

Herzlich Willkommen
zum Microsoft IT Camp
Windows 10 Cyber Defense & Security



Eric Berg



Senior IT-Architekt - Microsoft Modern Workplace and Datacenter



Modern Workplace and Datacenter



Azure, System Center, Windows 10



Eric.Berg@comparex.de



@ericberg_de



<http://ericberg.de/>



Alexander Benoit



Senior Consultant / Head of Competence Center Microsoft



Arbeitsplatz der Zukunft



System Center Configuration Manager // Windows 10



Alexander.Benoit@sepago.de



@ITPirate



<http://it-pirate.com/>



sepago®



Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung

Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen

- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung



Du bist hier: /IT-Camps

IT-CAMPS: AGENDA SLIDES SPEAKERPROFILE ▾ LINKS & DOWNLOADS



IT-Camps

Herzlich Willkommen zu den IT-Camps!

Wir freuen uns, dass du dabei bist!

In diesem ganztägigen Workshop fokussieren wir die wichtigsten Neuerungen, Features und Produkte innerhalb und rund um Windows 10. Dabei bearbeiten wir die beiden Schwerpunkte:

- Windows 10 Cyber Defense & Security
- Windows 10 Enterprise Deployment

in jeweils eigenen Tagesveranstaltungen.

Alle Infos zu den Inhalten beider Workshops, Verlinkungen, Downloads etc. findest du auf dieser Seite.
Solltest du dich für weitere IT-Camps interessieren - [hier](#) geht's zur Übersicht.

Du hast Fragen oder Feedback? Sprich uns bitte an, wir freuen uns! Alternativ kannst du dich auf den Feedback Bögen austoben.



VERANSTALTUNGEN

Nov 18

Microsoft IT Camp Berlin – Windows 10
Cyber Defense & Security
9:00 - 17:00 - Berlin

Nov 25

Microsoft IT Camp Frankfurt – Windows 10
Enterprise Deployment
9:00 - 17:00 - Frankfurt

Nov 22

Microsoft IT Camp Köln – Windows 10
Enterprise Deployment
9:00 - 17:00 - Köln

Nov 14

Microsoft IT Camp München – Windows 10
Cyber Defense & Security
9:00 - 17:00 - München

Devise des Tages:



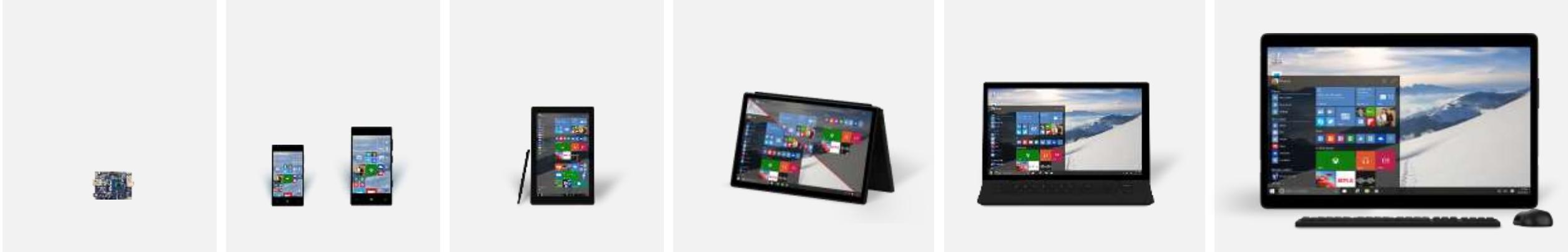
Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen

Einführung Windows 10

- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung



One converged Windows platform



2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

2004

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

2007

Windows Vista

- Bitlocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure "by default" configuration (Windows features and IE)

2009

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPsec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

2012

Windows 8

- Firmware Based TPM
- UEFI (Secure Boot)
- Trusted Boot (w/ELAM)
- Measured Boot
- Significant Improvements to ASLR and DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- Device Encryption (All SKU)
- BitLocker improvements and MBAM
- Virtual Smartcards
- Dynamic Access Control
- Built-in AV (Windows Defender)
- Improved Biometrics
- TPM Key Protection and Attestation
- Certificate Reputation
- Provable PC Health
- Remote Business Data Removable

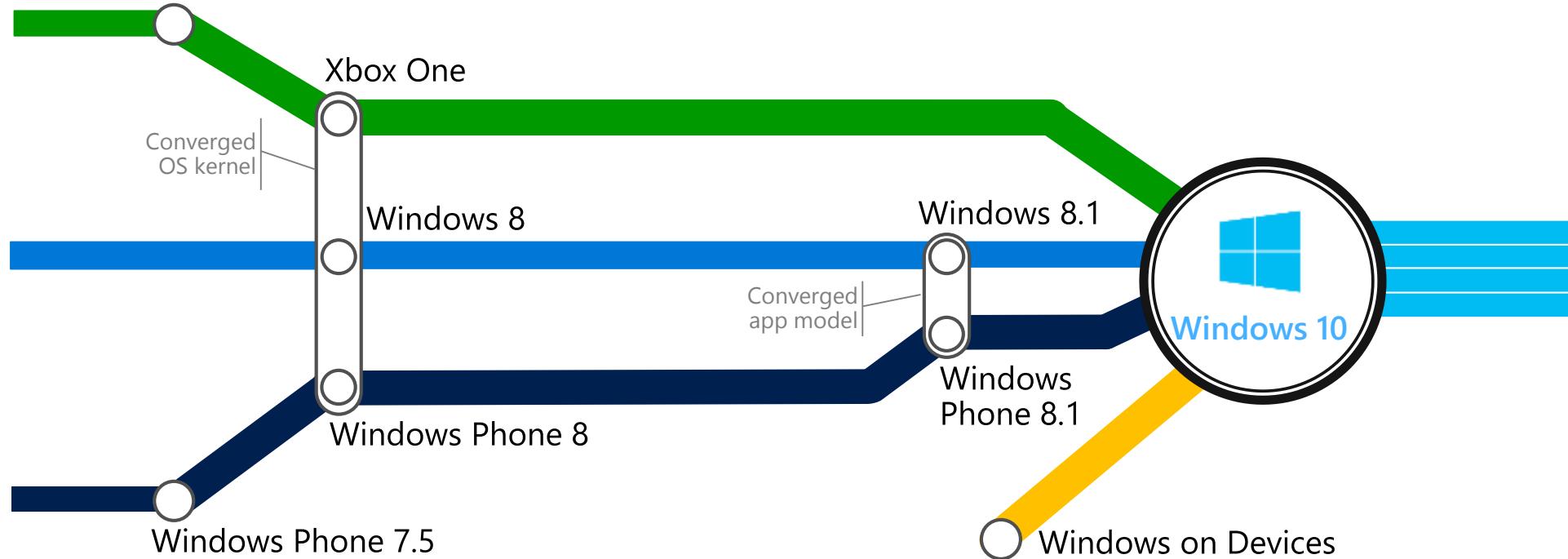
2015

Windows 10

- Virtual Secure Mode
- Virtual TPM
- Control Flow Guard
- Microsoft Passport
- Windows Hello
- Biometric Framework Improvements (Iris, Facial)
- Broad OEM support for Biometric enabled devices
- Enterprise Data Protection
- Device Encryption supported on broader range of devices
- DMA Attack Mitigations
- Device Guard
- URL Reputation Improvements
- App Reputation Improvements
- Windows Defender Improvements
- Provable PC Health Improvements

Convergence

Journey to Convergence



Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen

- Einführung Windows 10

● Neuer Ansatz Mobility

- Schutz von Geräten

- Schutz von Identitäten

- Schutz von Informationen

- Einbruchserkennung

Management Choices

Traditional Management

- Works with existing infrastructure
- Continued support for Group Policy and WMI

Modern Management

- Advanced MDM support
- Consistent across PC/phone
- 1st and 3rd party solutions

Available Choices

Identity

- Active Directory
- Azure Active Directory

Management

- Group Policy
- System Center Configuration Manager
- 3rd Party Infrastructure Management
- Microsoft Intune
- 3rd Party MDM

Updates & Upgrades

- Windows Update
- Windows Server Update Services
- Software Update Point (System Center Configuration Manager)
- Microsoft Intune
- 3rd Party MDM

Infrastructure

- On Premises
- Cloud

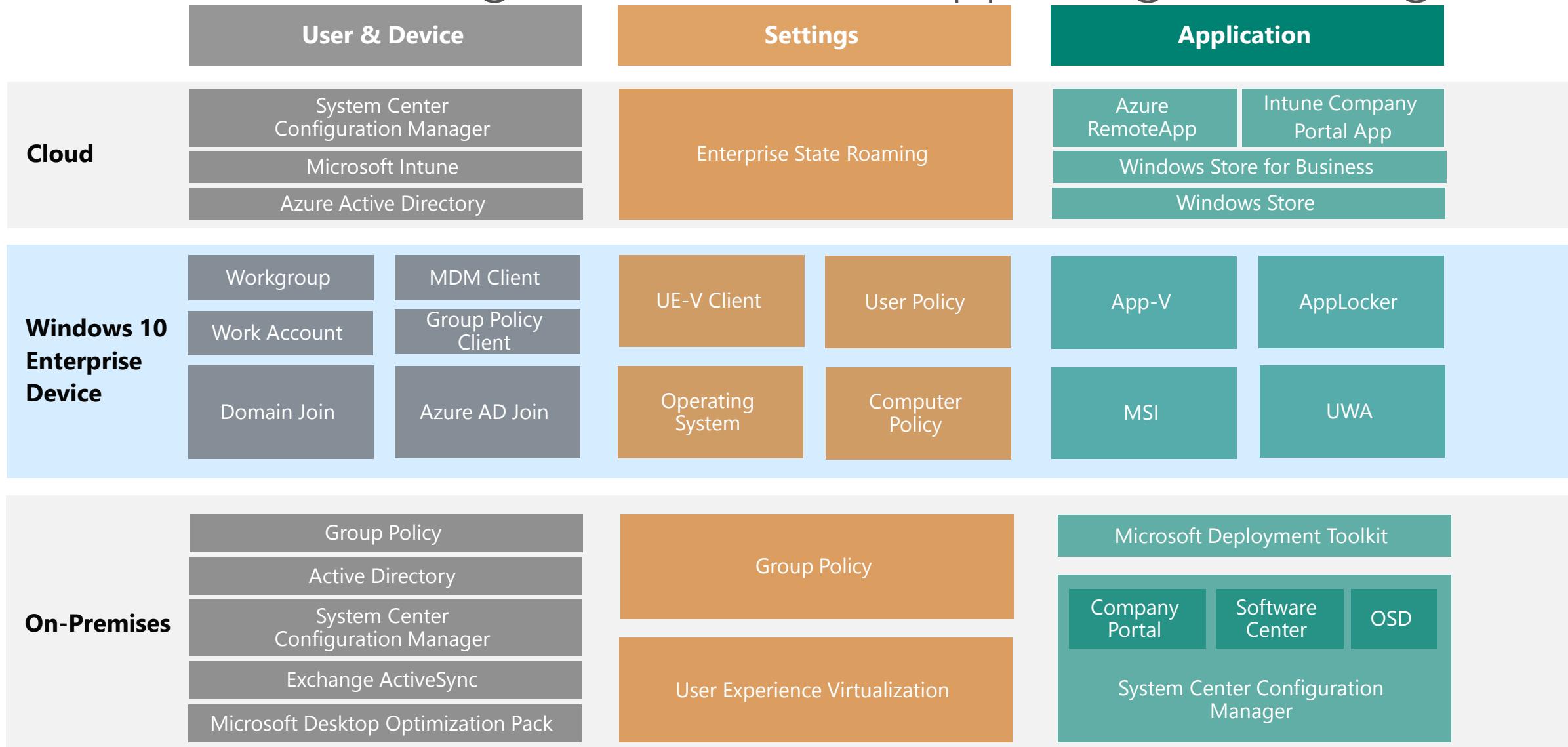
Ownership

- Corporate Owned
- Choose Your Own Device
- Bring Your Own Device

Management Capability & Scenario Matrix

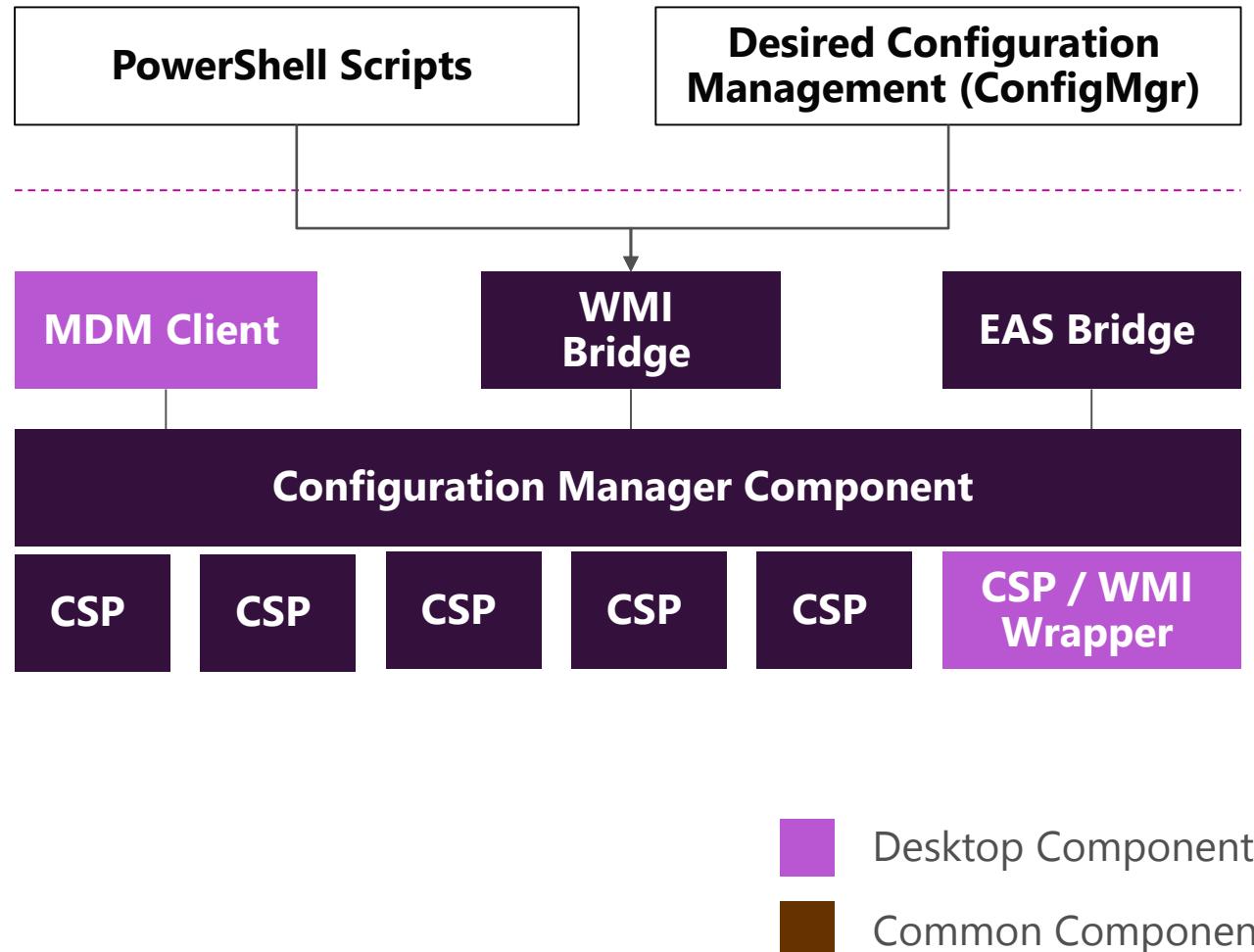
	Capabilities	Scenarios			
		Evergreen Windows 10 management	Take control of mobile devices	Familiar user experience	Reduce device onboarding costs
User & Device	Traditional Management	✓	✗	✓	✗
	Modern Management	✓	✓	✓	✗
	Provisioning	✗	✗	✗	✓
Settings	Policy Configuration	✓	✓	✓	✓
	OS Customization	✗	✓	✓	✗
	Enterprise State Roaming	✗	✗	✓	✗
	On-Premises Roaming	✗	✗	✓	✗
Applications	Device Targeted	✗	✗	✓	✗
	User Targeted	✗	✗	✓	✗
	Self Service	✗	✗	✓	✓

Windows 10 Management Stack & Supporting Technologies

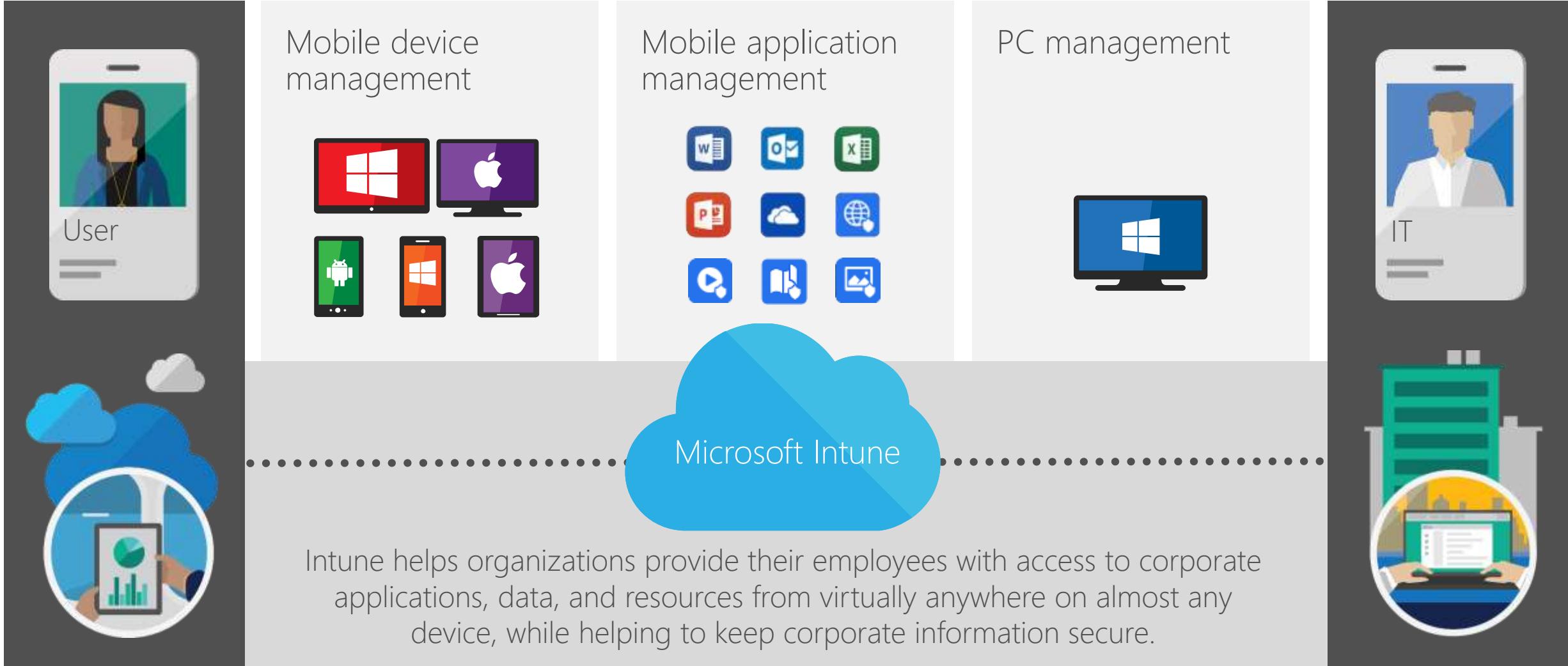


Management Architecture

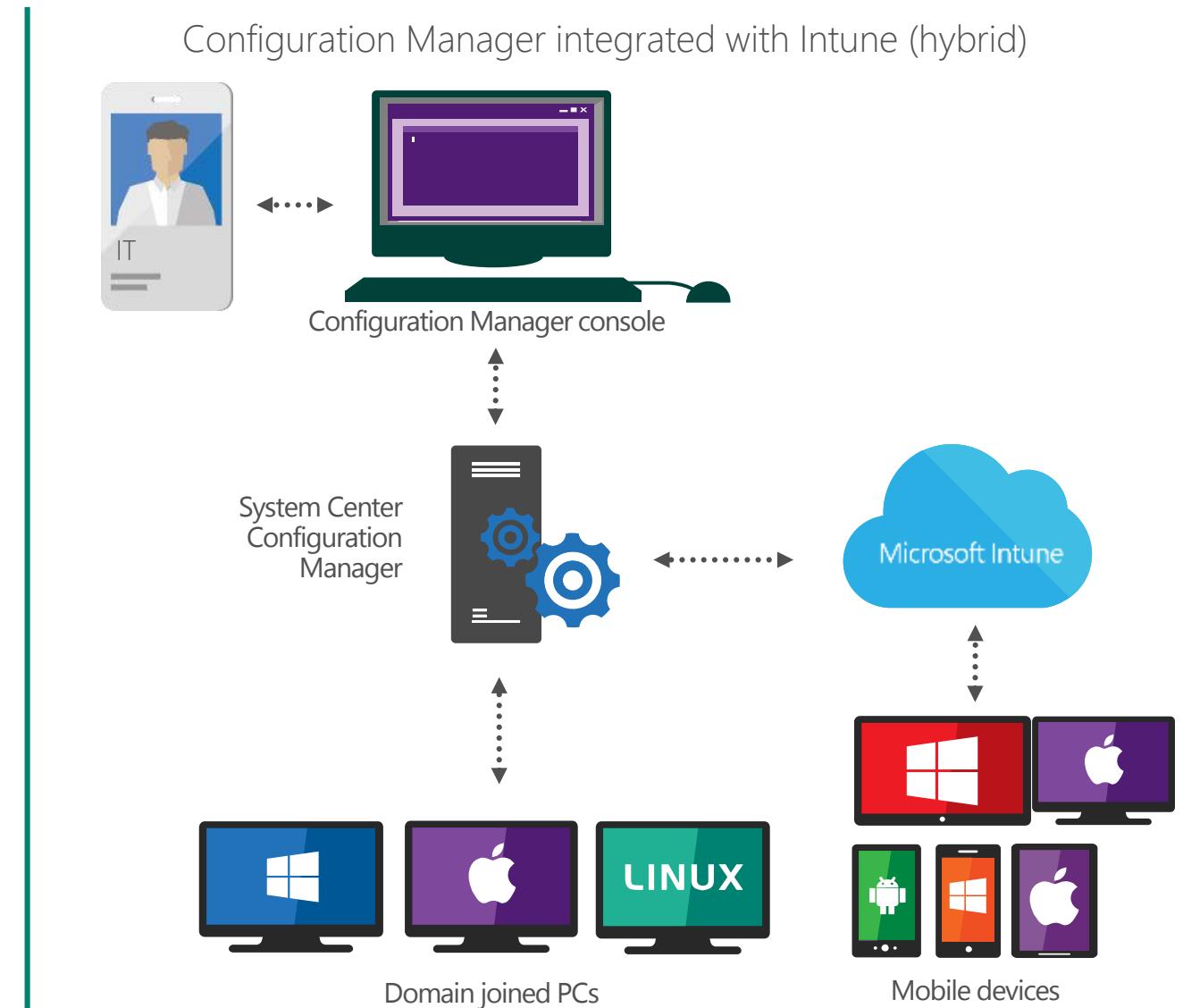
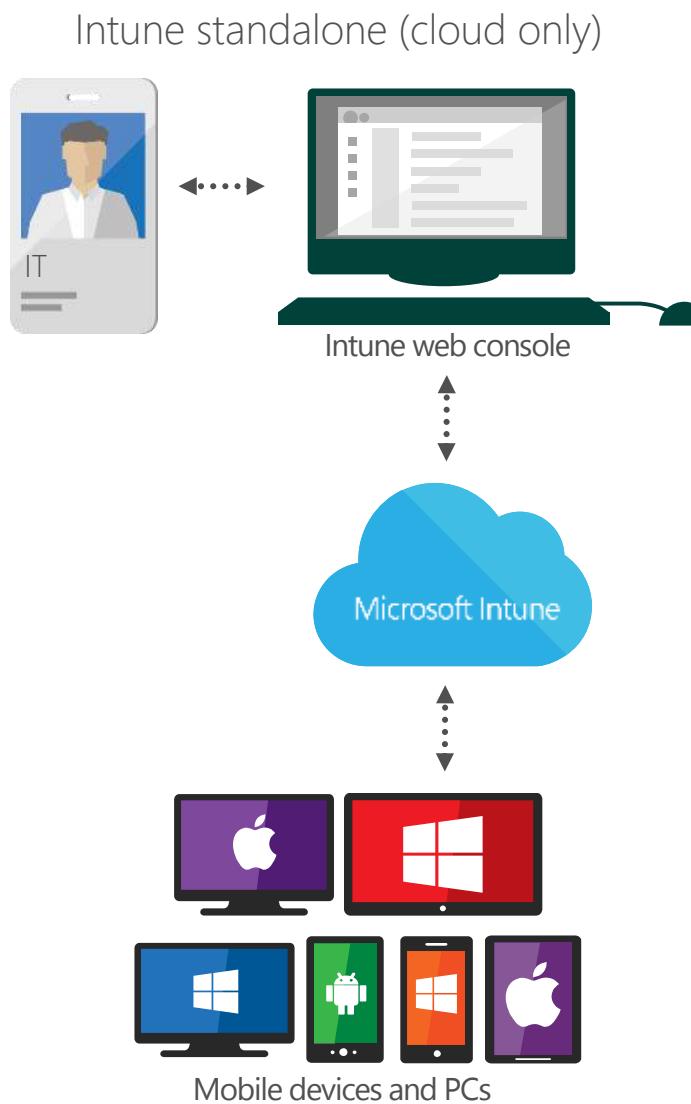
- Alternative method to Group Policy management.
 - Companies may use both approaches to manage devices .
-
- MDM client on Windows 10 talks through Configuration Manager component (not System Center) to other components including Configuration Service Providers (CSP) for additional MDM features / functionality
-
- WMI Bridge exposes MDM settings available, which administrators can be configured via DCM (ConfigMgr) or PowerShell



Modern Management with Microsoft Intune



Microsoft Intune Deployment Flexibility



Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung

MODERNE SICHERHEITSBEDROHUNGEN

**„ES GIBT IN DEN USA ZWEI ARTEN VON
GROßen UNTERNEHMEN: DIEJENIGEN, DIE
GEHACKT WURDEN, UND DIE, DIE NOCH
NICHT WISSEN, DASS SIE GEHACKT
WURDEN.“**

JAMES COMEY, FBI-DIREKTOR

"DIE CYBER-SICHERHEIT IST **CEO-AUFGABE**."

