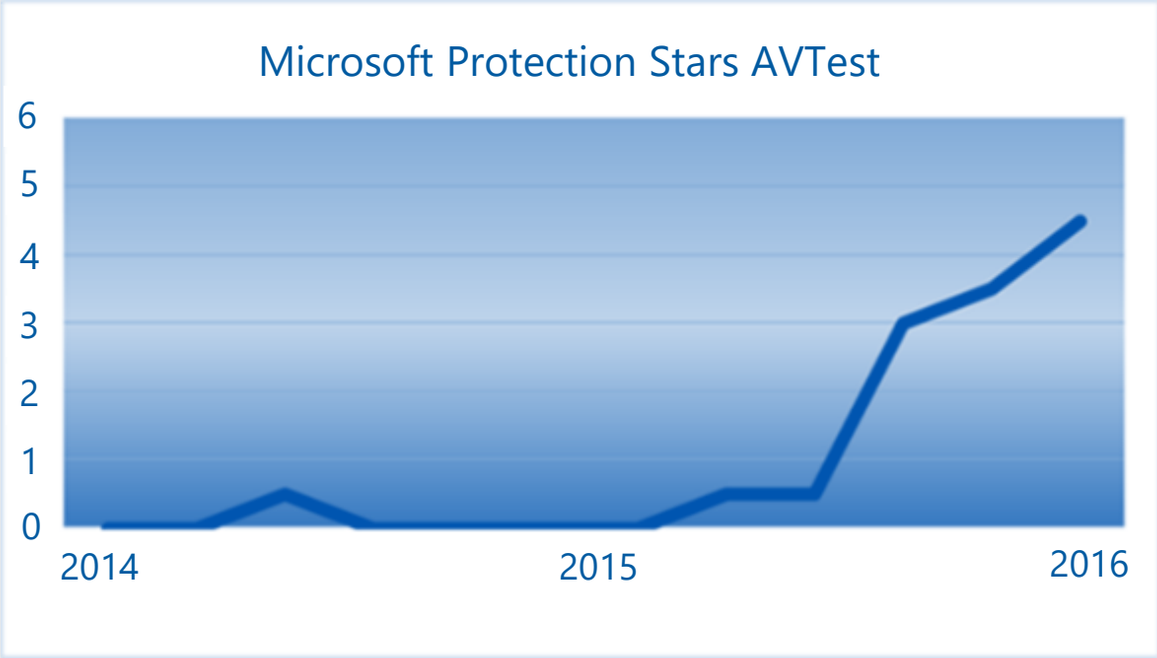
WINDOWS DEFENDER
ANTI-VIRUS PROTECTION

Protection that competes to win
Scored 98.1% detection rating from AV Comparatives testing against top competitors (March 2016).

Behavior and cloud-powered malware detection
Can detect fast changing malware varietals using behavior monitoring and cloud-powered protection that expedites signature delivery

Tamper Resistant
Windows Trusted Boot and platform isolation protect Windows Defender from attacks and enable it to self-repair

Built into Windows and Always Up-To-Date
No additional deployment & Infrastructure. Continuously up-to-date, lower costs



THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND

PRE-BREACH → POST-BREACH

Device protection

Device integrity

Device control

Threat resistance

SmartScreen

Windows Firewall

Microsoft Edge

Device Guard

Windows Defender

Identity protection

Windows Hello :)

