

#ScottishSummit2024

TWISTIWIKLW!



#ScottishSummit2024

The Windows 11 security tips I wish I knew last week!

Alexander Solaat Rødland & Olav Tvedt



Thank You to our Sponsors...



Platinum Sponsor



Gold Sponsors



#ScottishSummit2024

Thank You to our Sponsors...



With Thanks



#ScottishSummit2024

Alternative Speaker Bio



- 11 years Microsoft MVP
- I'm trying to (re-)build a W98 computer
- AI ranger in Storebrand
- I travel alone

***"It's easier to stay out,
than get out"***



#ScottishSummit2024

Olav Tvedt

Cloud Dude
Sparebanken Vest



- 17 x MVP Azure
- I know MS DOS!
- I am still learning Azure

"I never LOSE, I either WIN or LEARN"



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



<https://olavtvedt.blogspot.com/>



[olavtwitt](#)



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



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



#ScottishSummit2024

"Quotes, either from
Shakespeare, or a senior
technical expert make you
look smarter, like this one"
– Alexander 2024



"...Not a tech problem, it is
a 100% people problem..."

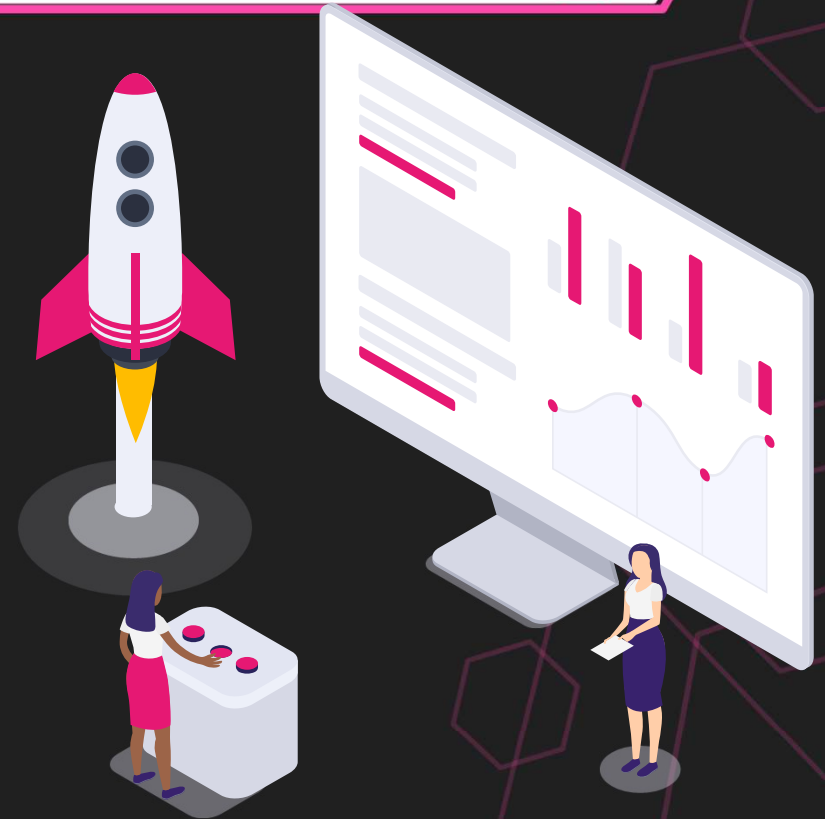
– Scott Hanselmann
Scottish Summit 2024





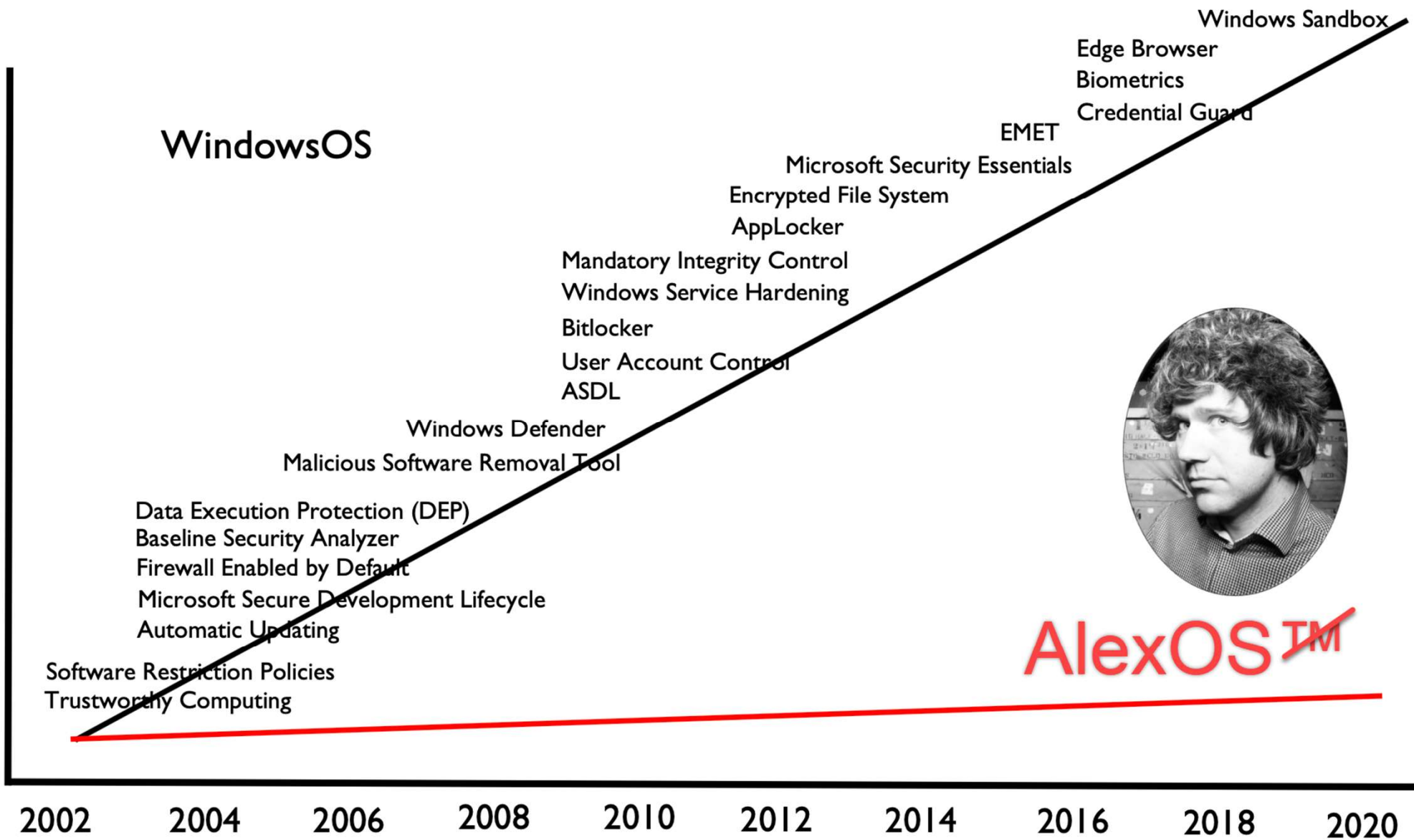
Security – ABC

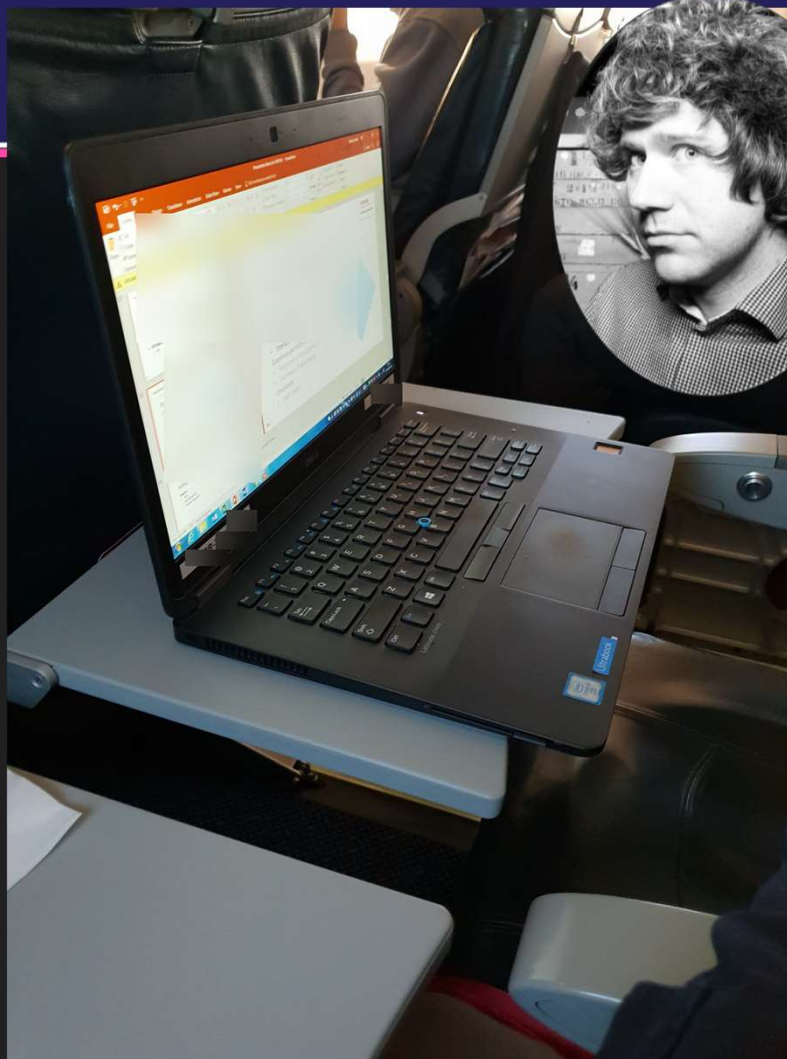
Let us start with the foundation...



#ScottishSummit2024

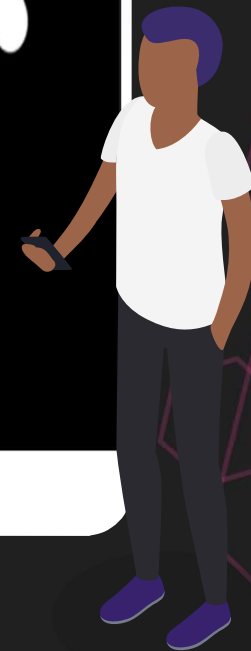
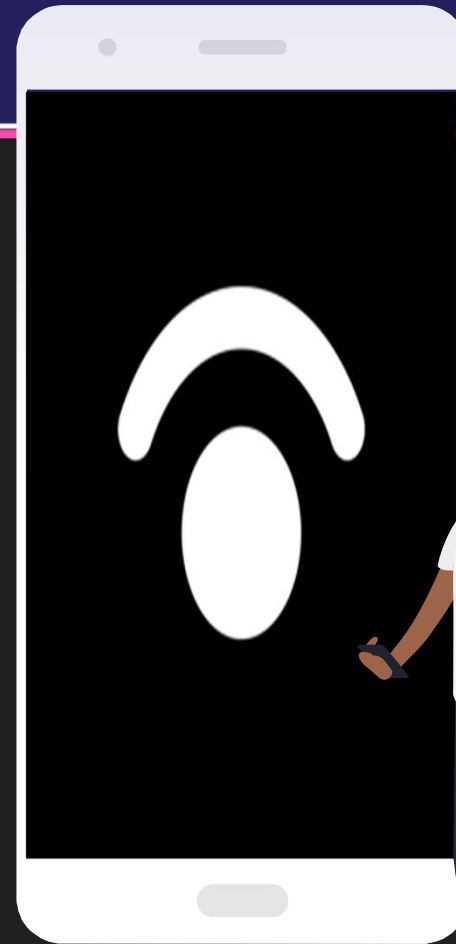
Security Controls





#ScottishSummit2024

Windows hello?

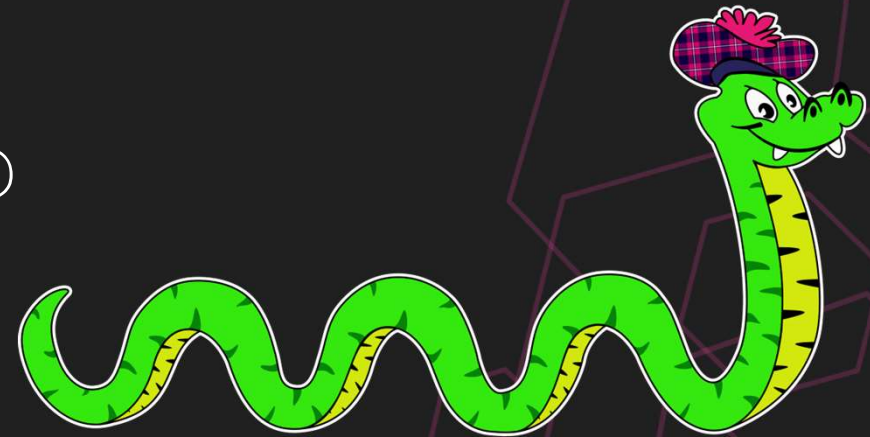


#ScottishSummit2024



What IS a Windows 11 PC?

The foundation – one more time!