- MCKINSEY

3,0 MRD. USD

Kosten durch Produktivitäts-
und Wachstumsverluste

3,5 MIO. US

Durchschnittliche **Kosten eines**
Datenverlustes (15 % Steigerung pro Jahr)

500 MIO. US

Haftung in
Unternehmen

CYBER-BEDROHUNGEN STELLEN EIN **MATERIELLES RISIKO**
FÜR IHR UNTERNEHMEN DAR

DIE ENTWICKLUNG DER **BEDROHUNGEN**

Unfug



Script-Kiddies

Schlicht

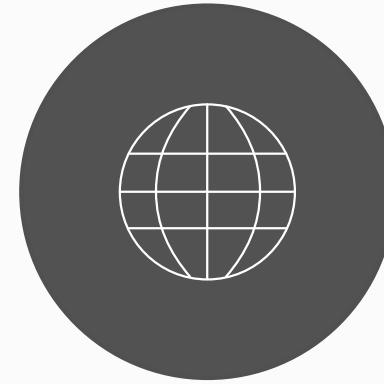
Betrug und Diebstahl



Organisierte Kriminalität

Ausgeklügelt

Schäden und Ausfälle



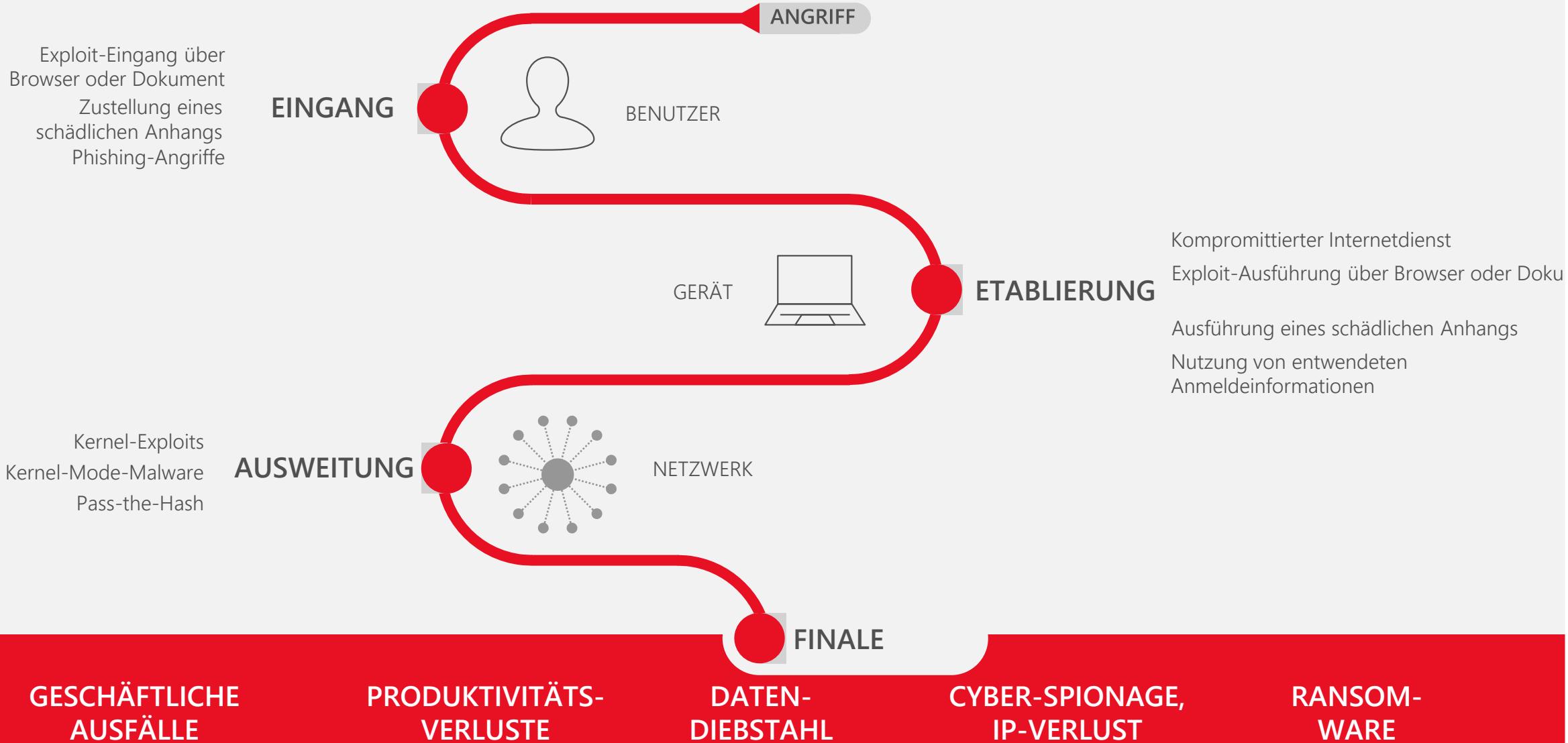
Staaten, Aktivisten, Terrororganisationen

Extrem ausgeklügelt mit starken Ressourcen

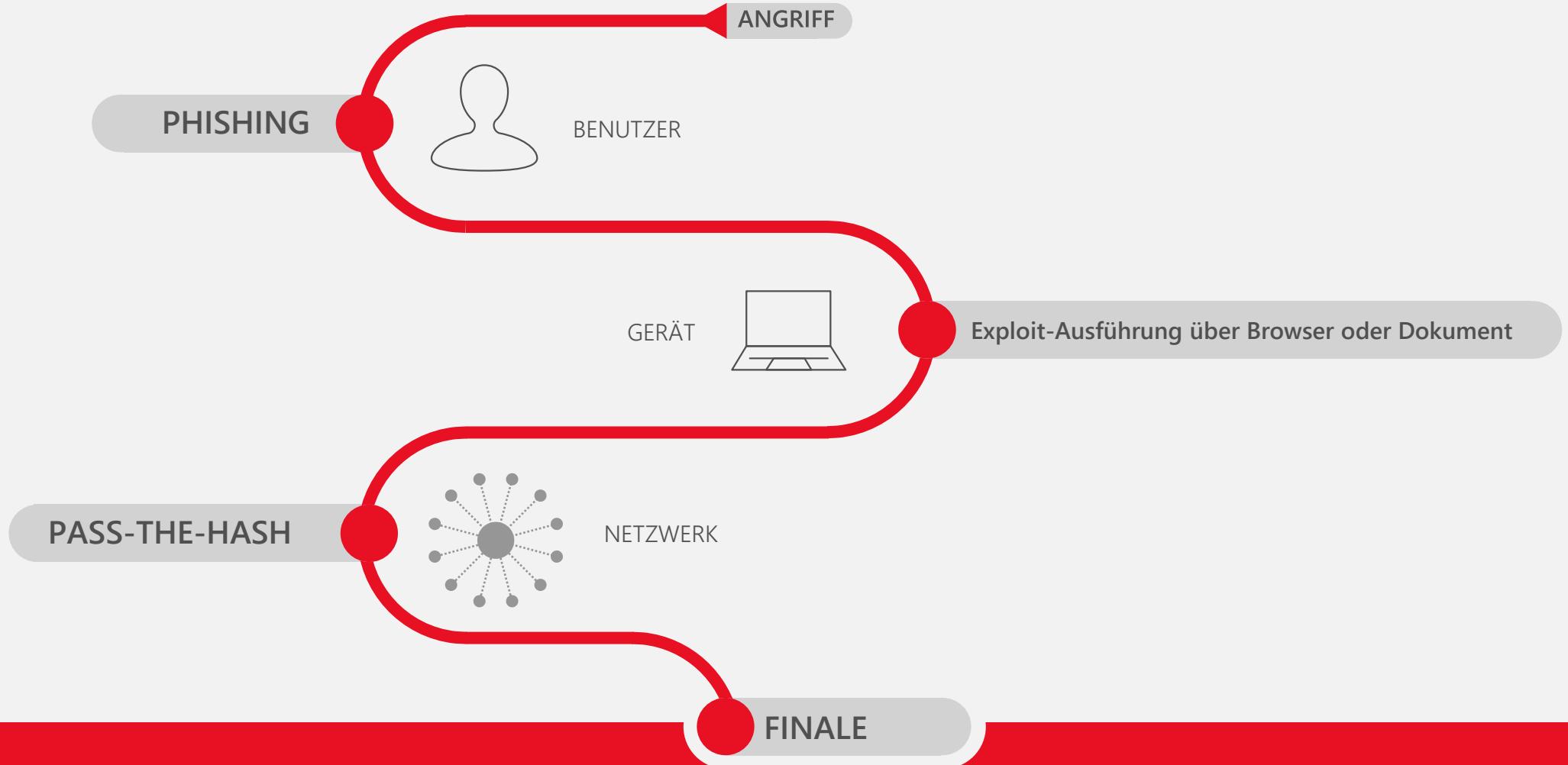
RANSOMWARE



DIE ANATOMIE EINES **ANGRIFFS**

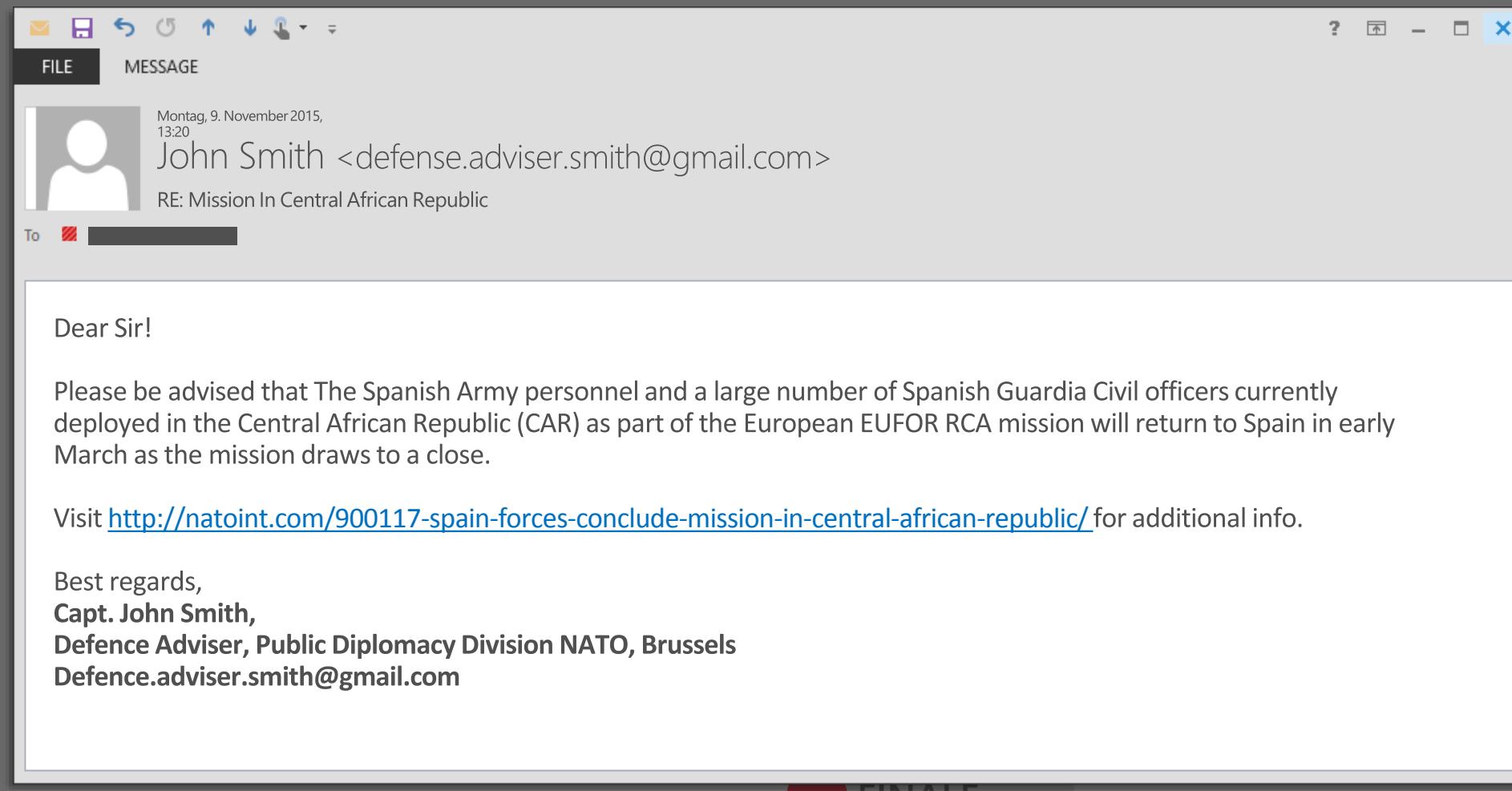


DIE ANATOMIE EINES **ANGRIFFS: STRONTIUM**



Diebstahl sensibler Informationen, Verwaltungsausfälle

DIE ANATOMIE EINES ANGRIFFS: STRONTIUM

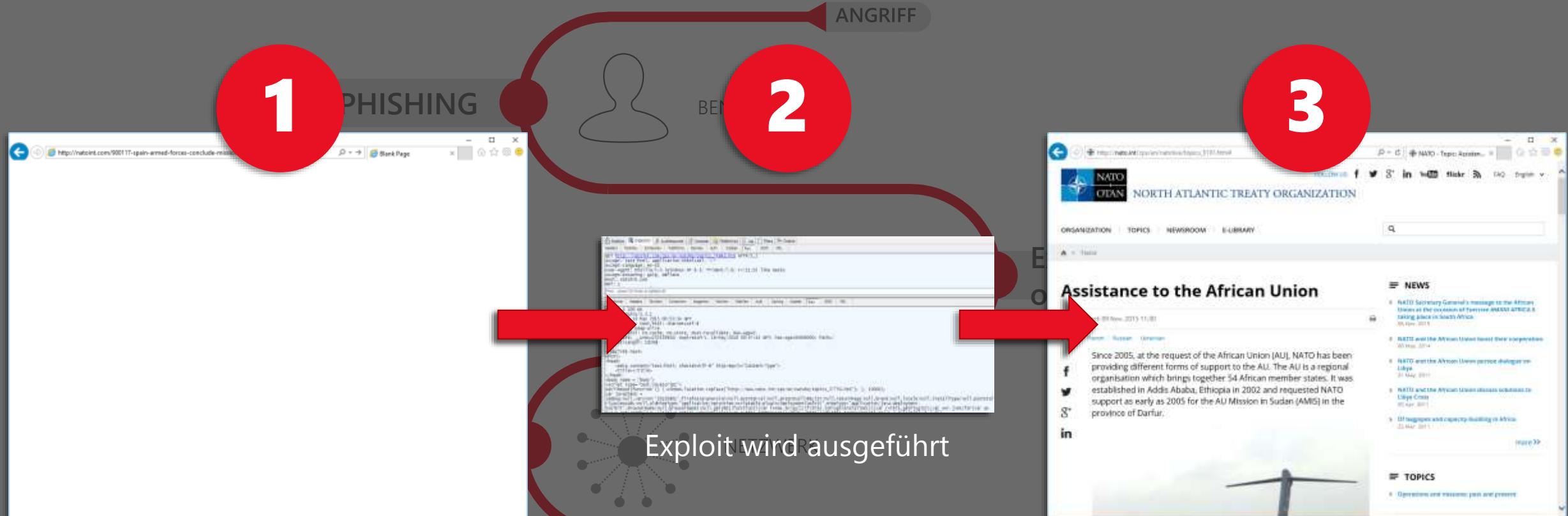


FINALE

Diebstahl sensibler Informationen, Verwaltungsausfälle

DIE ANATOMIE EINES ANGRIFFS: STRONTIUM

00:00.1



Diebstahl sensibler Informationen, Verwaltungsausfälle

DIE NEUE MICROSOFT-**SICHERHEITSHALTUNG**

Schützen

In der modernen Welt mit Clouds und mobilen Geräten ist eine höchstmögliche Sicherheit der Identitäten und der Daten erforderlich

Erkennen

Umfassende Überwachungs-tools, die Sie bei der Erkennung von Auffälligkeiten und bei der schnelleren Reaktion auf Angriffe unterstützen

Reagieren

Hervorragende Technologien zur Reaktion und Wiederherstellung sowie tief greifende Beratungskompetenz

DIE UMFASSENDE **SICHERHEITSVISION** VON MICROSOFT



Geräte



Apps



Benutzer



Daten

Schützen

Schutz auf allen Ebenen – Hardware, Software und Anwendungen

Schutz von Apps über sichere Entwicklungspraktiken zur Reduzierung der Angriffsfläche

Schutz durch weniger Diebstahlsmöglichkeiten von Anmeldeinformationen

Schutz der Daten unabhängig von deren Speicherort

Erkennen

Erkennung jeglicher Abweichungen von Baselines, Richtlinien oder Verhalten

Erkennung der Nutzung von nicht zugelassenen Apps oder von Bedrohungen für Apps

Erkennung von verdächtigem Verhalten und ungewöhnlichen Aktivitäten

Erkennung jeglicher nicht autorisierter Zugriffsversuche auf Daten

Reagieren

Dynamische Reaktion auf jegliche verdächtige Geräte oder Anwendungen

Dynamische Reaktion auf jegliche verdächtige Anwendungen

Reaktion durch strengere Zugriffsanforderungen auf Basis der Risiken

Reaktion auf jegliche Datenlecks durch Unterbindung oder Überwachung des Zugriffs

DER WINDOWS 10-SICHERHEITSSTACK

SCHÜTZEN, ERKENNEN UND REAGIEREN



Understanding threats through scenarios

	Capabilities	Scenarios			
		Protect Sensitive Data	Protect Administrators	Threat Resistance	Threat Detection
Secure Devices	Device Integrity	✓	✓	✓	✗
	Platform Integrity	✓	✓	✓	✓
Secure Identities	Hybrid Identity	✗	✗	✓	✗
	Secure User Credential	✗	✓	✓	✗
	Biometric Authentication	✗	✗	✓	✗
	Post-Breach Detection	✗	✗	✗	✓
Secure Data	Device Encryption	✓	✓	✓	✗
	Enterprise Data Protection	✓	✗	✗	✗
	Data Sharing Protection	✓	✗	✗	✗
	Conditional Access	✓	✗	✗	✗
Secure Applications	Secure Trusted Applications	✗	✓	✓	✗

Addressing the threats requires a new platform

Windows 7

Secured Devices

- Platform security built on software
- Malware tampers with defenses and hides

Secured Identities

- Passwords theft increasingly successful
- Multi-factor solutions too complex

Secure Data

- Optionally configurable disk encryption, lacks integrated Data Loss Prevention
- 3rd party solutions provide varying experiences on mobile and desktop

Secure Applications

- Apps are trusted until they're determined to be a threat
- No realistic way to detect 300K's+ new threats per day

Windows 10

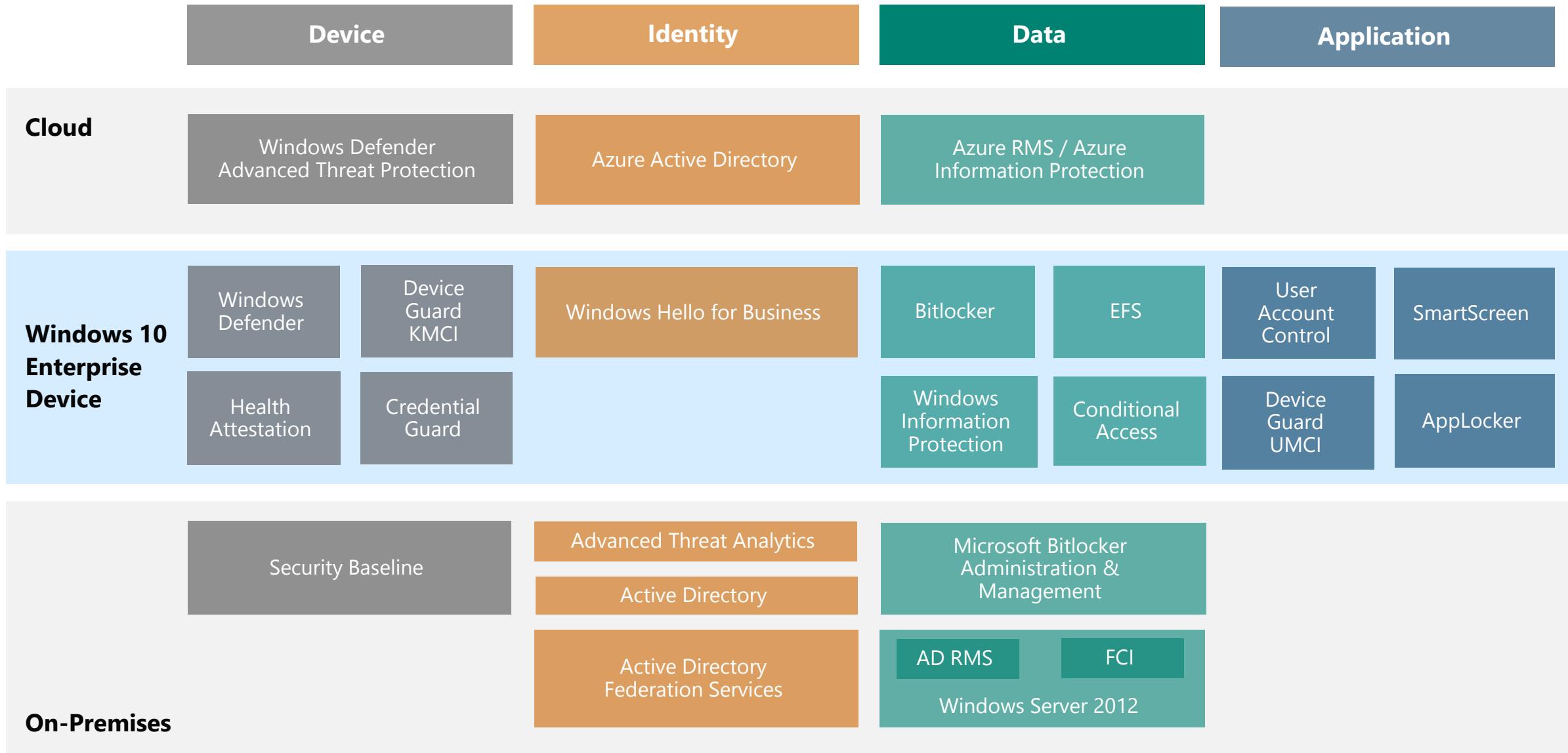
- Integrated platform and hardware security protects system integrity
- Eliminates opportunities for malware to tamper with and hide from the system

- A viable alternative to passwords arrives
- Easy and cost effective multi-factor authentication

- Disk encryption increasingly enabled OOB and is highly manageable
- Data loss prevention and data separation fully integrated into the experience

- Mobile level of lockdown possible for desktop machines
- Lock down Windows to only run trusted apps

