MVP Dagen

mvpdagen.no

The Windows 11 Security tips and tricks I wish I knew last week

MVP Dagen

The -> Pensjon <- tips and tricks I wish I knew last week

Kron.
fra Storebrand

MVP Dagen

The Windows 11 Security tips and tricks I wish I knew last week

MVP Dagen

Takk til våre sponsorer

mvpdagen.no

Hey!

Jeg er Sanna Diana

Jeg arbeider med Azure Security, Defender og Sentinel hos kunder av Accenture

Du finner meg på LinkedIn Sanna Diana Tomren

MVP Dagen

Hey!

Jeg er Alexander

Jeg arbeider med Microsoft 365, klienter og AI hos Storebrand

Du finner meg også på solaat.no og blåskjermbrødrene @spotify/YouTube

MVP Dagen

“Sitater, enten fra kjentfolk eller fra en kollega kan ofte dekke en hel slide, som dette”

– Alexander 2024

MVP Dagen

“Det perfekte sikkerhetsscenarioet, betinger at du ikke har brukere av løsningen”

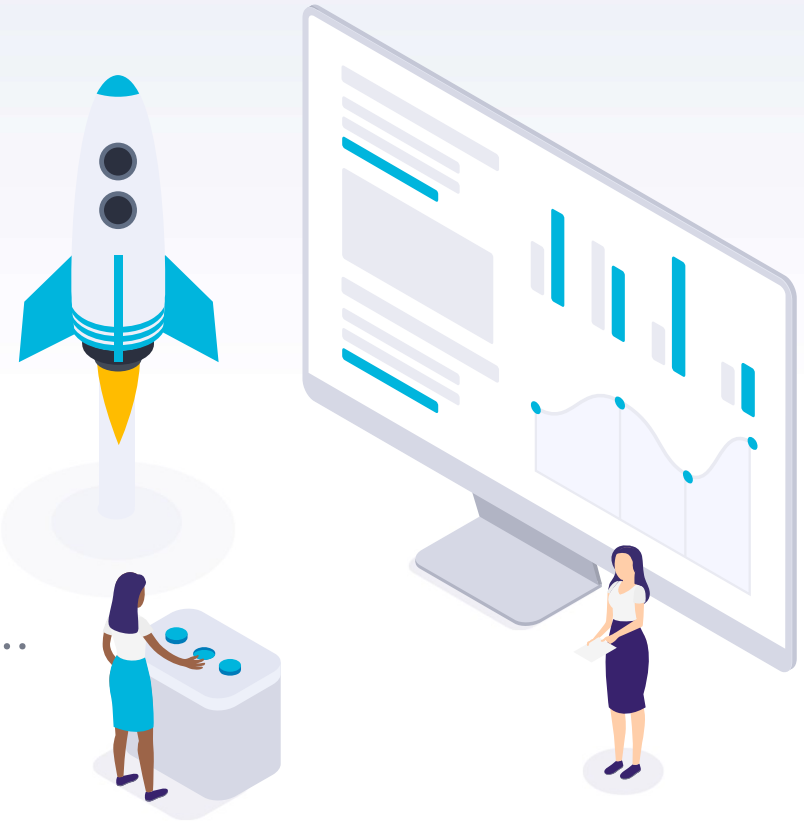
– Alexander 2024

MVP Dagen

1

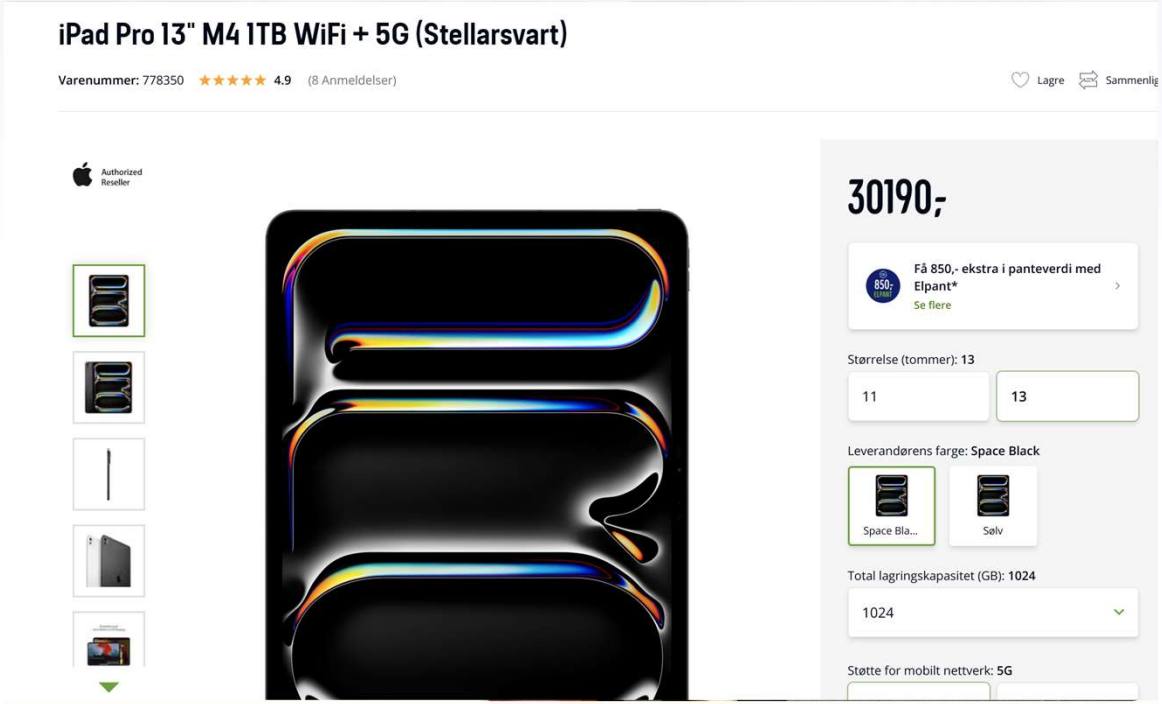
Sikkerhet - ABC

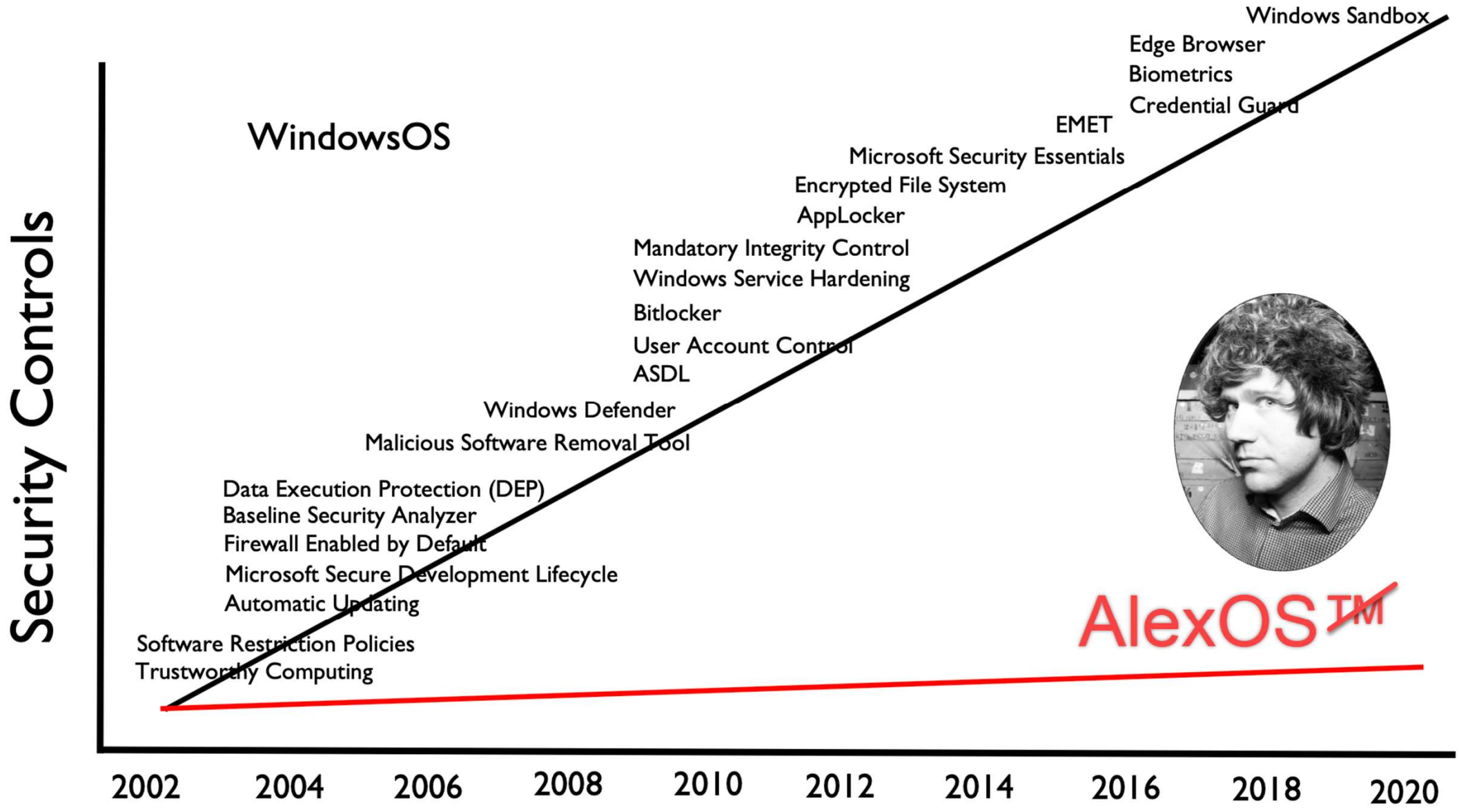
La oss starte med det grunnleggende...