Credential Guard

Information protection

BitLocker and BitLocker to Go

Windows Information Protection

Breach detection investigation & response

Conditional Access

Windows Defender ATP

WINDOWS 10 **IDENTITY GOALS**

Mainstream two-factor authentication

Make credentials theft resistant and breach and phish proof

Deliver solution to both consumer and business users

Provide a solution that works in all scenarios and industries

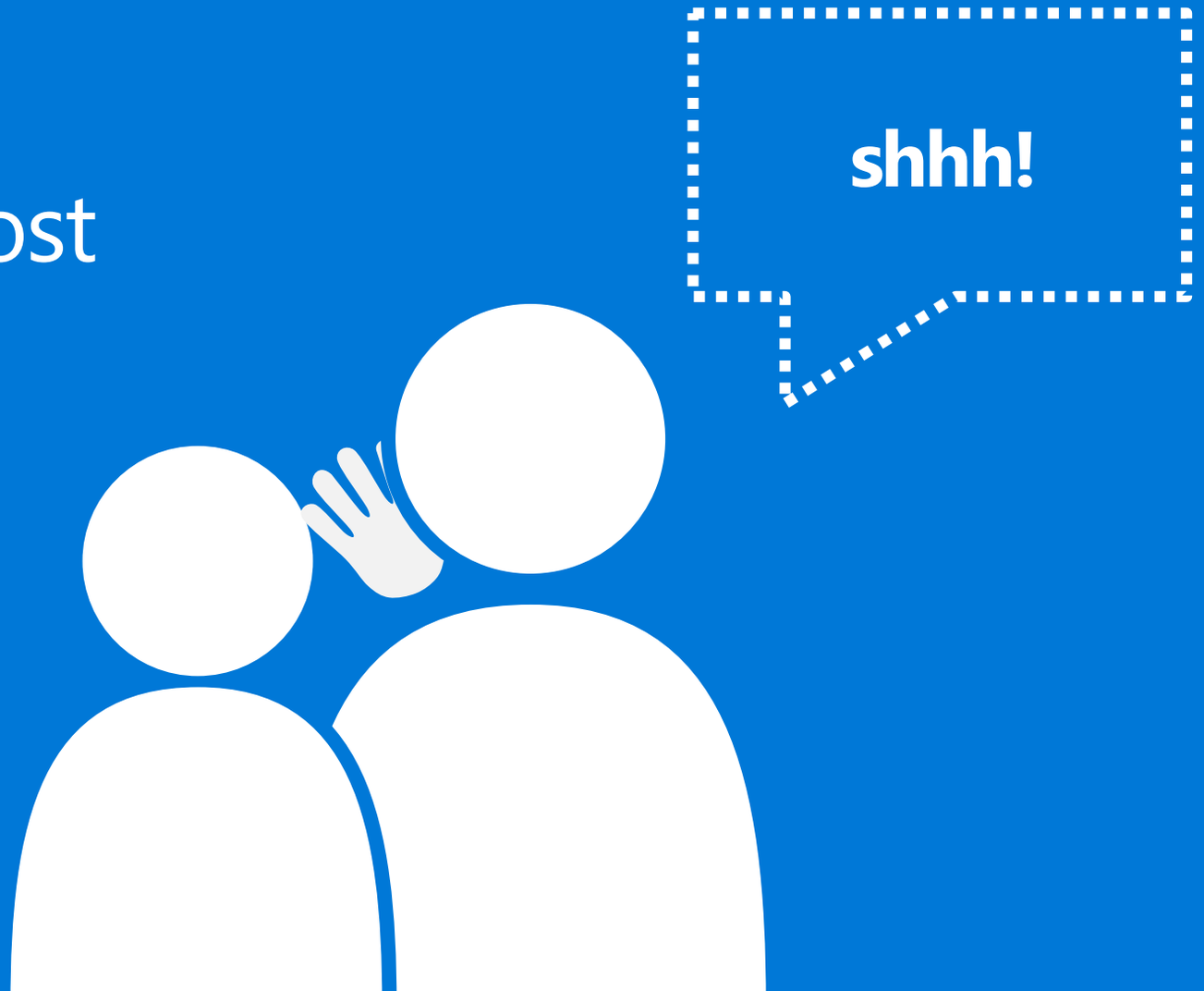
Windows 10

USER IDENTITY & AUTHENTICATION

SHARED SECRETS

Easily mishandled or lost

(Hint: The user is the problem)



PKI SOLUTIONS

Complex, costly, and under attack

ENTERPRISE DEMANDS

- Reduce costs
- Simplify implementation

WINDOWS **HELLO FOR BUSINESS**

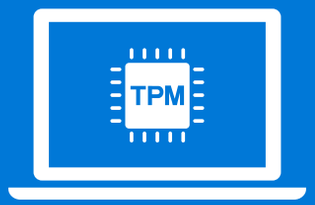
Device-Based Multi-Factor

UTILIZE FAMILIAR DEVICES

USER CREDENTIAL

An asymmetrical key pair

Provisioned via PKI or created locally via Windows 10



SECURED BY HARDWARE

FIDO ALLIANCE

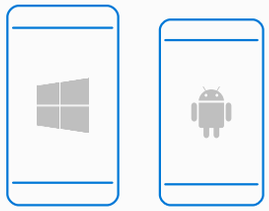
Example board level members				
Google	ARM	SAMSUNG	DISCOVER	PayPal
VISA	MasterCard	AMERICAN EXPRESS	yubico Trust the Net.	IdentityX
Lenovo	Bank of America	ING	NXP	Nok Nok LABS
RSA	oberthur TECHNOLOGIES THE M COMPANY	Synaptics	Daon	egis Technology
VASCO THE AUTHENTICATION COMPANY	USAA	CrucialTec	NTT docomo	Alibaba Group

BIOMETRIC **MODALITIES**

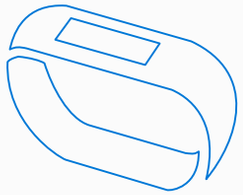
- Improved security
- Fingerprint and facial recognition
- Ease of use
- Impossible to forget
- VBS support

COMPANION DEVICE AUTHENTICATION

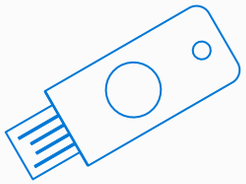
WINDOWS HELLO COMPANION DEVICE FRAMEWORK



Phone



Wearable

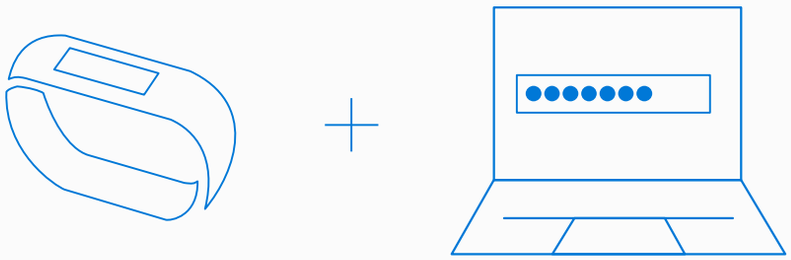


USB

Card

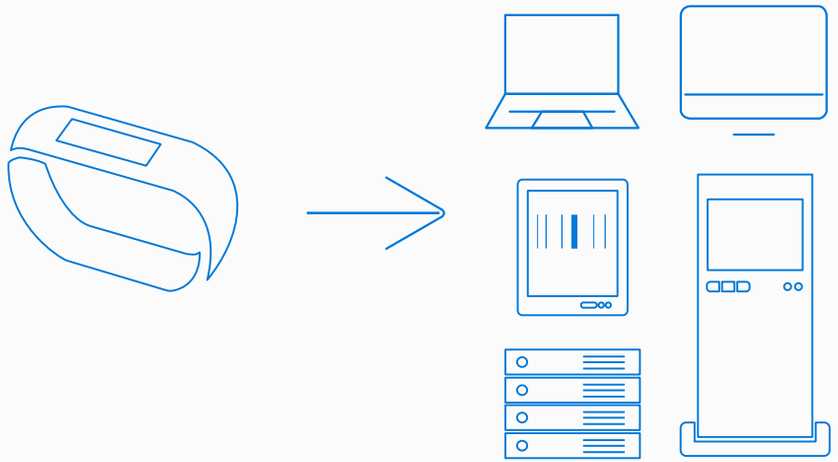
COMPANION DEVICE SCENARIOS

Companion as second factor



Increase convenience and improve security.

Credentials are mobile and remain on companion



Adds additional security by storing creds off of the device. Helps with compliance and convenience.