Windows 10 Defense Stack & Supporting Technologies

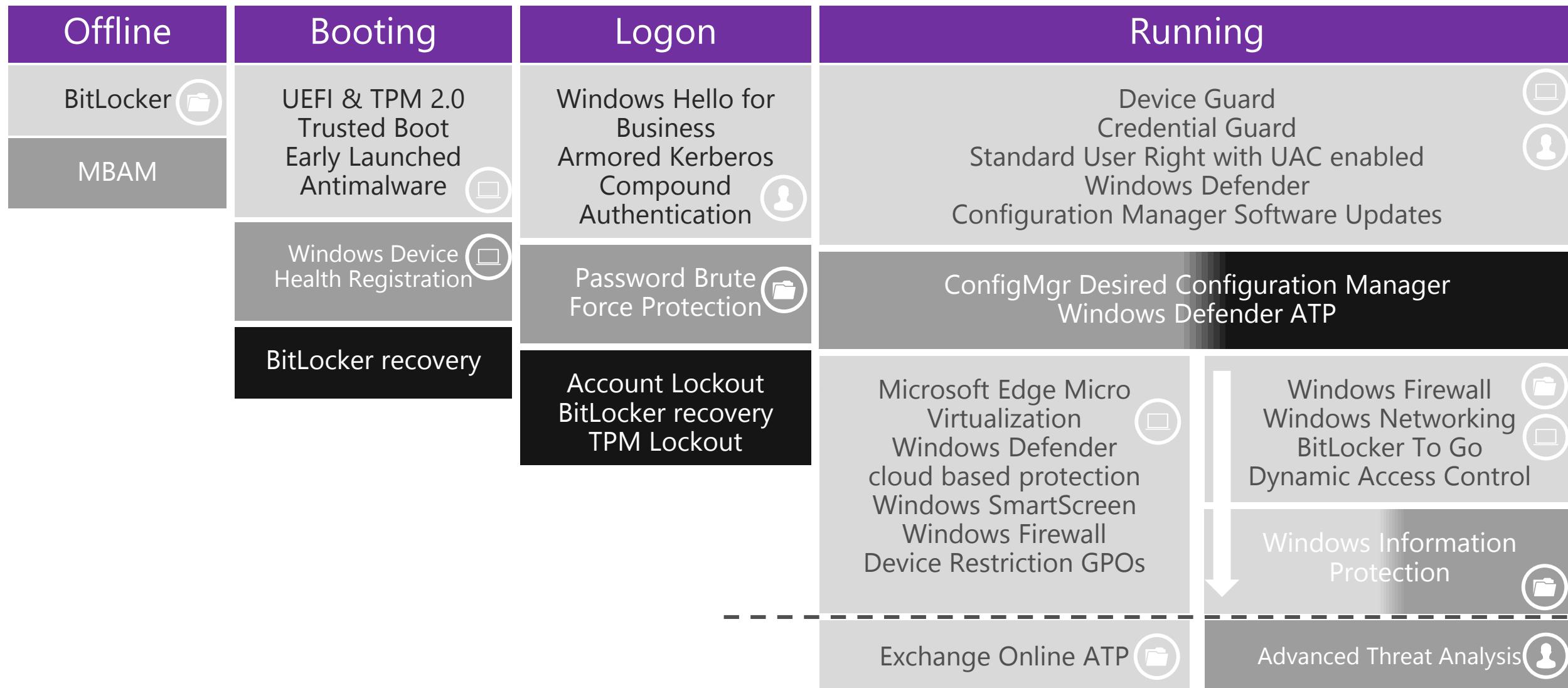


Windows 10 Defense Stack

Protect

Detect

Respond



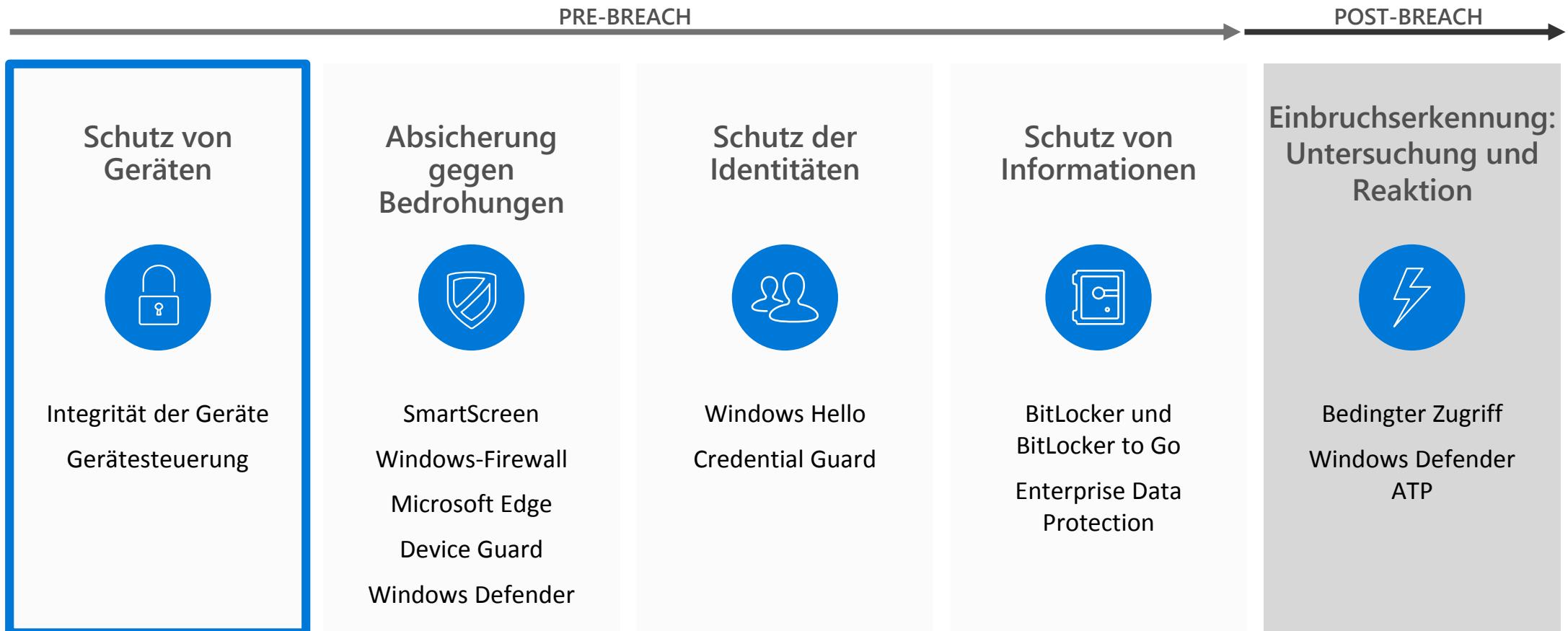
Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung

DER WINDOWS 10-SICHERHEITSSTACK

SCHÜTZEN, ERKENNEN UND REAGIEREN



SCHUTZ VON GERÄTEN

ROOTS OF TRUST-SICHERHEIT

Integrität der Geräte



Kryptographische Verarbeitung



Biometrische Sensoren

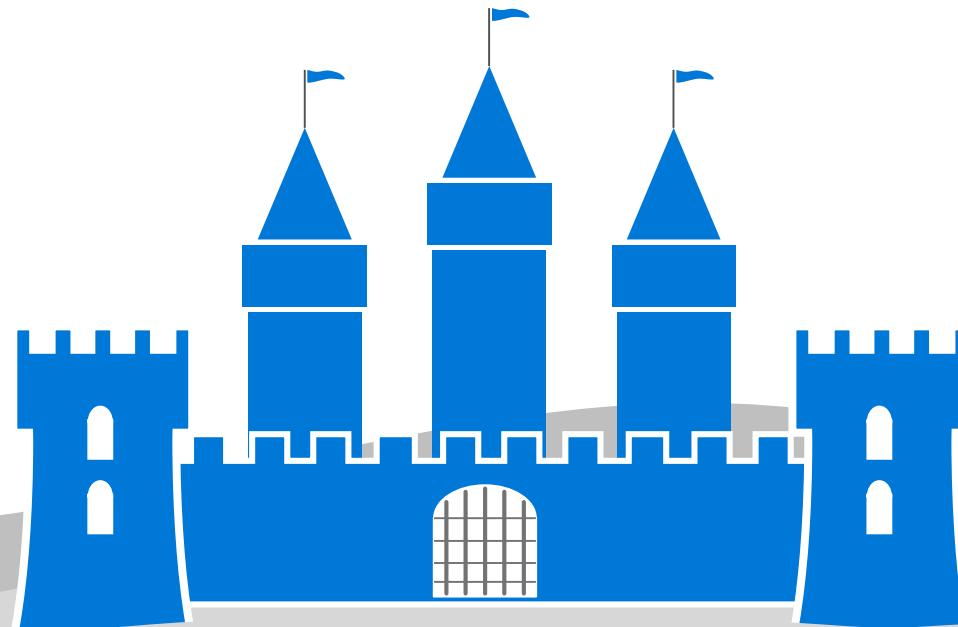


Virtualisierung



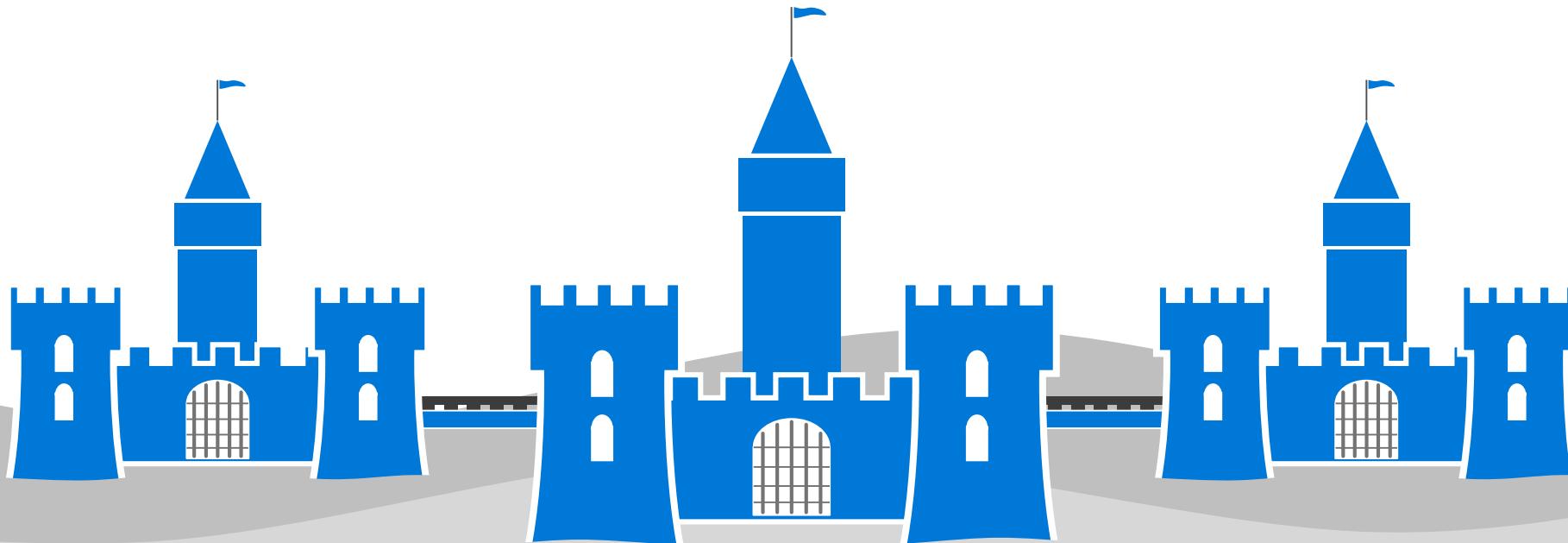
TRADITIONELLE PLATTFORMSICHERHEIT

EIN EINZIGER EINBRUCH KOMPROMITTiert ALLE
KOMPONENTEN

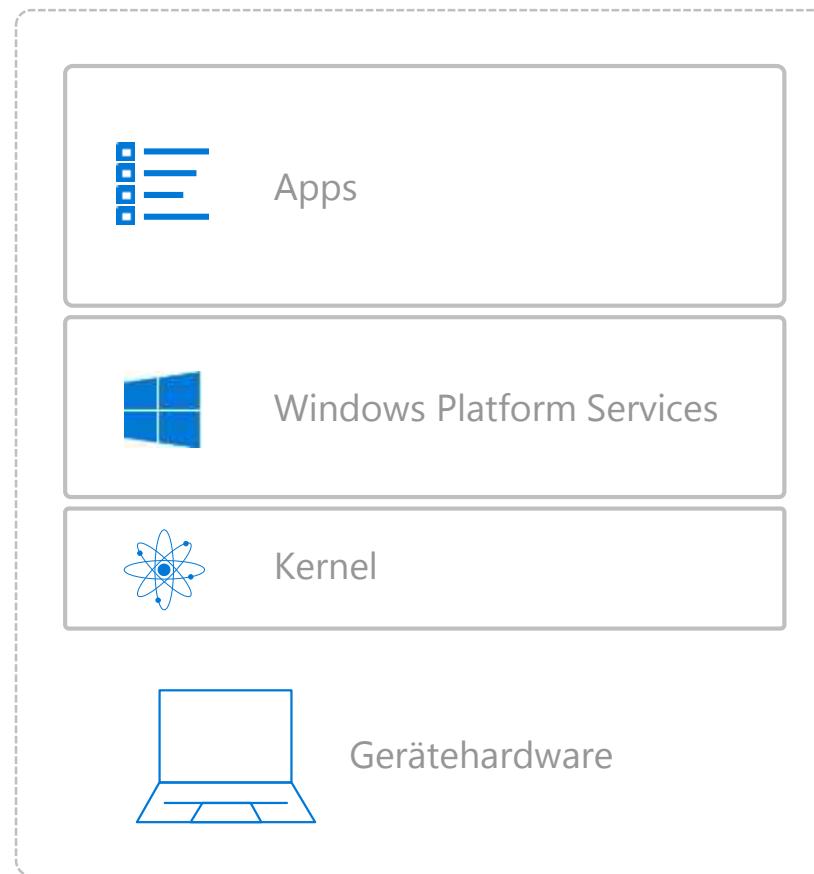


VIRTUALISIERTE PLATTFORMSICHERHEIT

WICHTIGE KOMPONENTEN SIND GETRENNT UND GESCHÜTZT

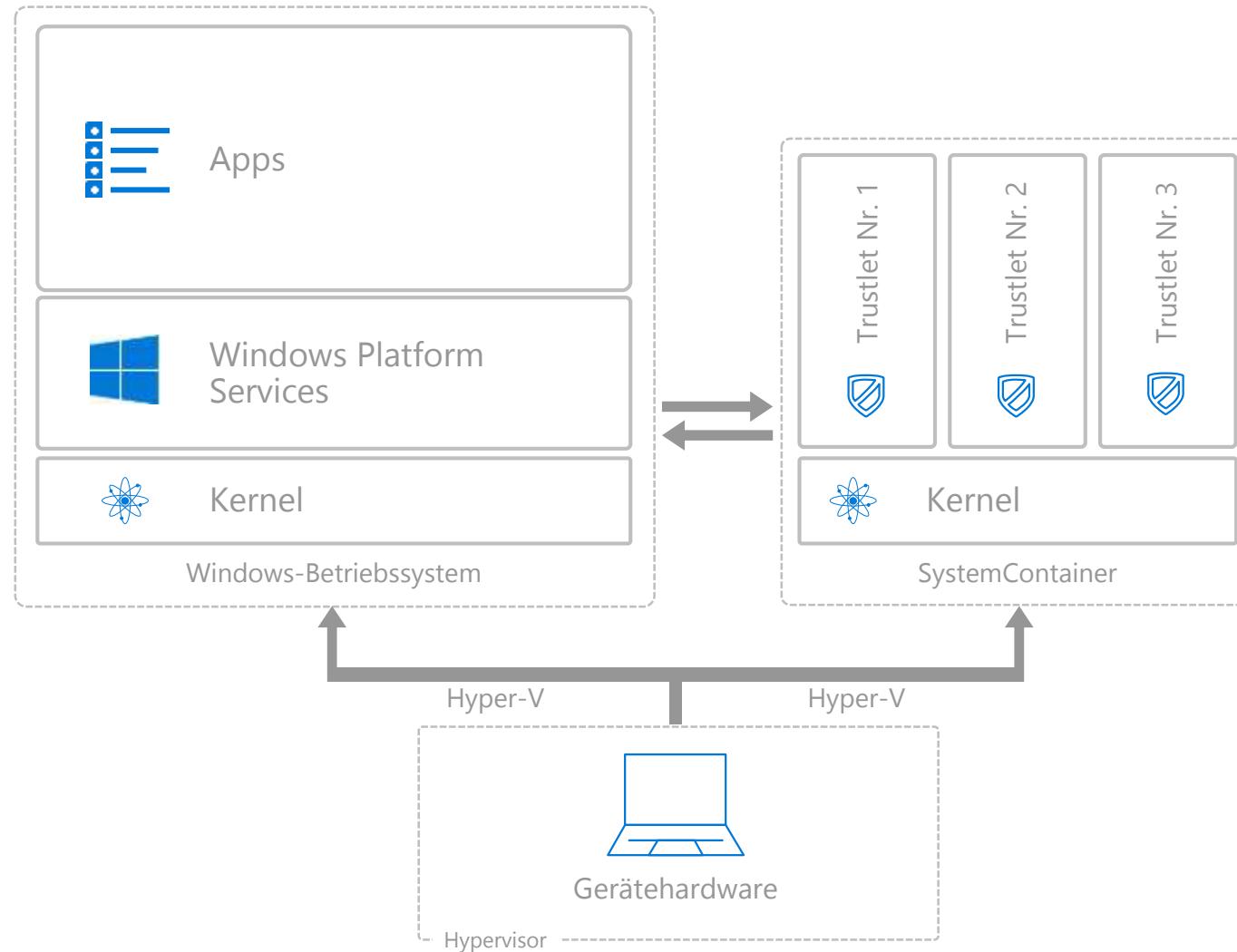


TRADITIONELLER PLATTFORM-STACK



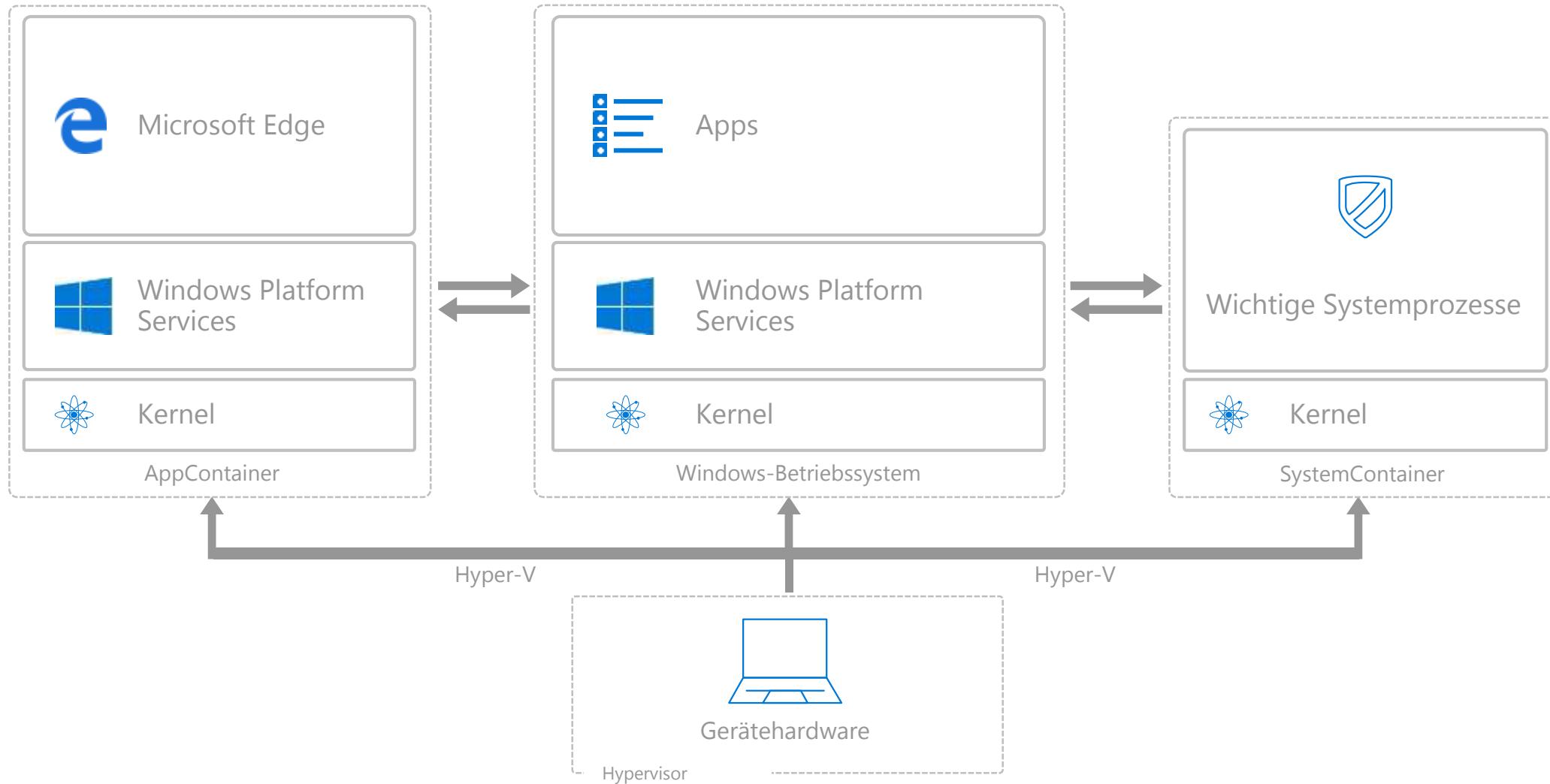
VIRTUALISIERUNGSBASIERTE SICHERHEIT

WINDOWS 10

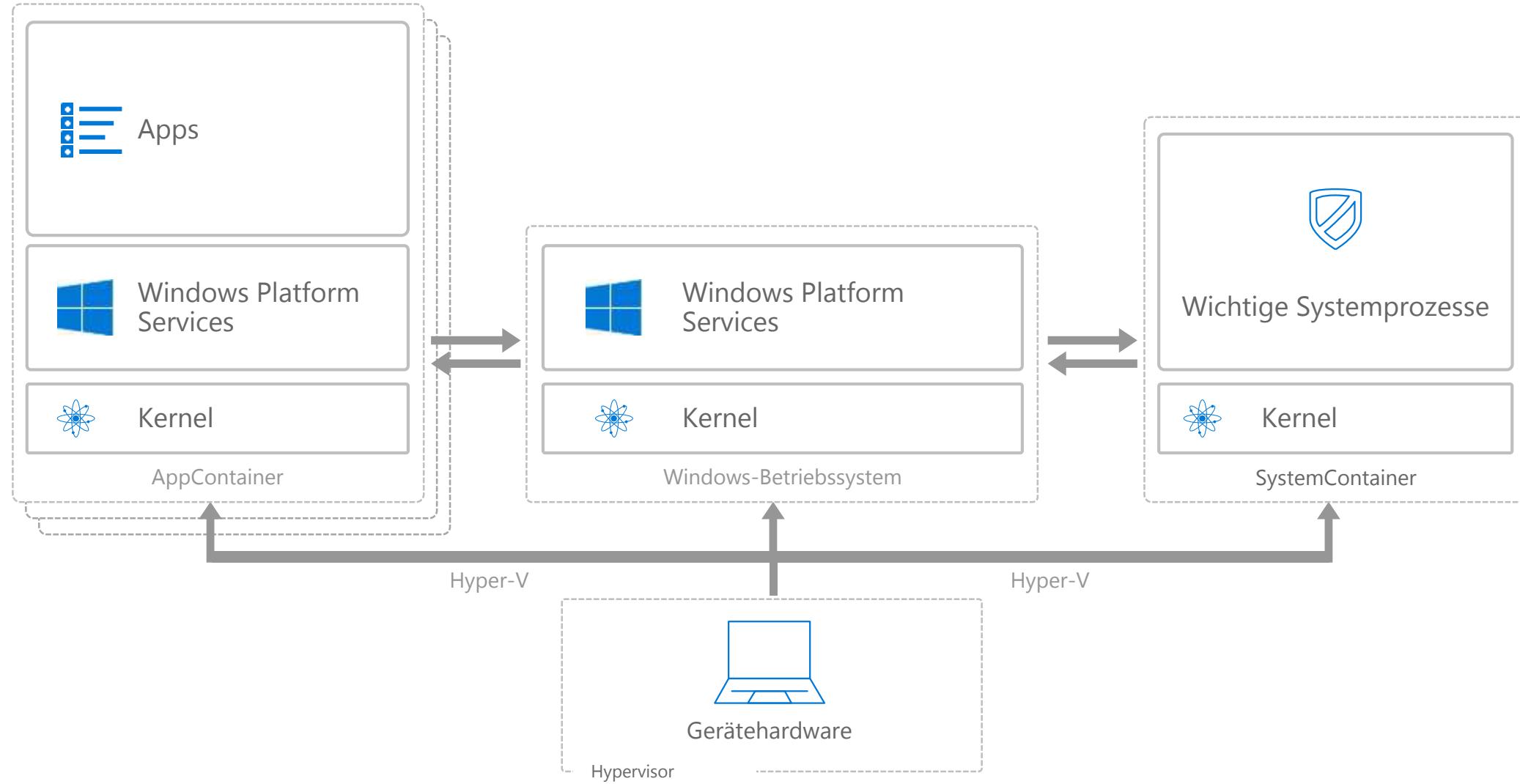


VIRTUALISIERUNGSBASIERTE SICHERHEIT

PREVIEW 2016 RTM 2017



VIRTUALISIERUNGSBASIERTE SICHERHEIT NACH 2017



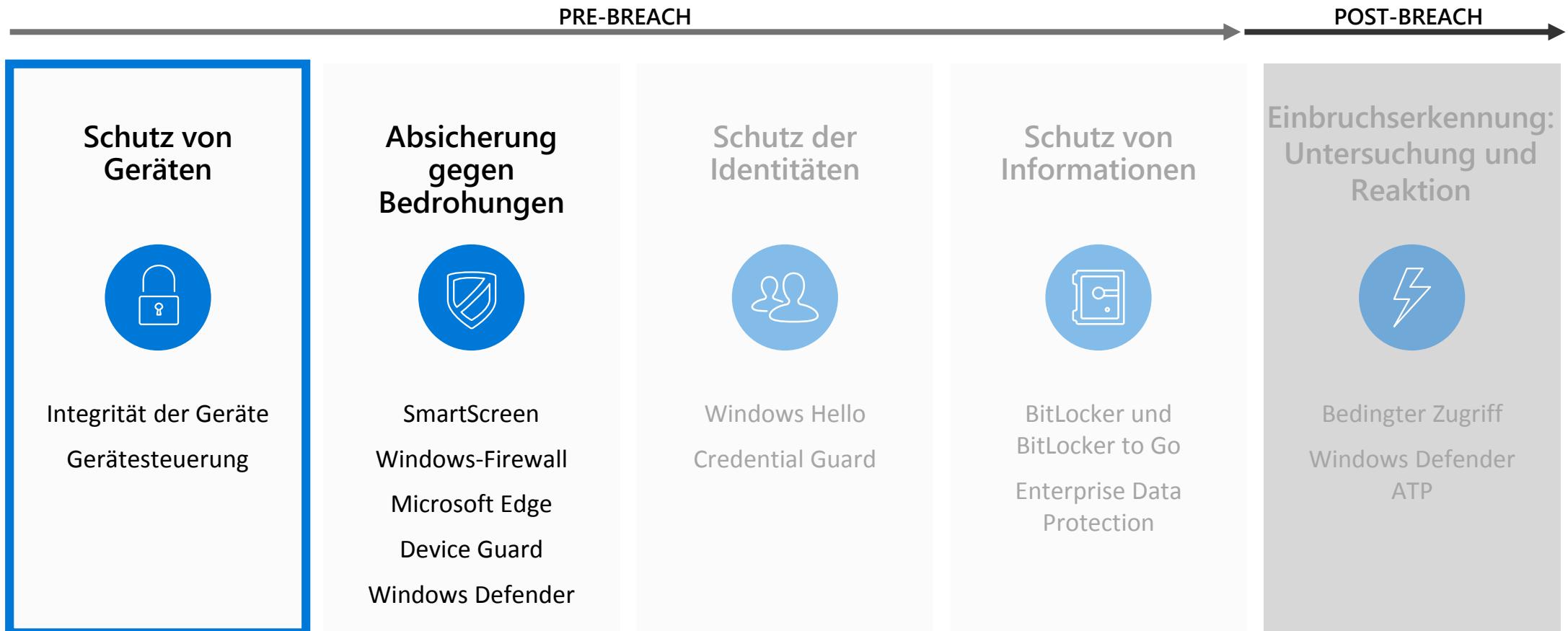
Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung

DER WINDOWS 10-SICHERHEITSSTACK

SCHÜTZEN, ERKENNEN UND REAGIEREN



TRADITIONELLER **ANSATZ**

Zu berücksichtigende und zu beseitigende Bedrohungen

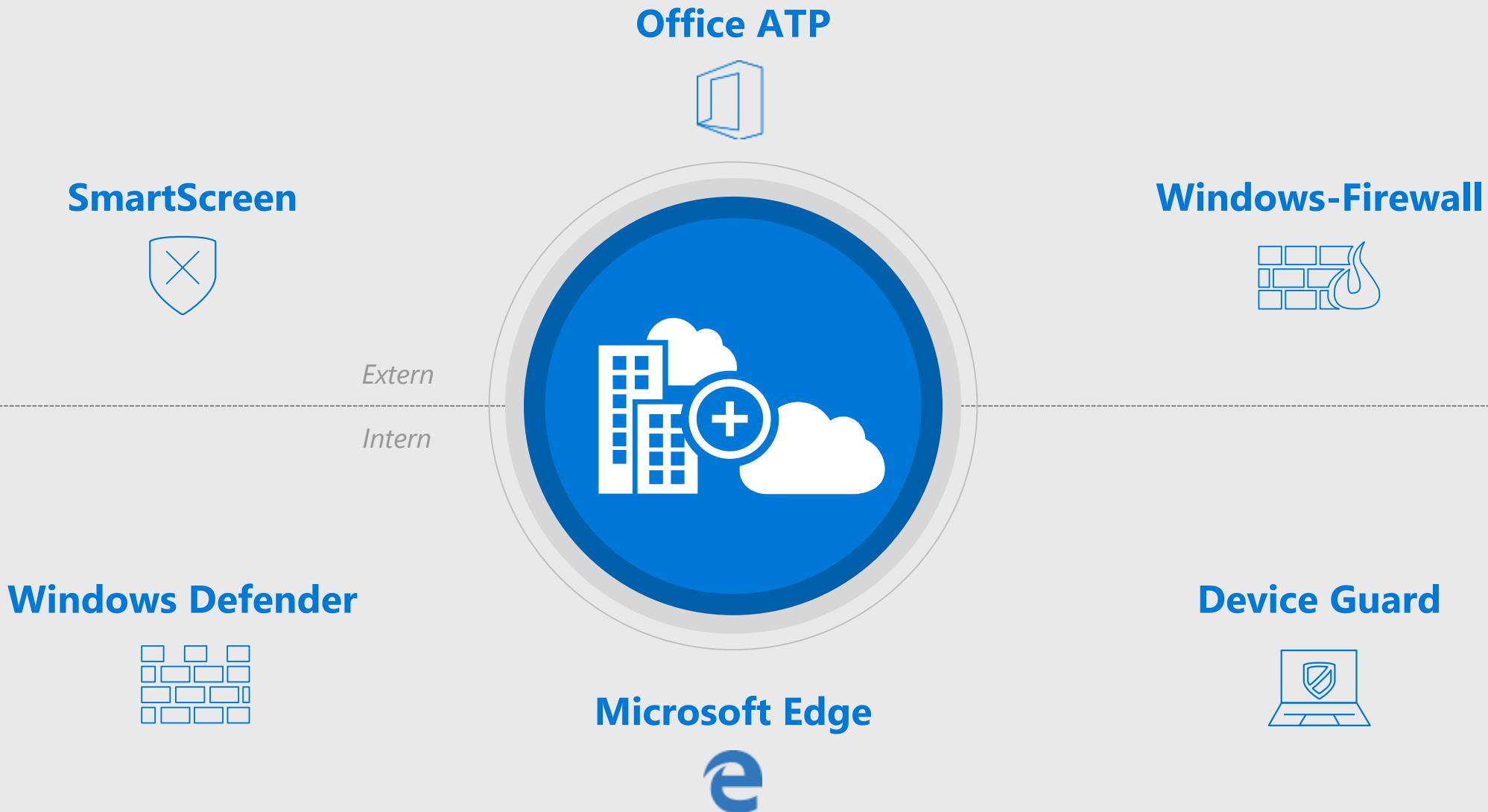
Veränderung von
Geräten (Tampering)

Sicherheitslücken

Malware

Phishing

UMFASSENDER SCHUTZ VOR BEDROHUNGEN



Windows 10

SCHUTZ NACH AUSSEN

Schützen von Geräten, bevor diese von
Bedrohungen betroffen sind

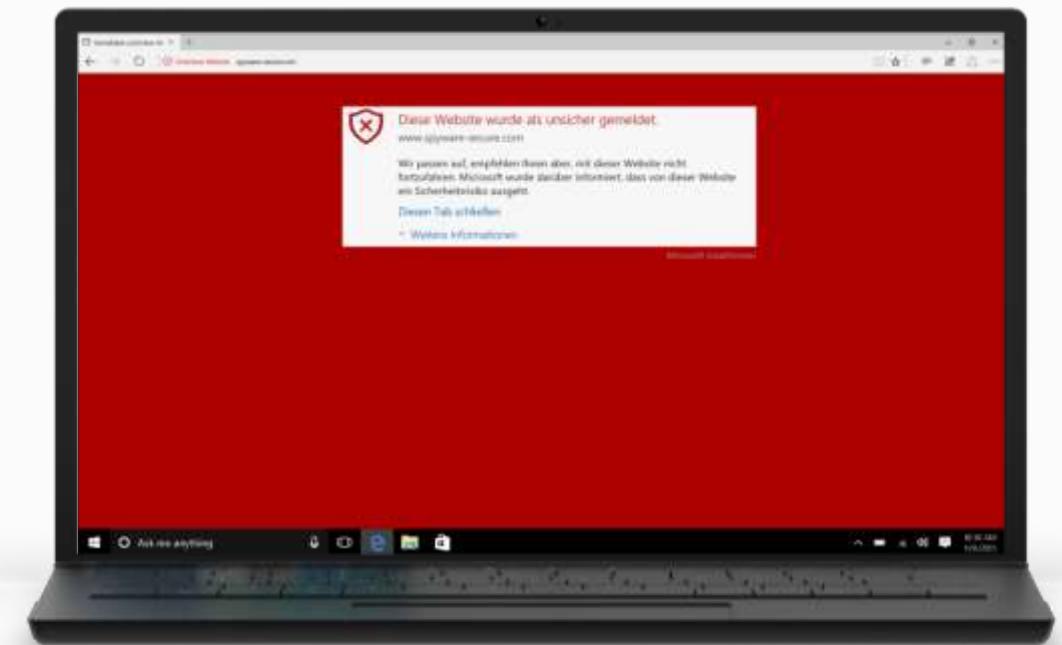
PROAKTIVE BEDROHUNGSERKENNUNG UND **SCHUTZ**

Microsoft SmartScreen

- Eine Phishing- und Malware-Filtertechnologie für Internet Explorer 11 und Microsoft Edge unter Windows 10.
- Ermöglicht den Schutz vor Drive-by-Angriffen.
- Ein Cloud-Dienst, der fortlaufend aktualisiert wird und nicht bereitgestellt werden muss.

Exchange Online Advanced Threat Protection

- Cloudbasierter Dienst zur E-Mail-Filterung, der vor unbekannter Malware und unbekannten Viren schützt.
- Eine URL-Trace-Technologie prüft möglicherweise schädliche Links.



Windows 10

SCHUTZ VON INNEN

Tief greifende Verteidigung gegen bereits eingedrungene Bedrohungen durch das Betriebssystem

MICROSOFT EDGE: ALS **SICHERER BROWSER** ENTWORFEN

Microsoft Edge ist der bislang sicherste Browser von Microsoft

Ziel

Sicheres Browsen im Web für unsere Kunden



Strategie

Das Finden und Ausnutzen von Sicherheitslücken in Microsoft Edge für die Angreifer so schwierig und kostenintensiv wie möglich gestalten



Taktiken



Beseitigung von Sicherheitslücken vor deren Entdeckung durch Angreifer



Unterbinden der von Angreifern verwendeten Techniken



Eindämmen des Schadens erfolgreicher Angriffe



Verhindern des Aufrufs bekannter schädlicher Websites

MICROSOFT EDGE: ENTWICKLUNG EINES SICHEREREN BROWSERS

Die grundlegend verbesserte Sicherheit sorgt für eine vertrauenswürdigere Nutzung des Internets unter Windows 10



SCHUTZ DER BENUTZER

Erkennen und Blockieren bekannter Betrugsversuche und Täuschungen

Schutz vor schädlichen Websites und Downloads ([SmartScreen](#))

Sicherere und komfortablere Anmeldeinformationen, die nicht von Angreifern entwendet werden können
([Microsoft Passport](#) und [Windows Hello](#))

Unterstützung neuer Web-Sicherheitsstandards, um gängige Angriffe und Identitätswechsel zu unterbinden
([Cert. Reputation](#), [EdgeHTML](#), [W3C Content Security Policy](#), [HTTP Strict Transport Security](#))



SCHUTZ DES BROWSERS

Neues Modell zur sichereren Ausführung von Browser-Erweiterungen, mehr Schutz vor Arbeitsspeicherangriffen

Microsoft Edge ist eine App, die standardmäßig in einer Sandbox arbeitet
([Universelle Windows-Plattform](#))

Bereich für die zufällige Speicheranordnung erheblich erweitert
([Windows Address Space Layout Randomization auf 64-Bit-Systemen](#))

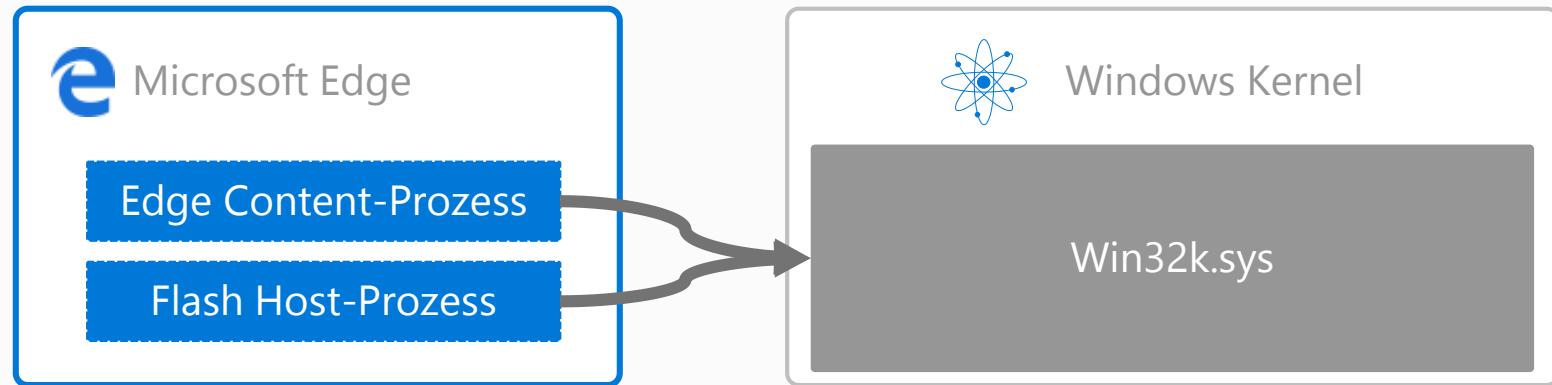
Automatische Speicherbereinigung für Programme ohne Speicherbereinigung
([MemGC](#))

Entwicklungstools, die das Übernehmen einer Anwendung erheblich erschweren
([Control Flow Guard](#))

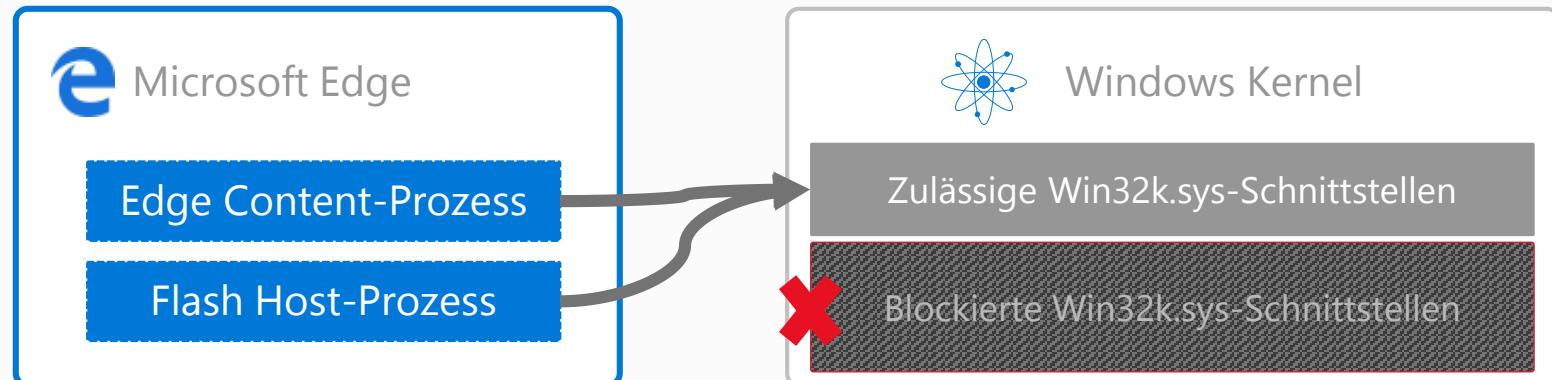
MICROSOFT EDGE **SICHERHEITSVERBESSERUNGEN**

- Microsoft Edge und Flash haben keinen Vollzugriff auf win32k.sys—API-Aufrufe werden gefiltert
- Nur 40 % der Schnittstellen stehen Flash und Edge zur Verfügung – dies verringert die Angriffsfläche
- Der Flash-Player hat jetzt seinen eigenen AppContainer
- Der Flash-Player wurde für einen besseren Speicherschutz gehärtet

Vorher – Vollzugriff auf Win32.sys

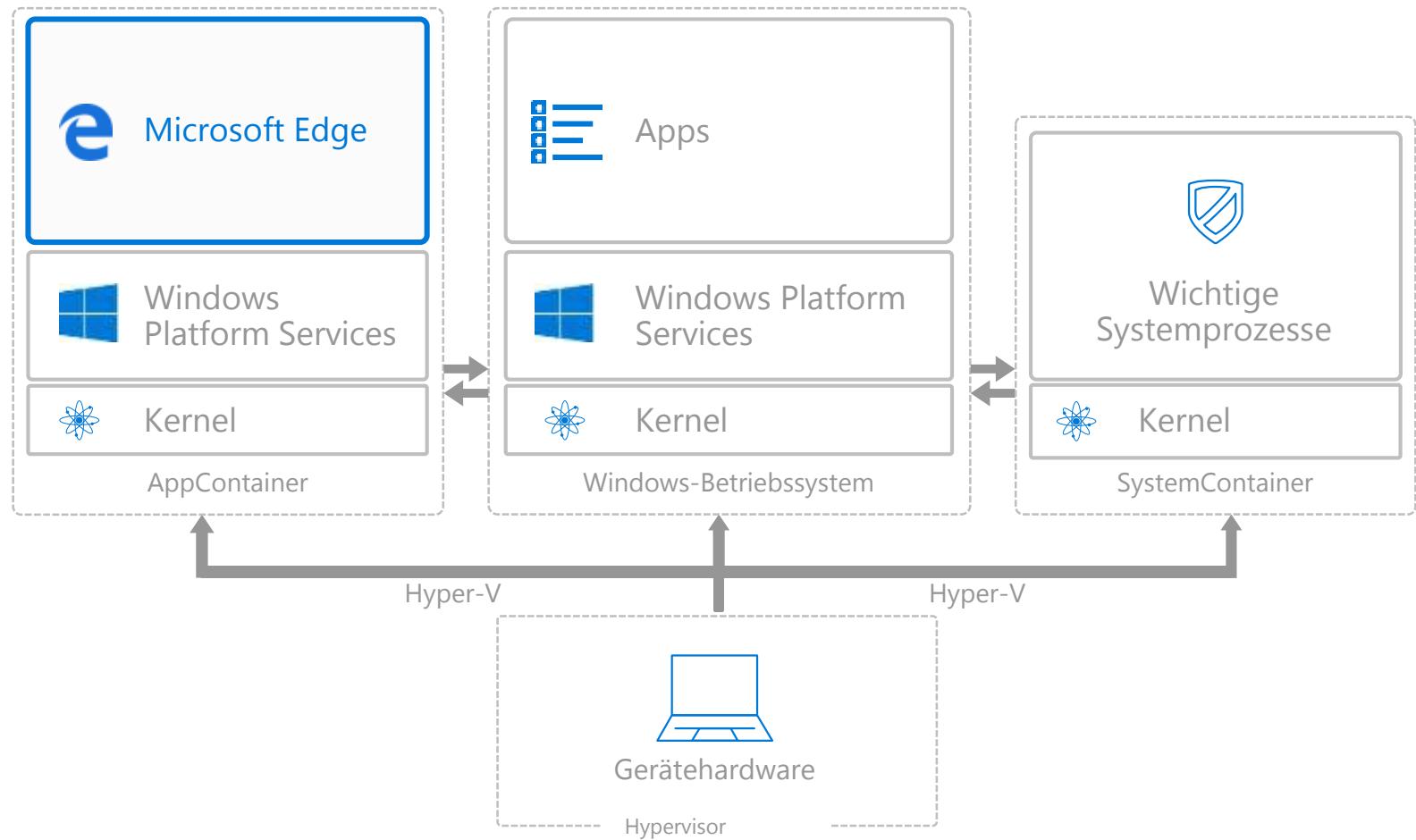


Heute – 60 % weniger Schnittstellen verfügbar

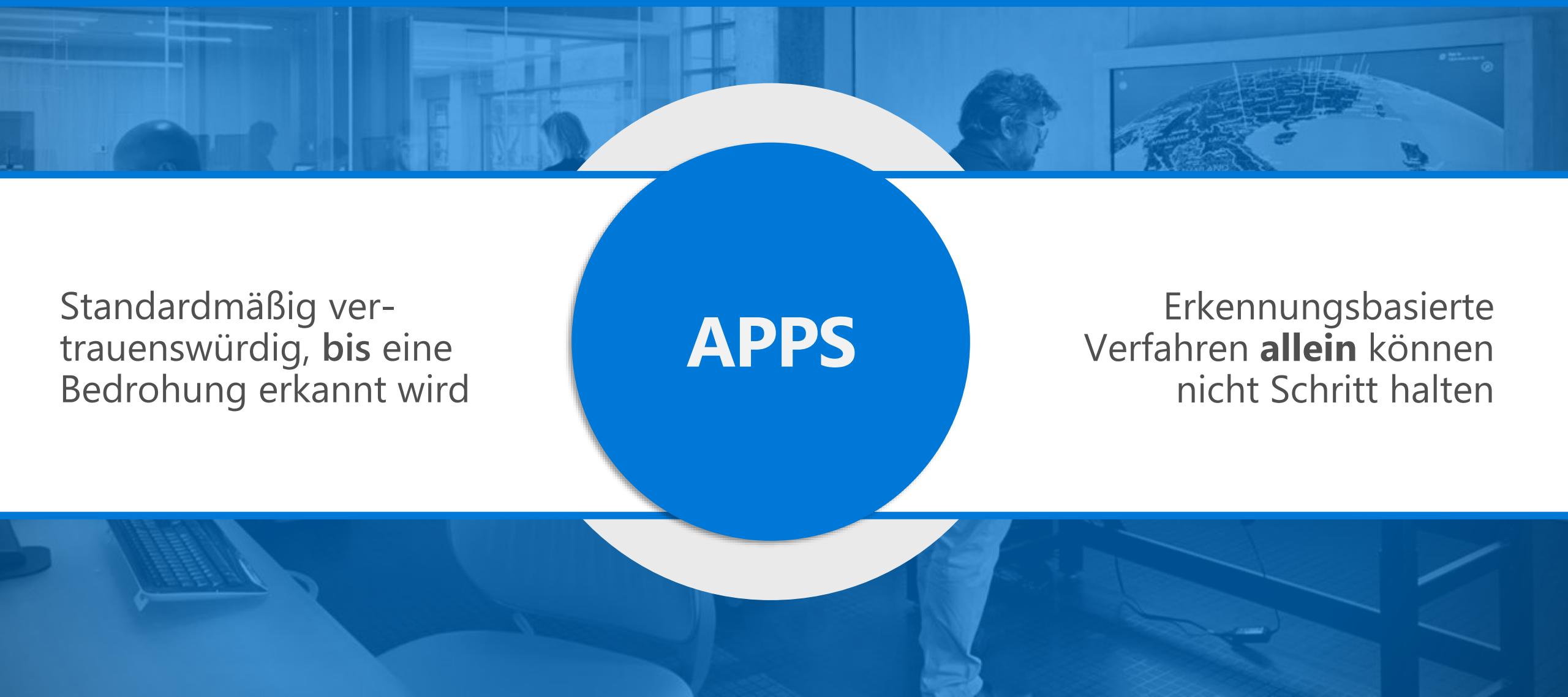


NACH AUßen GESICHERTES BROWSEN

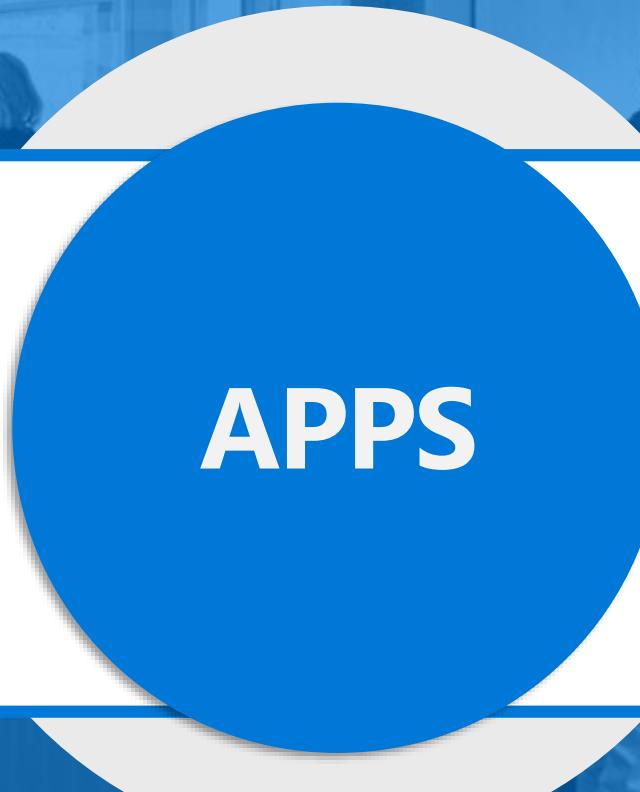
- Verschiebt Browsersitzungen in eine isolierte, virtualisierte Umgebung
- Sorgt für einen erheblich besseren Schutz und härtet den beliebtesten Zugang von Angreifern
- Preview in 2016, geplante Veröffentlichung in 2017



DIE AKTUELLE HERAUSFORDERUNG:



Standardmäßig vertrauenswürdig, bis eine Bedrohung erkannt wird



APPS

Erkennungsbasierte Verfahren **allein** können nicht Schritt halten

DIE BASIS FÜR **IHRE SICHERHEIT**

**APPS MÜSSEN VOR DER
NUTZUNG VERTRAUEN
ERWERBEN**



Windows 10

MODERNE APP-KONTROLLE

Absicherung Ihrer Geräte mit Device Guard

DEVICE **GUARD**

Hardwarebasierte App-Kontrolle

Windows-Desktops können für die ausschließliche Ausführung von vertrauenswürdigen Apps abgesichert werden (vergleichbar mit mobilen Betriebssystemen wie Windows Phone)

Nicht vertrauenswürdige Apps und ausführbare Dateien wie Malware können nicht gestartet werden

Schützt Kernel-Mode-Prozesse und Treiber per HVCI vor Zero-Day-Angriffen und Sicherheitslücken

Erfordert für Windows 8 oder höher zertifizierte Hardware mit VT-X und VT-D



DEVICE **GUARD**

Vertrauen auf Apps ausdehnen

Unterstützt alle Apps inkl. Universal- Desktop- Apps (Win32).