#ScottishSummit2024

Announcing Windows 11 Insider Preview Build 25905

Written By
Amanda Langowski
Brandon LeBlanc

published
July 12, 2023

Hello Windows Insiders, today we are releasing **Windows 11 Insider Preview Build 25905** to the Canary Channel. We are releasing ISOs for this build – they can be [downloaded here](#).

Starting with today's build, Windows Insiders in the Canary Channel will notice that the name of the branch shown in the desktop watermark has changed back to RS_PRERELEASE. As a result of this change, Insiders will notice that some features that were previously removed temporarily with the switch over to ZN_RELEASE have now returned – in addition to some new features mentioned below.

Windows 11, version 24H2 includes all the features and capabilities delivered as part of continuous innovation to Windows 11, now enabled by default. These include:

Rust in the Windows Kernel

Rust offers advantages in reliability and security over traditional programs written in C/C++. This preview shipped with an early implementation of critical kernel features in safe Rust. Specifically, `win32kbase_rs.sys` contains a new implementation of [GDI region](#). While this is a small trial, we will continue to increase the usage of Rust in the kernel. Stay tuned!

[We are beginning to roll this out, so the experience isn't available to all Insiders in the Canary Channel just yet as we plan to monitor feedback and see how it lands before pushing it out to everyone.]

Why should → I ← upgrade?



- ▶ VBS
- ▶ HVCI
- ▶ W11 recieve new features



#ScottishSummit2024

Coming availability of the newest AI experiences for Copilot+ PCs

We continue to introduce new AI features that light up more natural and conversational engagement with your devices, with experiences you can only get with [Copilot+ PCs](#). Windows Insiders with Copilot+ PCs will be the first to experience these new features, leveraging the valuable expertise of this community before they become broadly available to customers, with a phased rollout to select devices and markets beginning in November. We plan to [regularly share more information on the status](#) of each new feature and app closer to the availability date, including by region and device silicon technology. When these new features and apps become more widely available they will be released to Copilot+ PCs via:

Windows Update:

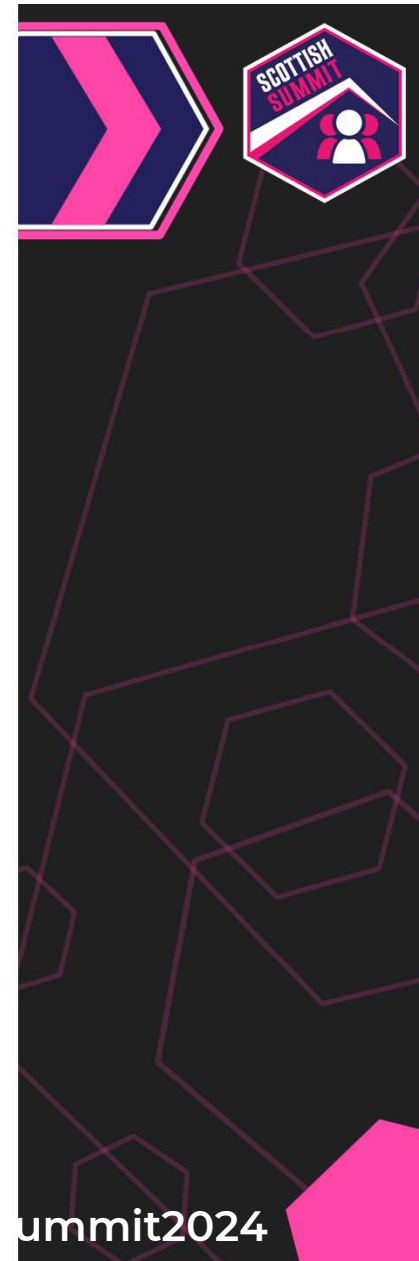
- Recall (Preview)¹
- Click to Do (Preview)
- Improved Windows Search

App updates from the Microsoft Store:

- Super resolution in Photos
- Generative fill and erase in Paint

The Windows 11 2024 Update

Starting today, we begin to release the Windows 11 2024 Update, also referred to as Windows 11, version 24H2. This update is a full operating system (OS) swap that contains new foundational elements required to deliver transformational AI experiences and exceptional performance. You can learn more about all the new features including enhanced battery saver; Bluetooth LE audio; HDR background support and support for Wi-Fi 7 in [What's new inside this update](#).



Why should → I ← upgrade?



- ▶ VBS
- ▶ HVCI
- ▶ W11 recieve new features
- ▶ AND...



#ScottishSummit2024

Who are we fooling anyways?!



endoflife.date

Search endoflife.date

Tags Recommendations Contribute Source API Release Data

Matomo
Mattermost
Mautic
MediaWiki
Meilisearch
Memcached
Micronaut Framework
Microsoft .NET
Microsoft .NET Framework
Microsoft Build of OpenJDK
Microsoft Exchange
Microsoft Nano Server
Microsoft Office
Microsoft PowerShell

Microsoft Windows

Microsoft OS WINDOWS

Last updated on 26 August 2024

 Microsoft Windows is the operating system developed by Microsoft Corporation to run on personal computers.

Release	Released	Active Support	Security Support	Latest
11 23H2 (E)	11 months ago (31 Oct 2023)	Ends in 2 years (10 Nov 2026)	Ends in 2 years (10 Nov 2026)	10.0.22631
11 23H2 (W)	11 months ago (31 Oct 2023)	Ends in 1 year (11 Nov 2025)	Ends in 1 year (11 Nov 2025)	10.0.22631
10 22H2	1 year and 11 months ago (18 Oct 2022)	Ends in 1 year (14 Oct 2025)	Ends in 1 year (14 Oct 2025)	10.0.19045

#ScottishSummit2024

But moOoOom, I don't want.. AI?!?!>



Paper to PC

Transition from typewriter, papers and handwritten notes and "old" data.



PC to server

From distributed storage, floppys and memory sticks to shared fileshares and centralized storage



Server to cloud

From expensive internal IT management to centralized "shop" in the cloud.



Cloud to...

Guess what, not our first rodeo!

W/10 → W/11?



Problem\Solution	New HW	Technical dept	Modern Security
Non- supported HW			
Upgrade W10-W11	N/A		
Wipe & load			



W/10 → W/11?



