SECURITY FROM CHIP TO CLOUD

ALEXANDER SOLAAT RØDLAND / OLAV TVEDT

AMESTO FOURTYTWO / SPAREBANKEN VEST

SECURITY FROM MIKROKIIBID TO PILV

ALEXANDER SOLAAT RØDLAND / OLAV TVEDT

AMESTO FOURTYTWO / SPAREBANKEN VEST

THANK YOU TO OUR SPONSORS!

Sparkle

PROXIMO3

dox42®

automate your documents
integrate your data

CRONOS
GROEP

CRMK

SOLITA

Tallinn

sturx oü

BC/NAV
TECH
DAYS
mibuso.com

Columbus® Once you know how...

PPUG
POWER PLATFORM USER GROUP ESTONIA

PROMISE
GRUPA APN PROMISE

FROM CHIP TO CLOUD

1.Cloud

2.Identity and Privacy

3.Applications

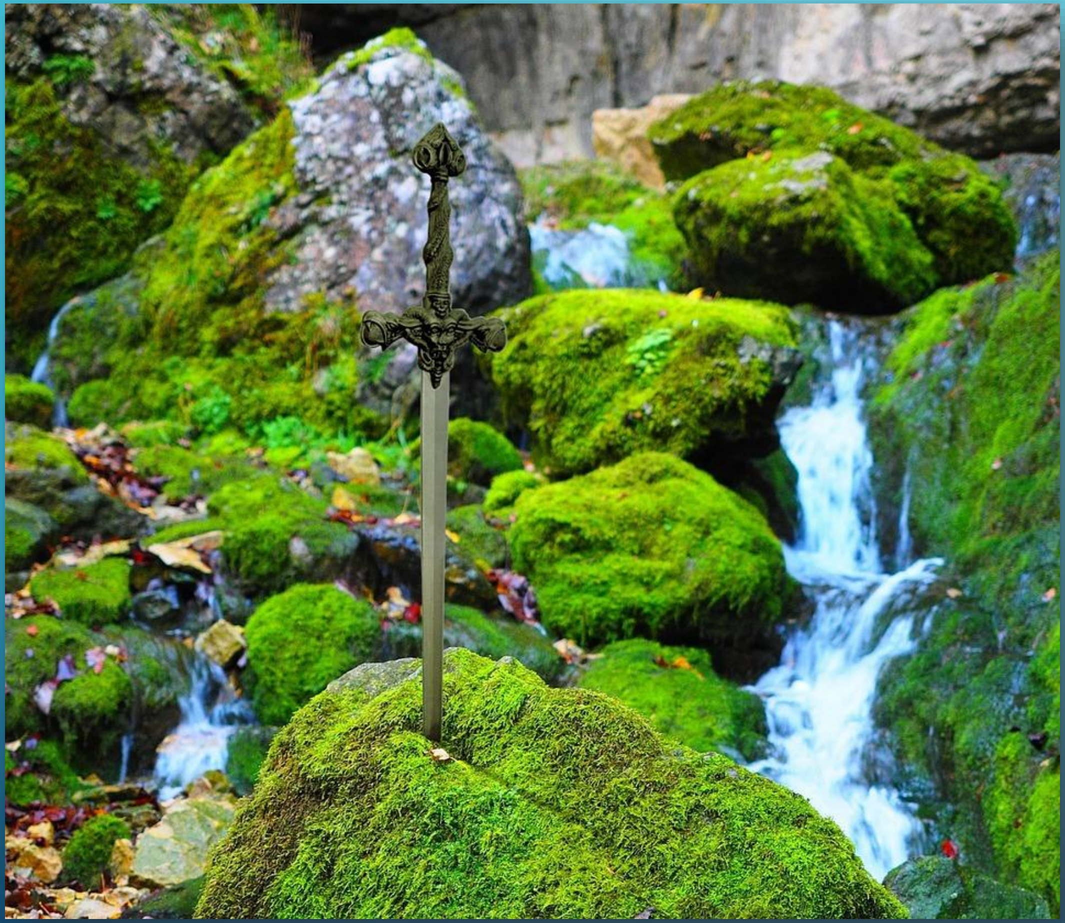
4.Operating System

5.Hardware/The Chips

WITH GREAT POWER…

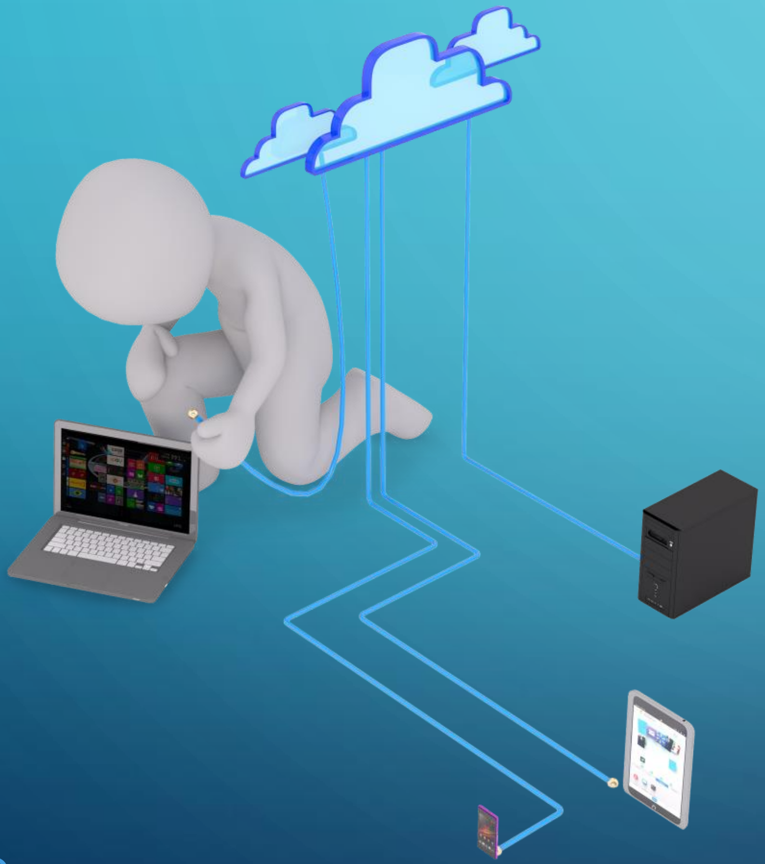
…Comes endless complexity

WITH GREAT POWER



- Low risk
- High reward
- "Bragging rights"

THE BEGINNING - THE CHIPS

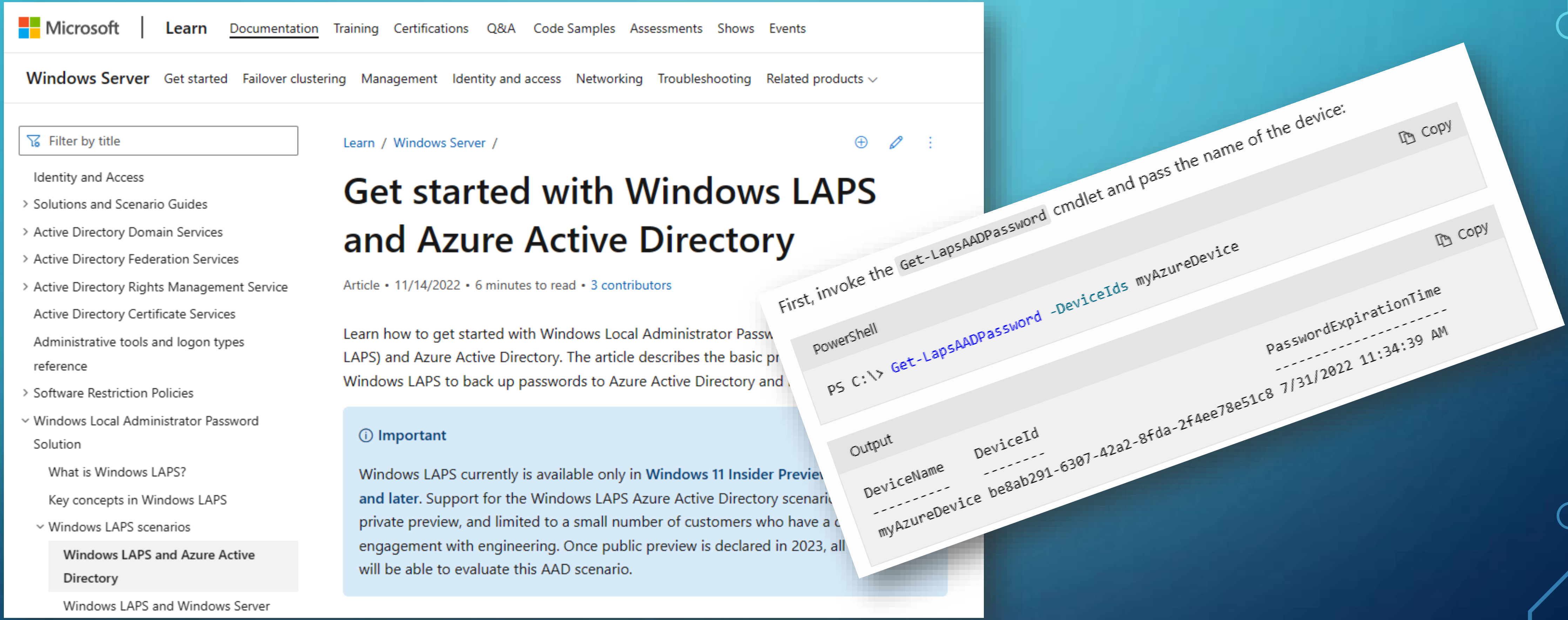


- Open access to a “secure” uefi/bios

What the hack!

- Local Admin ?

WINDOWS LAPS FOR AZURE AD



Microsoft | Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events
Windows Server Get started Failover clustering Management Identity and access Networking Troubleshooting Related products
Filter by title
Identity and Access
Solutions and Scenario Guides
Active Directory Domain Services
Active Directory Federation Services
Active Directory Rights Management Service
Active Directory Certificate Services
Administrative tools and logon types reference
Software Restriction Policies
Windows Local Administrator Password Solution
What is Windows LAPS?
Key concepts in Windows LAPS
Windows LAPS scenarios
Windows LAPS and Azure Active Directory
Windows LAPS and Windows Server
Learn / Windows Server /

Get started with Windows LAPS and Azure Active Directory

Article • 11/14/2022 • 6 minutes to read • 3 contributors

Learn how to get started with Windows Local Administrator Passw
LAPS) and Azure Active Directory. The article describes the basic pr
Windows LAPS to back up passwords to Azure Active Directory and

ⓘ **Important**

Windows LAPS currently is available only in **Windows 11 Insider Previe and later**. Support for the Windows LAPS Azure Active Directory scenari private preview, and limited to a small number of customers who have a c engagement with engineering. Once public preview is declared in 2023, all will be able to evaluate this AAD scenario.