Vertrauenswürdige Apps können über einen von Microsoft bereitgestellten Signierungsdienst von IHV, ISV und Organisationen erstellt werden.

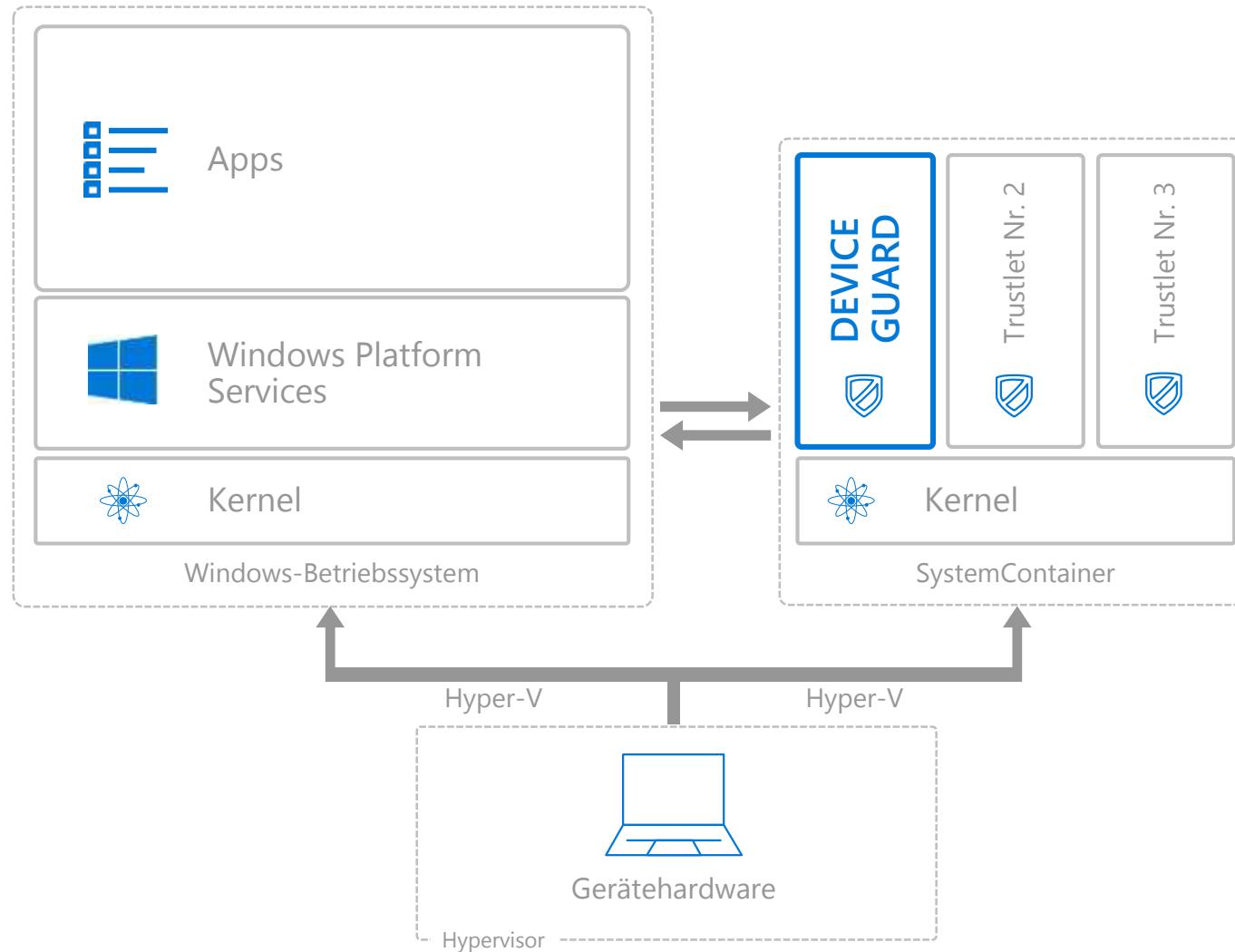
Die Apps müssen vom Microsoft- Signierungsdienst signiert werden. Keine weiteren Modifikationen erforderlich.

Der Signierungsdienst steht für OEMs, IHV, ISVs und Unternehmen bereit.



DEVICE GUARD IN VBS-UMGEBUNGEN

GEZIELTER SCHUTZ



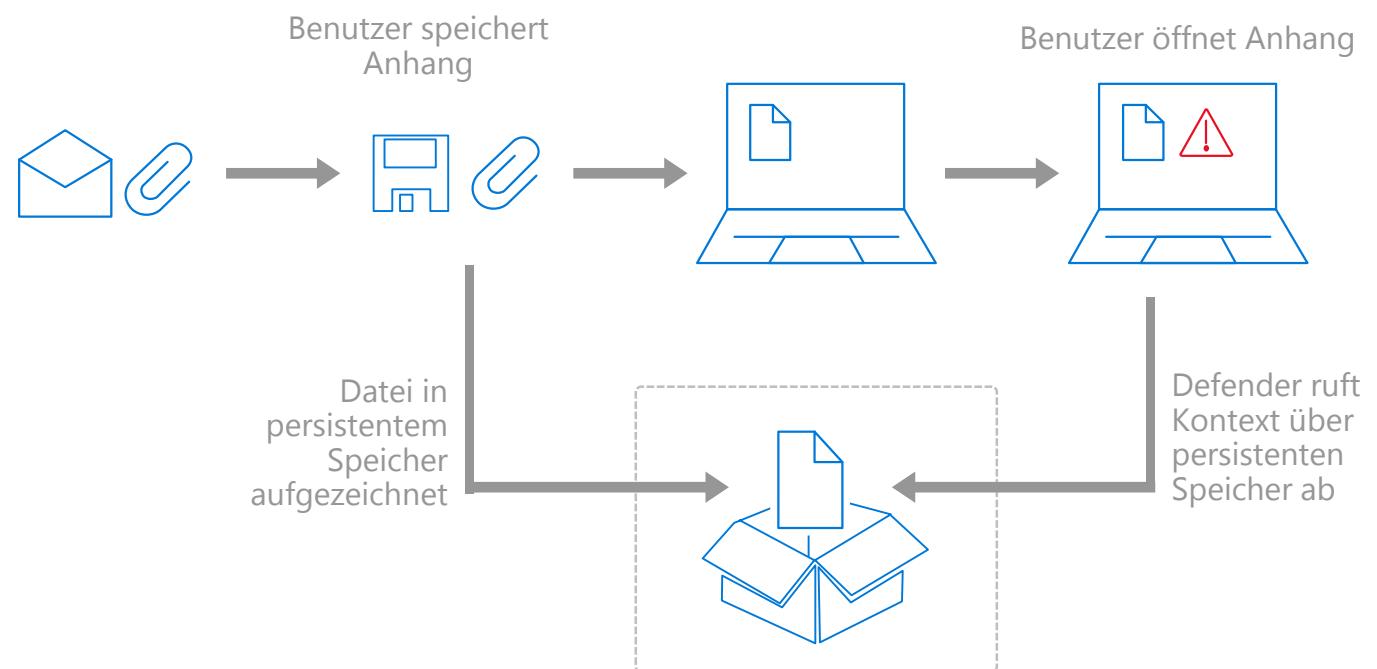
DEMO + ÜBUNG



WINDOWS DEFENDER

Tief greifende Integration mit Windows-Sicherheitssystemen

- Anti-Tampering (Schutz wichtiger abhängiger Betriebssystemdienste)
- Härtung der Registrierung für "dateilose" Malware
- Intelligente Benutzerkontensteuerung
- Persistenter Speicher



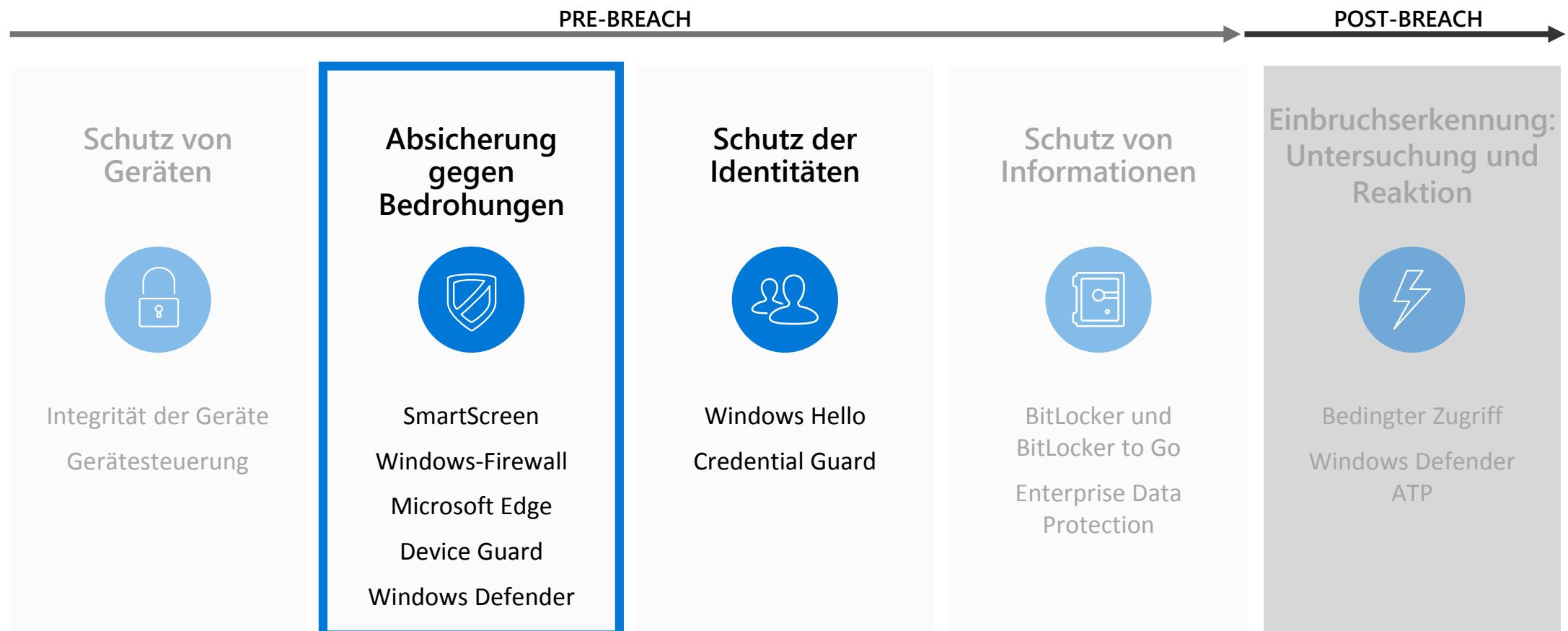
Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

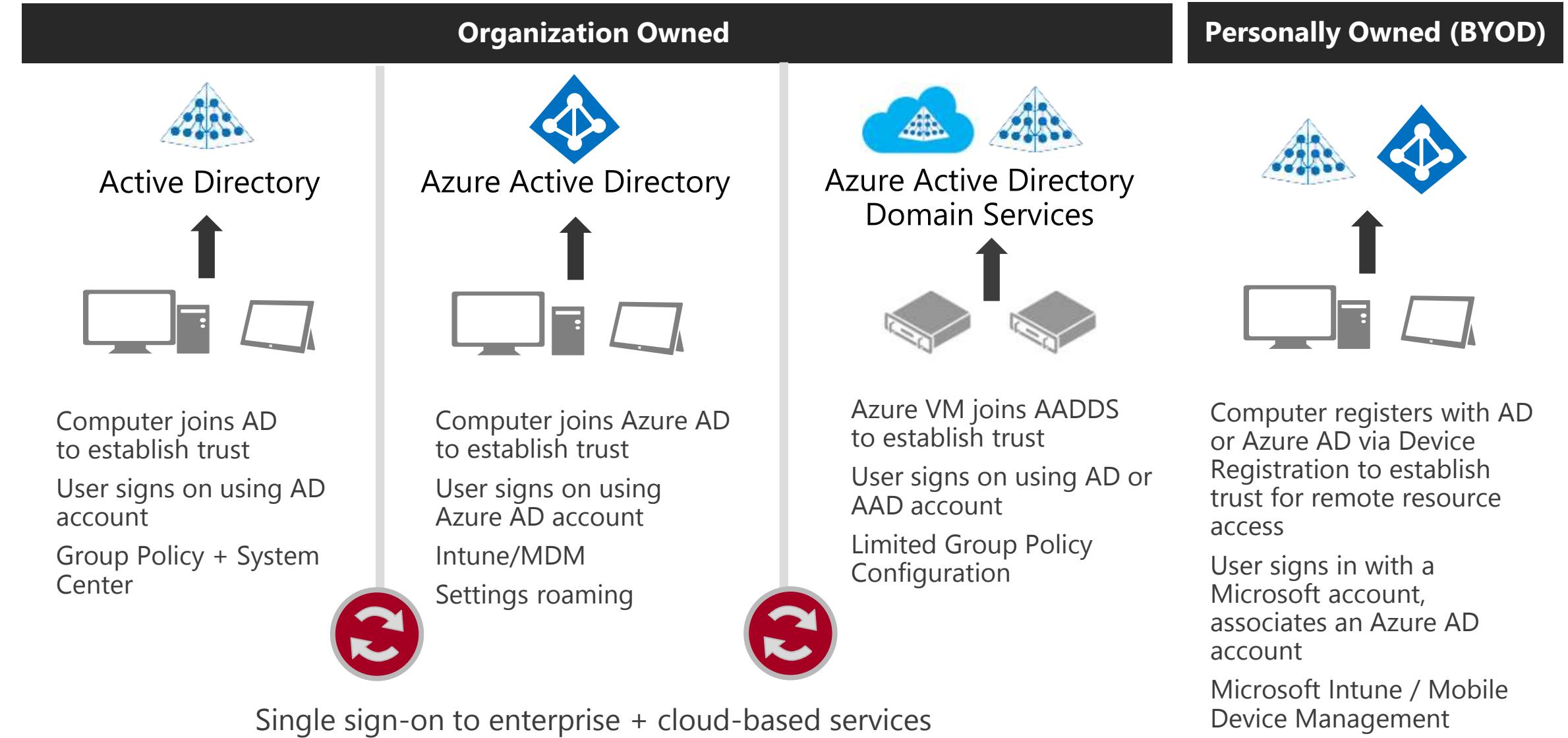
- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung

DER WINDOWS 10-SICHERHEITSSTACK

SCHÜTZEN, ERKENNEN UND REAGIEREN



Identity Choices



WINDOWS 10-**IDENTITÄTEN**

Allgemein verfügbare
zweistufige
Authentifizierung

Vor Diebstahl,
Angriffen und
Phishing geschützte
Anmelde-
informationen

Lösung für End-
verbraucher und
Unternehmens-
benutzer

Nutzung von
Anmeldeinfor-
mationen auf
vertrauten mobilen
Geräten zur
Anmeldung am
Desktop

IDENTITÄTEN FÜR UNTERNEHMEN

Mehr als nur Kennwörter – mit einer zweistufigen Authentifizierung

PINs oder Biometrie gemeinsam mit dem Gerät (PC oder Smartphone)

Vor Hacks, Diebstahl und Phishing geschützte Anmeldeinformationen

Einmalige Anmeldung – lokal, im Internet und standortübergreifend

Einmaliges Anmelden an Geräten über Azure Active Directory



A blue-tinted photograph of a medical professional, likely a doctor, wearing a white coat and a stethoscope around their neck. They are looking down at a tablet device held in their hands. In the background, there are some medical equipment and supplies.

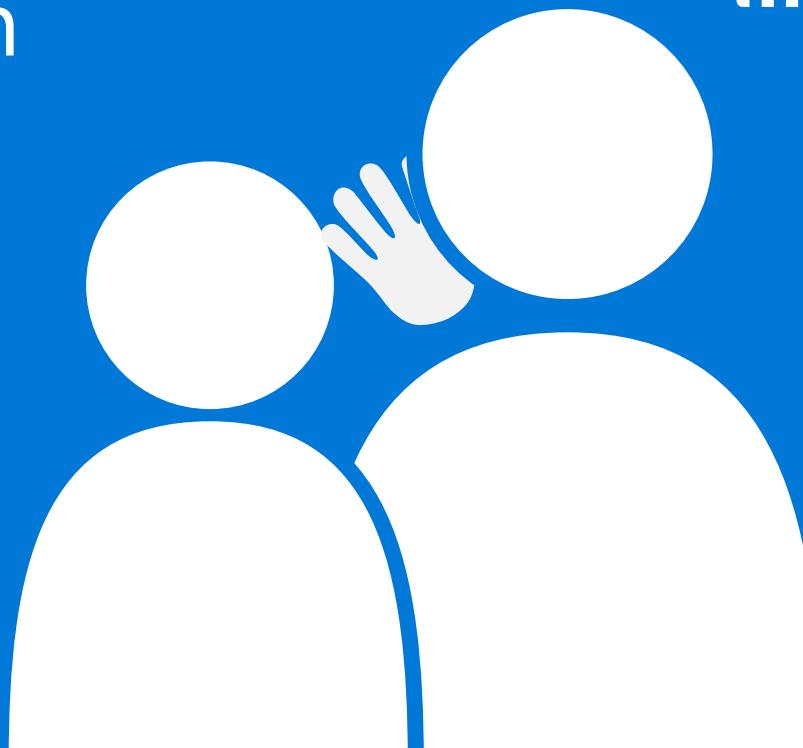
Windows 10

BENUTZERIDENTITÄT UND AUTHENTIFIZIERUNG

GEHEIME INFORMATIONEN

Können leicht verloren gehen
oder missbraucht werden

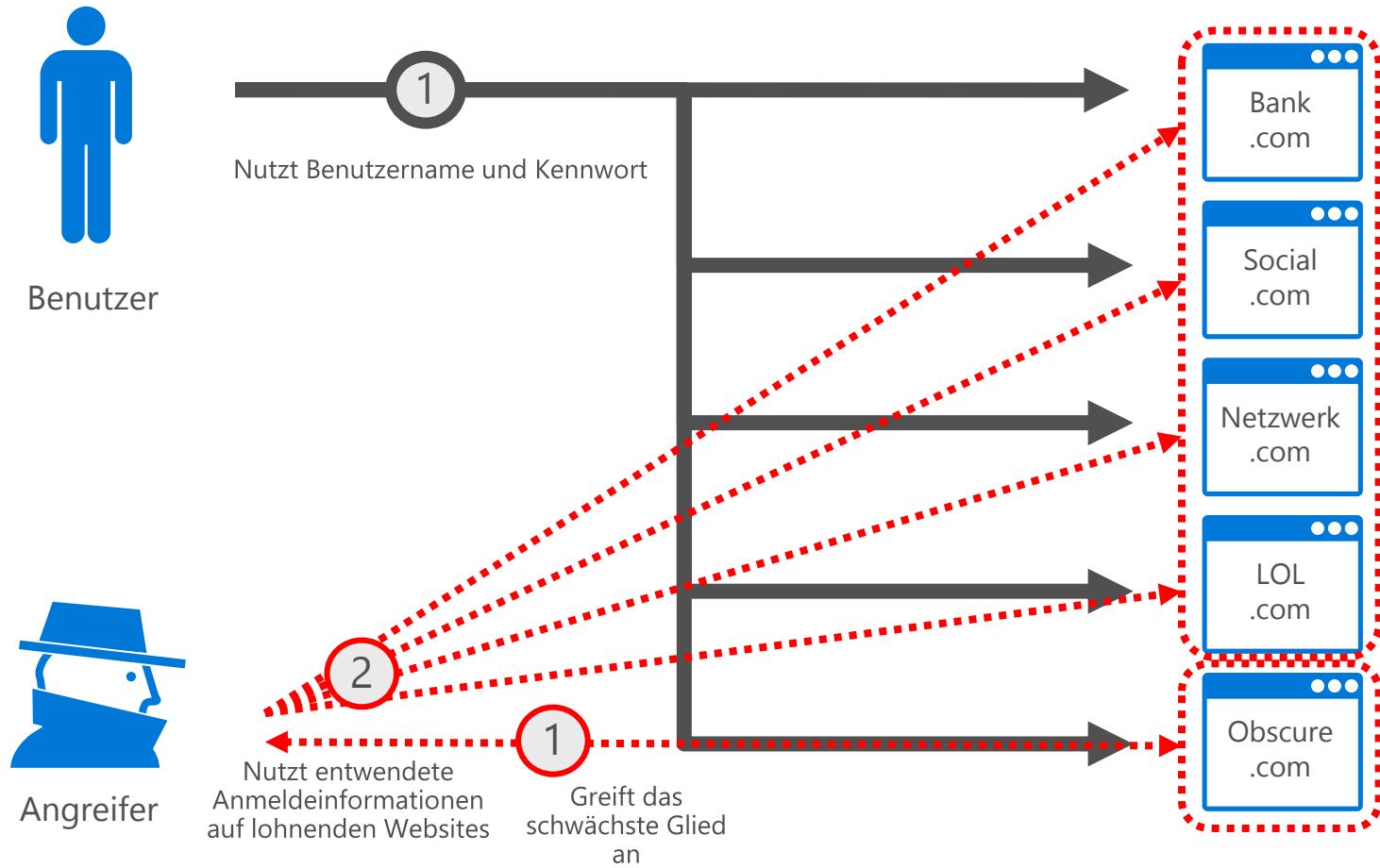
(Das Problem ist der Benutzer)



Pssst!