Problem\Solution	New HW	Technical dept	Modern Security
Non- supported HW			
Upgrade W10-W11	N/A		
Wipe & load			



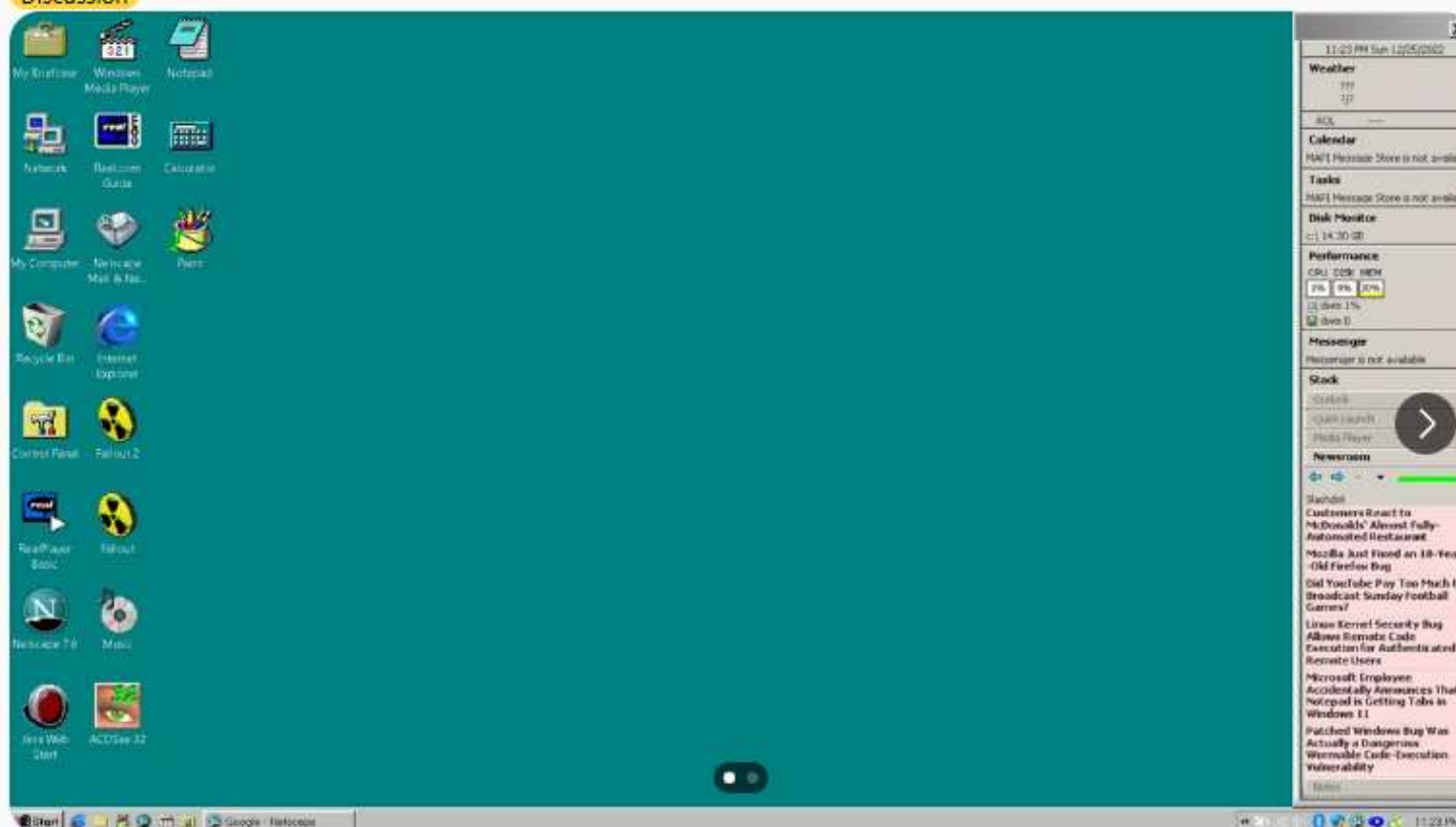


r/Windows11 • 2 yr. ago
[deleted]



I now have the ultimate Win95/98 theme for Windows 11 Correct fonts, taskbar, icons, sound scheme, screen savers, etc... (Nostalgic overload!!!)

Discussion





Wax-on Wax-off

Always start with the basics!



#ScottishSummit2024

Pre-boot



Purchase

Security hardware and features enabled directly from factory – no legacy or post-configuration



Secure Boot

Only authenticated and unaltered components are loaded during the boot process to maintain the integrity of the system



Bitlocker

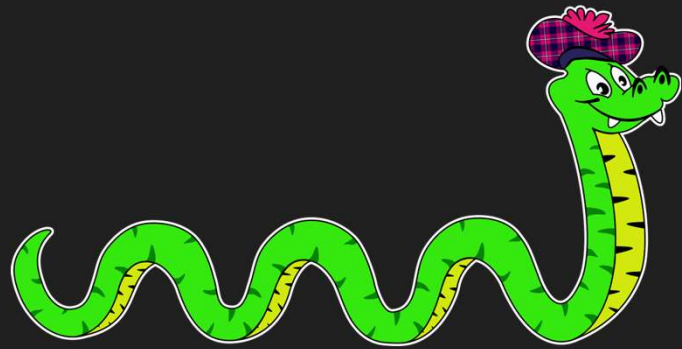
BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices



VBA

Kerberos, NTLM, and Credential Manager isolate secrets by using Virtualization-based security (VBS). Previous versions of Windows stored secrets in its process memory