Demo
Windows Hello for Business

Windows 10

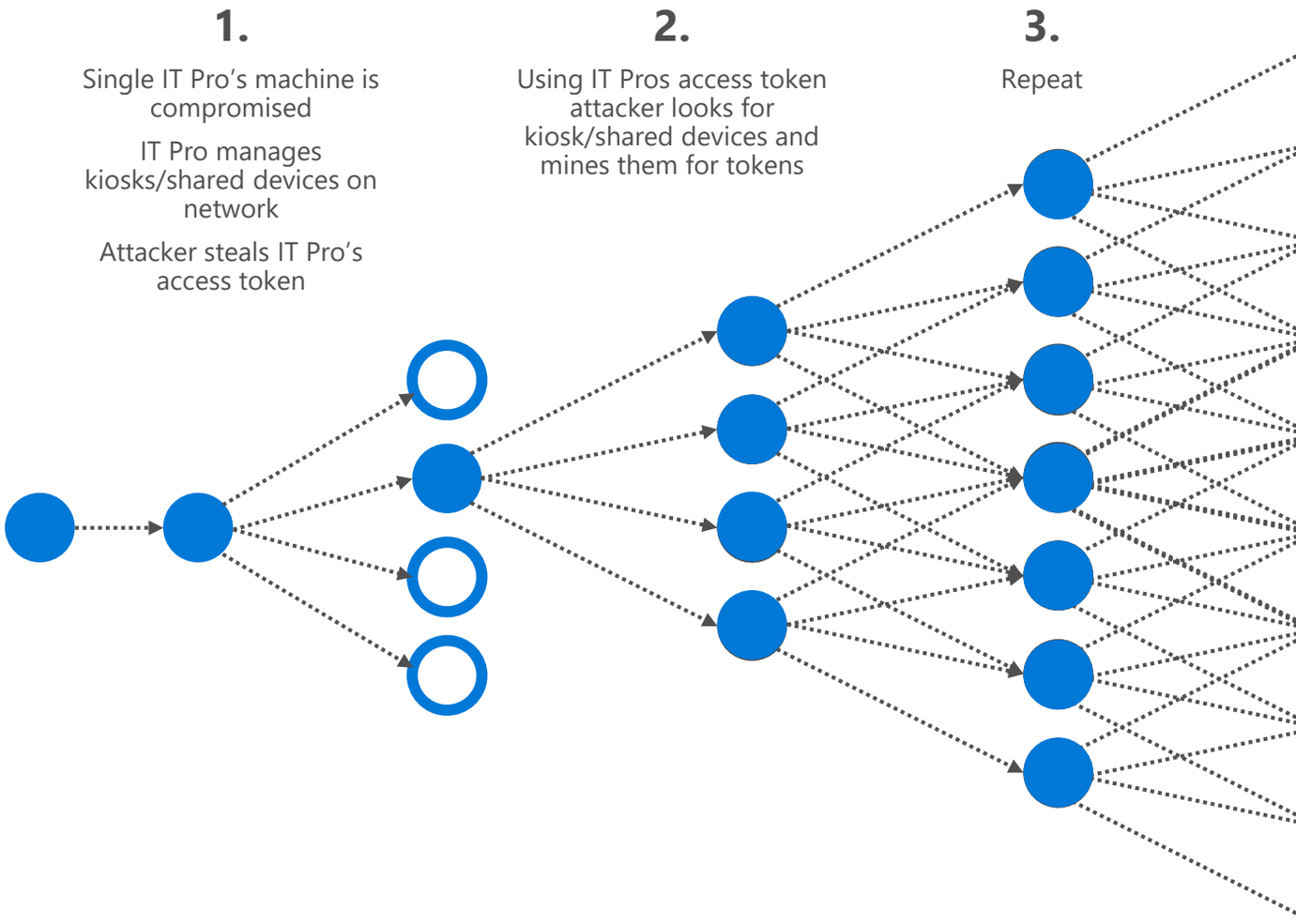
DERIVED CREDENTIALS & ACCESS TOKENS

“PASS THE HASH” ATTACKS

Today’s security challenge

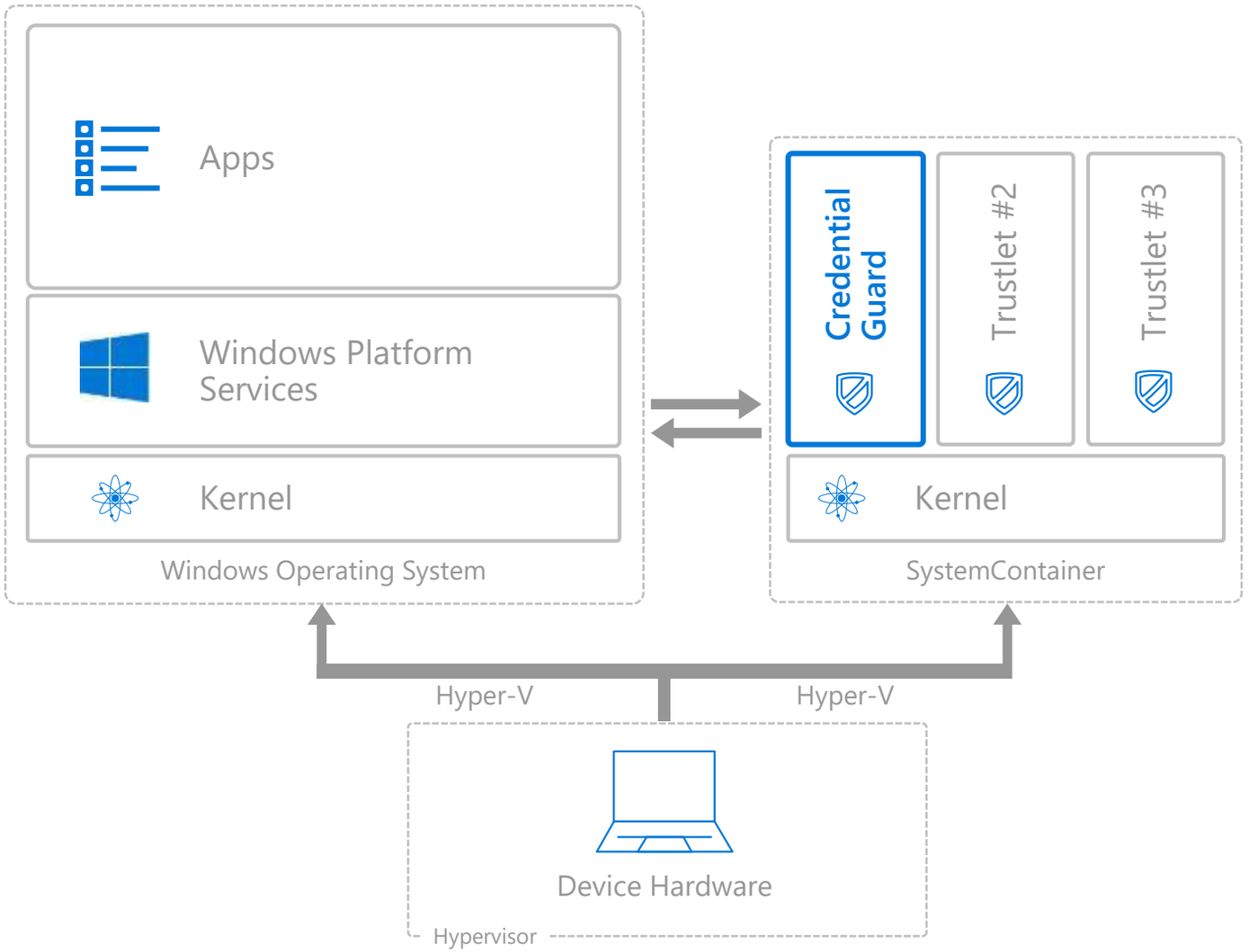
TODAY'S SECURITY CHALLENGE:
PASS THE HASH ATTACKS

Access to one device can lead to access to many



TODAY'S SOLUTION: **CREDENTIAL GUARD**

- Pass the Hash (PtH) attacks are the #1 go-to tool for hackers. Used in nearly every major breach and APT type of attack
- Credential Guard uses VBS to isolate Windows authentication from Windows operating system
- Protects LSA Service (LSASS) and derived credentials (NTLM Hash)
- Fundamentally breaks derived credential theft using MimiKatz,



Demo
Credential Guard

THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND

PRE-BREACH → POST-BREACH

Device protection

Device integrity

Device control

Threat resistance

SmartScreen

Windows Firewall

Microsoft Edge

Device Guard

Windows Defender

Identity protection

Windows Hello :)

Credential Guard

Information protection

BitLocker and BitLocker to Go

Windows Information Protection

Breach detection investigation & response

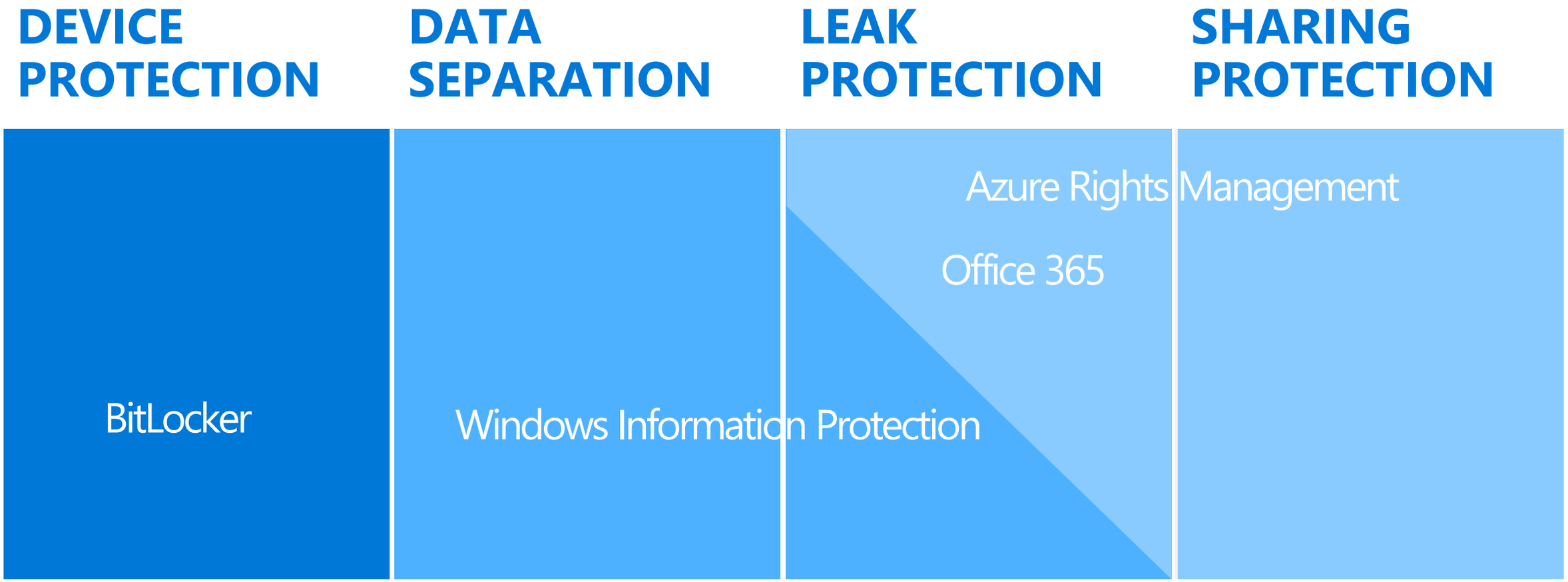
Conditional Access

Windows Defender ATP

YOUR INFORMATION **PROTECTION NEEDS**

DEVICE PROTECTION	DATA SEPARATION	LEAK PROTECTION	SHARING PROTECTION
Protect system and data when device is lost or stolen	Containment Data separation	Prevent unauthorized users and apps from accessing and leaking data	Protect data when shared with others, or shared outside of organizational devices and control