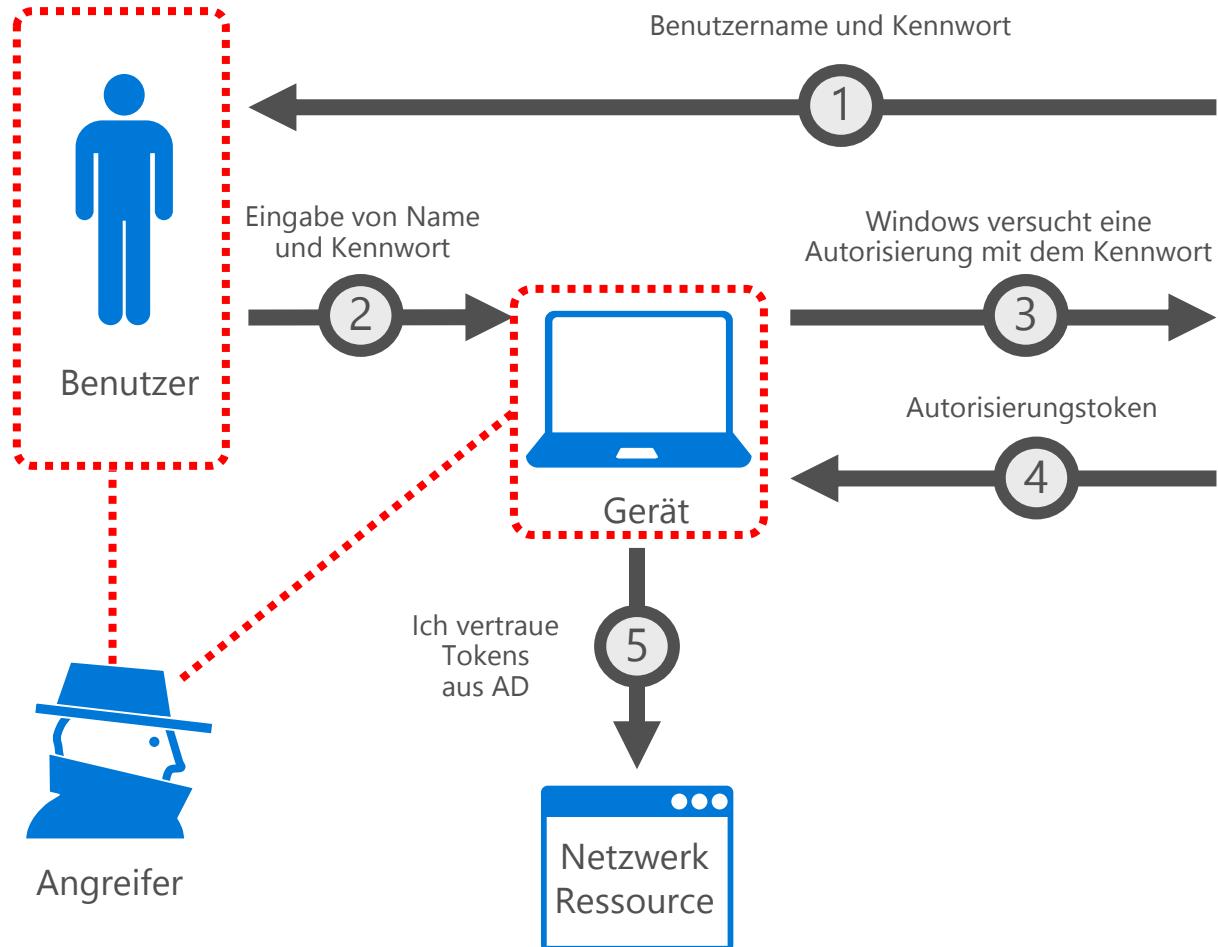
INTERNET – BENUTZERNAME UND KENNWORT

Die von uns
verwendeten
Websites
stellen eine
Schwachstelle
dar



UNTERNEHMEN – BENUTZERNAME UND KENNWORT

Der Benutzer und
das Gerät bilden
die Schwach-
stellen



Identitäts-
anbieter



Identitäts-
anbieter



Identitäts-
anbieter

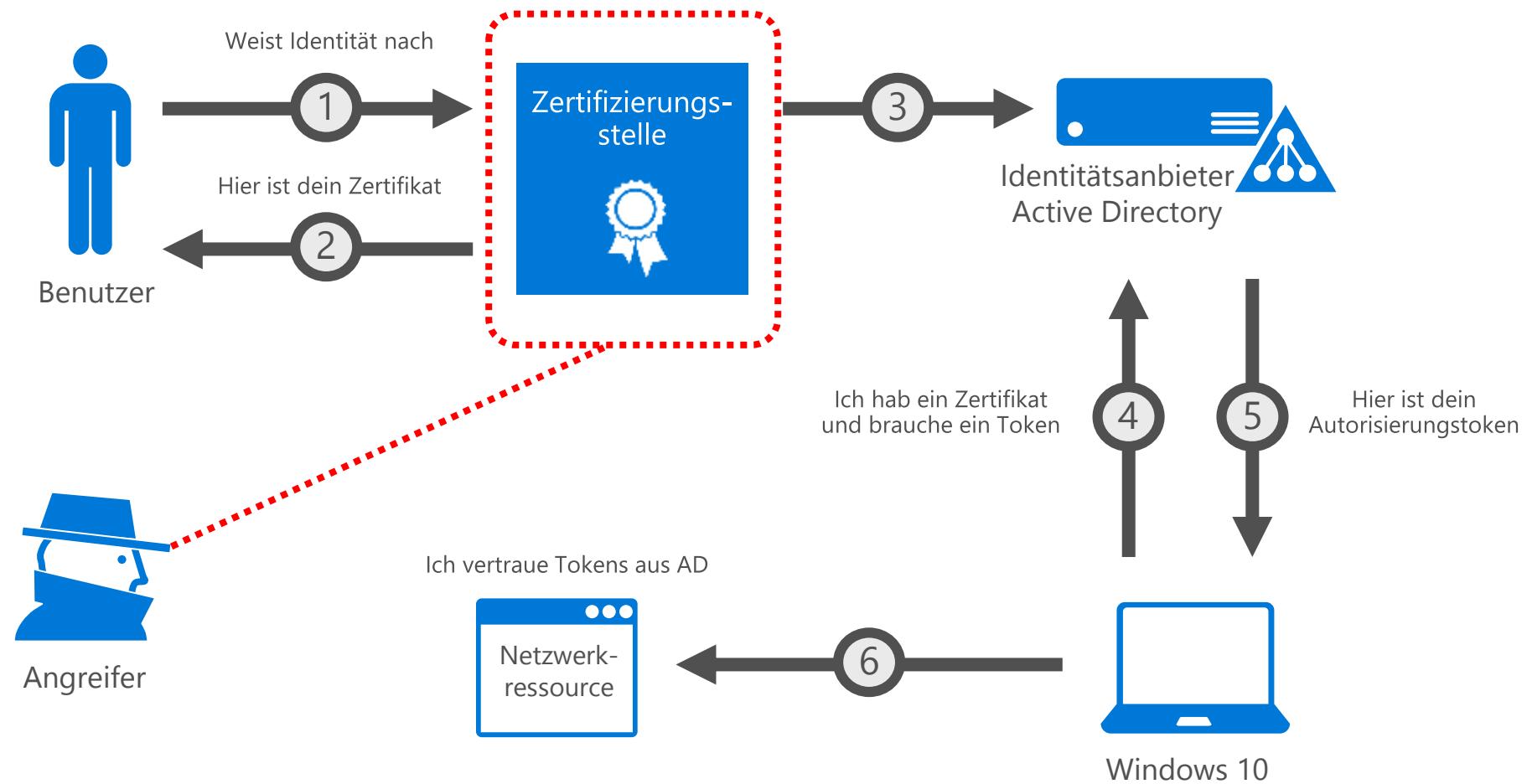
PKI-LÖSUNGEN

Komplex, teuer
und Angriffsziel



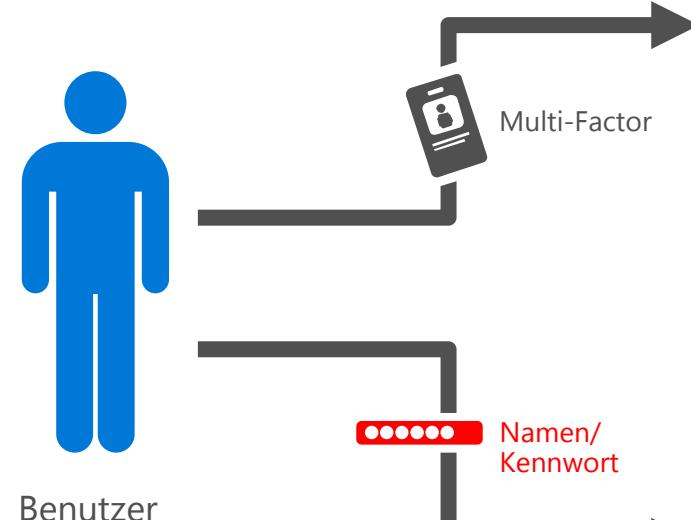
PKI-BASIERTE AUTHENTIFIZIERUNG

Die Zertifizierungsstelle wird angegriffen



TYPISCHE MULTI-FACTOR-AUTHENTIFIZIERUNGSIMPLEMENTIERUNGEN

Der eingeschränkter Einsatz der MFA sorgt für Schwachstellen



Wichtige Ressourcen

VPN	Zertifizierungsstelle

Allgemeine Netzwerkressourcen

Dateiserver	OneDrive

E-Mail	WLAN

ANFORDERUNGEN IN UNTERNEHMEN



Geringere
Kosten



Einfache
Implementierung



MULTI-FACTOR MIT VORHANDENEN GERÄTEN

Vereinfachte
Bereitstellung



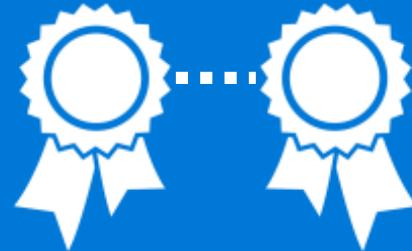
WINDOWS **HELLO**

Gerätebasierte Multi-Factor-Authentifizierung

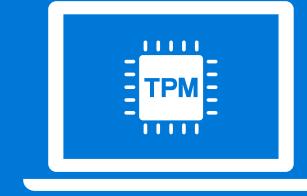


**EINSATZ
VERTRAUTER
GERÄTE**

BENUTZER- ANMELDUNG



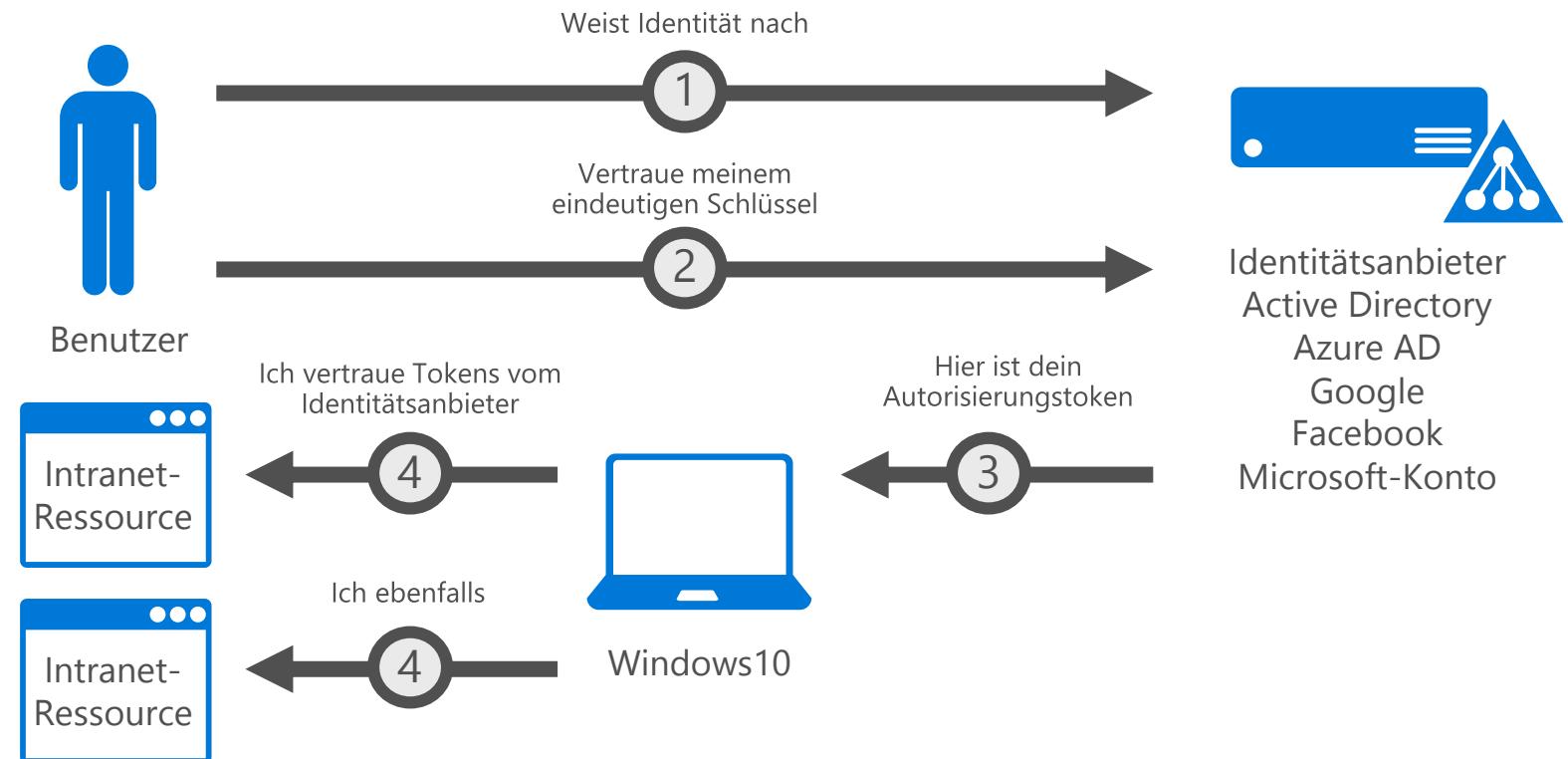
Ein asymmetrisches Schlüsselpaar
Per PKI bereitgestellt oder lokal
über Windows 10 erstellt



**DURCH
HARDWARE
GESICHERT**

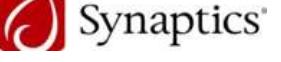
WINDOWS HELLO – SCHLÜSSELBASIERTE AUTHENTIFIZIERUNG

Ein neuer
Ansatz



FIDO ALLIANCE

Einige
Mitglieder des
Gremiums

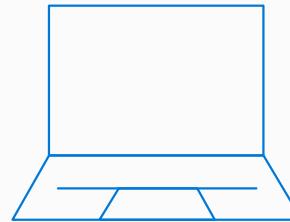
	 Microsoft			
				
	 MasterCard		 Trust the Net.	
		 ING		
				
				

BIOMETRISCHE MÖGLICHKEITEN

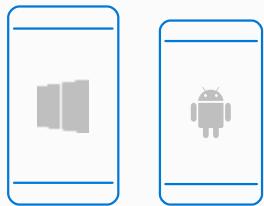
- Mehr Sicherheit
- Einfache Nutzung
- Benutzer muss sich nichts merken
- Fingerabdruck- und Gesichtserkennung
- Unterstützung von VBS
- Credential Guard schützt den gesamten Stack



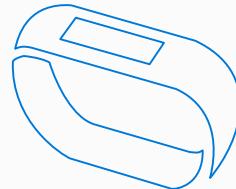
AUTHENTIFIZIERUNG PER BEGLEITGERÄT



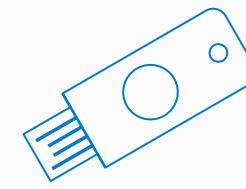
WINDOWS HELLO-BEGLEITGERÄTE



Smartphone



Wearable



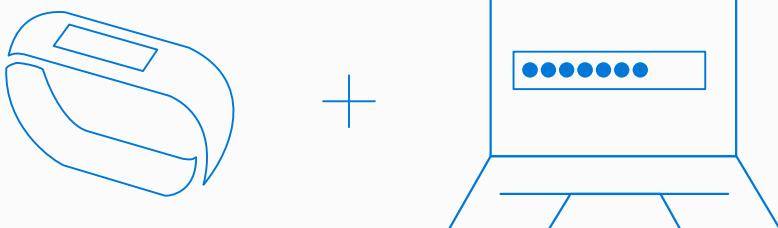
USB



Karte

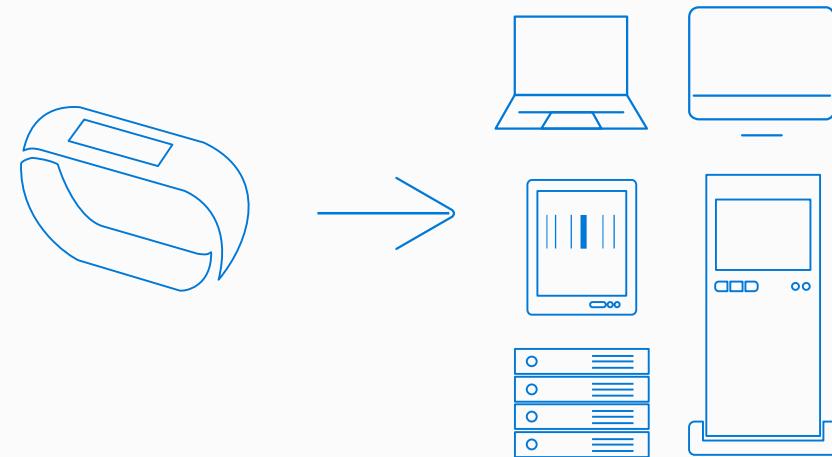
SZENARIEN FÜR BEGLEITGERÄTE

Begleitgerät als zweiter Faktor



Mehr Komfort und Sicherheit.

Anmeldedaten sind mobil
und bleiben auf dem
Begleitgerät



Zusätzliche Sicherheit durch die Speicherung der
Anmeldedaten auf einem anderen Gerät. Unterstützt
die Compliance und bietet Komfort.

A blue-tinted photograph of a doctor in a white coat and stethoscope, looking down at a patient's chart.

Windows 10

**ABGELEITETE
ANMELDEDATEN UND
ZUGRIFFSTOKENS**

A man with light brown hair, wearing a dark long-sleeved shirt, sits at a rustic wooden table. He is looking down at his smartphone, which is held in his right hand. The background consists of weathered wooden planks, suggesting an outdoor or industrial setting.

"PASS THE HASH"- ANGRIFFE

Eine modere
Sicherheitsherausforderung

MODERNE SICHERHEITSHERAUSFORDERUNGEN:

PASS THE HASH-ANGRIFFE

Pass the Hash-Angriffe haben sich von einer theoretischen zu einer ganz konkreten Bedrohung entwickelt

Sie ermöglichen einem Angreifer über gängige Hacking-Tools wie Mimikatz, Benutzeranmeldeinformationen zu entwenden

Danach kann ein Angreifer häufig weitere abgeleitete Anmeldeinformationen entwenden und sich im Netzwerk bewegen

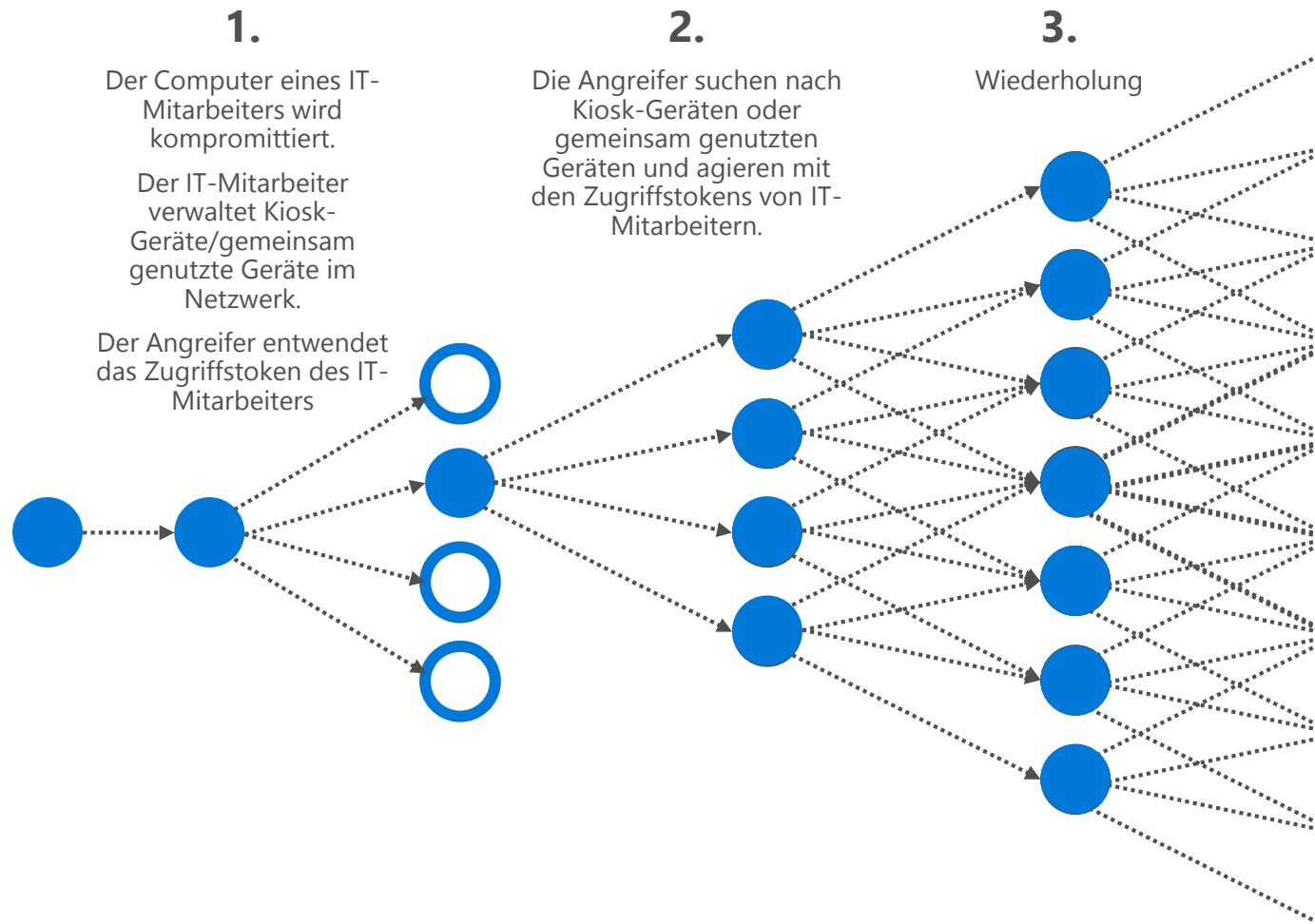
Der Angreifer kann sich häufig auch bei einer Entdeckung im Netzwerk halten, indem er von einer Identität zur nächsten wechselt



MODERNE SICHERHEITSHERAUSFORDERUNGEN:

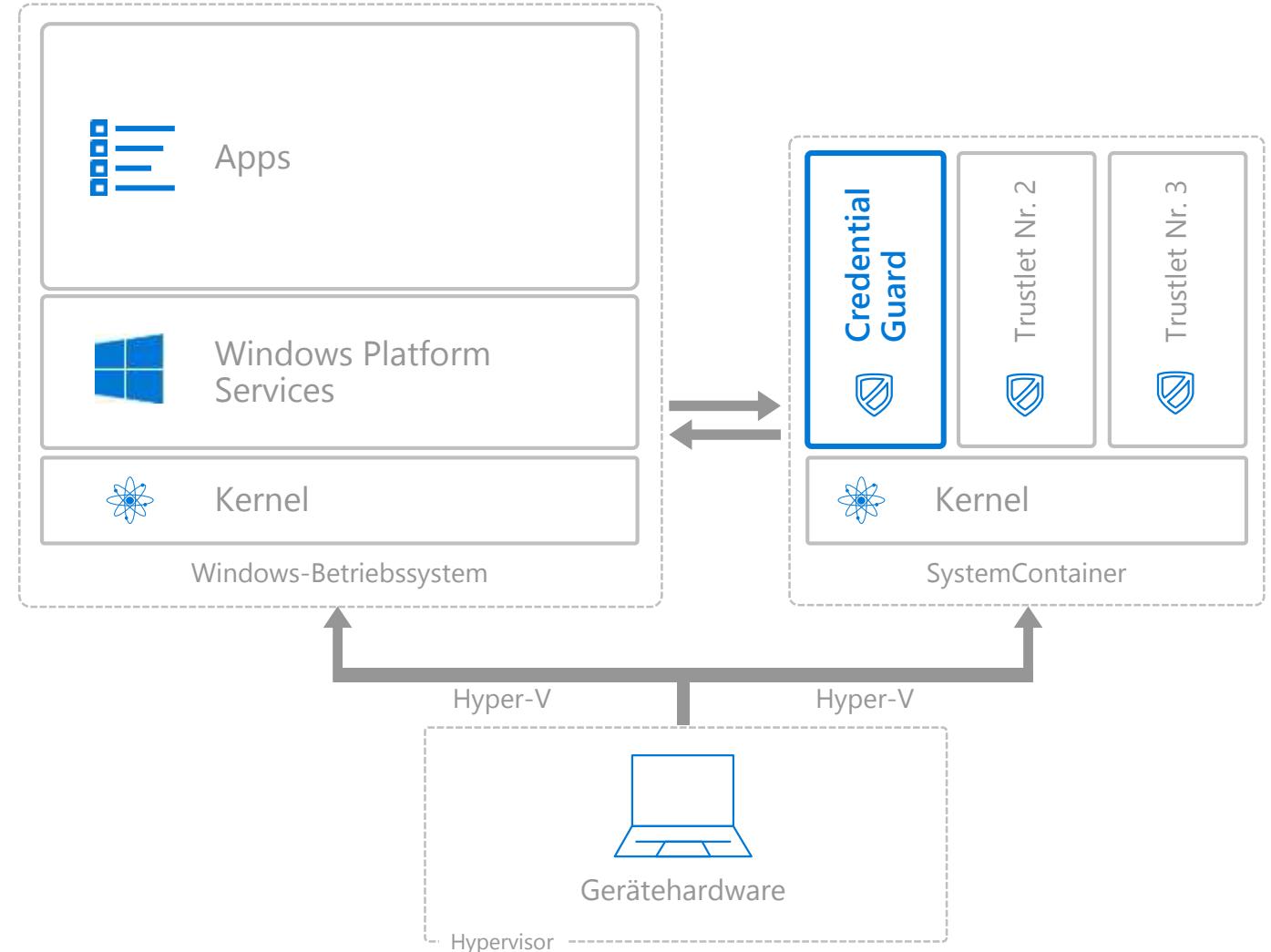
PASS THE HASH-ANGRIFFE

Der Zugriff auf ein Gerät kann den Zugriff auf viele weitere Geräte ermöglichen



DIE MODERNE LÖSUNG: **CREDENTIAL GUARD**

- Pass the Hash-Angriffe (PtH) sind das wichtigste Tool der Hacker Sie werden bei nahezu jedem großen Hack und Angriffstyp eingesetzt
- Credential Guard nutzt VBS, um die Windows-Authentifizierung vom Windows-Betriebssystem zu isolieren
- Der LSA Service (LSASS) und die abgeleiteten Anmeldedaten (Kerberos-Ticket, NTLM-Hash) werden geschützt
- Die Entwendung von abgeleiteten Anmeldeinformationen über Mimikatz wird verhindert