First, invoke the `Get-LapsAADPassword` cmdlet and pass the name of the device:

PowerShell Copy

```
PS C:\> Get-LapsAADPassword -DeviceIds myAzureDevice
```

Output Copy

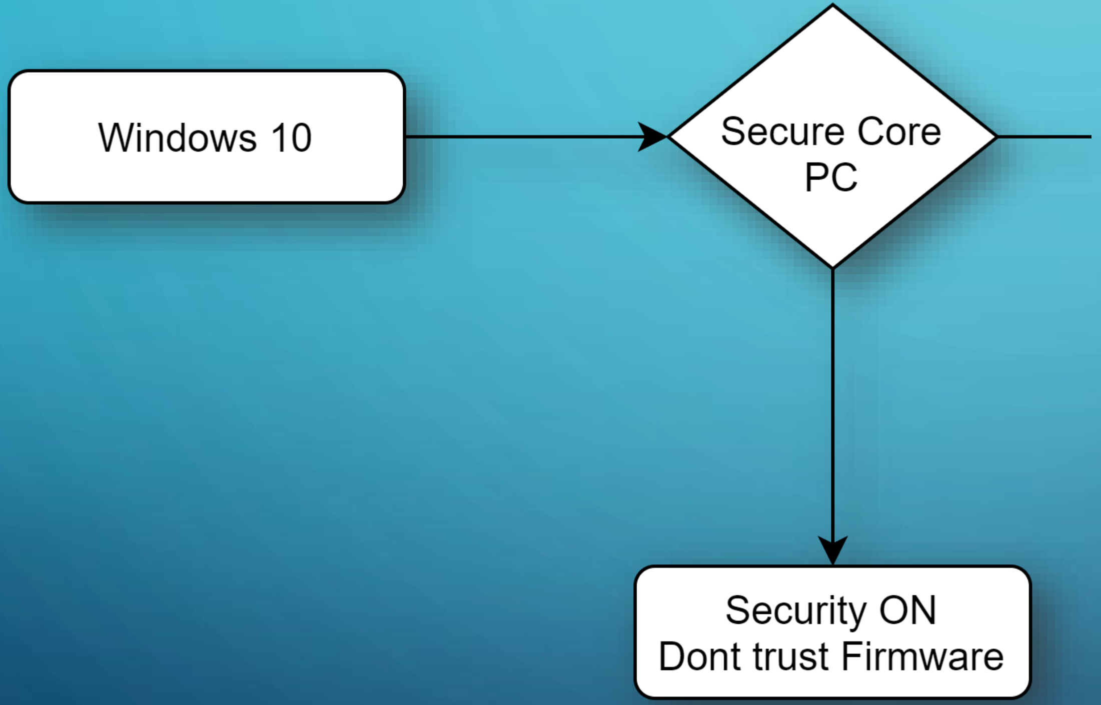
```
DeviceName    DeviceId                             PasswordExpirationTime
----------    --------                             ----------------------
myAzureDevice be8ab291-6307-42a2-8fda-2f4ee78e51c8 7/31/2022 11:34:39 AM
```

https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-scenarios-azure-active-directory

WINDOWS 10 ROAD TO SECURITY

Windows 10

WINDOWS 10



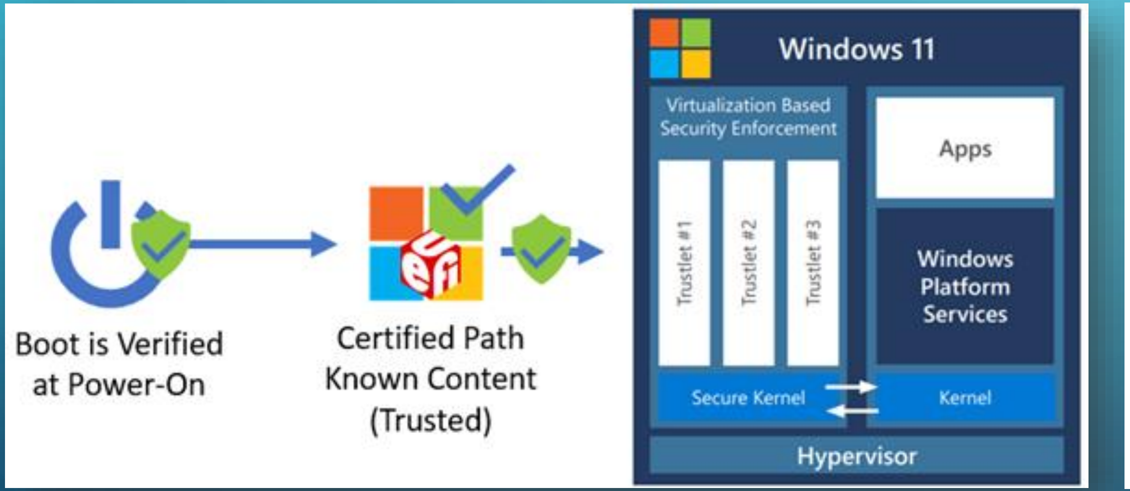
Windows 10

Secure Core PC

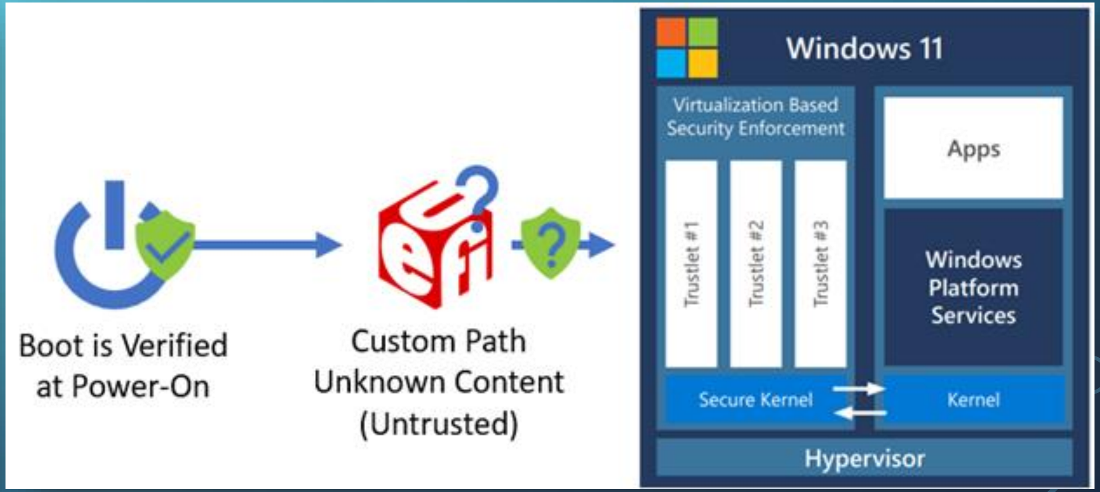
Security ON
Dont trust Firmware

FIRMWARE ATTACK SURFACE REDUCTION (FASR)

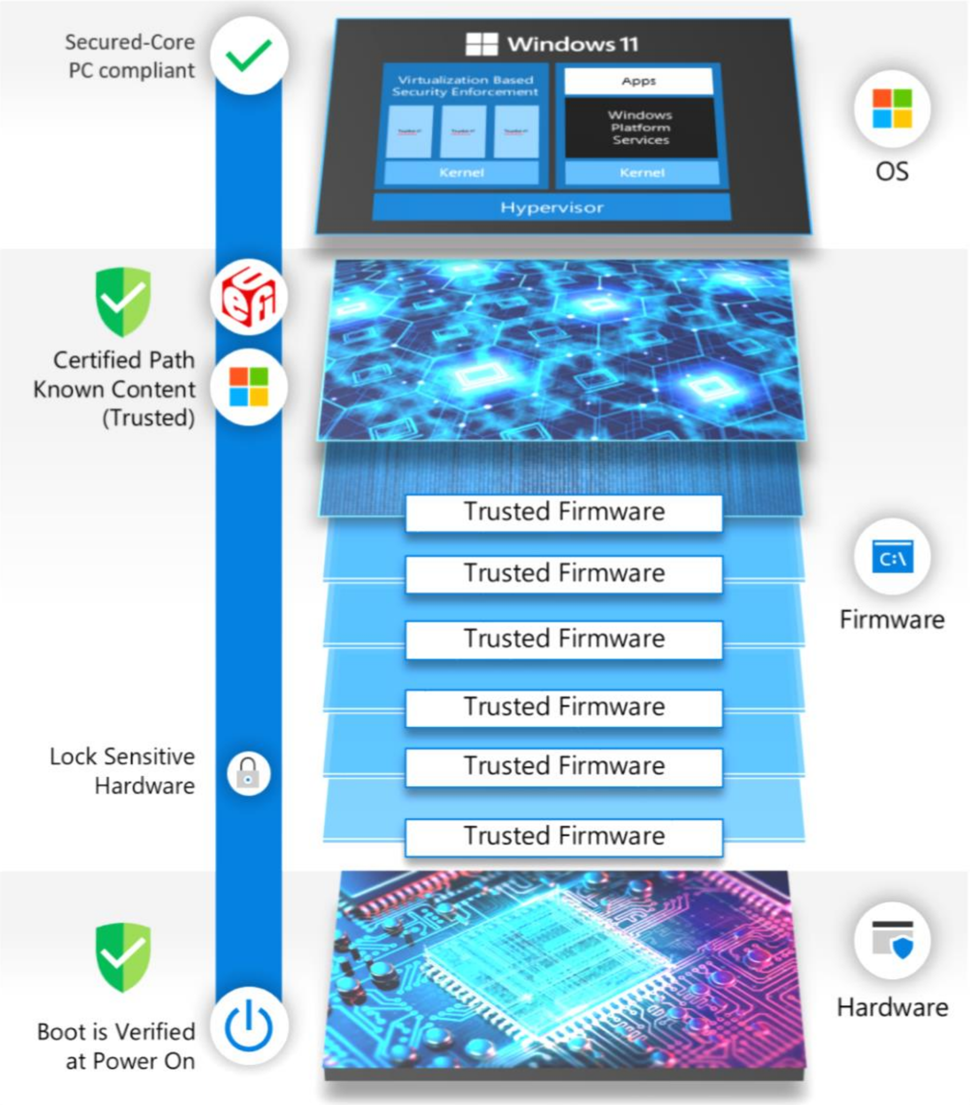
CERTIFIED BOOT PATH


Boot is Verified at Power-On
Certified Path Known Content (Trusted)
Windows 11
Virtualization Based Security Enforcement
Trustlet #1
Trustlet #2
Trustlet #3
Apps
Windows Platform Services
Secure Kernel
Kernel
Hypervisor

CUSTOM BOOT PATH

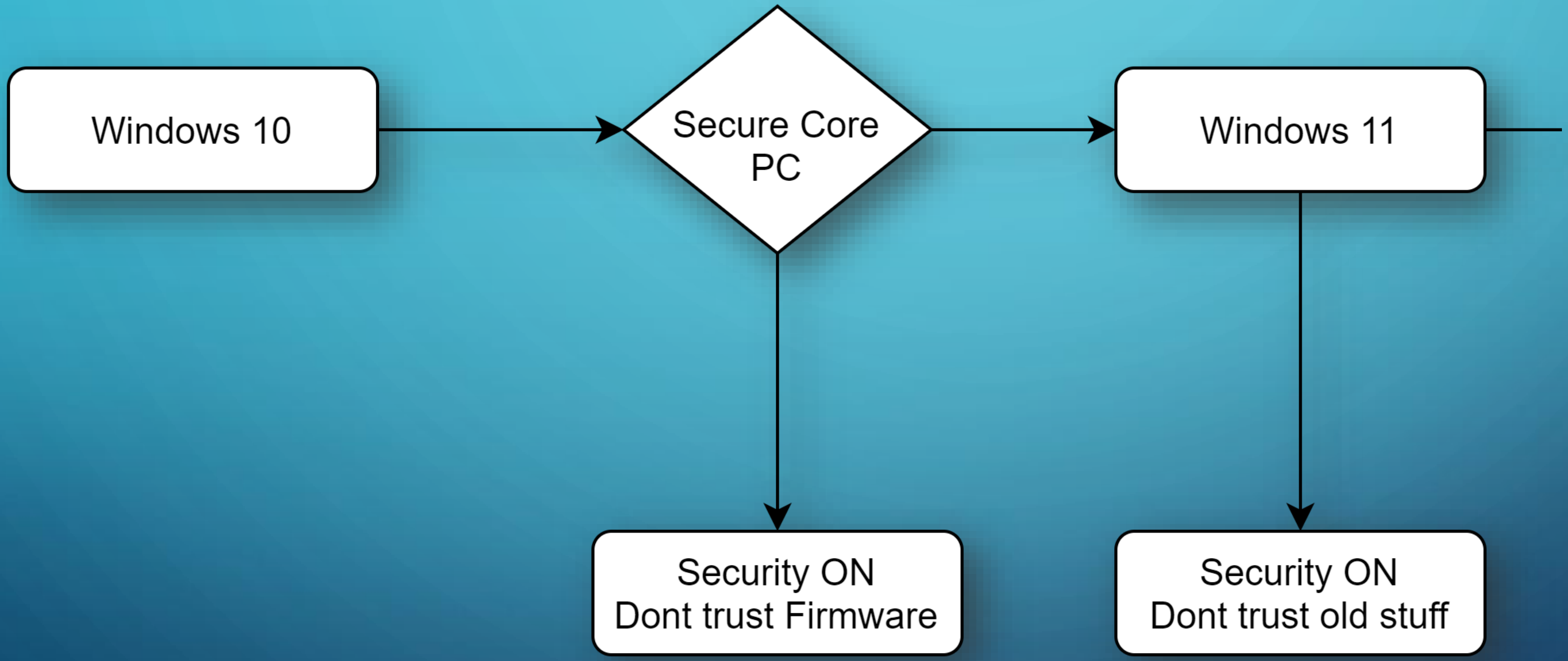

Boot is Verified at Power-On
Custom Path Unknown Content (Untrusted)
Windows 11
Virtualization Based Security Enforcement
Trustlet #1
Trustlet #2
Trustlet #3
Apps
Windows Platform Services
Secure Kernel
Kernel
Hypervisor

FASR



Secured-Core PC compliant
Windows 11
Virtualization Based Security Enforcement
Apps
Windows Platform Services
Kernel
Kernel
Hypervisor
OS
Certified Path Known Content (Trusted)
Trusted Firmware
Trusted Firmware
Trusted Firmware
Trusted Firmware
Trusted Firmware
Trusted Firmware
Firmware
C:\
Lock Sensitive Hardware
Boot is Verified at Power On
Hardware