INFORMATION **PROTECTION NEEDS**



Windows 10

DATA-AT-REST PROTECTION

The threat of lost or stolen devices

DEVICE **ENCRYPTION**

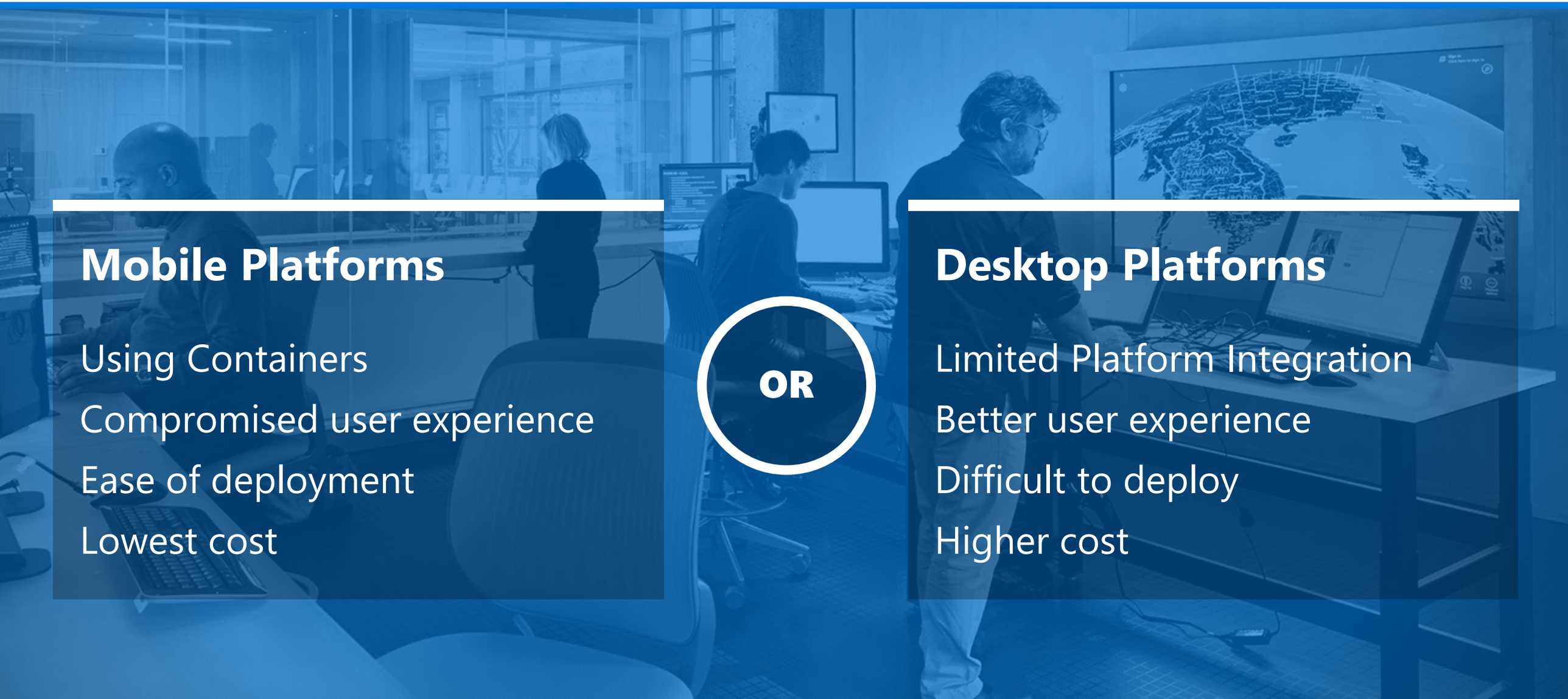
BitLocker

- Modern devices may be encrypted **out-of-box** with BitLocker technology
- Increased global acceptance of TPM
- TPM pervasive on Windows devices by end 2015
- Easiest deployment, leading security, reliability, and performance
- Single sign-on for modern devices and configurable Windows 7 hardware
- Enterprise grade management (MBAM) and compliance (FIPS)

INFORMATION **PROTECTION NEEDS**

DEVICE PROTECTION	**DATA SEPARATION**	**LEAK PROTECTION**	**SHARING PROTECTION**
Protect system and data when device is lost or stolen	Containment Data separation	Prevent unauthorized apps from accessing data	