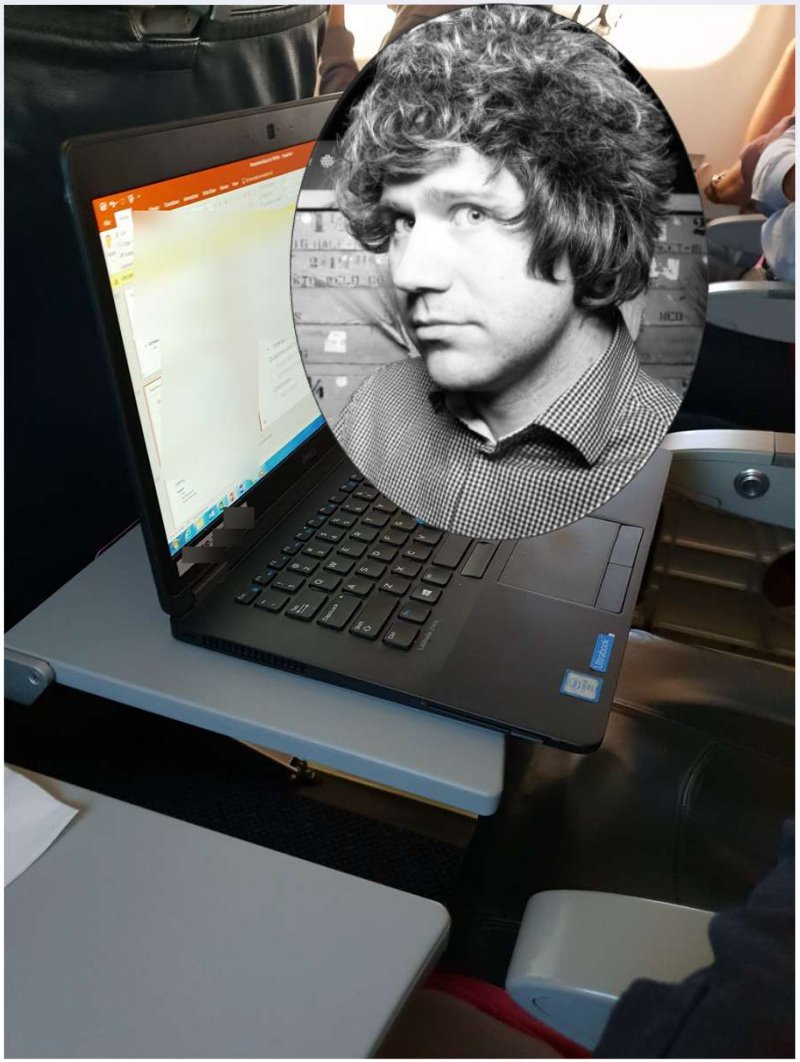
MVP Dagen

Design creep




Security Controls
WindowsOS
Windows Sandbox
Edge Browser
Biometrics
Credential Guard
EMET
Microsoft Security Essentials
Encrypted File System
AppLocker
Mandatory Integrity Control
Windows Service Hardening
Bitlocker
User Account Control
ASDL
Windows Defender
Malicious Software Removal Tool
Data Execution Protection (DEP)
Baseline Security Analyzer
Firewall Enabled by Default
Microsoft Secure Development Lifecycle
Automatic Updating
Software Restriction Policies
Trustworthy Computing
AlexOS™
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020

1

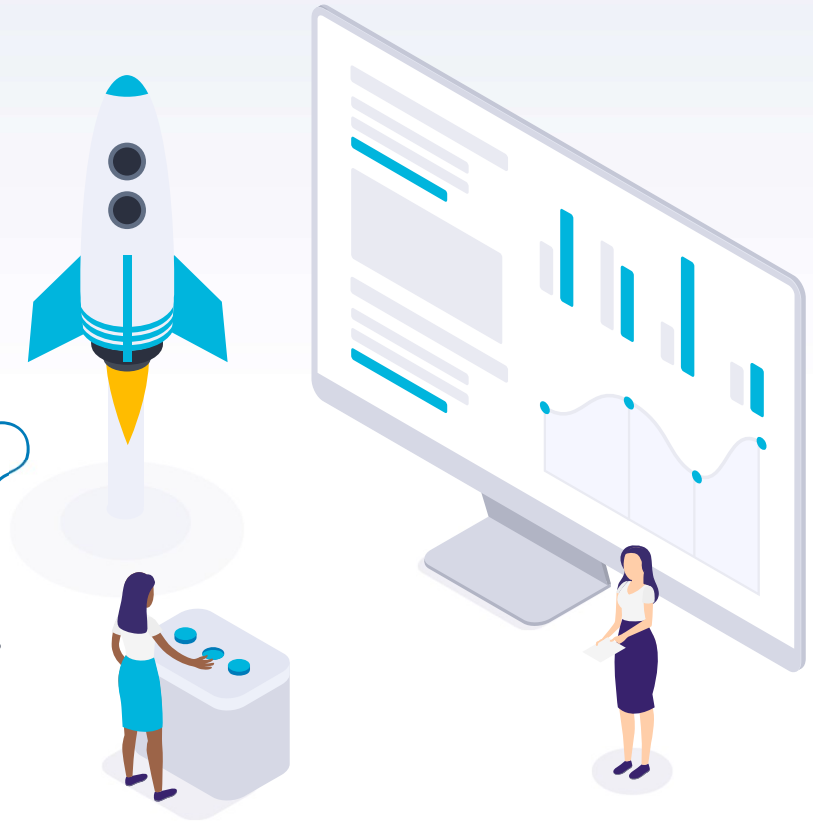


MVP Dagen

2

Hva er en Windows 11 PC?

La oss starte me det grunnleggende...



MVP Dagen

2

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.]