WINDOWS 10 -> 11



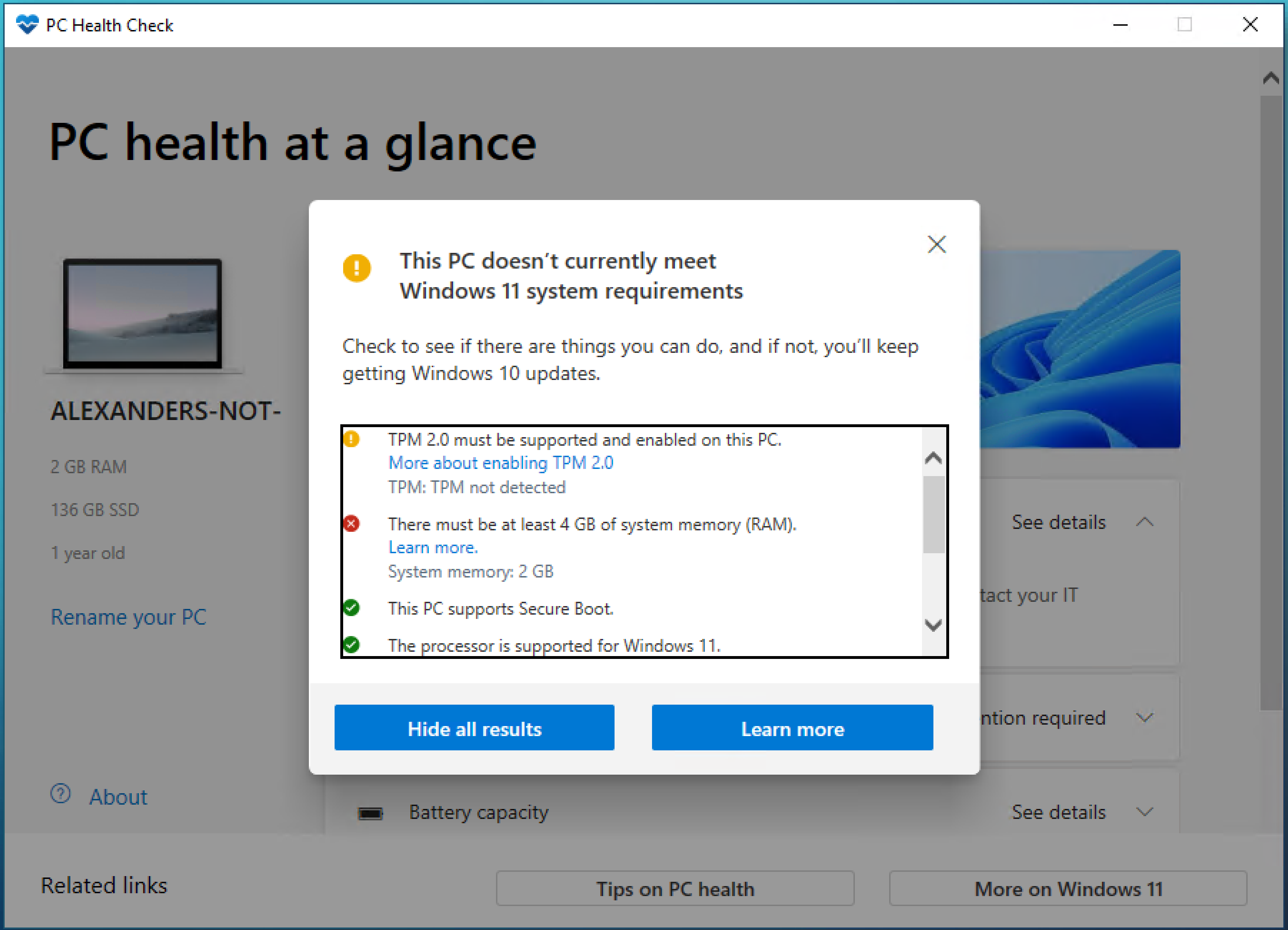
Windows 10

Secure Core PC

Windows 11

Security ON
Dont trust Firmware

Security ON
Dont trust old stuff



PC Health Check

PC health at a glance

ALEXANDERS-NOT-

2 GB RAM

136 GB SSD

1 year old

Rename your PC

About

This PC doesn’t currently meet Windows 11 system requirements

Check to see if there are things you can do, and if not, you’ll keep getting Windows 10 updates.

⚠ TPM 2.0 must be supported and enabled on this PC.
More about enabling TPM 2.0
TPM: TPM not detected

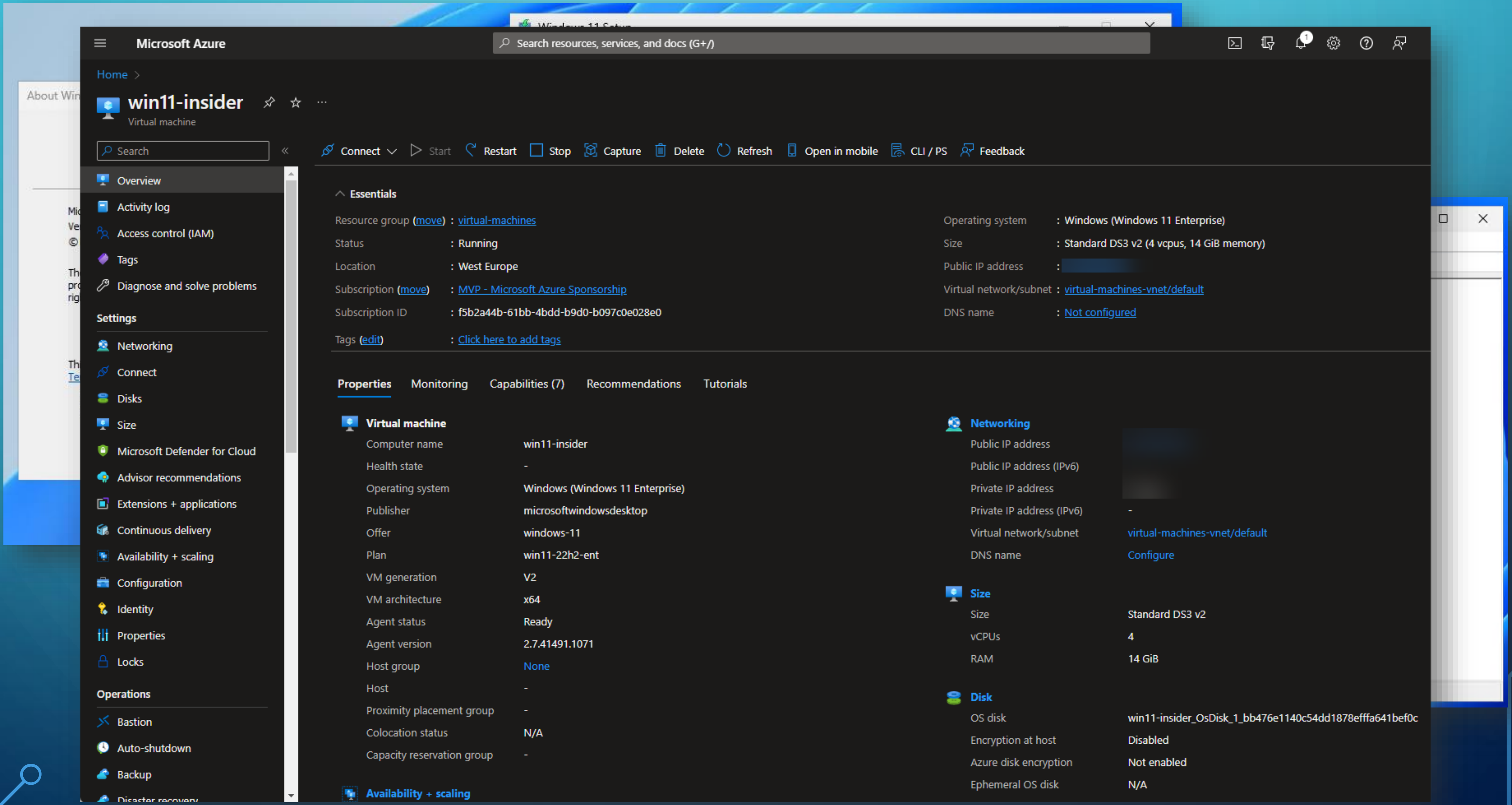
✗ There must be at least 4 GB of system memory (RAM).
Learn more.
System memory: 2 GB

✓ This PC supports Secure Boot.

✓ The processor is supported for Windows 11.

Related links

WHO ARE CHEATING?



win11-insider

Virtual machine

Essentials

Resource group (move) : virtual-machines
Status : Running
Location : West Europe
Subscription (move) : MVP - Microsoft Azure Sponsorship
Subscription ID : f5b2a44b-61bb-4bdd-b9d0-b097c0e028e0
Tags (edit) : Click here to add tags

Operating system : Windows (Windows 11 Enterprise)
Size : Standard DS3 v2 (4 vcpus, 14 GiB memory)
Public IP address : [redacted]
Virtual network/subnet : virtual-machines-vnet/default
DNS name : Not configured

Virtual machine

Computer name	win11-insider
Health state	-
Operating system	Windows (Windows 11 Enterprise)
Publisher	microsoftwindowsdesktop
Offer	windows-11
Plan	win11-22h2-ent
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1071
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-

Availability + scaling

Networking

Public IP address	[redacted]
Public IP address (IPv6)	[redacted]
Private IP address	[redacted]
Private IP address (IPv6)	-
Virtual network/subnet	virtual-machines-vnet/default
DNS name	Configure

Size

Size	Standard DS3 v2
vCPUs	4
RAM	14 GiB

Disk

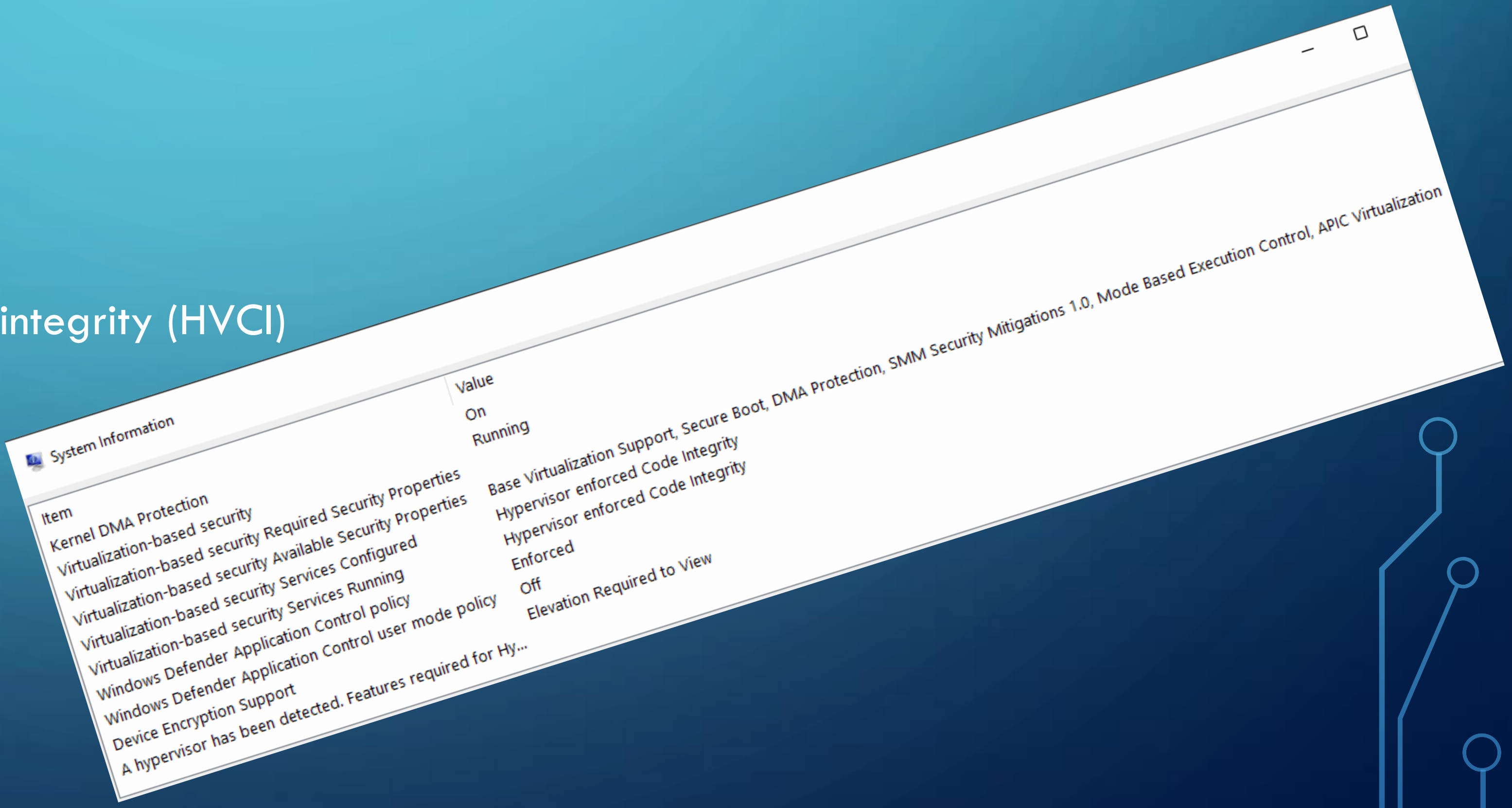
OS disk	win11-insider_OsDisk_1_bb476e1140c54dd1878effa641bef0c
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A