Defence in levels and layers



Smart App Control



Windows 11

Clean installation of
Windows 11

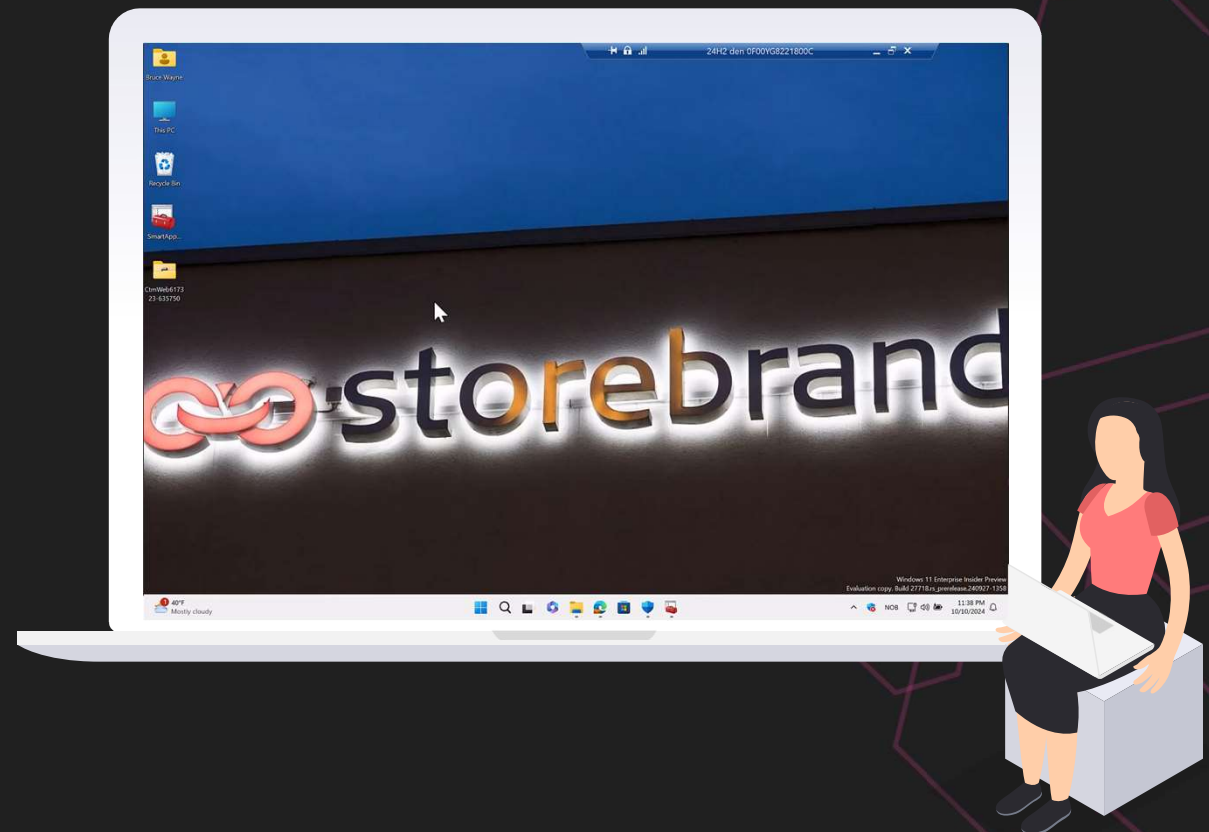
Signature validation

Turned on, valid
signature/certificate
required for apps to
run, blocked if not

Bypass SAC

Evaluation mode,
Off/On,
No bypass for
individual
applications

Smart Appkontroll



#ScottishSummit2024

Search > Files > computrace.msi

Device Inventory > desktop-gv22s72

desktop-gv22s72

No known risks Criticality: None

Overview Incidents and alerts Timeline Security policies Security recommendations Inventories Discovered vulnerabilities Missing KBs Adva

Copy to clipboard Export computrace

Event time	Event	Additional information	Entities	Action type
Oct 10, 2024 11:39:19.561 PM	Computrace.exe deleted setup.exe	T1070.004: File Deletion	userinit.exe > explorer.exe > Computrace.exe > s...	FileDeleted
Oct 10, 2024 11:39:10.654 PM	Event of type [AppControlCIScriptBlocked] observed on device			AppControlCIScriptBlocked
Oct 10, 2024 11:39:10.439 PM	setup.exe loaded ISSetup.dll which has a different PE original file name like...	T1036.005: Match Legitimate Name or Location	explorer.exe > Computrace.exe > setup.exe > IS...	MismatchingOriginalNameWindowsDll
Oct 10, 2024 11:39:07.967 PM	computrace.exe created process setup.exe		explorer.exe > computrace.exe > setup.exe	ProcessCreated
Oct 10, 2024 11:39:05.356 PM	computrace.exe created process setup.exe		explorer.exe > computrace.exe > setup.exe	ProcessCreated
Oct 10, 2024 11:39:04.224 PM	explorer.exe created process Computrace.exe		userinit.exe > explorer.exe > Computrace.exe	ProcessCreated
Oct 10, 2024 11:39:04.218 PM	User AzureAD\BruceWayne launched process Computrace.exe	T1204: User Execution	winlogon.exe > userinit.exe > explorer.exe > Co...	UserFileExecution
Oct 10, 2024 11:39:04.218 PM	explorer.exe created process Computrace.exe with an empty PE original fil...	T1036.005: Match Legitimate Name or Location	winlogon.exe > userinit.exe > explorer.exe > Co...	MismatchingOriginalNameWindowsBinary
Oct 10, 2024 11:37:50.476 PM	Computrace.exe deleted setup.exe	T1070.004: File Deletion	userinit.exe > explorer.exe > Computrace.exe > s...	FileDeleted
Oct 10, 2024 11:37:28.227 PM	computrace.exe created process setup.exe		explorer.exe > computrace.exe > setup.exe	ProcessCreated
Oct 10, 2024 11:37:27.436 PM	explorer.exe created process Computrace.exe		userinit.exe > explorer.exe > Computrace.exe	ProcessCreated
Oct 10, 2024 11:37:27.432 PM	User AzureAD\BruceWayne launched process Computrace.exe	T1204: User Execution	winlogon.exe > userinit.exe > explorer.exe > Co...	UserFileExecution
Oct 10, 2024 11:37:27.432 PM	explorer.exe created process Computrace.exe with an empty PE original fil...	T1036.005: Match Legitimate Name or Location	winlogon.exe > userinit.exe > explorer.exe > Co...	MismatchingOriginalNameWindowsBinary
Oct 10, 2024 11:28:43.908 PM	Computrace.exe deleted setup.exe	T1070.004: File Deletion	userinit.exe > explorer.exe > Computrace.exe > s...	FileDeleted
Oct 10, 2024 11:28:43.765 PM	Computrace.exe opened named pipe \Device\NamedPipe\srvsvc	T1559: Inter-Process Communication	userinit.exe > explorer.exe > Computrace.exe	NamedPipeEvent
Oct 10, 2024 11:28:40.652 PM	Unknown process file observed on host		Computrace.exe	AntivirusReport
Oct 10, 2024 11:28:40.652 PM	Unknown process file observed on host		Computrace.exe	AntivirusReport
Oct 10, 2024 11:28:37.059 PM	Event of type [AppControlCIScriptBlocked] observed on device			AppControlCIScriptBlocked
Oct 10, 2024 11:28:36.161 PM	setup.exe loaded ISSetup.dll which has a different PE original file name like...	T1036.005: Match Legitimate Name or Location	explorer.exe > Computrace.exe > setup.exe > IS...	MismatchingOriginalNameWindowsDll

Event of type [AppControlCIScriptBlocked] observed on device

Event info

Event

Event of type [AppControlCIScriptBlocked] observed on device

Event time

Oct 10, 2024 11:39:10 PM

Action type

AppControlCIScriptBlocked

User

azuread\brucewayne

Entities

services.exe > svchost.exe > setup.exe > Computrace.msi

Event entities graph

[984] services.exe

[6460] svchost.exe -k netsvcs -p -s Appinfo

[11296] setup.exe

Process ID

11296

Execution time

Oct 10, 2024 11:39:07 PM

Command line

"setup.exe"

Image file path

c:\users\brucewayne\appdata\local\temp\varsx0\setup.exe

Image file SHA1

7d8cd844ee9c57b47db05fe9112d1781f4a8e812

Image file SHA256

fd0e7280847eed363c52386103d5b539e7eb41a30d217c747210a9f6724cd5d2

Signer

Absolute Software Corp.
Revoked certificate

Issuer

VeriSign Class 3 Code Signing
2010 CA

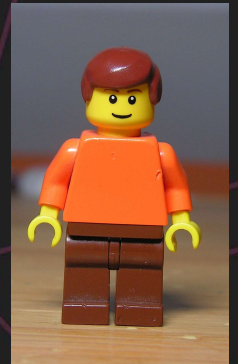
VirusTotal detection ratio

0/70

Computrace.msi

Hunt for related events

What local admin?