2 Hvorfor skal JEG oppgradere?!

- VBS
- HVCI
- W11 utvikles i features og sikkerhet

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

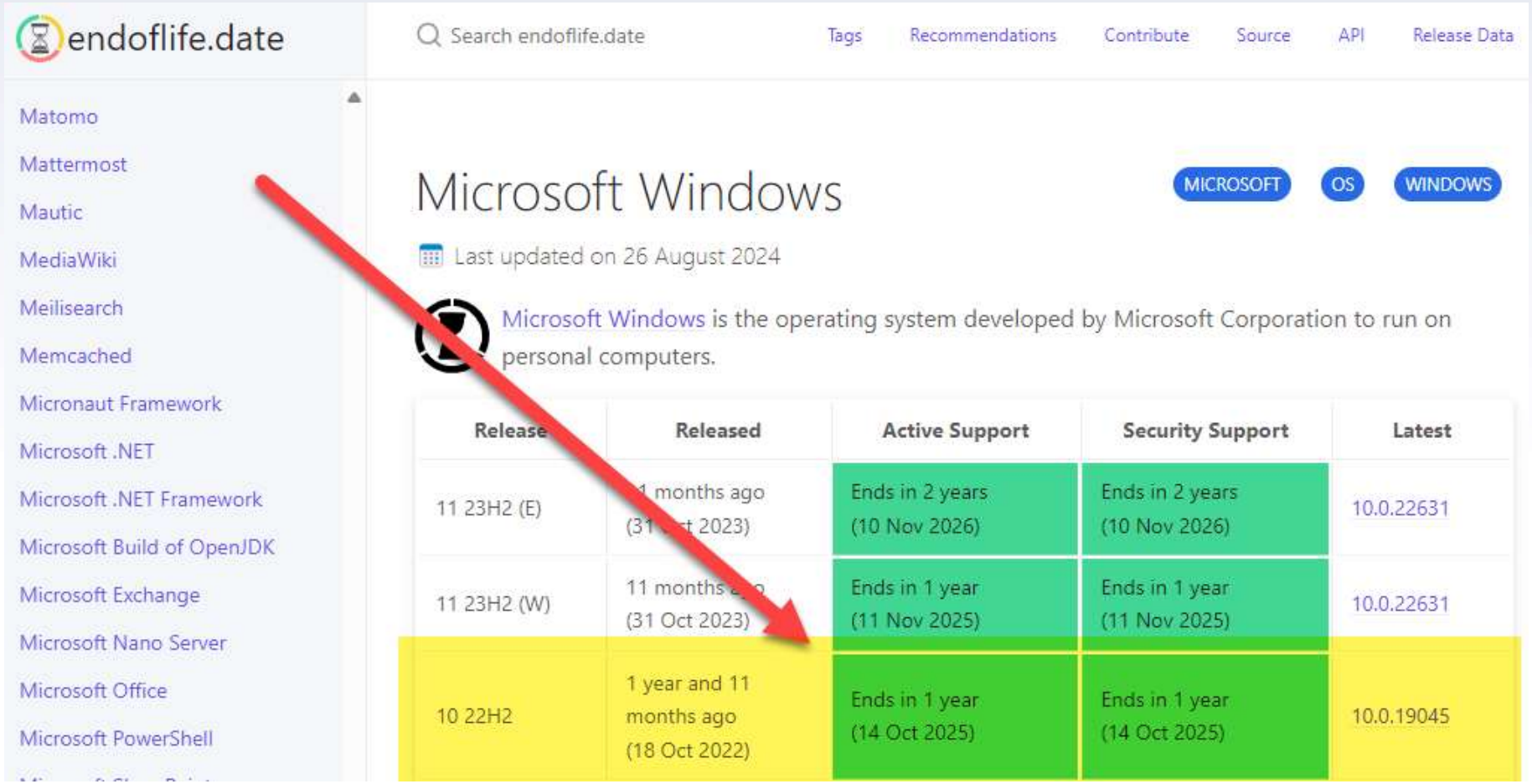
The Windows 11 2024 Update

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.

2

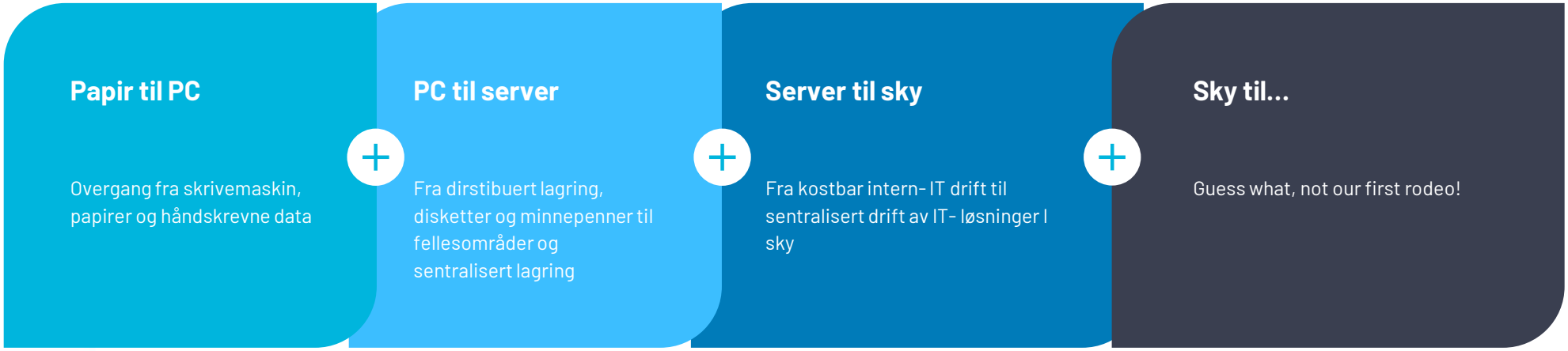
MVP Dagen

2


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)
Ends in 2 years (10 Nov 2026)
Ends in 2 years (10 Nov 2026)
10.0.22631
11 23H2 (W)
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

MVP Dagen

Men jeg vil ikke ha… AI!?!



2 W10 → W11?

Problem\Løsning	Ny HW	Teknisk gjeld	Moderne sikkerhet
Ikke supportert HW	👍	👎	👎
Oppgrader W10-W11	N/A	👍	👎
Wipe & load	⚙	🐷	👍

MVP Dagen

2 W10 → W11?

Problem\Løsning	Ny HW	Teknisk gjeld	Moderne sikkerhet
Ikke supportert HW	👍	👎	👎
Oppgrader W10-W11	N/A	👍	👎
Wipe & load	🐷	🐷	👍