DEMO + ÜBUNG



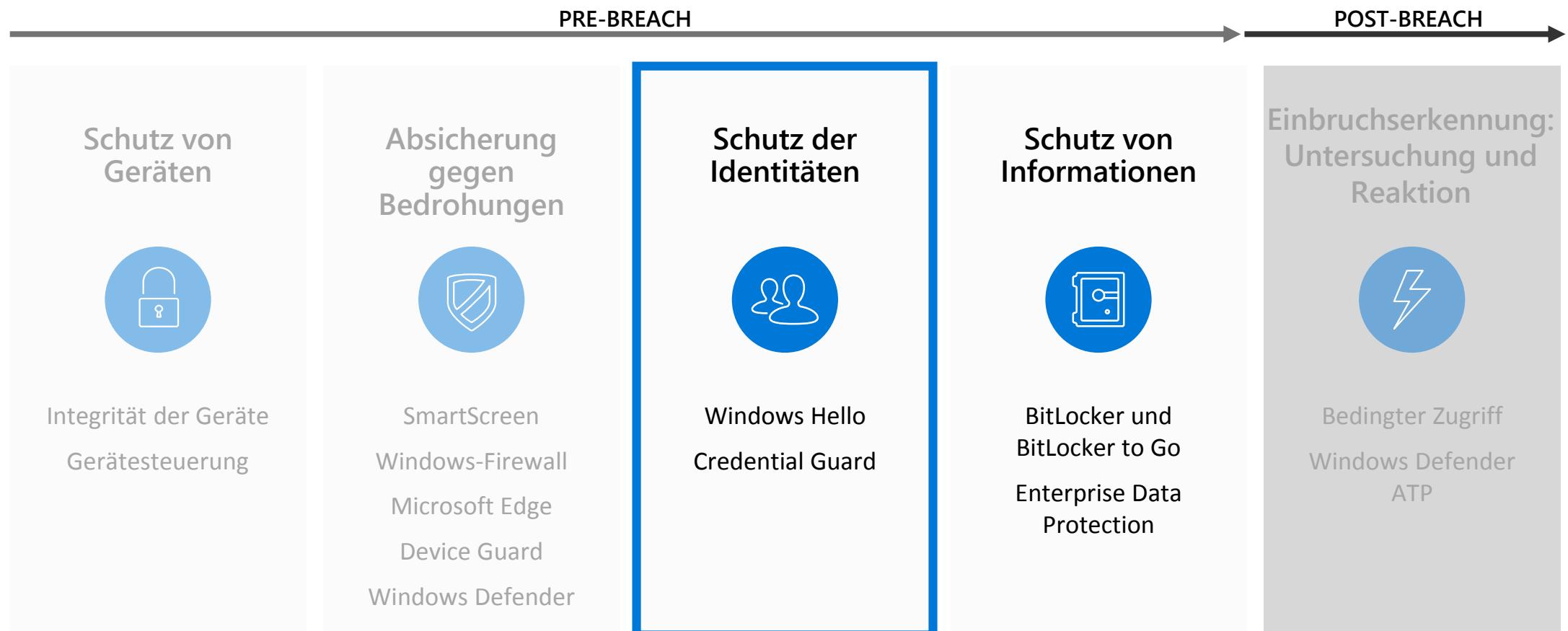
Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

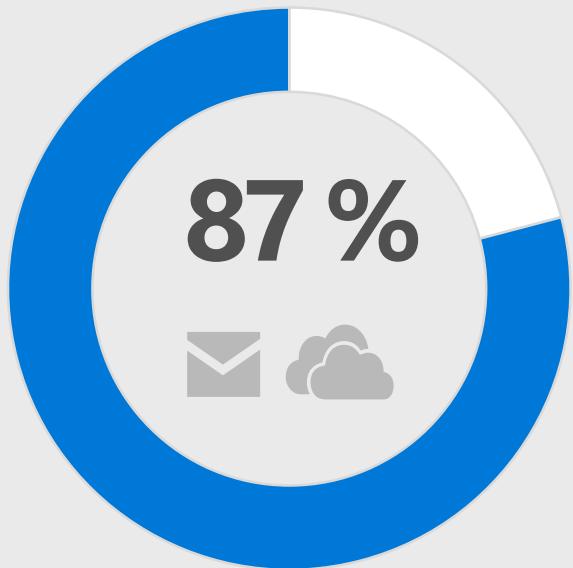
- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung

DER WINDOWS 10-SICHERHEITSSTACK

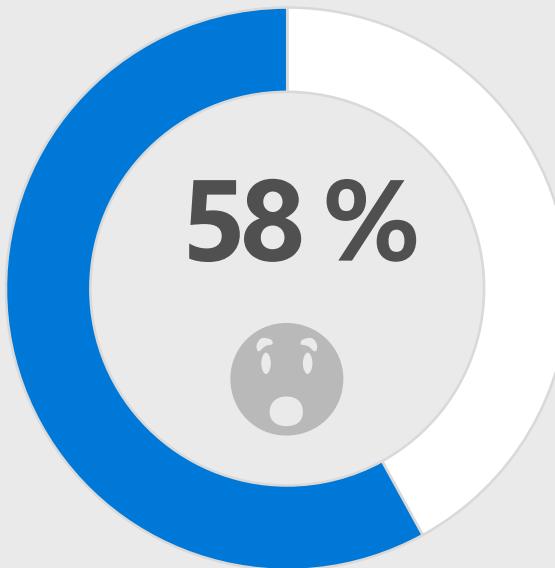
SCHÜTZEN, ERKENNEN UND REAGIEREN



DATENVERLUSTE

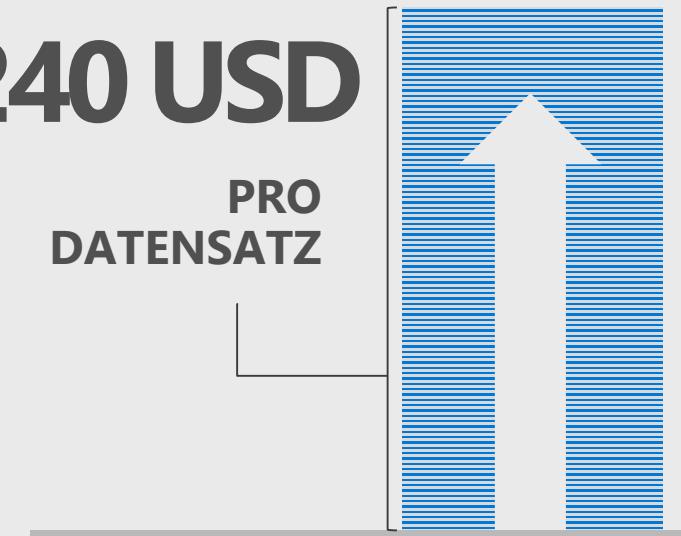


... der Führungskräfte speichern
regelmäßig berufliche Dateien in einem
privaten E-Mail- oder Cloud-Konto.¹



... haben schon einmal versehentlich
sensible Informationen an einen falschen
Empfänger geschickt.¹

240 USD
PRO
DATENSATZ



... Durchschnittskosten pro Datensatz
bei einem Datenverlust.²

¹Stroz Friedberg, "On The Pulse: Information Security In American Business," 2013

²HIPPA Secure Now, "A look at the cost of healthcare data breaches," Art Gross, 30. März 2012

EINE NICHT BERÜCKSICHTIGTE BEDROHUNG

“Eine aktuelle Untersuchung . . . stellte fest,
dass tausende sensibler Dokumente . . .
dafür sorgen, dass Organisationen
Datenschutzrechte verletzen . . .
Mitarbeiter die Datenschutzimplikationen
ihrer Handlungsweise nicht überblicken . . .
Sie sehen Cloud-Dienste als einfache
Möglichkeit zum Austausch von
Dokumenten.”

Zulasten der Sicherheit,
Google-Dorking gibt es
noch immer

Dan Goodin
ARS Technica
17. Mai 2016

ANFORDERUNGEN FÜR DEN **INFORMATIONSSCHUTZ**

SCHUTZ VON GERÄTEN

Schutz des Systems und der Daten im Fall von verlorenen oder gestohlenen Geräten

TRENNUNG VON DATEN

Eindämmung Trennung der Daten

SCHUTZ VOR LEAKS

Verhindern des Zugriffs und von Daten-Leaks durch nicht autorisierte Benutzer und Apps

SCHUTZ BEI WEITERGABE

Schutz der Daten bei der Weitergabe an andere oder außerhalb der Geräte und Kontrolle der Organisation

ANFORDERUNGEN FÜR DEN **INFORMATIONSSCHUTZ**

SCHUTZ VON GERÄTEN

BitLocker

TRENNUNG VON DATEN

Windows Information Protection

SCHUTZ VOR LEAKS

Azure Rights Management
Office 365

SCHUTZ BEI WEITERGABE

Management

A blue-tinted photograph of a person sitting in a car, viewed from the side. They are wearing a patterned shirt and have a smartphone resting on their lap. The background is blurred.

Windows 10

SCHUTZ GESPEICHERTER DATEN

Verlorene oder gestohlene Geräte

SCHUTZ GESPEICHERTER DATEN

Unverschlüsselte Geräte gefährden mehr als nur die Daten

Benutzeranmeldedaten können entwendet und administrative Kennwörter mit Offlinetools zurückgesetzt werden

Entsorgte Desktopcomputer und Server können Risiken aufwerfen



VERSCHLÜSSELUNG VON GERÄTEN

BitLocker

Moderne Geräte sind möglicherweise bereits **standardmäßig** über die BitLocker-Technologie verschlüsselt

TPM wird immer häufiger eingesetzt

TPM ist seit Ende 2015 auf allen neuen Windows-Geräten vorhanden

Einfachere Bereitstellung und eine hohe Sicherheit, Zuverlässigkeit und Leistung

Einzelanmeldung für moderne Geräte und für konfigurierbare Windows 7-Hardware

An Unternehmen ausgerichtete Verwaltung (MBAM) und Compliance (FIPS)



ANFORDERUNGEN FÜR DEN **INFORMATIONSSCHUTZ**

SCHUTZ VON GERÄTEN

Schutz des Systems und der Daten im Fall von verlorenen oder gestohlenen Geräten

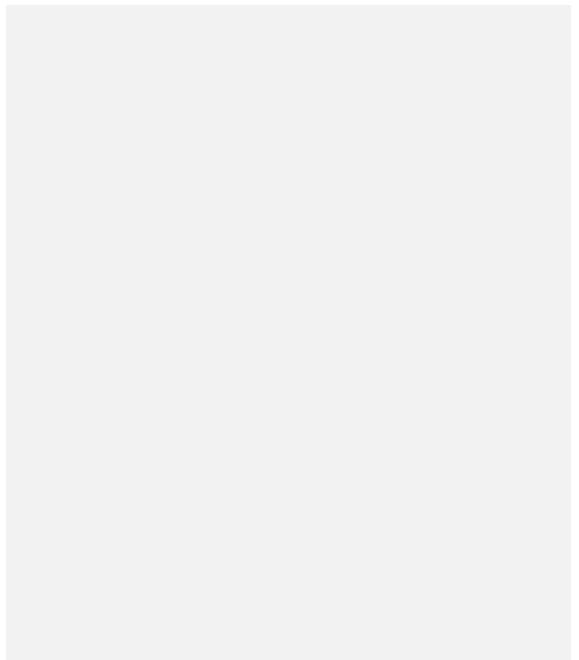
TRENNUNG VON DATEN

Eindämmung Trennung der Daten

SCHUTZ VOR LEAKS

Verhindern des Zugriffs durch nicht autorisierte Apps

SCHUTZ BEI WEITERGABE



LÖSUNGEN

ZUM SCHUTZ VOR DATENVERLUSTEN

Mobile Plattformen

Einsatz von Containern
Schlechtere Benutzererfahrung
Einfache Bereitstellung
Geringe Kosten

ODER

Desktop-Plattform

Beschränkte
Plattformintegration
Bessere Benutzererfahrung
Schwierige Bereitstellung
Höhere Kosten

WINDOWS INFORMATION PROTECTION

Integrierter Schutz vor ungewollten Daten-Leaks



Schützt lokal und auf mobilen Datenträgern gespeicherte Daten.



Eine Umgebung auf allen Windows 10-Geräten mit Schutz gegen Copy&Paste.



Bereitstellung mit Windows 10 Anniversary Update



Persönliche Daten und Unternehmensdaten werden identifiziert und können gelöscht werden.

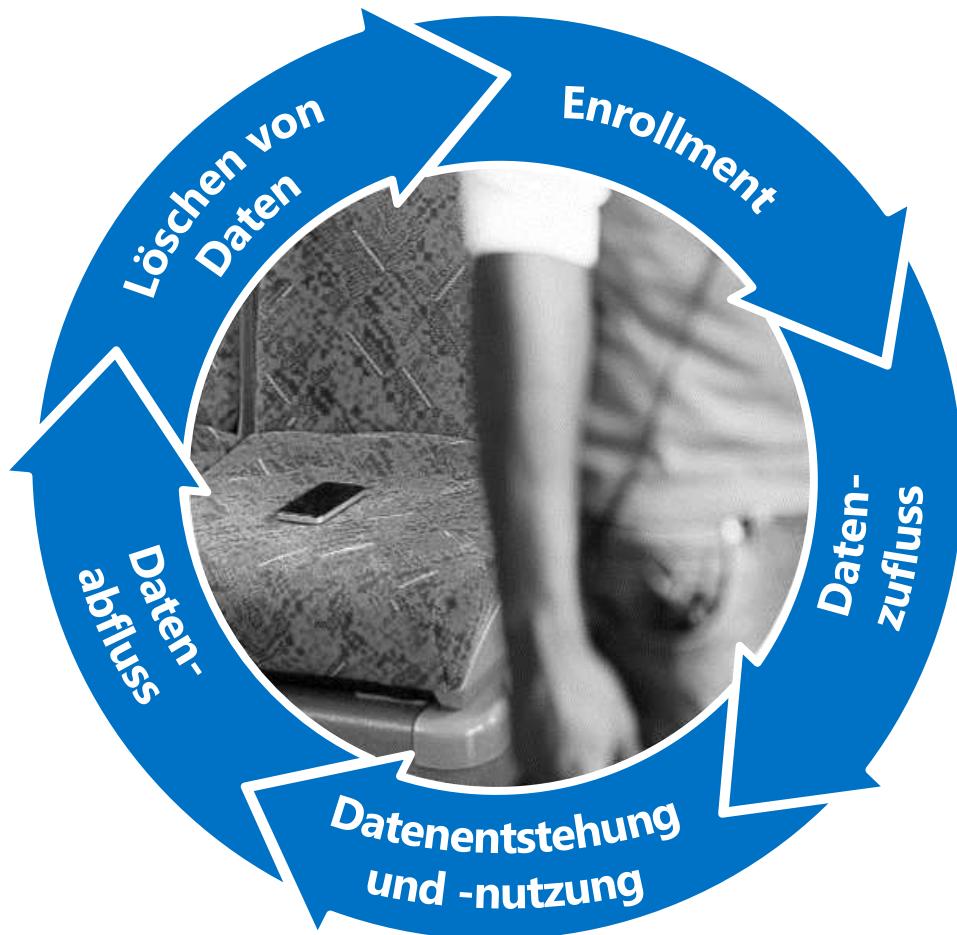


Nahtlose Integration in die Plattform. Kein Wechseln oder Starten von Apps erforderlich.

Verhindert den Zugriff auf Unternehmensdaten durch nicht autorisierte Apps und Leaks durch Benutzer über Copy&Paste.



WINDOWS INFORMATION PROTECTION LEBENSZYKLUS



Richtlinien und Schlüssel werden auf Gerät bereitgestellt

Aus dem Unternehmensnetzwerk kommende Daten werden automatisch von WIP geschützt

Eine App kann Daten automatisch schützen, oder Benutzer können Daten als privat oder geschäftlich definieren

Der Schutz kann überall auf dem Gerät und beim Verschieben von Daten auf mobile Datenträger aufrechterhalten werden. Azure Information Services kann in B2B-Szenarien zum Schutz eingesetzt werden

Unternehmensdaten können bei Bedarf oder bei Außerbetriebsstellung des Gerätes selektiv gelöscht werden

ANFORDERUNGEN FÜR DEN **INFORMATIONSSCHUTZ**

SCHUTZ VON GERÄTEN

TRENNUNG VON DATEN

SCHUTZ VOR LEAKS

SCHUTZ BEI WEITERGABE

Eindämmung
**TRENNUNG BYOD-
DATEN**

Verhindern des
Zugriffs durch nicht
autorisierte Apps

Schutz der Daten
bei der Weitergabe
an andere oder
außerhalb der
Geräte und
Kontrolle der
Organisation

SCHUTZ BEI WEITERGABE

Rechteverwaltungsdienste

Schutz aller Dateitypen an jedem Ort – unterwegs, Cloud, E-Mail, BYOD etc.

Unterstützung gängiger Geräte und Systeme – Windows, OSX, iOS, Android

Unterstützung von B2B und B2B per Azure Active Directory

Unterstützung von lokalen Szenarien und Cloud-basierten Szenarien (z. B. Office 365)

Nahtlose und einfachere Bereitstellung und Unterstützung von FIPS 140-2-Richtlinien und Compliance-Vorgaben



Persistenter und nicht entferbarer Schutz für die Daten



Erhebliche Verbesserungen gegenüber Windows 7

DEMO + ÜBUNG



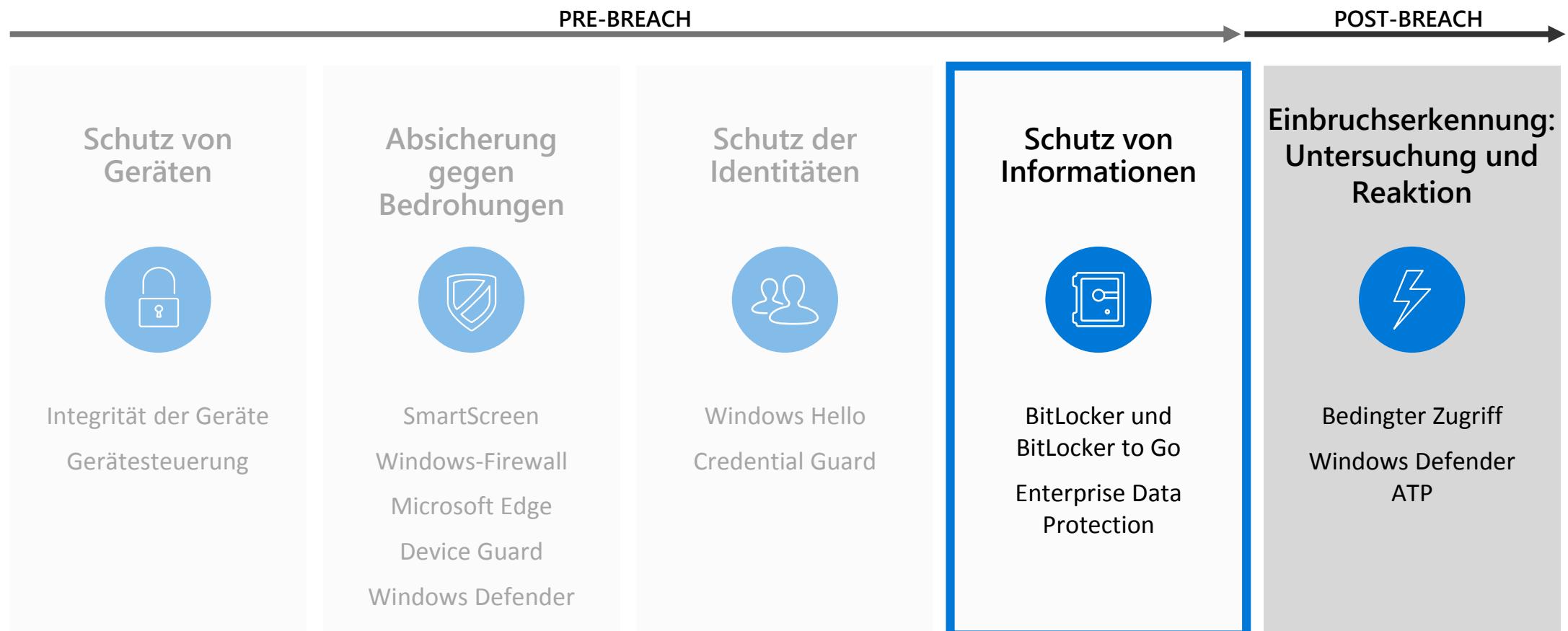
Microsoft IT Camps – Windows 10 Cyber Defense & Security

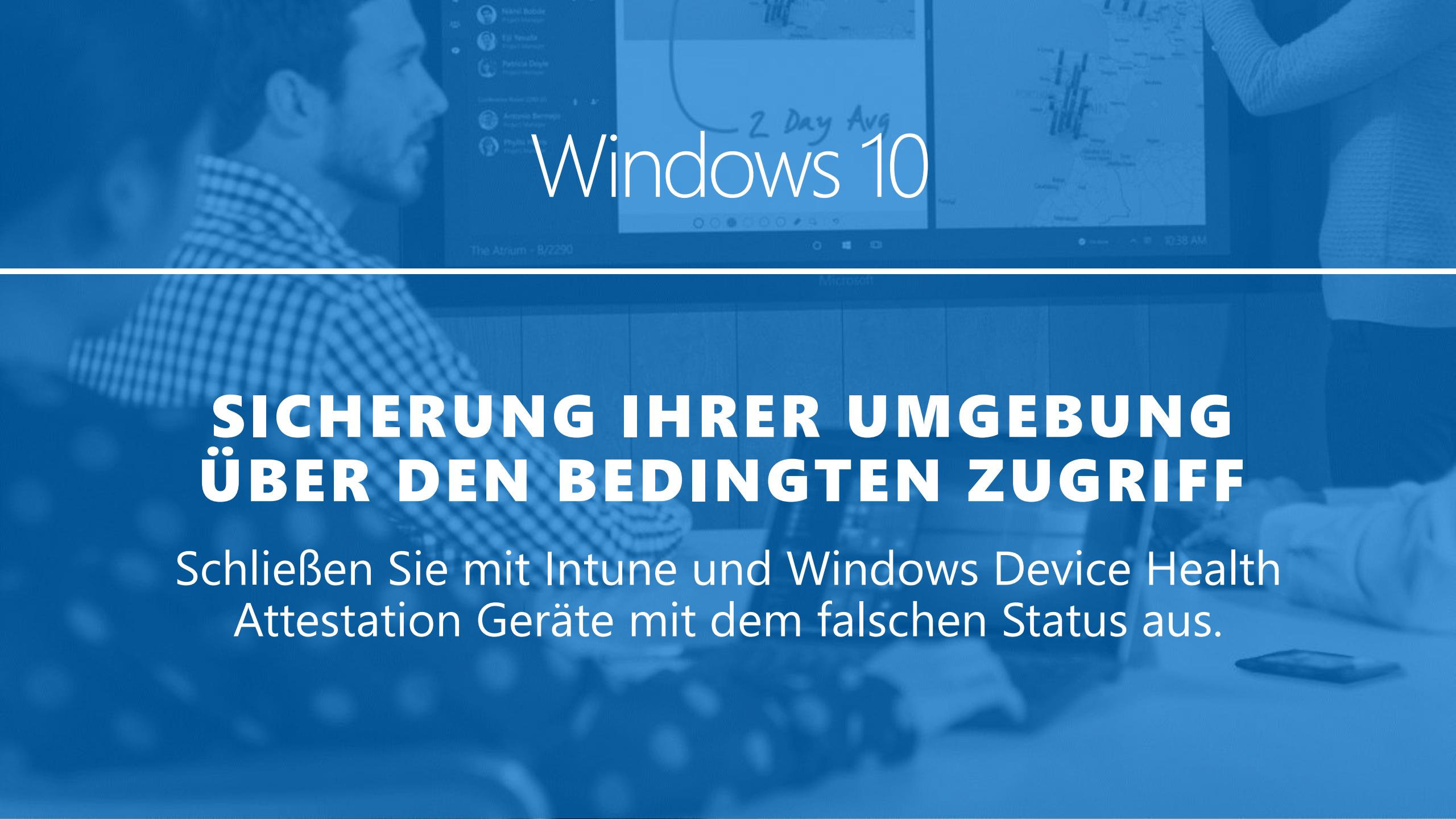
AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Schutz von Geräten
- Schutz von Identitäten
- Schutz von Informationen
- Einbruchserkennung

DER WINDOWS 10-SICHERHEITSSTACK

SCHÜTZEN, ERKENNEN UND REAGIEREN





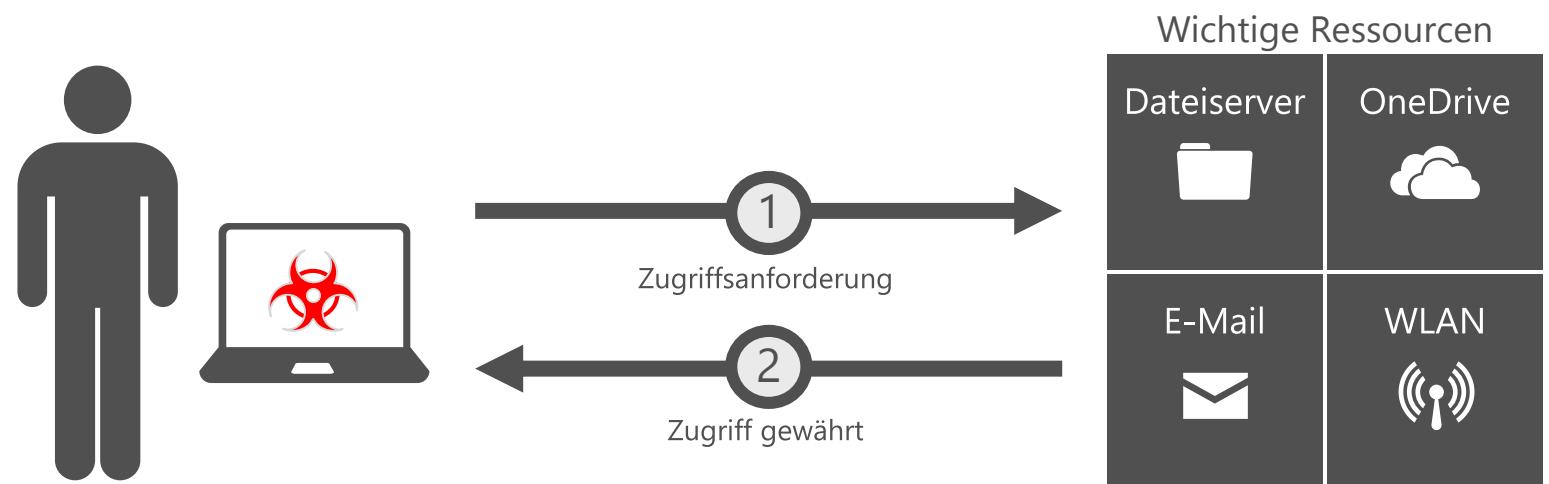
Windows 10

SICHERUNG IHRER UMGEBUNG ÜBER DEN BEDINGTEN ZUGRIFF

Schließen Sie mit Intune und Windows Device Health Attestation Geräte mit dem falschen Status aus.