THE PERFECT HARDWARE

ESSENTIALS FUNCTIONALITIES

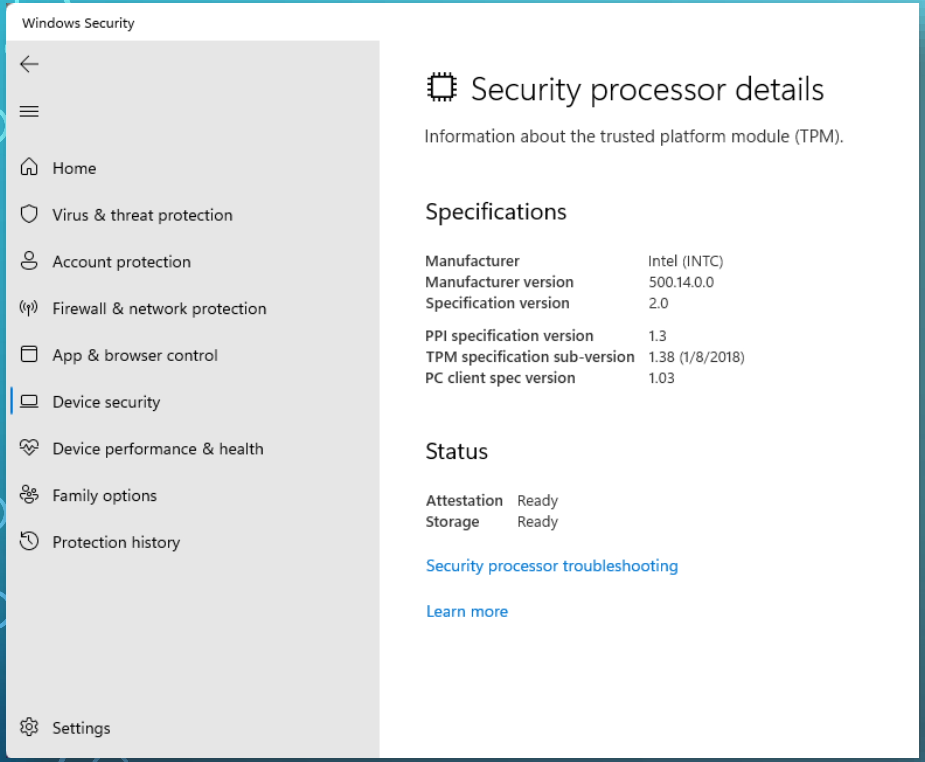
- VBS (Virtualization-based security)
  - Secure Boot
  - Virtual Secure Mode (VSM)
  - Credential Guard
  - Device Guard
  - Application Guard
  - Hypervisor-protected code integrity (HVCI)
  - System Guard
  - Windows Sandbox
  - And so on….

- TMP 2.0
  - Cryptoprocessor


System Information

Item	Value
Kernel DMA Protection	On
Virtualization-based security	Running
Virtualization-based security Required Security Properties	
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, SMM Security Mitigations 1.0, Mode Based Execution Control, APIC Virtualization
Virtualization-based security Services Configured	Hypervisor enforced Code Integrity
Virtualization-based security Services Running	Hypervisor enforced Code Integrity
Windows Defender Application Control policy	Enforced
Windows Defender Application Control user mode policy	Off
Device Encryption Support	Elevation Required to View
A hypervisor has been detected. Features required for Hy...	

TPM



Security processor details

Information about the trusted platform module (TPM).

Specifications

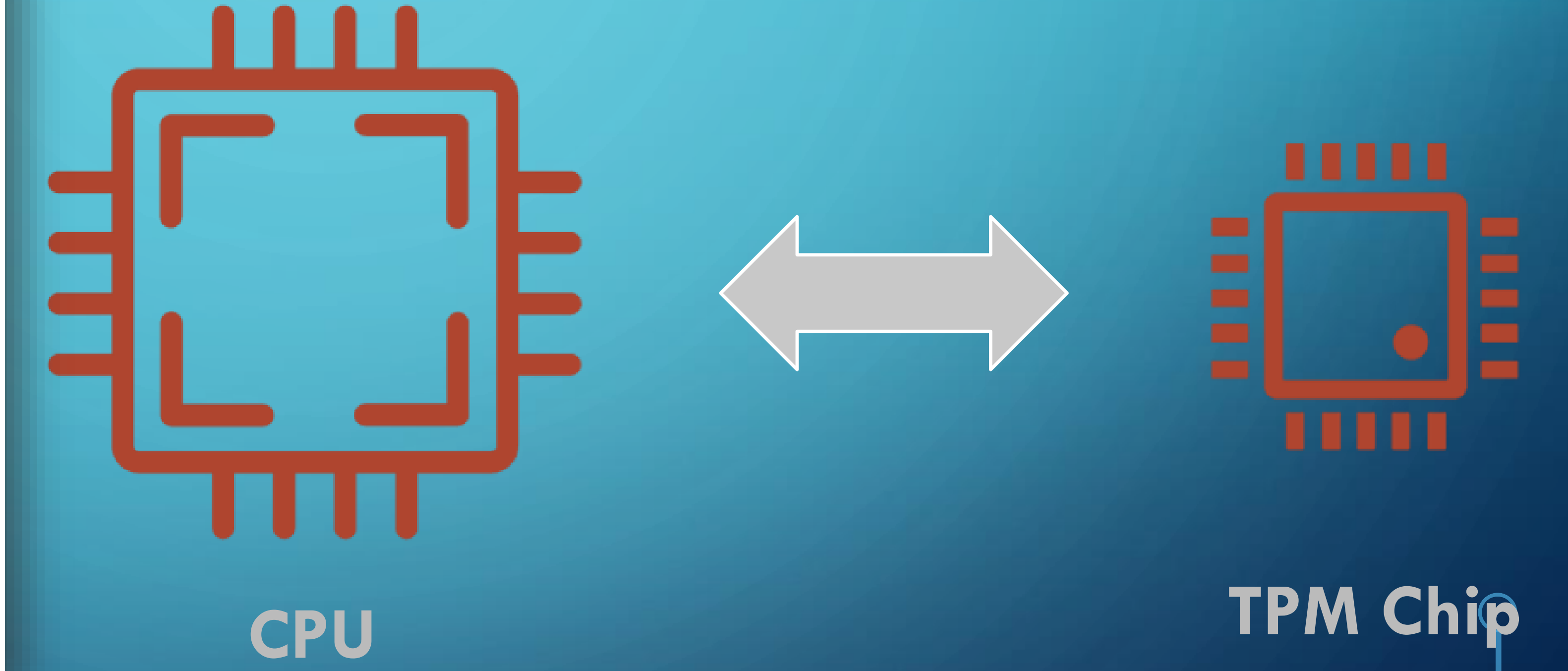
Manufacturer	Intel (INTC)
Manufacturer version	500.14.0.0
Specification version	2.0
PPI specification version	1.3
TPM specification sub-version	1.38 (1/8/2018)
PC client spec version	1.03