#ScottishSummit2024

What if?



/ Windows Insider Blog

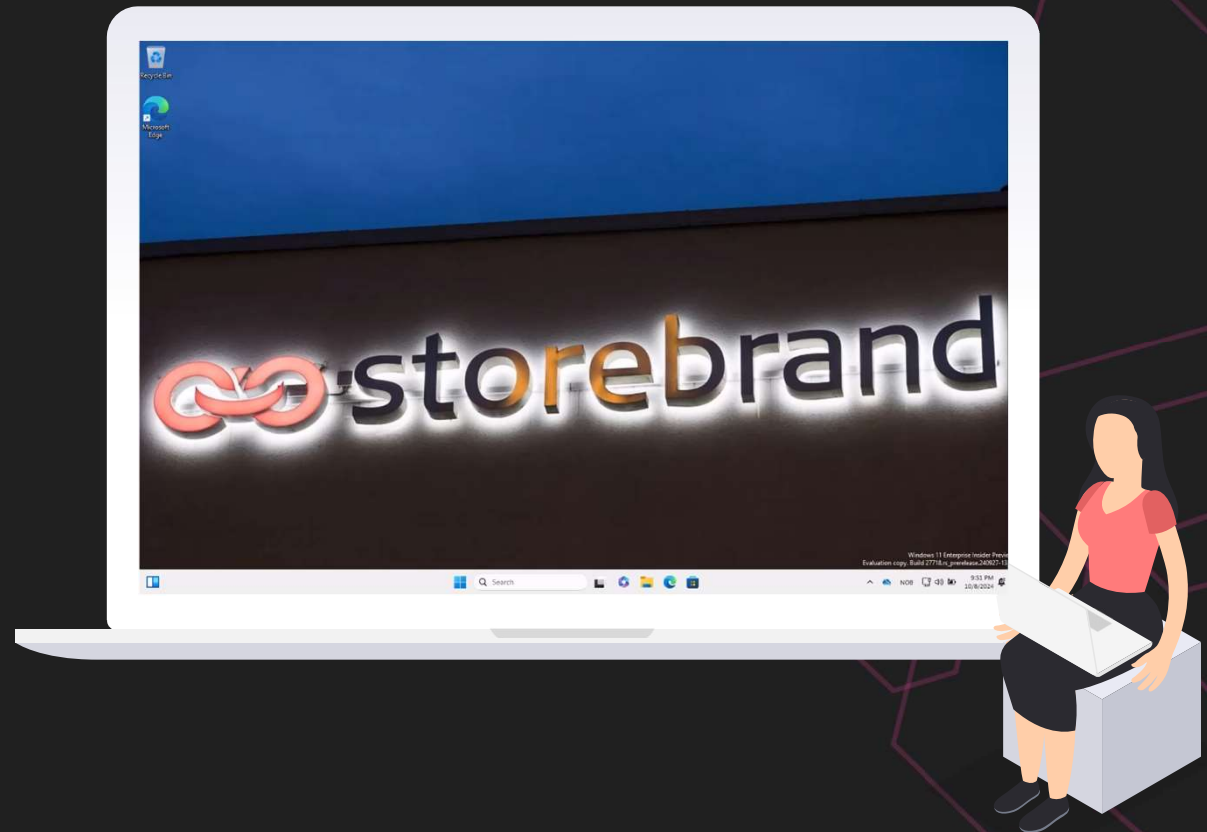
[Administrator protection]

- Administrator protection is an upcoming platform security feature in Windows 11, which aims to protect free floating admin rights for administrator users allowing them to still perform all admin functions with just-in-time admin privileges. This feature is off by default and needs to be enabled via group policy. We plan to share more details about this feature at [Microsoft Ignite](#).



#ScottishSummit2024

Protected admin rights



#ScottishSummit2024

The non-local admin



Microsoft Intune admin center

Home > Devices > Windows > Windows > Enrollment > Windows Autopilot deployment profiles > 42MIWindowsAutopilotZTID > Properties >

Edit profile

1 Out-of-box experience (OOBE) 2 Review + save

Configure the out-of-box experience for your Autopilot devices

Deployment mode

Join to Microsoft Entra ID as

Microsoft Software License Terms

[Important information about hiding license terms](#)

Privacy settings

Specify whether users are administrators or standard users on the device. Note that this setting does not apply to Global Administrator or Company Administrator accounts. These accounts cannot be standard users because they have access to all administrative features in Microsoft Entra ID.

User account type

Allow pre-provisioned deployment

Language (Region)

Automatically configure keyboard

Apply device name template

Create a unique name for your devices. Names must be 15 characters or less, and can contain letters (a-z, A-Z), numbers (0-9), and hyphens. Names must not contain only numbers. Names cannot include a blank space. Use the %SERIAL% macro to add a hardware-specific serial number. Alternatively, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.

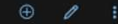
Enter a name *

#ScottishSummit2024



Intune add-in?

Learn / Microsoft Intune / Intune service /



Use Endpoint Privilege Management with Microsoft Intune

Article • 08/01/2024 • 6 contributors

Feedback

In this article

- Prerequisites
- Government cloud support
- Getting started with Endpoint Privilege Management
- Important concepts for Endpoint Privilege Management

[Show 3 more](#)

Note

This capability is available as an Intune add-on. For more information, see [Use Intune Suite add-on capabilities](#).

With Microsoft Intune **Endpoint Privilege Management (EPM)** your organization's users can run as a standard user (without administrator rights) and complete tasks that require elevated privileges. Tasks that commonly require administrative privileges are application installs (like Microsoft 365 Applications), updating device drivers, and running certain Windows diagnostics.

Endpoint Privilege Management supports your [Zero Trust](#) journey by helping your organization achieve a broad user base running with least privilege, while allowing users to still run tasks allowed by your organization to remain productive. For more information, see [Zero Trust with Microsoft Intune](#).

The following sections of this article discuss requirements to use EPM, provide a functional overview of how this capability works, and introduce important concepts for EPM.