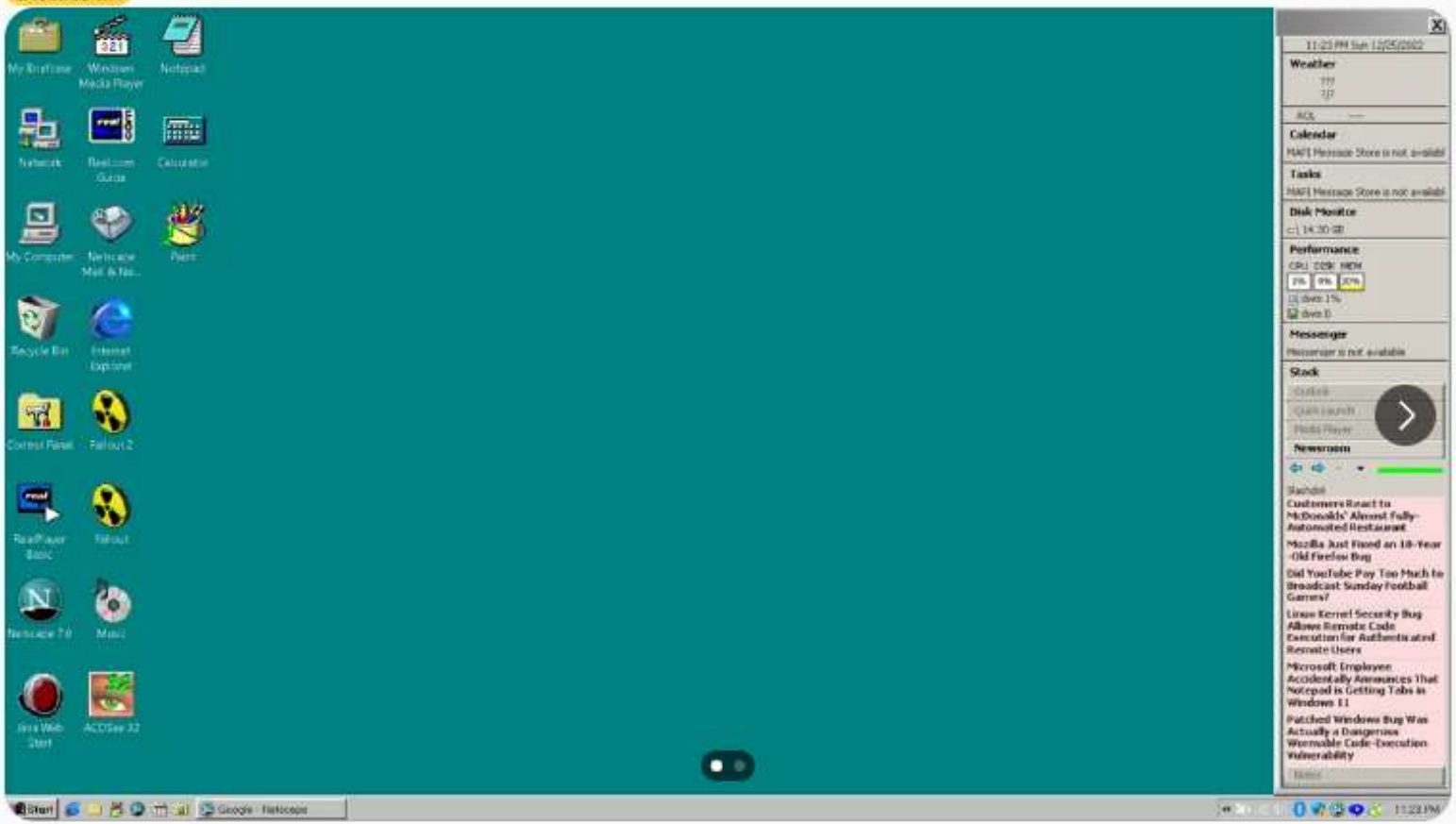
MVP Dagen

3

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



MVP Dagen

3

Wax-on Wax-off

Begynn med det grunnleggende

MVP Dagen

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

Forsvar i lag og nivåer

Smart App Control

Widows 11

Clean installation of Windows 11

Signature validation

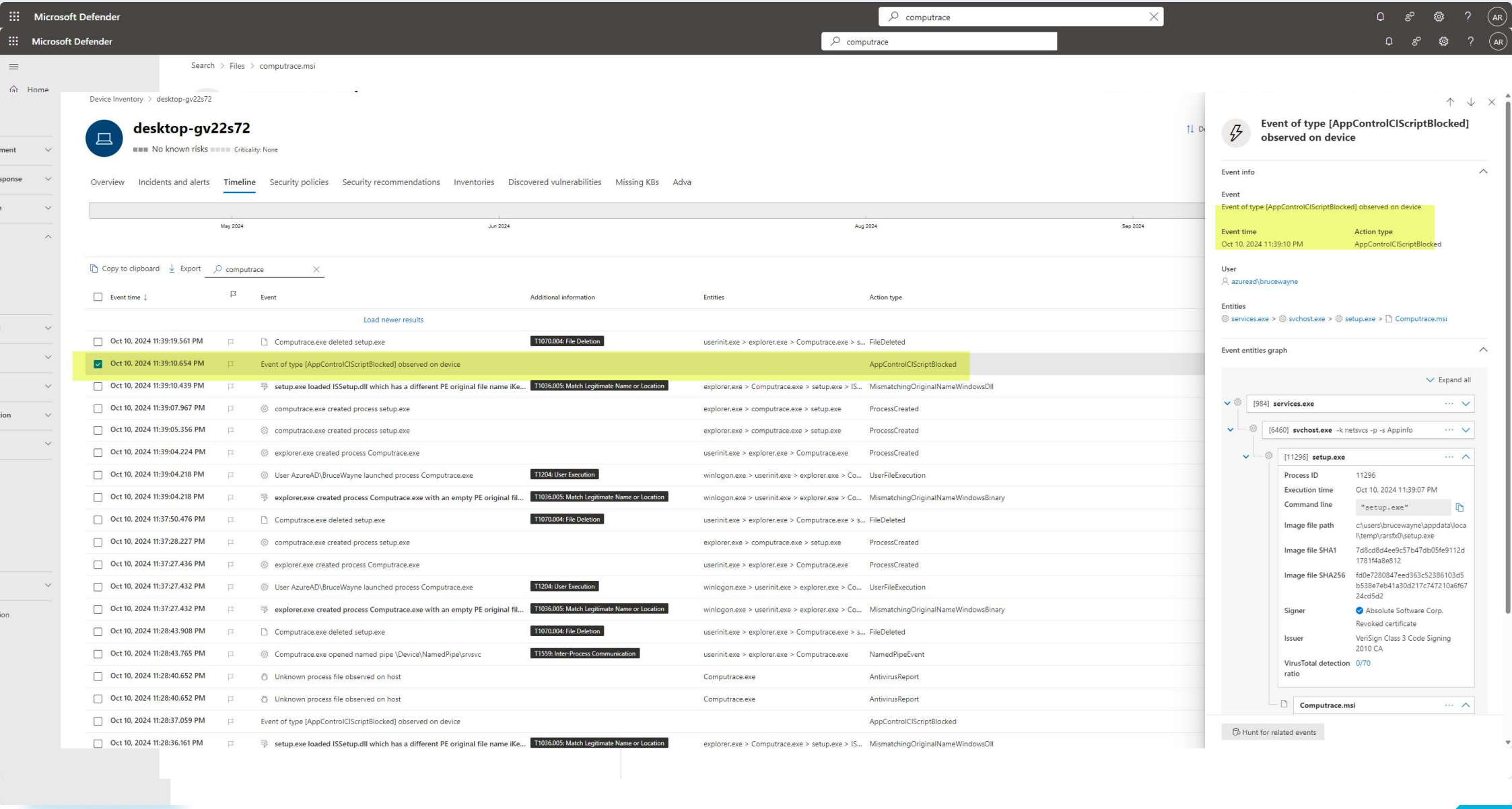
Turned on, valid signature/certificate required for apps to run, blocked if not