Status

Attestation	Ready
Storage	Ready

Security processor troubleshooting

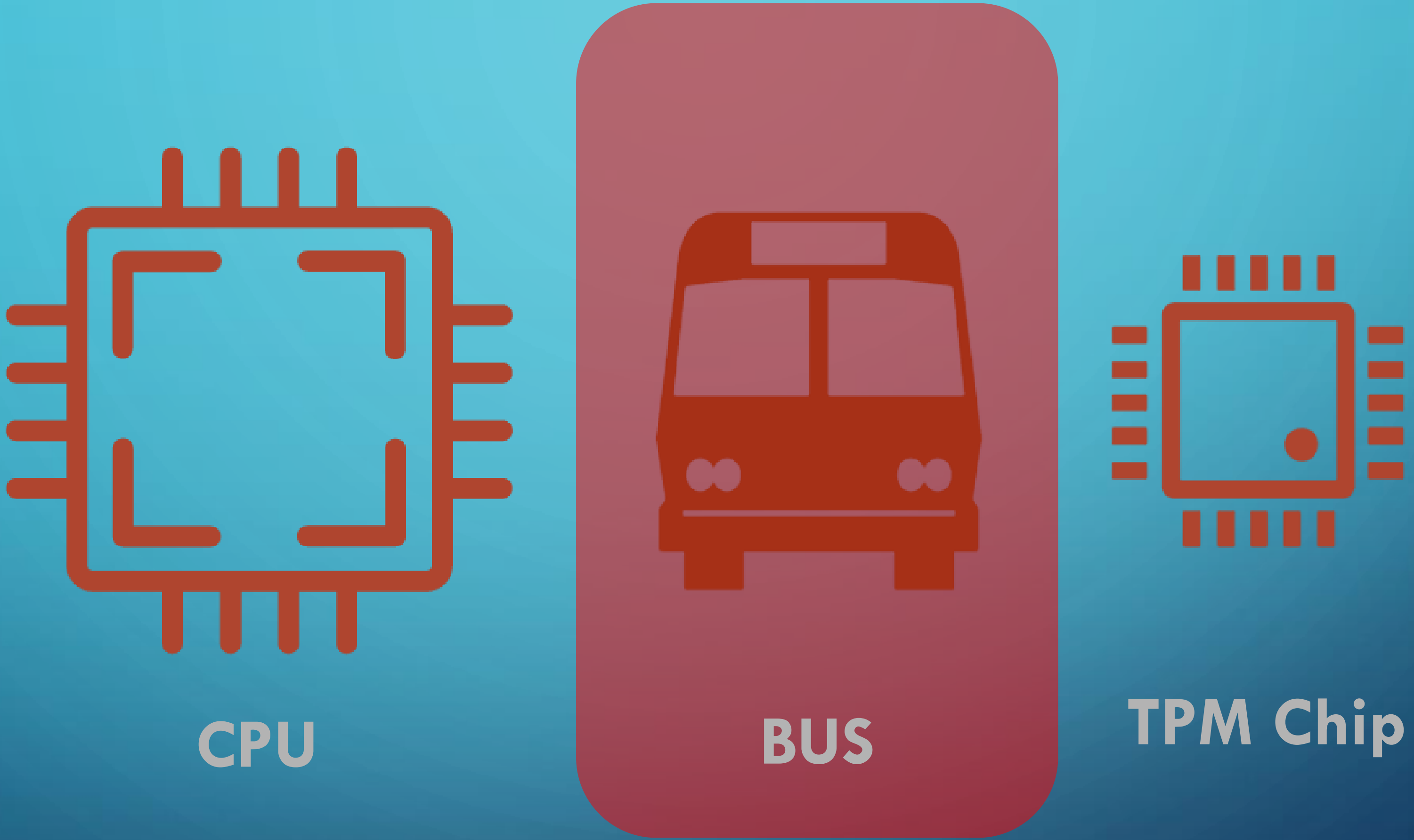
Learn more



CPU

TPM Chip

TPM

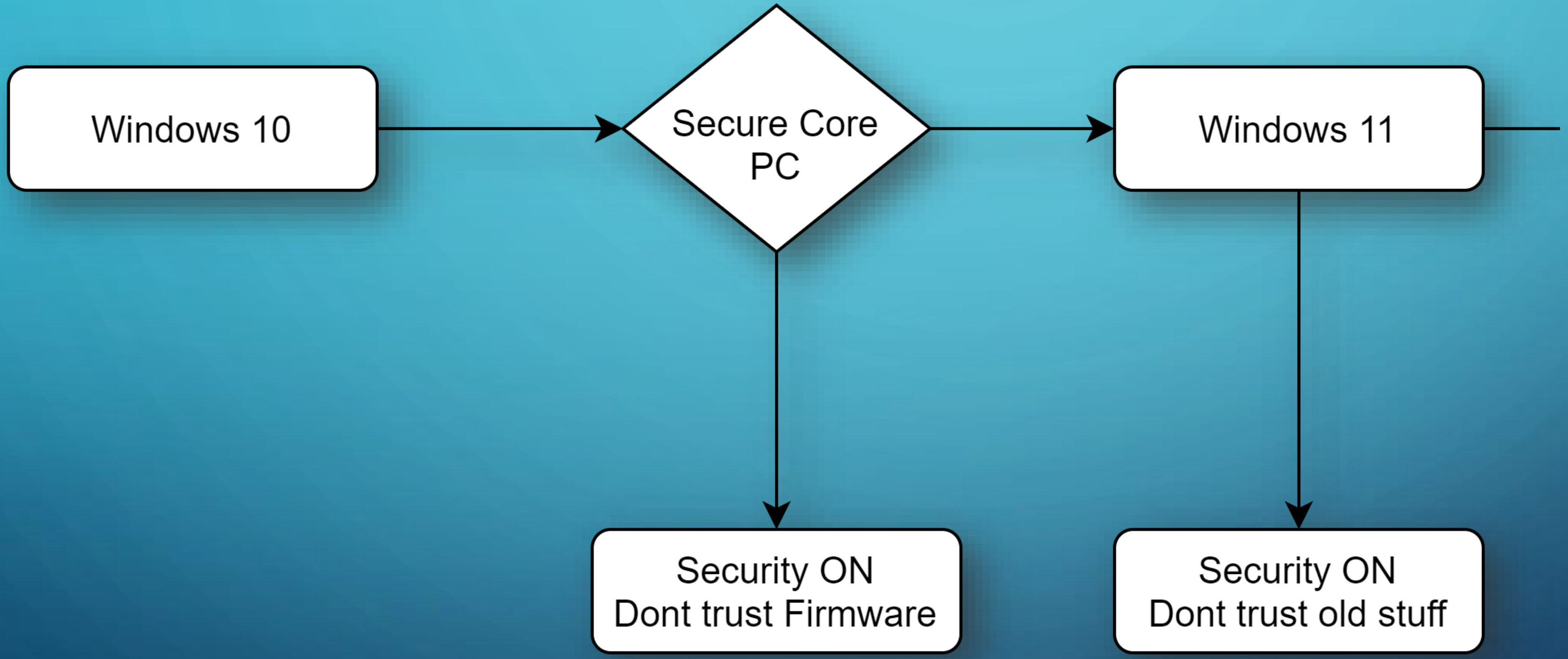


CPU

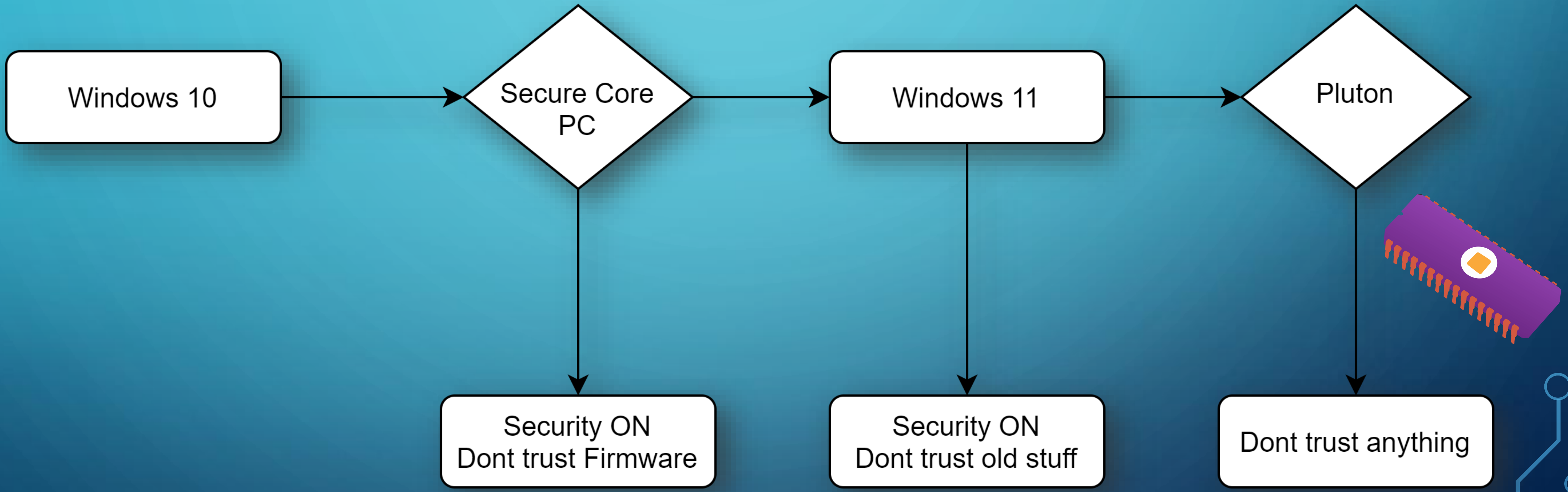
BUS

TPM Chip

WINDOWS 10 -> 11


Windows 10
Secure Core PC
Windows 11
Security ON Dont trust Firmware
Security ON Dont trust old stuff

WINDOWS 10 -> 11 -> ?



Windows 10

Secure Core PC

Security ON
Dont trust Firmware

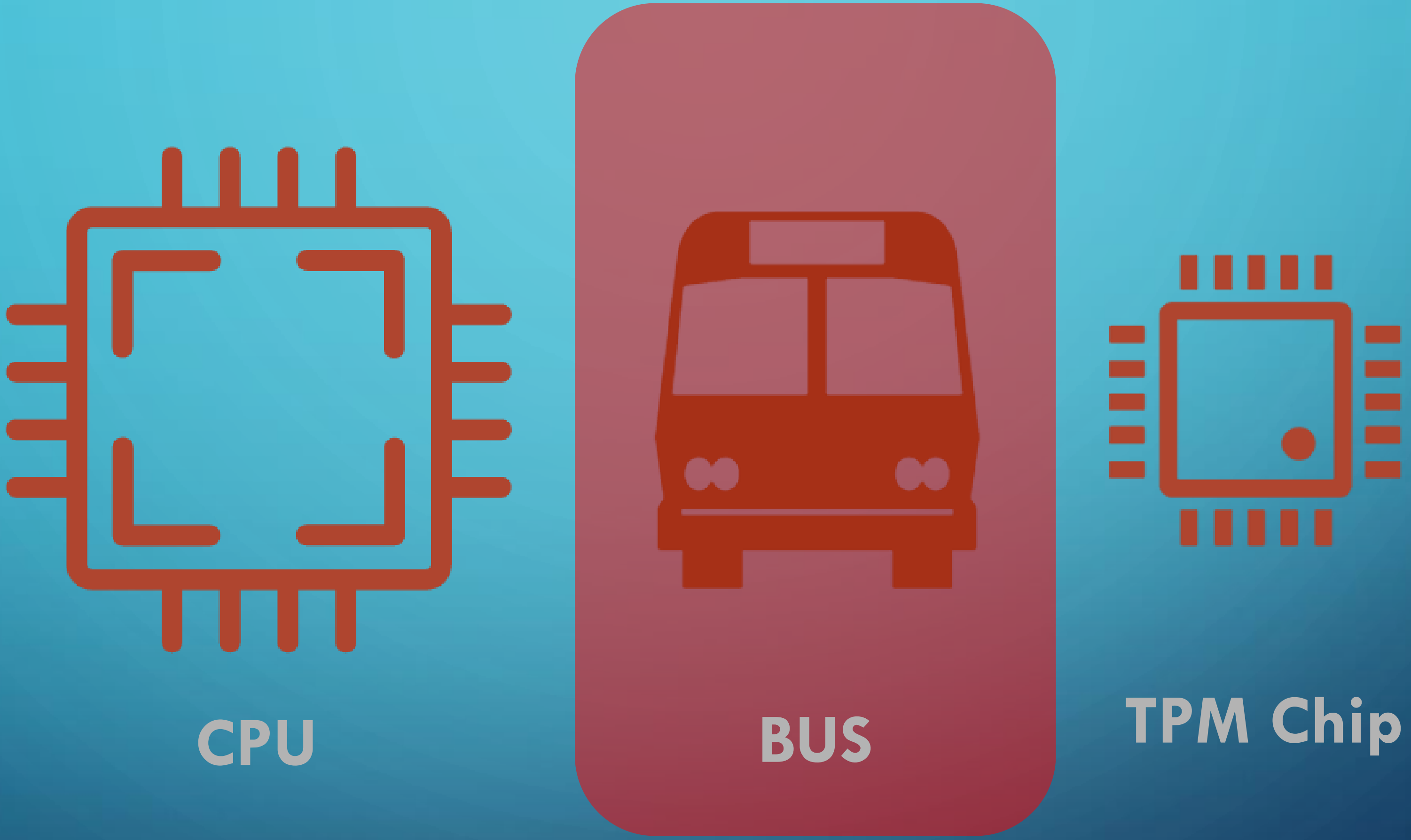
Windows 11

Security ON
Dont trust old stuff

Pluton

Dont trust anything

TPM



CPU

BUS

TPM Chip

PLUTON

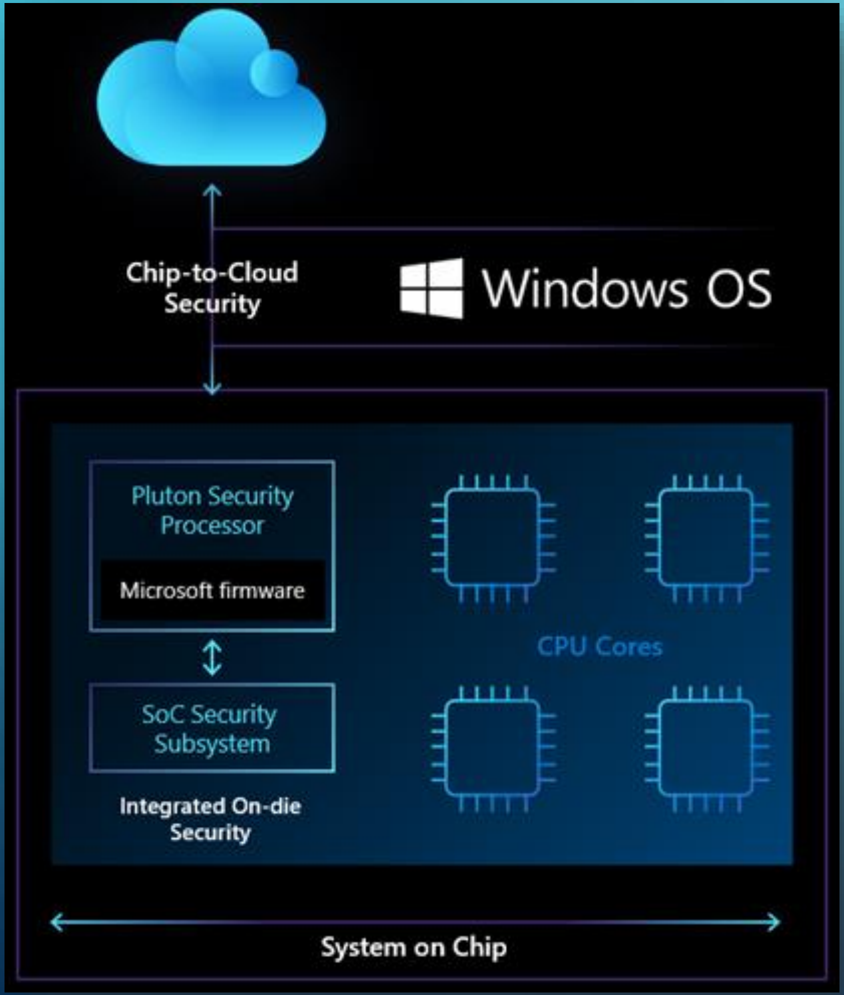
Pluton

Now you have to have a scanning electron microscope if you want to sniff that bus.

- John Shock, Principal Software Engineer at Microsoft and lead for the UEFI firmware development on Surface.

PROTECT AGAINST WHAT?