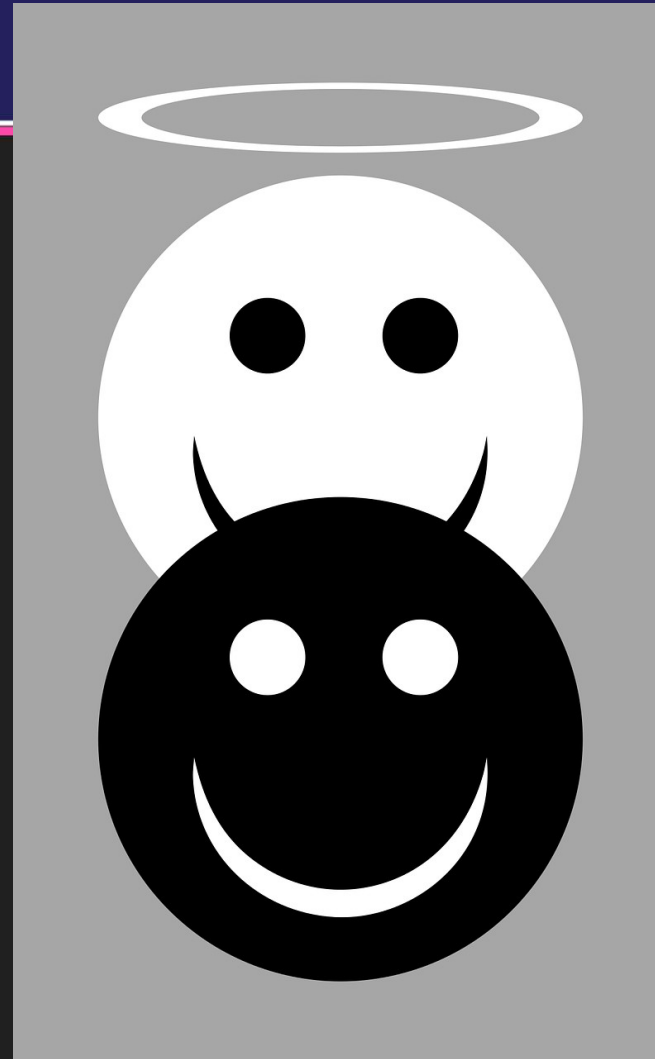
#ScottishSummit2024

Entra ID Joined Device Local Administrator



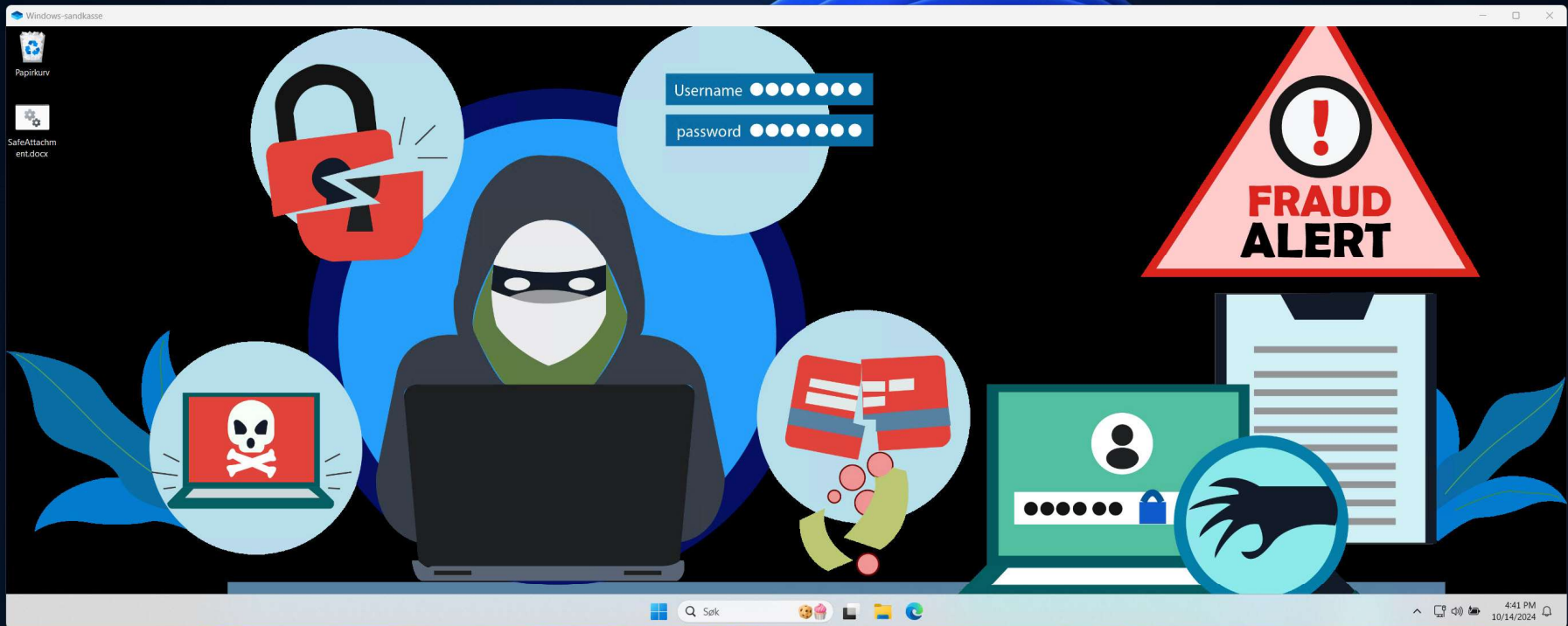
#ScottishSummit2024

Naaah, what
could go wrong
anyways?!