MARKET SOLUTIONS
FOR DATA LOSS PREVENTION



Mobile Platforms

Using Containers

Compromised user experience

Ease of deployment

Lowest cost

OR

Desktop Platforms

Limited Platform Integration

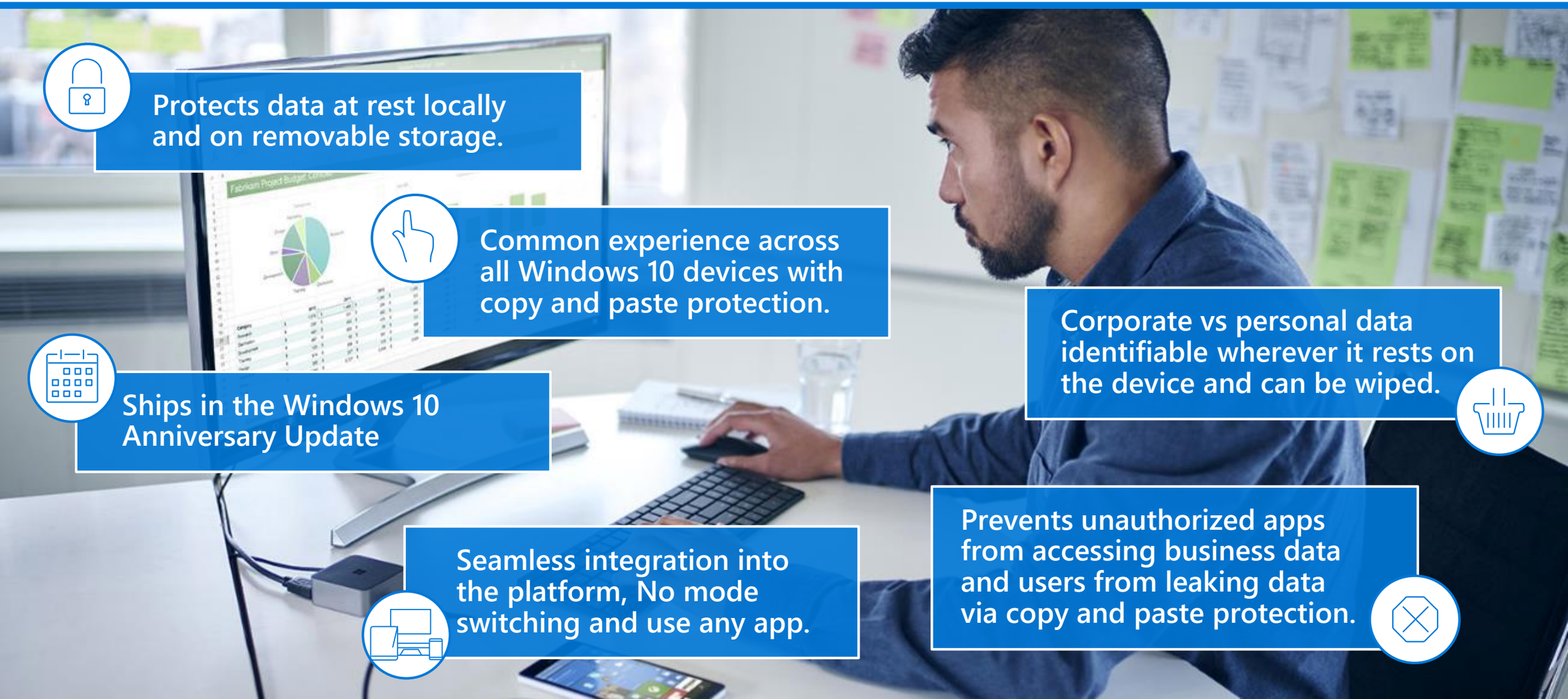
Better user experience

Difficult to deploy

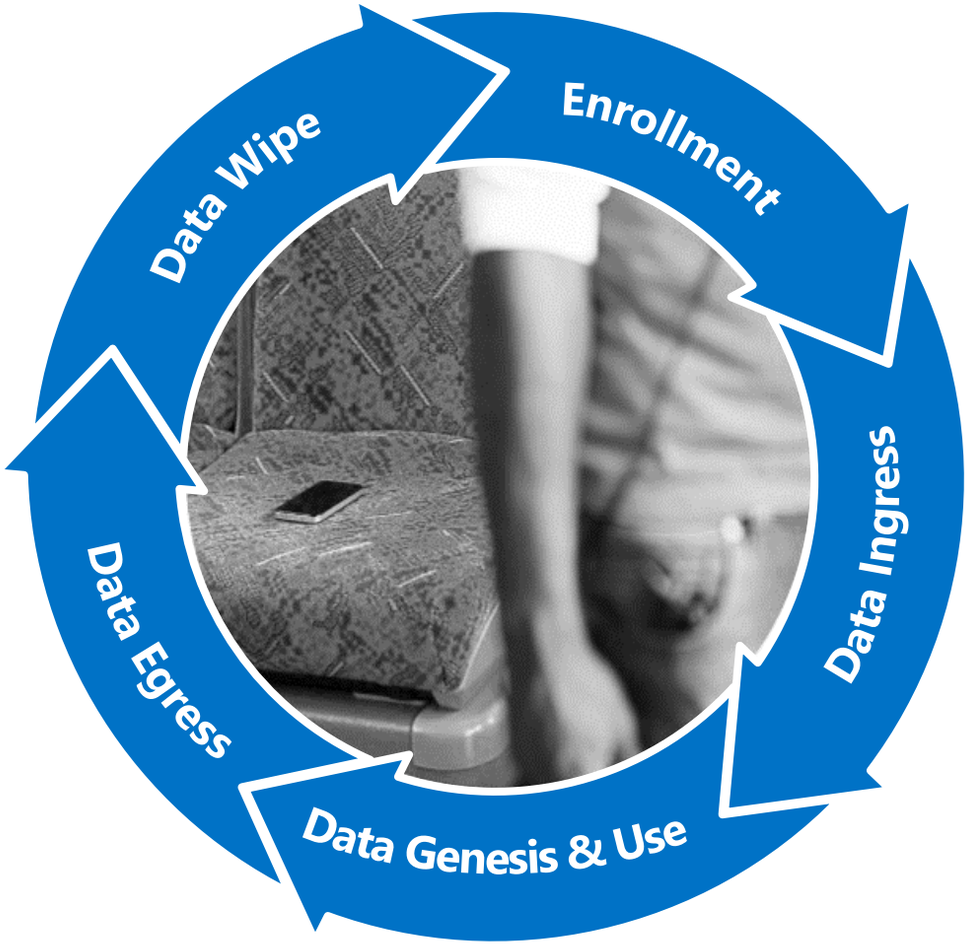
Higher cost

INTRODUCING **WINDOWS INFORMATION PROTECTION**

Integrated protection against accidental data leaks



WINDOWS INFORMATION PROTECTION **LIFECYCLE**



Policy and keys provisioned to device

Data coming from corporate network location automatically protected by WIP

App can automatically protect data or users can define data as personal or corporate

Protection can be maintained anywhere on the device or when data moves to removable storage. Azure Information Services can be used to maintain protection in B2B scenarios.

Selectively wipe corporate data demand or when device is unenrolled

INFORMATION **PROTECTION NEEDS**

DEVICE PROTECTION	DATA SEPARATION	LEAK PROTECTION	SHARING PROTECTION
	Containment BYOD separation	Prevent unauthorized apps from accessing data	Protect data when shared with others, or shared outside of organizational devices and control

SHARING **PROTECTION**

Rights Management Services

Protect all file types, everywhere they go, cloud, email, BYOD, …

Support for all commonly used devices and systems – Windows, OSX, iOS, Android

Support for B2B and B2B via Azure AD

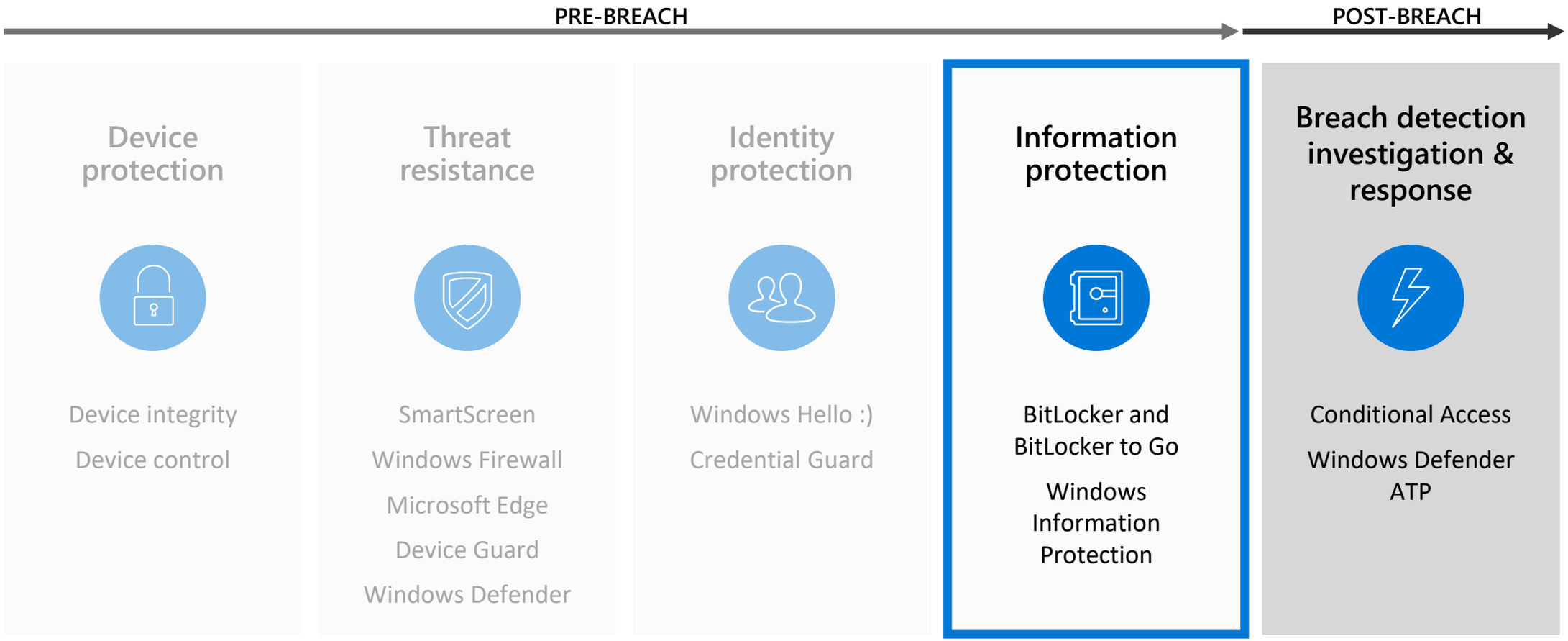
Support for on premise and cloud based scenarios (e.g.: Office 365)