Bypass Smart App Control

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

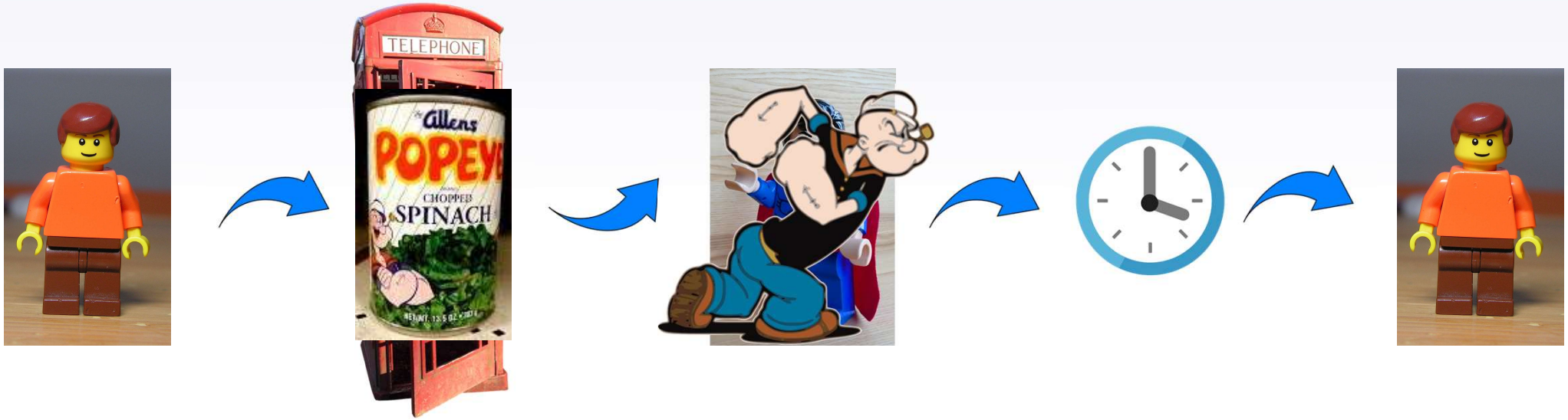
Smart Appkontroll

MVP Dagen


Microsoft Defender
computrace
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
May 2024
Jun 2024
Aug 2024
Sep 2024
Copy to clipboard
Export
Event time
Event
Additional information
Entities
Action type
Load newer results
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 iKe... 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 iKe... 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
Expand all
[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\rarsfx0\setup.exe
Image file SHA1 7d8cd8d4ee9c57b47db05fe9112d1781f4a8e812
Image file SHA256 fd0e7280847eed363c52386103d5b538e7eb41a30d217c747210a6f6724cd5d2
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

Et eventyr …eller?

What local admin?



MVP Dagen

What if?

/ Windows Insider Blog

[Administrator protection]

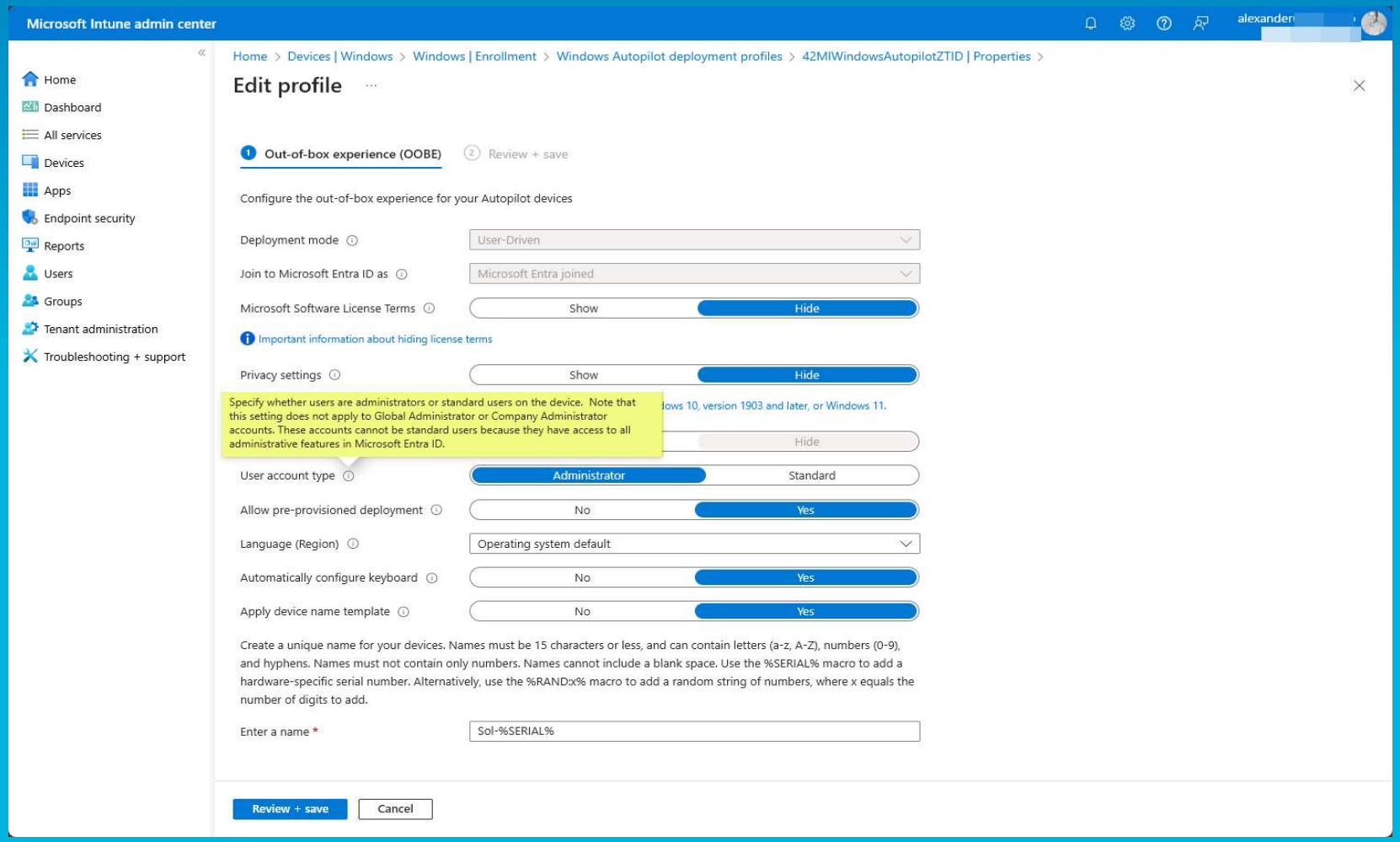
- Administrator protection is an upcoming platform security feature in Windows 11, which aims to protect free floating admin rights for administrator users allowing them to still perform all admin functions with just-in-time admin privileges. This feature is off by default and needs to be enabled via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