SECURITY AT CORE- LEVEL



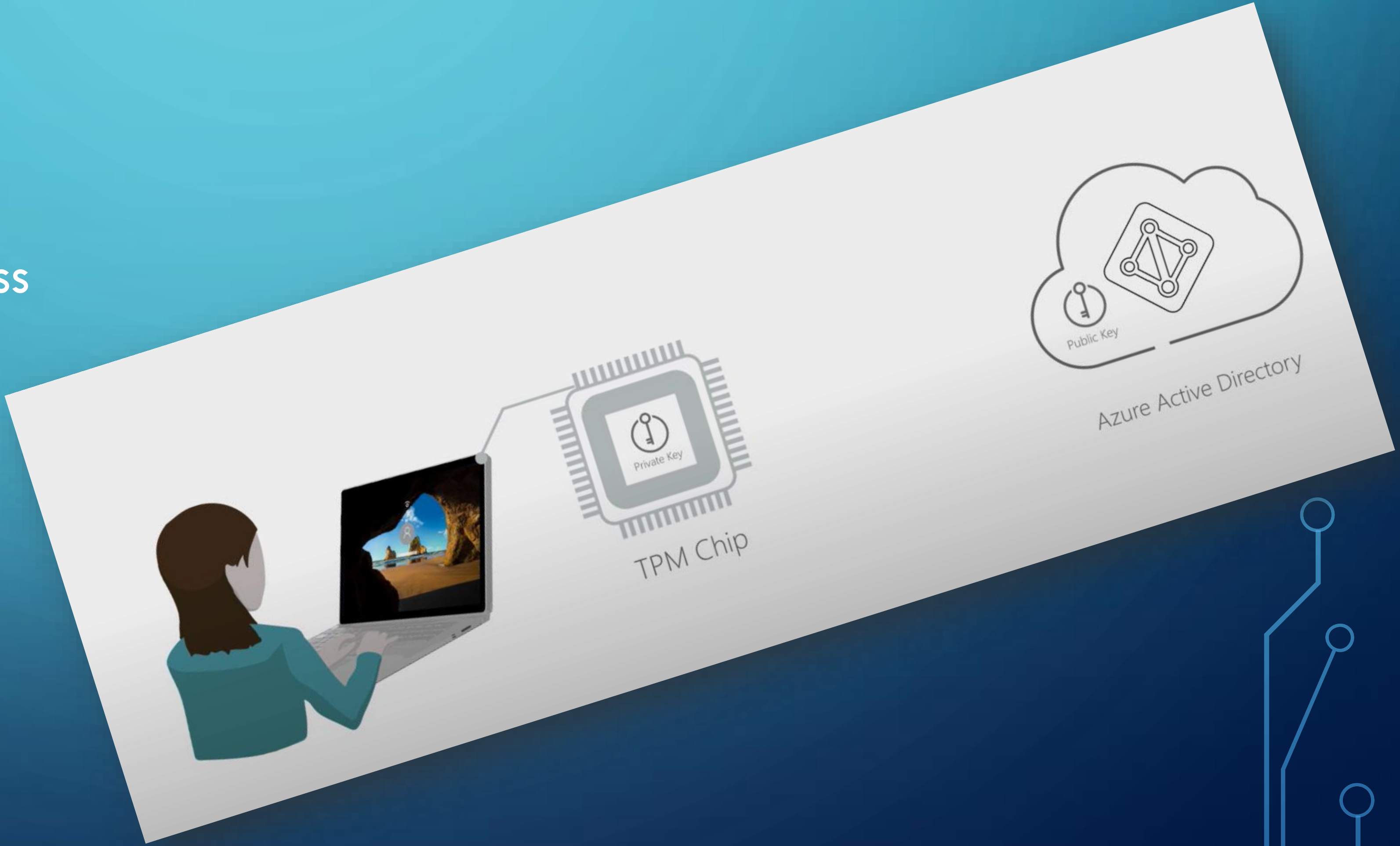
MELTDOWN & SPECTRE?

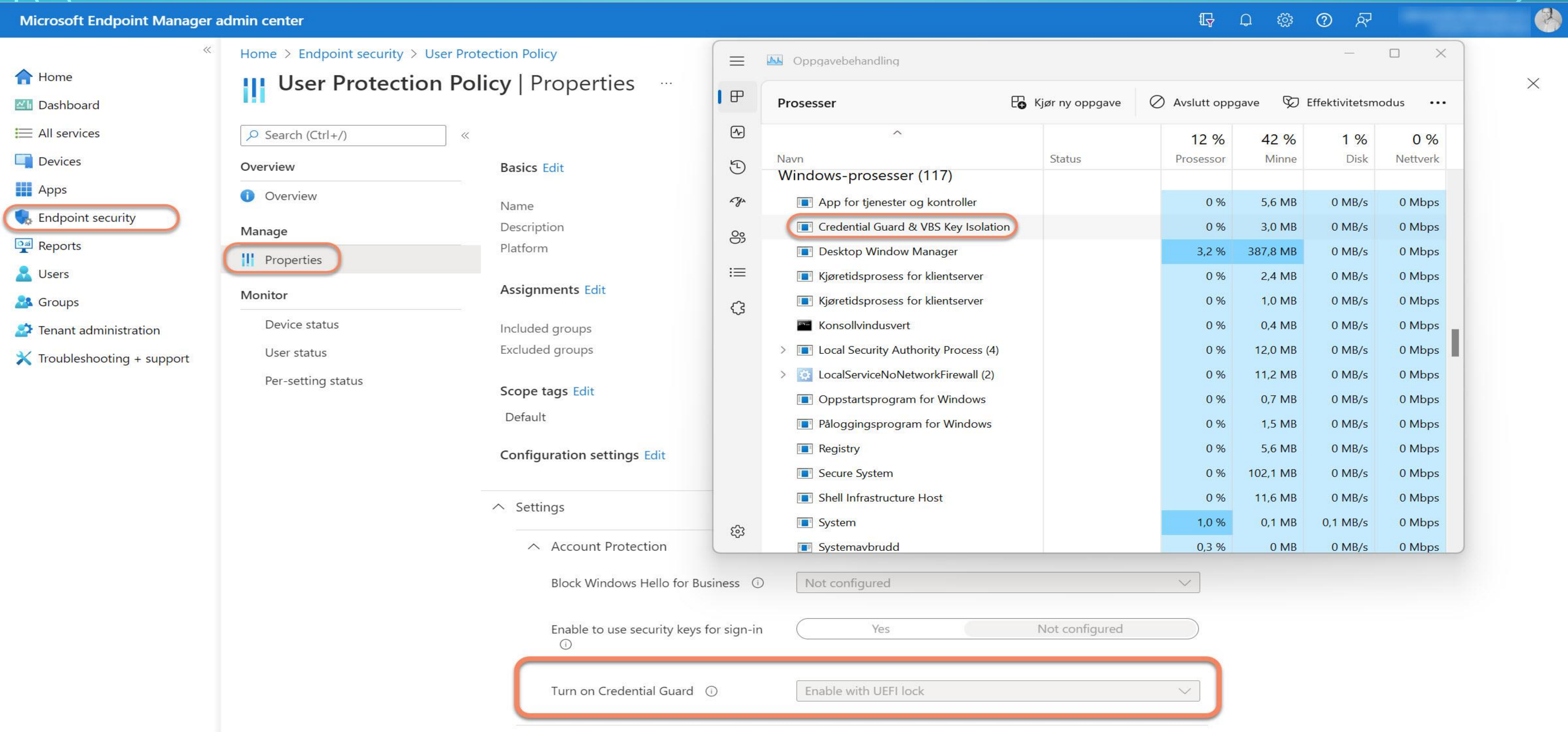
- Thwart future spinoffs
- Keys never leave Pluton
- Integrated to the CPU die
- Pre-tested since 2013-ish
- It might be disabled(!)

THE PERFECT HARDWARE 2.0

VBS AND TPM PROTECTS USER-CONTEXT

- Device guard
- Credential guard
- Windows Hello for Business





Microsoft Endpoint Manager admin center

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security > User Protection Policy

User Protection Policy | Properties

Search (Ctrl+/)

Overview
- Overview

Manage
- Properties

Monitor
- Device status
- User status
- Per-setting status

Basics Edit

Name
Description
Platform

Assignments Edit

Included groups
Excluded groups

Scope tags Edit

Default

Configuration settings Edit

Settings

Account Protection

Block Windows Hello for Business: Not configured

Enable to use security keys for sign-in: Yes / Not configured

Turn on Credential Guard: Enable with UEFI lock

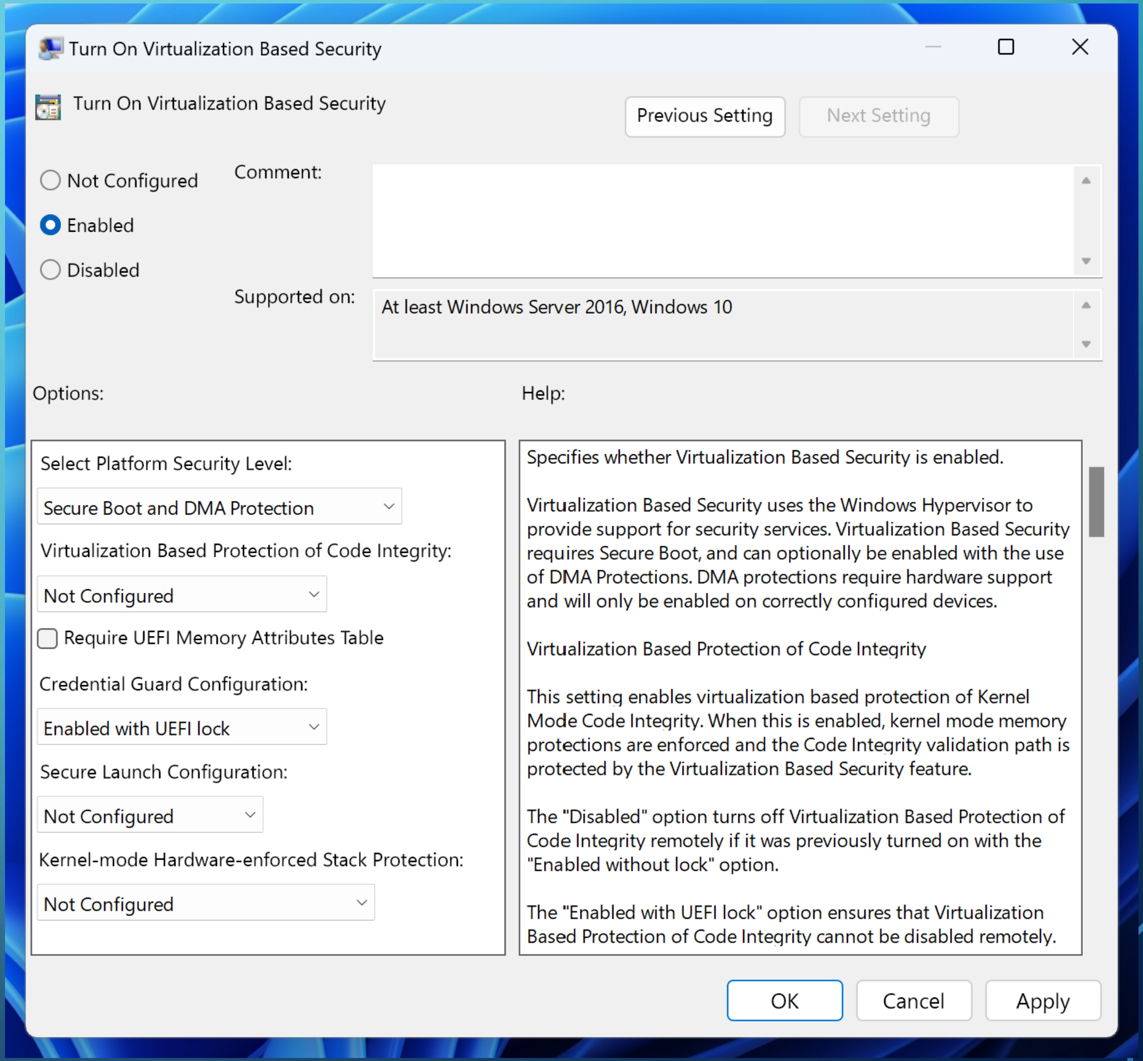
Oppgavebehandling

Prosesser — Kjør ny oppgave — Avslutt oppgave — Effektivitetsmodus

Navn	Status	12 % Prosessor	42 % Minne	1 % Disk	0 % Nettverk
Windows-prosesser (117)					
App for tjenester og kontroller		0 %	5,6 MB	0 MB/s	0 Mbps
Credential Guard & VBS Key Isolation		0 %	3,0 MB	0 MB/s	0 Mbps
Desktop Window Manager		3,2 %	387,8 MB	0 MB/s	0 Mbps
Kjøretidsprosess for klientserver		0 %	2,4 MB	0 MB/s	0 Mbps
Kjøretidsprosess for klientserver		0 %	1,0 MB	0 MB/s	0 Mbps
Konsollvindusvert		0 %	0,4 MB	0 MB/s	0 Mbps
Local Security Authority Process (4)		0 %	12,0 MB	0 MB/s	0 Mbps
LocalServiceNoNetworkFirewall (2)		0 %	11,2 MB	0 MB/s	0 Mbps
Oppstartsprogram for Windows		0 %	0,7 MB	0 MB/s	0 Mbps
Påloggingsprogram for Windows		0 %	1,5 MB	0 MB/s	0 Mbps
Registry		0 %	5,6 MB	0 MB/s	0 Mbps
Secure System		0 %	102,1 MB	0 MB/s	0 Mbps
Shell Infrastructure Host		0 %	11,6 MB	0 MB/s	0 Mbps
System		1,0 %	0,1 MB	0,1 MB/s	0 Mbps
Systemavbrudd		0,3 %	0 MB	0 MB/s	0 Mbps

DEMO – ENABLE CREDENTIAL GUARD

- Lsalso.exe - GPO



Turn On Virtualization Based Security

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2016, Windows 10

Options:

Select Platform Security Level: Secure Boot and DMA Protection

Virtualization Based Protection of Code Integrity: Not Configured

□ Require UEFI Memory Attributes Table

Credential Guard Configuration: Enabled with UEFI lock

Secure Launch Configuration: Not Configured

Kernel-mode Hardware-enforced Stack Protection: Not Configured

Help:

Specifies whether Virtualization Based Security is enabled.

Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based Security requires Secure Boot, and can optionally be enabled with the use of DMA Protections. DMA protections require hardware support and will only be enabled on correctly configured devices.

Virtualization Based Protection of Code Integrity

This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.

The "Disabled" option turns off Virtualization Based Protection of Code Integrity remotely if it was previously turned on with the "Enabled without lock" option.

The "Enabled with UEFI lock" option ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely.

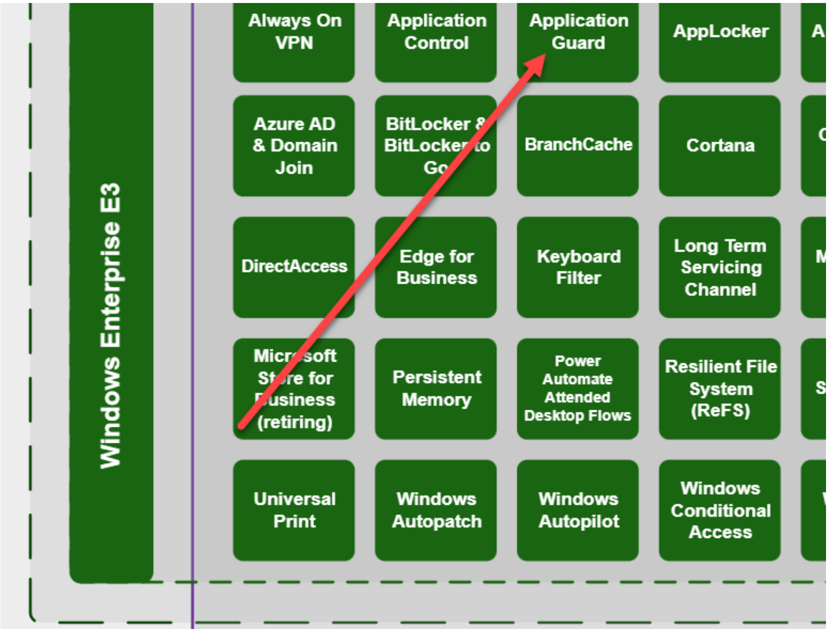
EXAMPLES HOW VBS PROTECTS APPLICATIONS

- Sandboxing
  - WDAG
  - Sandbox
- Smart App Control

Remember me?

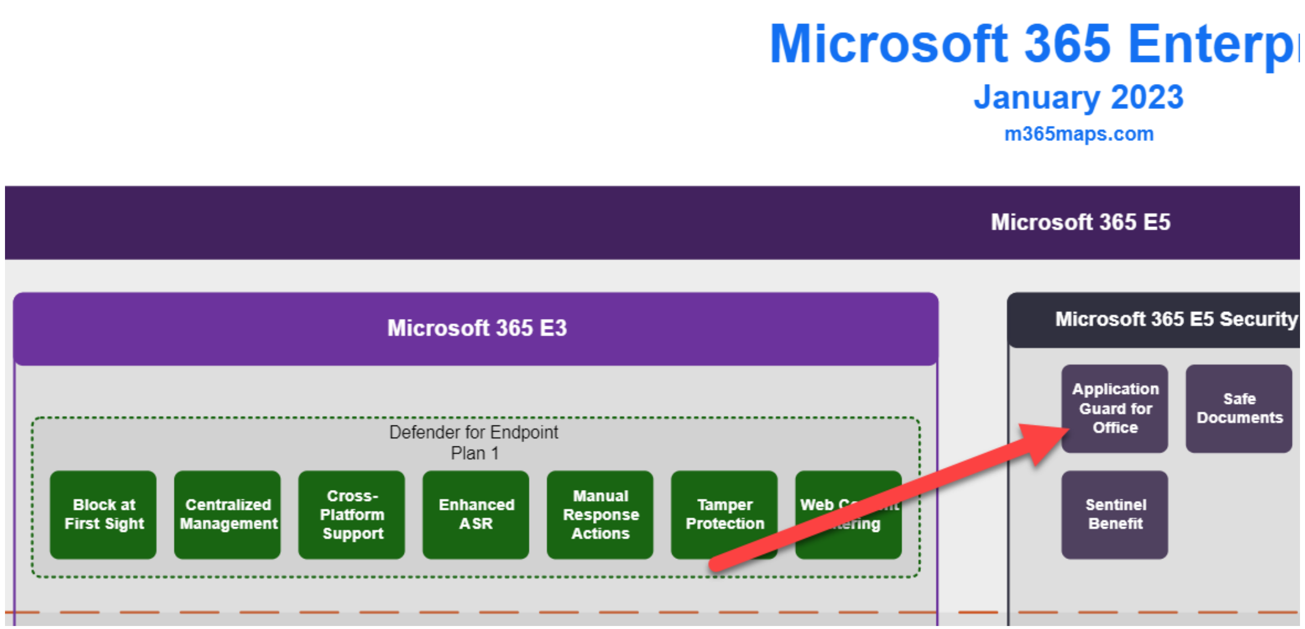
DEMO WDAG

Alexander The Great
This PC
Recycle Bin
BlåSkjermBrødrene



Windows Enterprise E3

Always On VPN	Application Control	Application Guard	AppLocker	A
Azure AD & Domain Join	BitLocker & BitLocker to Go	BranchCache	Cortana	C
DirectAccess	Edge for Business	Keyboard Filter	Long Term Servicing Channel	M
Microsoft Store for Business (retiring)	Persistent Memory	Power Automate Attended Desktop Flows	Resilient File System (ReFS)	S
Universal Print	Windows Autopatch	Windows Autopilot	Windows Conditional Access	W



Microsoft 365 Enterp

January 2023

m365maps.com

Microsoft 365 E5

Microsoft 365 E3

Defender for Endpoint Plan 1

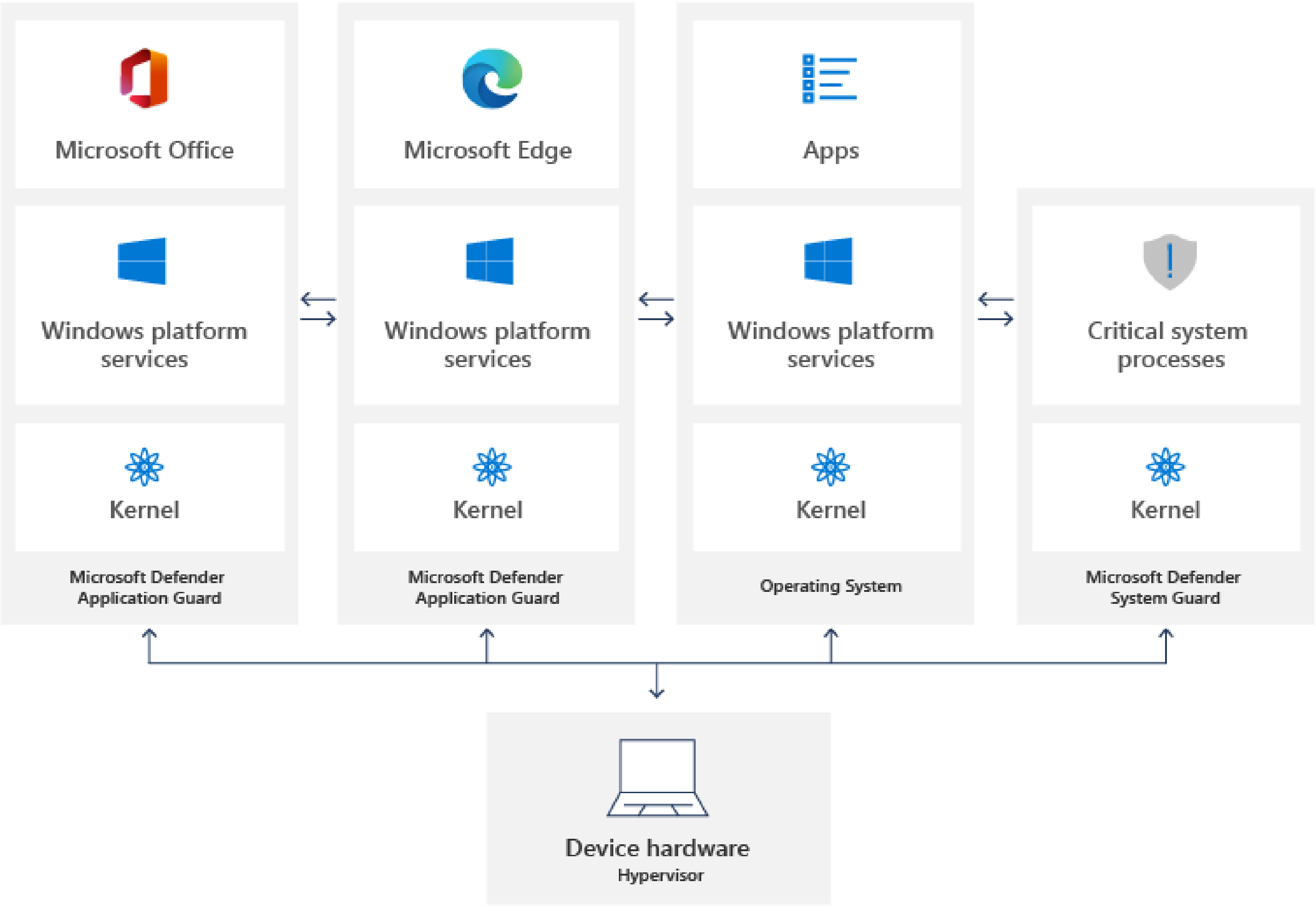
Block at First Sight	Centralized Management	Cross-Platform Support	Enhanced ASR	Manual Response Actions	Tamper Protection	Web Content Filtering