Seamless, easy to provision and support for FIPS 140-2 regulation and compliance

Demo
Windows Information Protection

THE **WINDOWS 10** DEFENSE STACK

PROTECT, DETECT & RESPOND

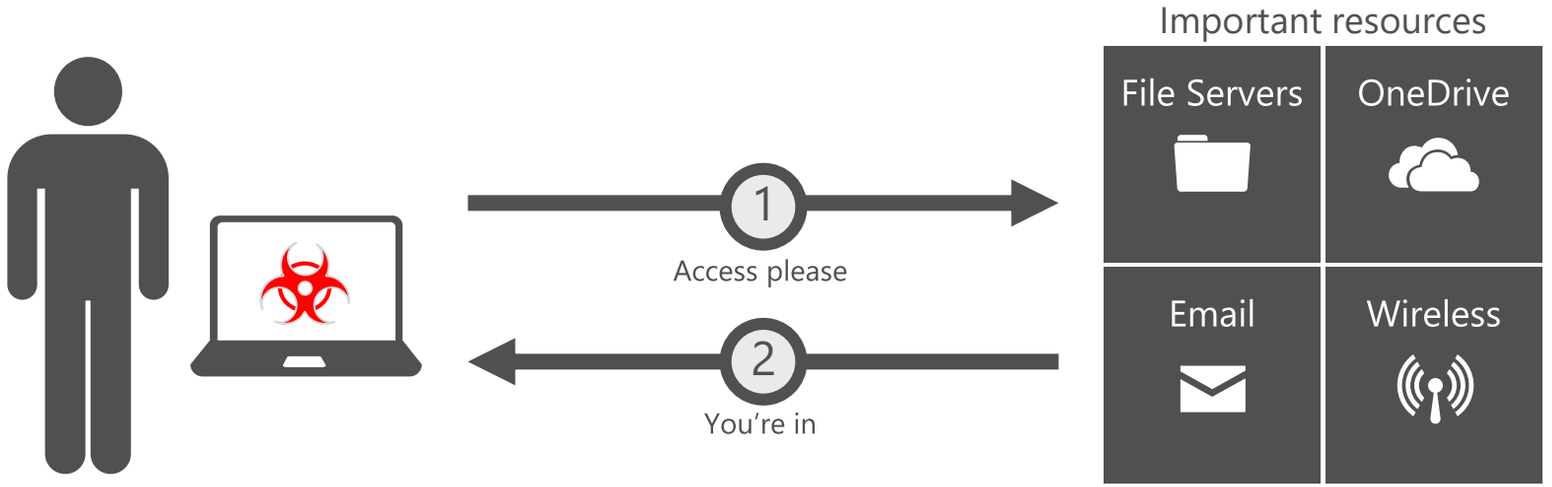


SECURE YOUR ENVIRONMENT WITH CONDITIONAL ACCESS

Keep unhealthy devices out with Intune and Windows Device Health Attestation.