MVP Dagen

Protected admin rights

MVP Dagen

The non-local admin



MVP Dagen

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.

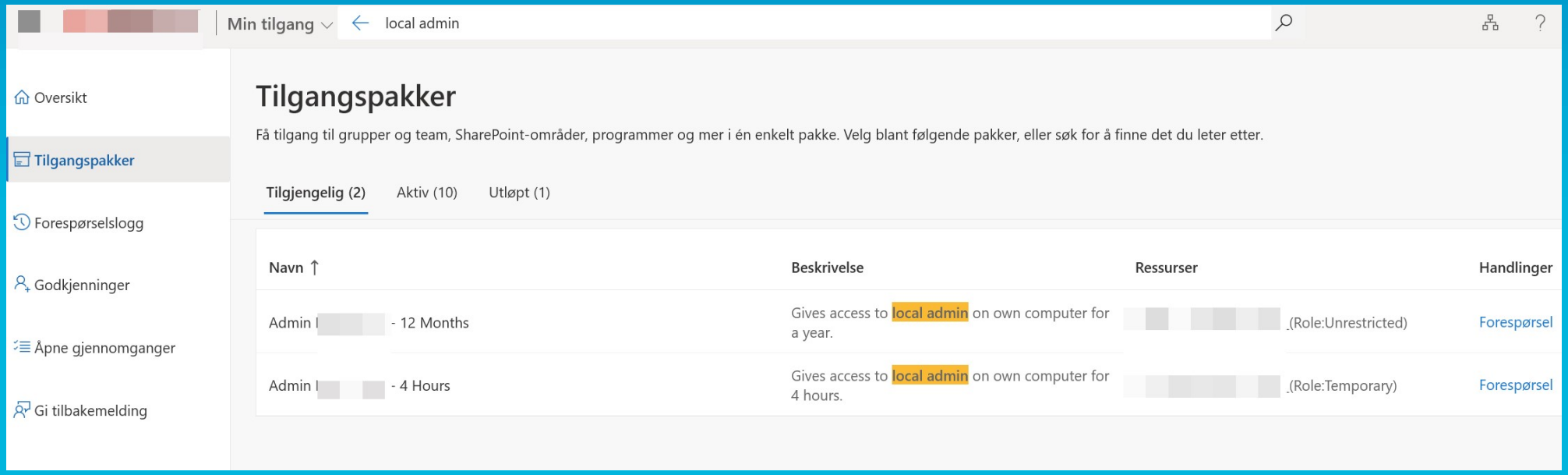
The following sections of this article discuss requirements to use EPM, provide a functional overview of how this capability works, and introduce important concepts for EPM.

MVP Dagen

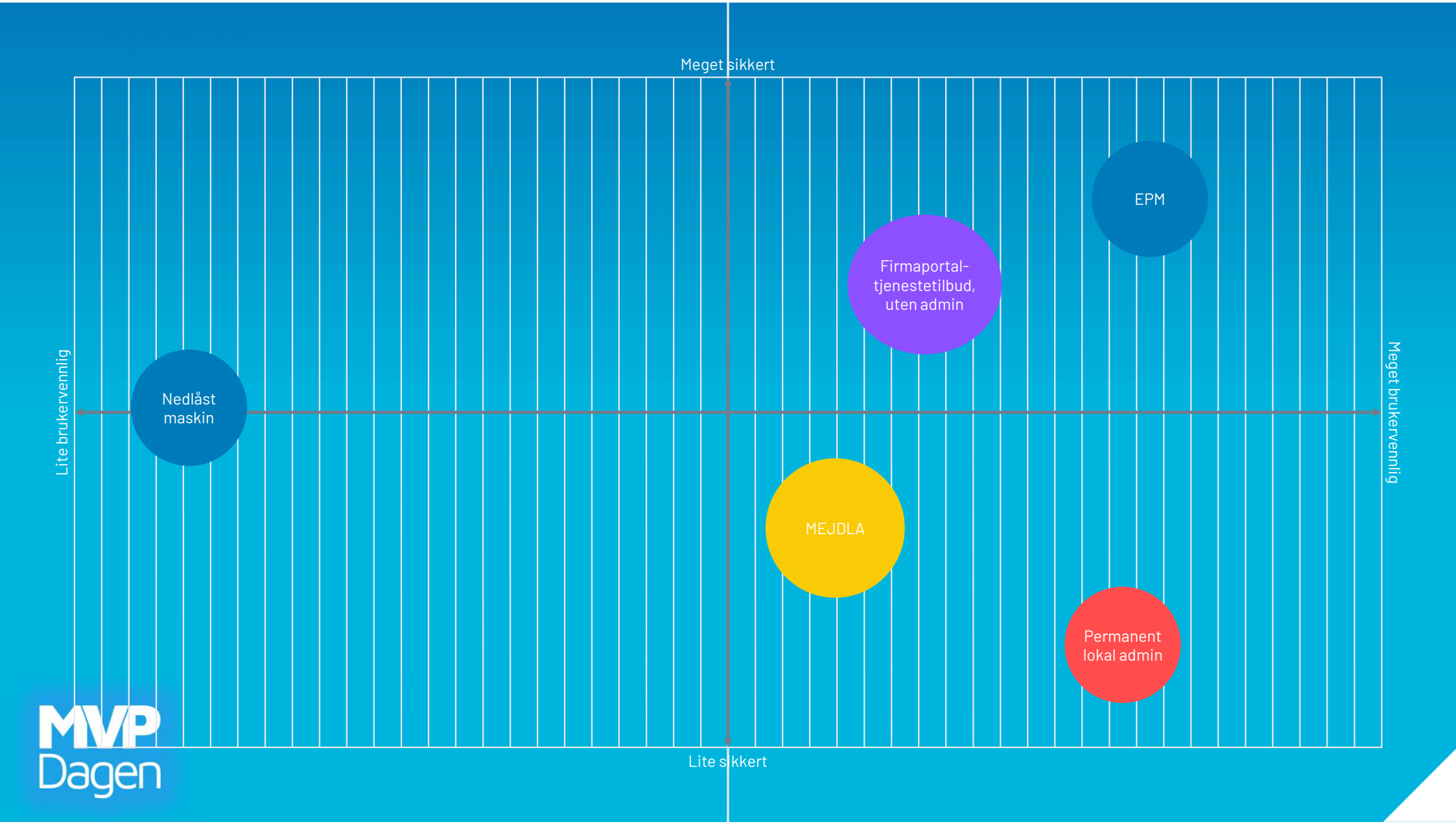
Entra ID Joined Device Local Administrator