UNBEKANNTER PC-STATUS

Zurzeit wird ein korrekter Status angenommen



BEDINGTER **ZUGRIFF**

Blockierung von kompromittierten Geräten zum Schutz der Ressourcen
und zur Verhinderung von Proliferation-Angriffen

Der WDHA-Dienst
(Windows Device Health
Attestation) sorgt für die
Validierung der
Geräteintegritätsdaten.

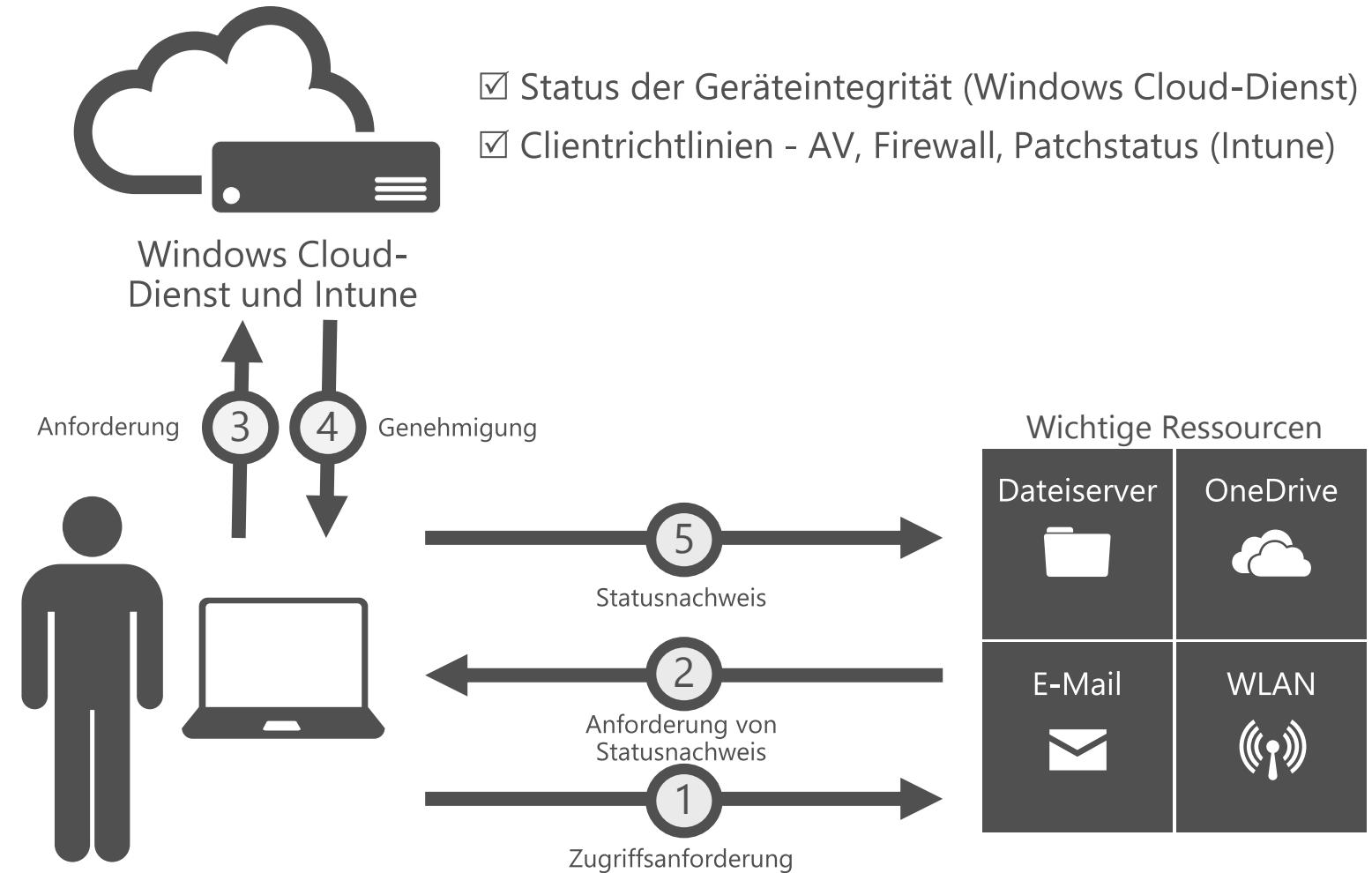
Management-Systeme (z.
B. Intune) können
WDHA-bestätigte
Integritätsdaten zur
Umsetzung des
bedingten Zugriffs auf
Ressourcen nutzen.

Dir durch WDHA
bestätigten Integritäts-
daten können mit zu-
sätzlichen Statusdaten (z.
B. Patchstatus) gekoppelt
werden und so einen
noch umfassenderen
Blick auf den Geräte-
status ermöglichen.

Die Integritätsdaten des
WDHA-Dienstes stehen
für Drittanbieterlösun-
gen zum Netzwerkzu-
griff, für die Sicherheit
und die Verwaltung zur
Verfügung.

WINDOWS DEVICE HEALTH ATTESTATION

MDMS für den
Zugriff auf Basis
von Gerätestatus
und -integrität



ANGRIFFE PASSIEREN SCHNELL UND SIND **SCHWER AUFZUHALTEN**

Wenn ein Angreifer eine E-Mail an **100 Mitarbeiter** Ihres Unternehmens sendet,

...



... wird diese von **23 Mitarbeiter** geöffnet, ...



... **11 Mitarbeiter** von den 23 öffnen den Anhang ...



... und **sechs Mitarbeiter** machen dies innerhalb der **ersten Stunde**.



WINDOWS DEFENDER ADVANCED THREAT PROTECTION

ERKENNEN VON ERWEITERTEN ANGRIFFEN UND
BESEITIGEN VON EINBRÜCHEN



In Windows integriert

Keine zusätzliche Bereitstellung und Infrastruktur. Immer auf dem neuesten Stand bei geringen Kosten.



Verhaltensbasierte und Cloud-gestützte Einbruchserkennung

Aussagekräftige und korrelierte Alarne für bekannte und unbekannte Bedrohungen. Echtzeitdaten und Verlaufsdaten.



Umfangreicher Untersuchungszeitraum

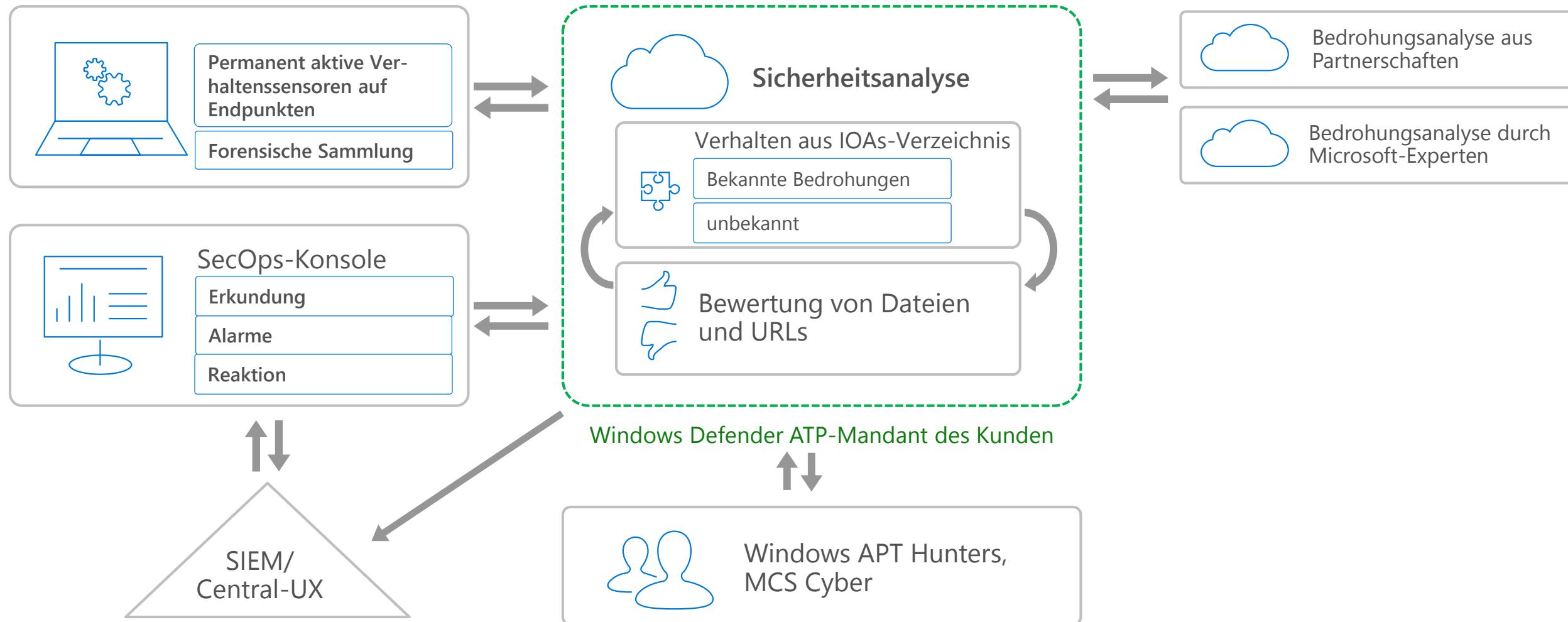
Umfang des Einbruchs leicht zu überblicken. Verschieben von Daten auf Endpunkten. Tief greifende Datei- und URL-Analyse.



Einzigartige Informationsdatenbank mit Bedrohungsinformationen

Einzigartige Ressourcen ermöglichen detaillierte Profile der Akteure. Bedrohungsdaten von Microsoft und Drittanbietern.







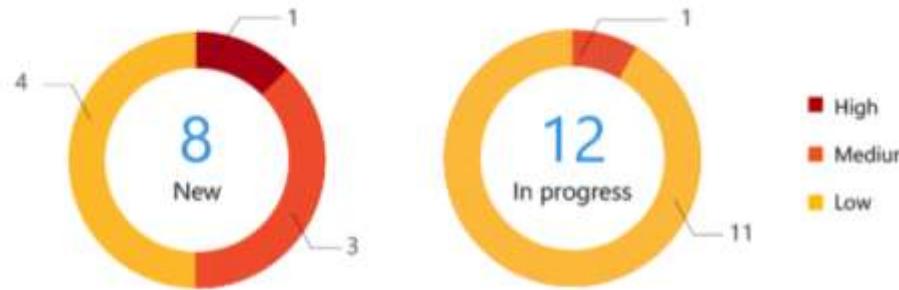
Machine

Search (File, IP, URL, Machine)



ATP alerts

All time



Latest ATP alerts

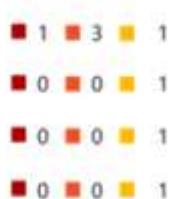
Go to all alerts

Feb 18 18:07:01	NeroBlaze attack detected	High
Feb 18 11:54:02	Outlook dropped and executed a PE file	Medium
Feb 18 14:34:00	A suspicious Powershell commandline was executed	Medium
Feb 18 13:01:09	A reverse shell was detected	Medium

Top machines with ATP alerts

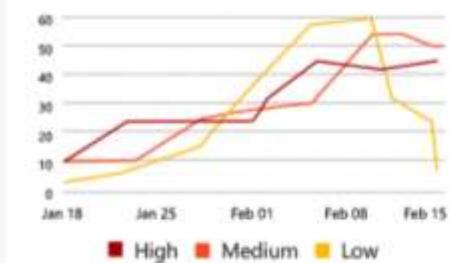
Go to machine view

- ⑤ CONT-LIZBEAN
- ① CONT-LILYJARVIS
- ① CONT-RODGERANDR
- ① CONT-ERICGAYLOR



ATP alert trends

30 days



ATP alerts mapping

30 days



High severity malware

All time

Ransomware	5	1	12
Backdoor	7	0	16
Exploit	35	3	52
Trojan	17	0	25

Machines reporting

30 days



Status

Service status	
Total machines reporting	3,547
Open message center	



Machine ▾

Search (File, IP, URL, Machine)



Queue > NeroBlaze attack detected

NeroBlaze attack detected

NeroBlaze

NeroBlaze attack detected

02.25.2016 08:08:32

Today

Command And Control

cont-lizbean-x5



More info about this alert

A set of behaviors likely associated with the NeroBlaze adversary was detected on this machine.

Recommended Actions

New

1. Contact your Incident Response team, NOTE: If you don't have an Incident Response team, contact the Microsoft Consulting Services (MCS) for architectural remediation and forensic investigation. A forensic investigation is important to assess the damage that might have been done.
2. Disconnect this machine and block the Command and Control (C2) URLs if you suspect significant data loss.
3. Identify the potentially-compromised accounts and begin monitoring for anomalous usage. Reset passwords and/or decommission confirmed affected user accounts.
4. Ensure your software has the latest patch, update your malware signatures, and close the vectors of attack.
5. Collect and provide the investigation team with indicators of compromise (IOC) for further analysis.

Alert timeline

	Description	First Observed	Details	
02.25.2016				
08:08:32	powershell.exe	02.25.2016	3a9c990d346176b91f44b235a9c50b2d9bca046f	
08:08:32	104.209.186.8	02.25.2016		



Machine ▾

Search (File, IP, URL, Machine)



Queue > NeroBlaze attack detected

NeroBlaze attack detected

NeroBlaze

NeroBlaze attack detected

02.25.2016 08:08:32

Today

Command And Control

cont-lizbean-x5

⋮

NEROBLAZE

Introduction

Active since 2007, NeroBlaze is an activity group that has been used primarily to target government bodies, diplomatic institutions and political advisors. Frequent use of zero-day vulnerabilities, spear-phishing and a number of other distribution methods, makes NeroBlaze a highly resilient threat.

Interests

We have seen NeroBlaze target government agencies, diplomatic institutions, and military organizations/installations in NATO member states, and certain Eastern European countries. We have also observed it target organizations associated with political activism in central Asia.

Tools, tactics, and processes

NeroBlaze seeks out victim information through open-source intelligence and social media interaction. It uses simple spear phishing attacks to obtain victims' email account credentials, compiling information for further attacks. It uses email accounts from generic email providers in order to imitate the email provider to disguise the spear phishing emails as a notification from the generic email provider, such as 'a privacy alert.' NeroBlaze persistently sends spear phishing attacks over many months to the same victims.

NeroBlaze attacks higher-value targets with emails that contain lures designed to take control of the victims' machines. NeroBlaze uses a breadth of tactics using lure emails that include:

- URLs to websites containing zero-day exploits
- URLs to websites that use social engineering techniques that cause the victim to download malware
- Document attachments that contain zero-day exploits

NeroBlaze usually packages these emails into a lure that might be interesting to the victim. NeroBlaze tries to provide credibility to these emails by associating the sender with a real organization.

Exfiltration of information from the victim's network can happen through dedicated command and control (C2) infrastructure. NeroBlaze attempts to disguise this traffic through domain names that are associated with common tasks on the network, such as updates and malware checks. On rare instances, we have observed that NeroBlaze uses legitimate servers, such as local SMTP mail servers, to extract information. Overall, NeroBlaze tries to blend into the network traffic to avoid suspicion.

Areas affected



Recommended defenses

- Use the latest, up-to-date operating system and software versions with latest security mitigations
- Conduct enterprise software security awareness training, and build awareness about malware infection

Machine

Search (File, IP, URL, Machine)



Queue > NeroBlaze attack detected > cont-lizbean-x5

Machine

cont-lizbean-x5

Domain: contoso.org

OS: windows10

Machine IP Addresses

Last external IP: 40.122.164.91
Last internal IP: 10.0.0.13

Machine Reporting

First seen: 15 hours ago
Last seen: 10 minutes ago

Alerts related to this machine



02.25.2016	A port scanning tool was detected	Suspicious Activity	New
02.25.2016	NeroBlaze attack detected	Command And Control	New
02.25.2016	Anomaly detected in ASEP registry Software\Microsoft\Windows\CurrentVersion\Run	Persistence	New
02.25.2016	A potential reverse shell has been detected	Command And Control	New
02.25.2016	A suspicious Powershell commandline was executed on the machine	Lateral Movement	New
02.25.2016	Outlook dropped and executed a PE file.	Suspicious Activity	New

Machine in organization

Filter by: All - Verbose -





02.25.2016



	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Today
08:06:33	MpCmdRun.exe communicated with 23.96.212.225				↳ MpCmdRun.exe > MpCmdRun.exe > 23.96.212.225		
08:06:31		↳ A suspicious Powershell commandline was executed on the machine					
08:06:29	install.exe ran cmd.exe				↳ OUTLOOK.EXE > install.exe > process		🔗 liz.bean
08:06:29	cmd.exe ran PowerShell.exe as 'hidden'				↳ install.exe > cmd.exe > process		🔗 liz.bean
08:06:28		↳ Outlook dropped and executed a PE file.					
08:06:28	OUTLOOK.EXE created a PE file under Users folder				↳ explorer.exe > OUTLOOK.EXE > file		🔗 liz.bean
08:06:28	OUTLOOK.EXE created install.exe				↳ explorer.exe > OUTLOOK.EXE > install.exe		
08:06:18	OUTLOOK.EXE created 2 processes				↳ explorer.exe > OUTLOOK.EXE > 2 processes		🔗 liz.bean
08:06:18	OUTLOOK.EXE ran an Office application				↳ explorer.exe > OUTLOOK.EXE > process		🔗 liz.bean
08:05:56	Dropbox.exe ran cmd.exe				↳ runonce.exe > Dropbox.exe > process		🔗 liz.bean
08:05:55	Dropbox.exe communicated with 3 IPs				↳ runonce.exe > Dropbox.exe > 3 IPs		
08:05:41	OUTLOOK.EXE communicated with 2 IPs				↳ explorer.exe > OUTLOOK.EXE > 2 IPs		
08:05:40	OneDrive.exe communicated with 2 IPs				↳ explorer.exe > OneDrive.exe > 2 IPs		
08:05:38	explorer.exe created an ASEP				↳ userinit.exe > explorer.exe > process		🔗 liz.bean
08:05:37	explorer.exe created 2 processes				↳ userinit.exe > explorer.exe > 2 processes		🔗 liz.bean
08:05:37	explorer.exe ran WScript.exe				↳ userinit.exe > explorer.exe > process		
08:05:36	explorer.exe ran 2 Office applications				↳ userinit.exe > explorer.exe > 2 processes		🔗 liz.bean
08:05:27	SearchUI.exe communicated with 204.79.197.200				↳ svchost.exe > SearchUI.exe > 204.79.197.200		
08:05:24	explorer.exe communicated with 5 IPs				↳ userinit.exe > explorer.exe > 5 IPs		
08:05:22	winlogon.exe ran userinit.exe				↳ smss.exe > winlogon.exe > process		🔗 SYSTEM

02.25.2016

	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016	Today
08:06:33	MpCmdRun.exe communicated with 23.96.212.225				MpCmdRun.exe > MpCmdRun.exe > 23.96.212.225		
08:06:31	A suspicious Powershell commandline was executed on the machine						
08:06:29	install.exe ran cmd.exe				OUTLOOK.EXE > install.exe > process		liz.bean
08:06:29	cmd.exe ran PowerShell.exe as 'hidden'				install.exe > cmd.exe > process		liz.bean
	<pre>graph TD; A["\\Device\\HarddiskVolume1\\Program Files (x86)\\Microsoft Office\\Office15\\OUTLOOK.EXE"] --> B["install.exe
4d9afe998034519122b4a0eb6a24806725015ea0
C:\\Users\\liz.bean\\Documents\\install.exe
install.exe"]; B --> C["cmd.exe
4347de5f4e446a17c050b5c242a750b07b40f1c0
C:\\Windows\\SysWOW64\\cmd.exe
cmd.exe /c \"\"C:\\Users\\LIZ-1.BEA\\AppData\\Local\\Temp\\RarSFX0\\ymtr_ps.bat\"\""]; C --> D["powershell.exe
3a9c990d346176b91f44b235a9c50b2d9bca046f
C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe
powershell.exe -NoP -NonI -W Hidden -Exec Bypass -Command \"Invoke-Expression \$(New-Object IO.StreamReader \$(\$New-Object IO.Compression.DeflateStream \$(\$New-Object IO.MemoryStream \$(\$([Convert]::FromBase64String \"nVRRb9plEH7nV4ysPclWsOMEmjZYkUqhaXNXaC6kSe8QOj32gLesd531OjGh/Pcbg4+kr/fi9Yxn5/tm5hu2B7iA905rOpTyKsu1sa6zQqNQdk6DREhHmI [IO.Compression.CompressionMode]::Decompress), [Text.Encoding]::ASCII)).ReadToEnd());\""</pre>						
08:06:28	Outlook dropped and executed a PE file.						
08:06:28	OUTLOOK.EXE created a PE file under Users folder				explorer.exe > OUTLOOK.EXE > file		liz.bean



cont-lizbean-x5 > file

File worldwide



4347de5f4e446a17c050b5c242a750b07b40f1c0

MD5: a750b985779465f4d06331cadd9eb3fd

Size: 198.0 KB

Signer: Microsoft Windows

Issuer: Microsoft Development PCA 2014

Prevalence worldwide

16

First seen: 10 days ago

Last seen: 8 days ago

Deep analysis

Deep analysis request

Submit

File in organization

Filter by: 30 days



Prevalence in organization

Last 30 days

16

First seen: 10 days ago

Last seen: 8 days ago

Names seen in organization

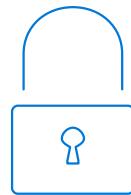
cmd.exe

02.25.2016



Windows 10

ZWEI STÄRKSTE SICHERHEITSFUNKTIONEN ABERN REICHEN DEN



Sichere
Geräte



Sichere
Identitäten



Schutz von
Informationen



Absicherung vor
Bedrohungen



Windows 10