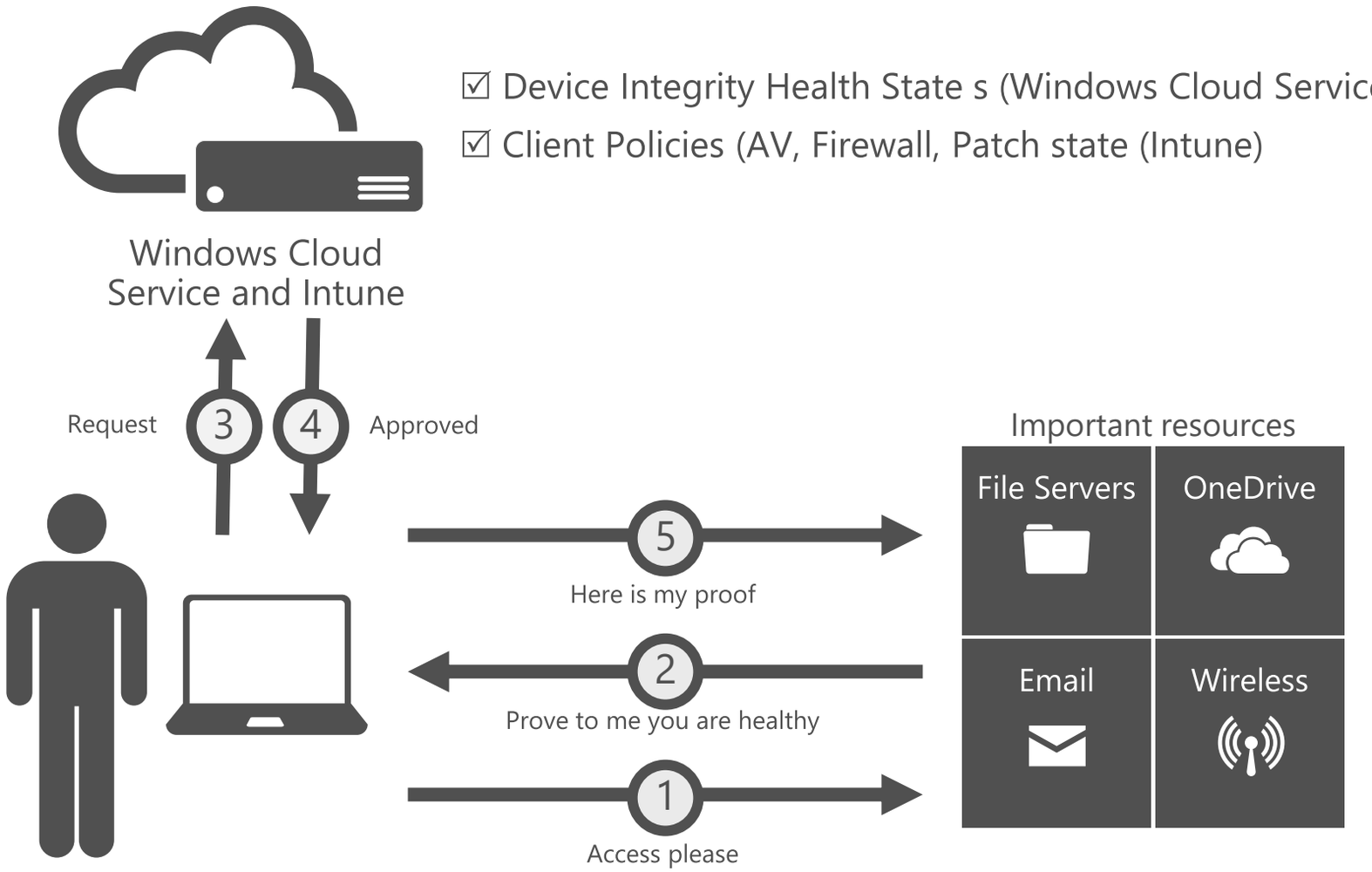
UNKNOWN **PC HEALTH**

Today health is assumed



WINDOWS DEVICE HEALTH ATTESTATION ENABLES:

MDMS to gate access based on device integrity and health



ATTACKS HAPPEN FAST AND ARE **HARD TO STOP**

If an attacker sends an email to **100 people** in your company…

…**23 people** will open it…

…**11 people** will open the attachment…

…and **six** will do it in the **first hour.**

Source: Verizon 2015 Data Breach Investigations Report

WINDOWS DEFENDER
ADVANCED THREAT PROTECTION

DETECT ADVANCED ATTACKS AND REMEDIATE BREACHES

Built into Windows
No additional deployment & Infrastructure. Continuously up-to-date, lower costs.

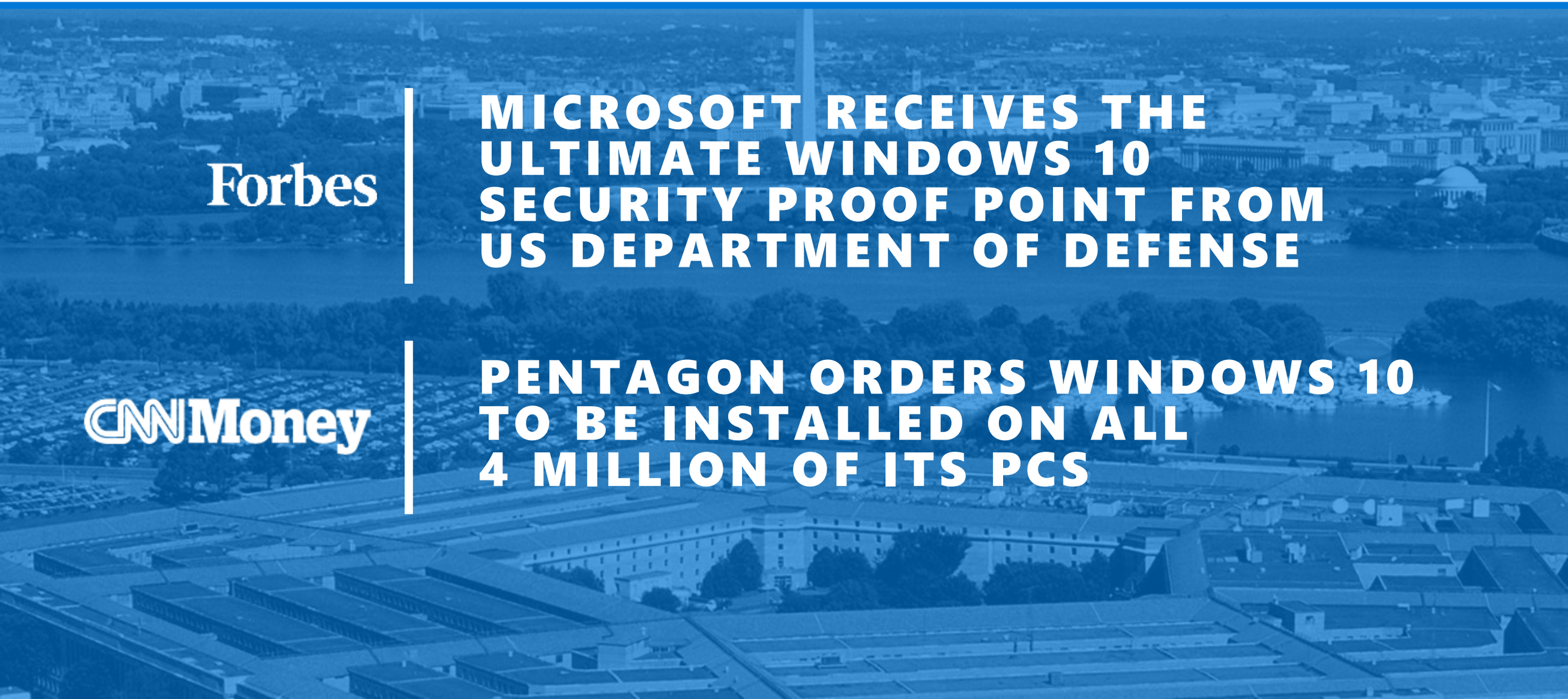
Behavior-based, cloud-powered breach detection
Actionable, correlated alerts for known and unknown adversaries. Real-time and historical data.

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.

Demo
Windows Defender Advanced Threat Protection

US DEPARTMENT OF DEFENSE



Forbes

MICROSOFT RECEIVES THE ULTIMATE WINDOWS 10 SECURITY PROOF POINT FROM US DEPARTMENT OF DEFENSE

CNNMoney

PENTAGON ORDERS WINDOWS 10 TO BE INSTALLED ON ALL 4 MILLION OF ITS PCS

Windows 10

Secure devices

Secured identities

Information protection

Threat resistance

Resources:

Register for another IT Innovation Series event

Further topics: Windows Server 2016, Azure and more.

aka.ms/ITInnovation

Continue your learning

Download the presentation, access online training and demos, try Windows 10 for free.

aka.ms/ITInnovationResources

Build your IT Pro skills

Attend the Microsoft Tech Summit.

www.microsoft.com/techsummit

Thank you!