- Alexander Solaat R...
- Denne PCen
- Papirkurv



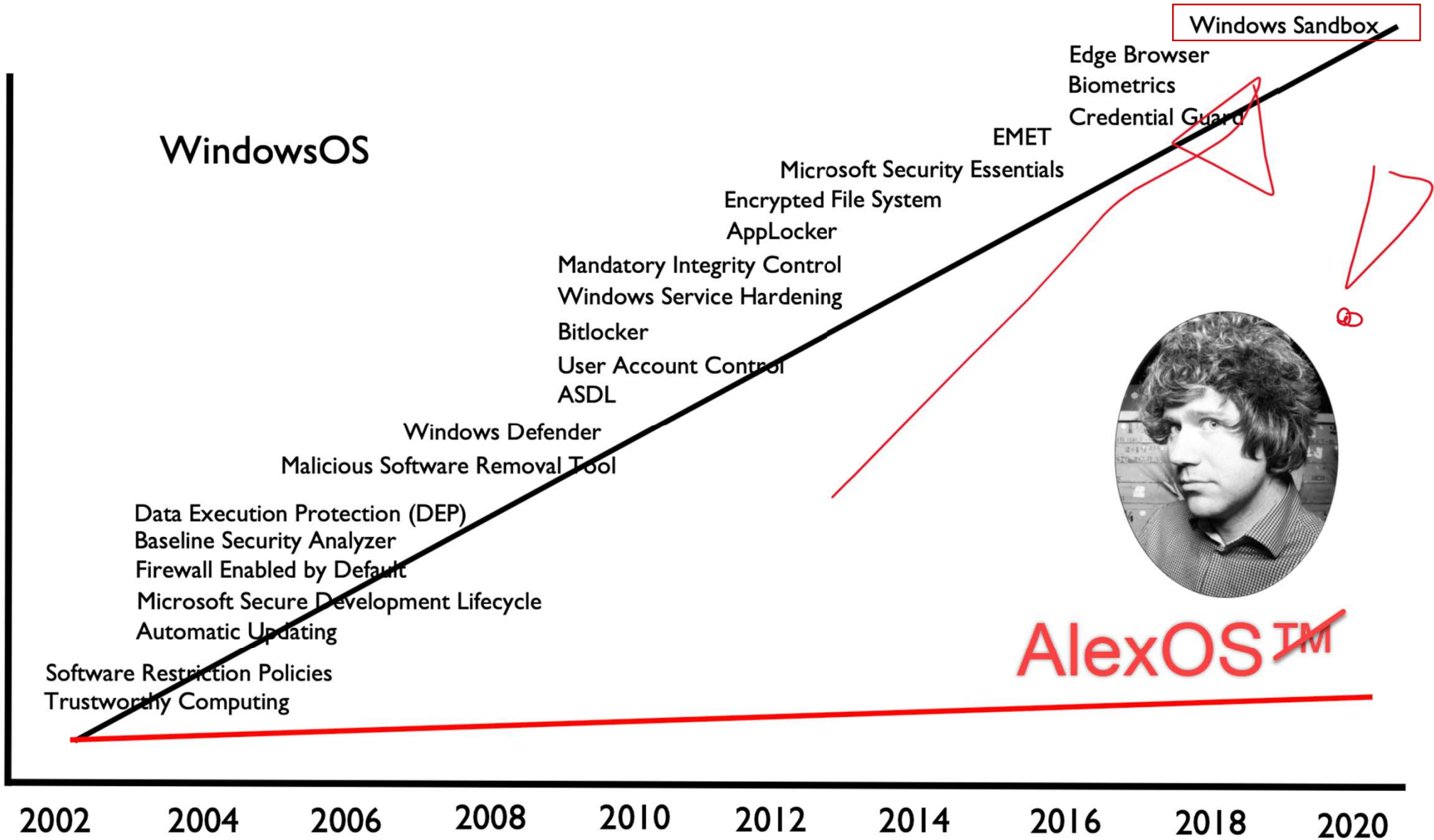
7°C
Delvis sol



16:41
14.10.2024

#ScottishSummit2024

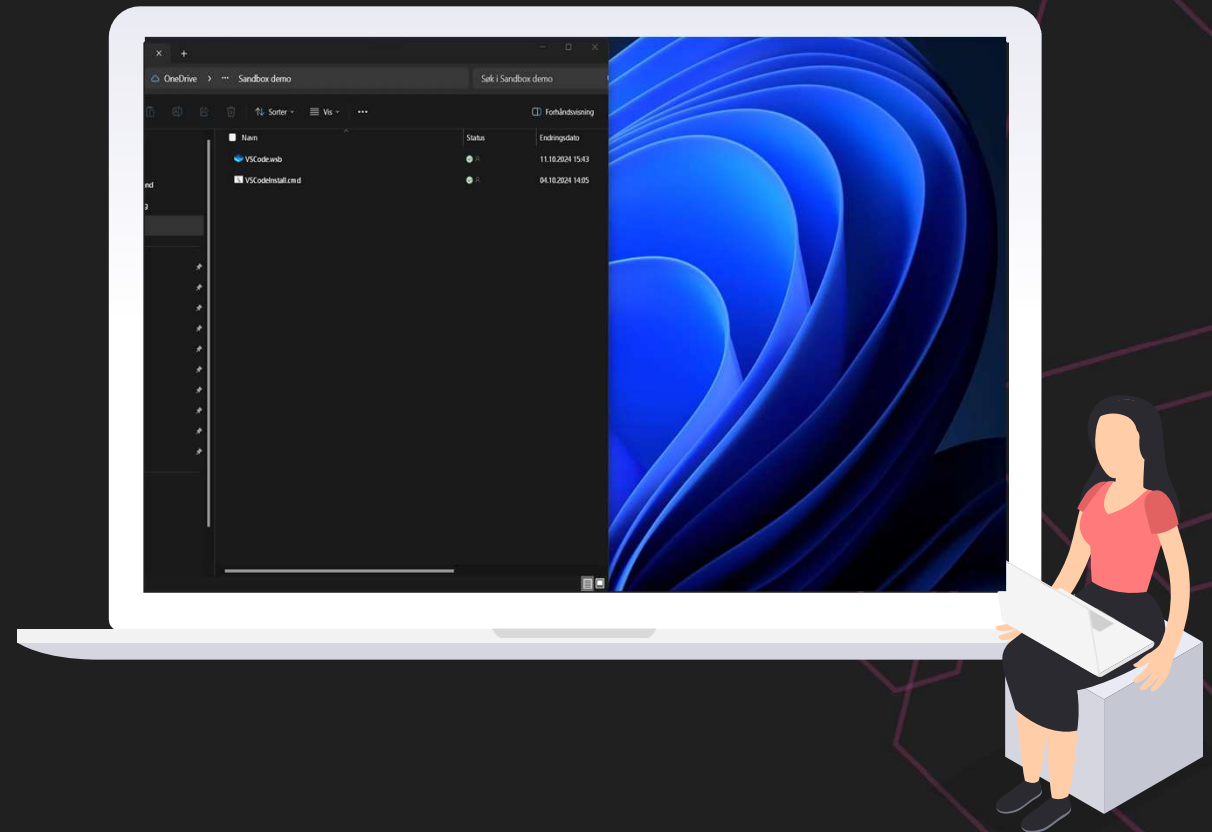
Security Controls



Sandbox

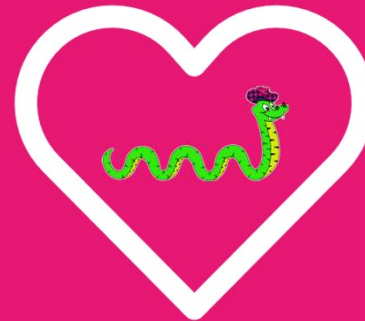


What if v2...



Thank You

- It does not end here
- Implement security features
- Don't annoy the users (too much)
- The presentation however?!
 - THAT ends here!



*"It's OK to
be not OK"*