Microsoft 365 E5 Security

Application Guard for Office	Safe Documents
Sentinel Benefit	

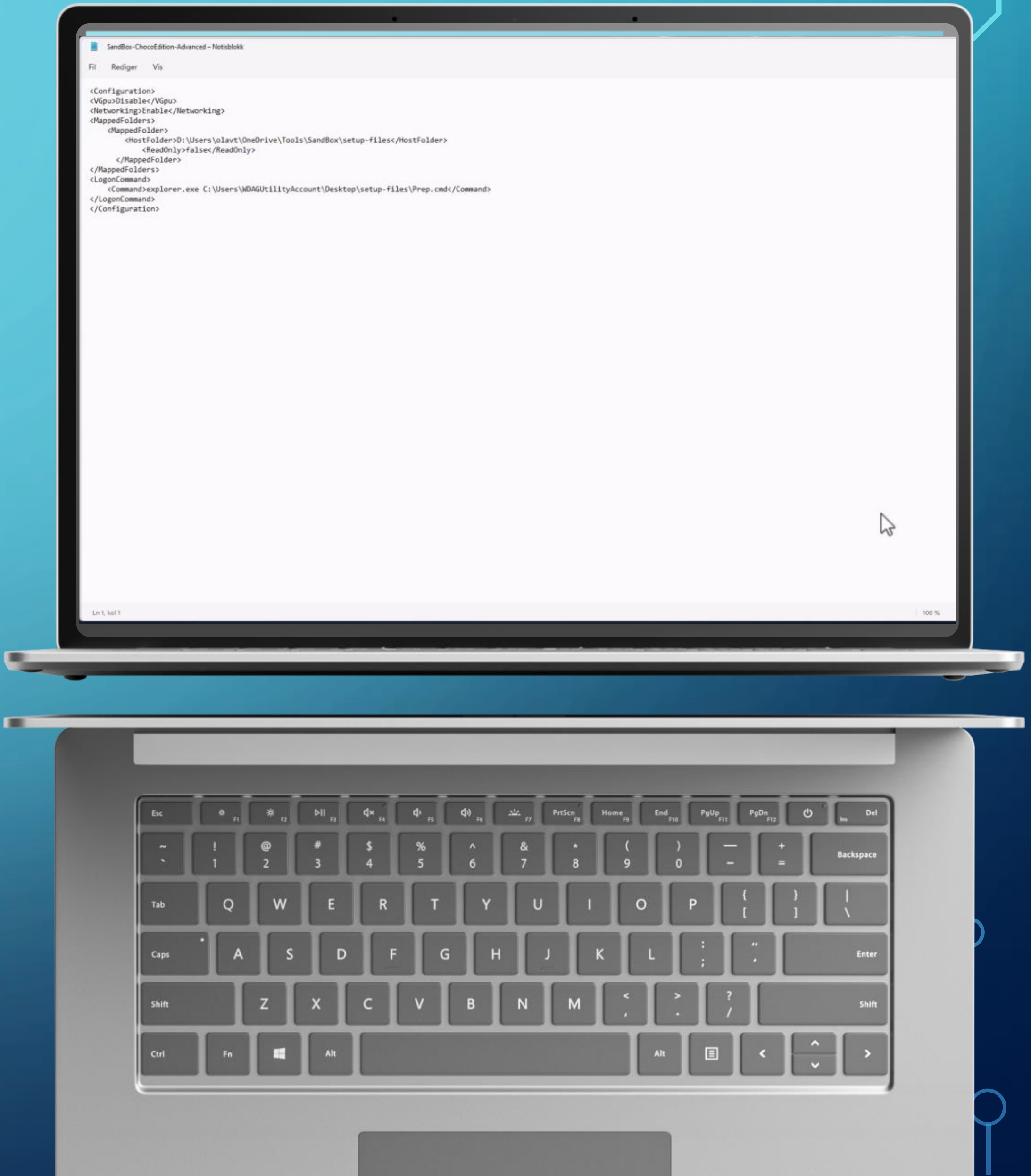
WDAG LICENSE REQUIREMENTS

Hardware isolation of **Microsoft Edge** & **Microsoft Office** with **Microsoft Defender Application Guard**



Microsoft Office
Windows platform services
Kernel
Microsoft Defender Application Guard
Microsoft Edge
Windows platform services
Kernel
Microsoft Defender Application Guard
Apps
Windows platform services
Kernel
Operating System
Critical system processes
Kernel
Microsoft Defender System Guard
Device hardware
Hypervisor

Demo Sandbox



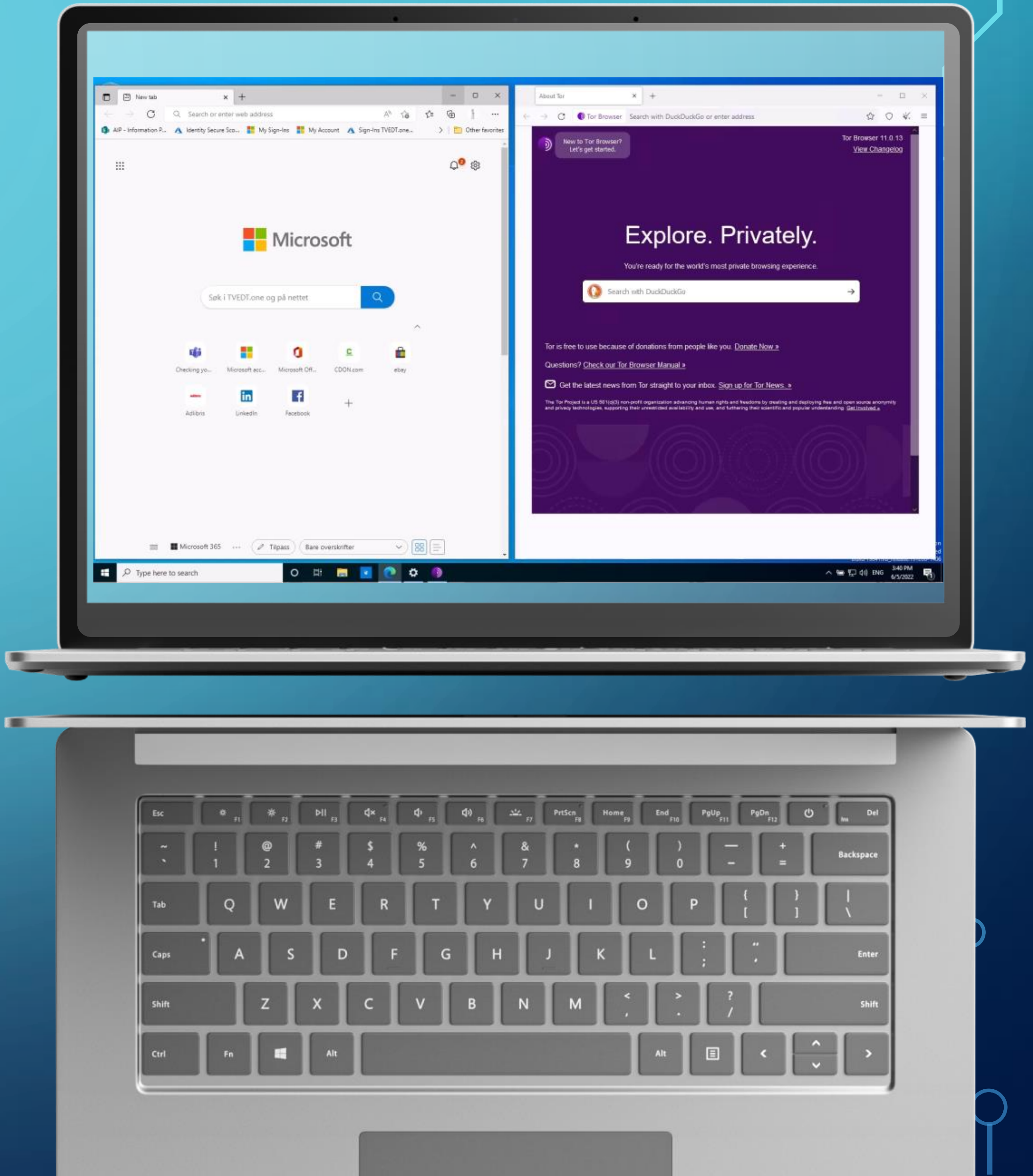
```
<Configuration>
<VGpu>Disable</VGpu>
<Networking>Enable</Networking>
<MappedFolders>
    <MappedFolder>
        <HostFolder>D:\Users\olavt\OneDrive\Tools\SandBox\setup-files</HostFolder>
            <ReadOnly>false</ReadOnly>
      </MappedFolder>
</MappedFolders>
<LogonCommand>
    <Command>explorer.exe C:\Users\WDAGUtilityAccount\Desktop\setup-files\Prep.cmd</Command>
</LogonCommand>
</Configuration>
```

Config files:
https://github.com/OTvedt/Scripts-For-Sharing

CLOUD AI

- Microsoft Defender for Identity
  - User risk
  - Sign-in risk
- Microsoft Defender for Endpoint
- Microsoft Defender for Office
- Microsoft Endpoint Manager
- Smart App Control
- And so on…

Demo Sign-in risk


Microsoft
Søk i TVEDT.one og på nettet
Tor Browser 11.0.13
New to Tor Browser? Let's get started.
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Tor is free to use because of donations from people like you. Donate Now »
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »
Type here to search

Demo JIT Admin

FROM CHIP TO CLOUD

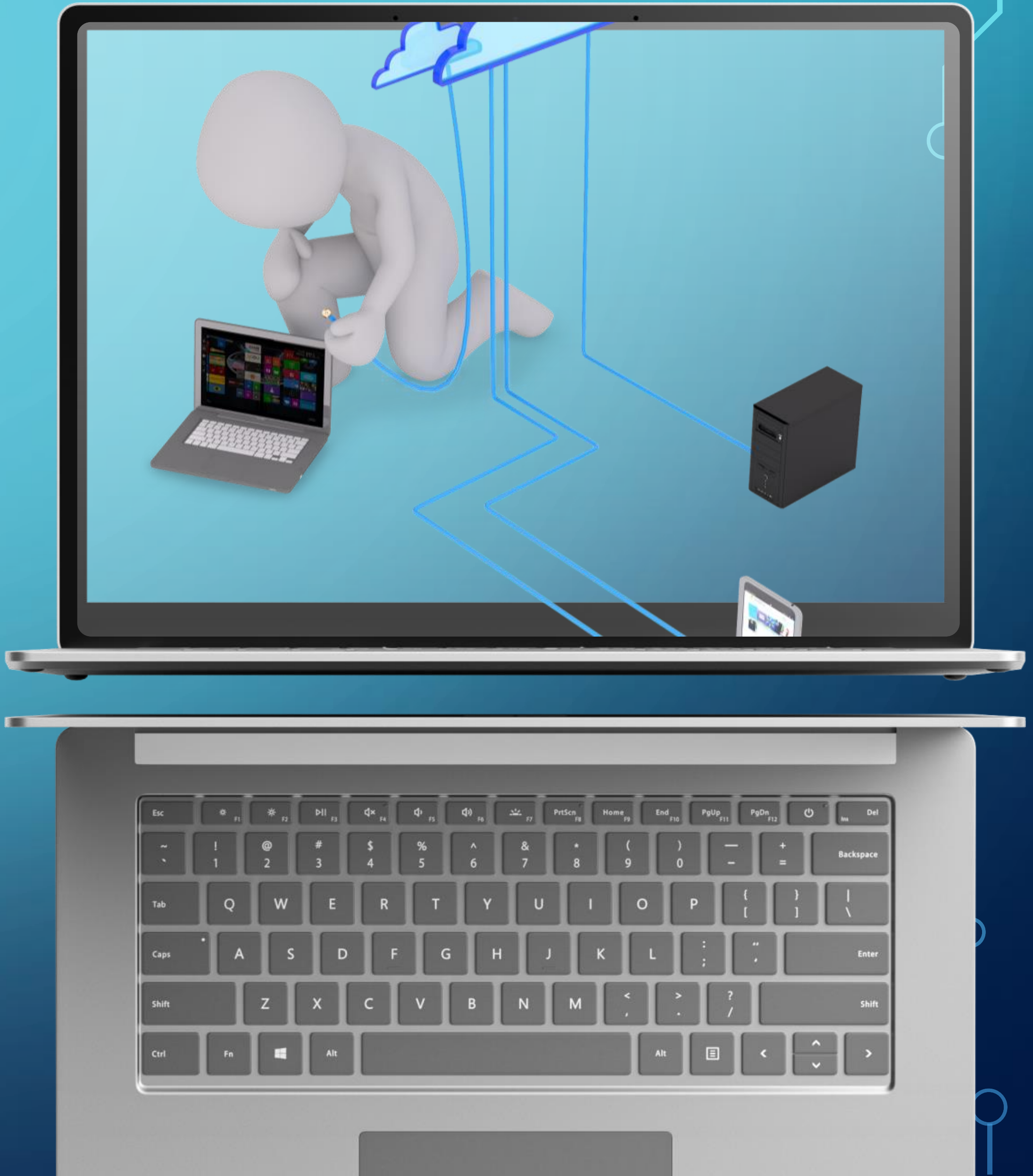
1.Cloud

2.Identity and Privacy

3.Applications

4.Operating System

5.Hardware/The Chips



SPEAKER
OLAV BLUESCREEN

SparebankenVest
Azure Janitor

- 15 x MVP
  - Setup & Deployment
  - Software Packaging, Deployment & Servicing
  - Windows Expert – IT Pro
  - Office and Applications
  - Cloud & Server Installation and Servicing
  - Cloud and Datacenter

olavtwitt

https://www.linkedin.com/in/otvedt/

https://olavtvedt.blogspot.com/

https://github.com/OTvedt/Scripts-For-Sharing

https://www.youtube.com/@bluescreenbrothers

SPEAKER
ALEX BLUESCREEN

amesto
Fortytwo

M365 Janitor

- 9x MVP
  - Surface
  - Windows and Devices for IT
- 5 x MVP Windows Insider

alexsolaat

https://www.linkedin.com/in/alexsolaat/

https://solaat.no/

https://www.youtube.com/@bluescreenbrothers

GIVE US YOUR FEEDBACK!

Cloud Technology Townhall Tallinn session feedback