MVP Dagen

Access package?



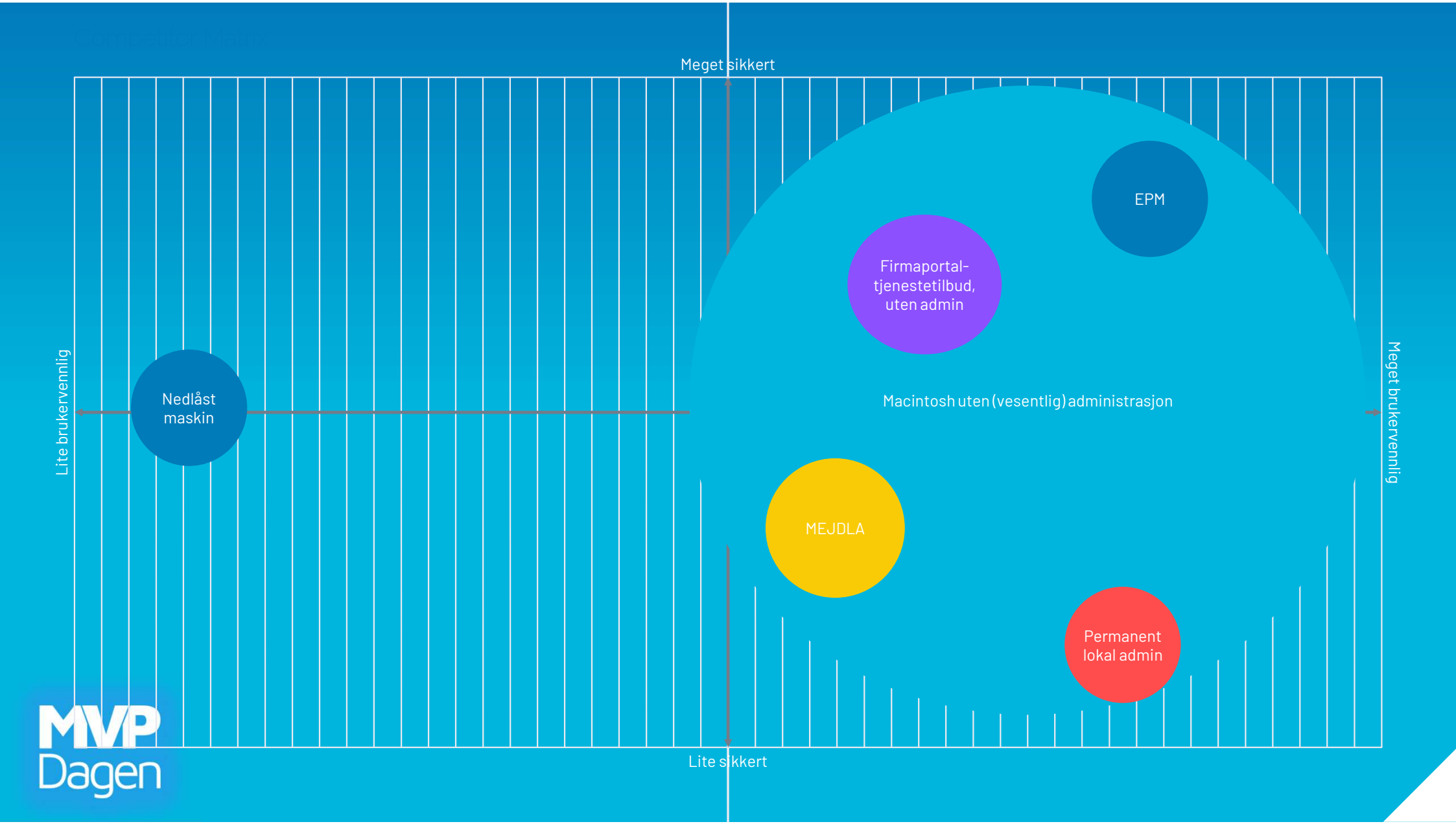
MVP Dagen


Meget sikkert
Lite sikkert
Lite brukervennlig
Meget brukervennlig
Nedlåst maskin
Firmaportal-tjenestetilbud, uten admin
EPM
MEJDLA
Permanent lokal admin

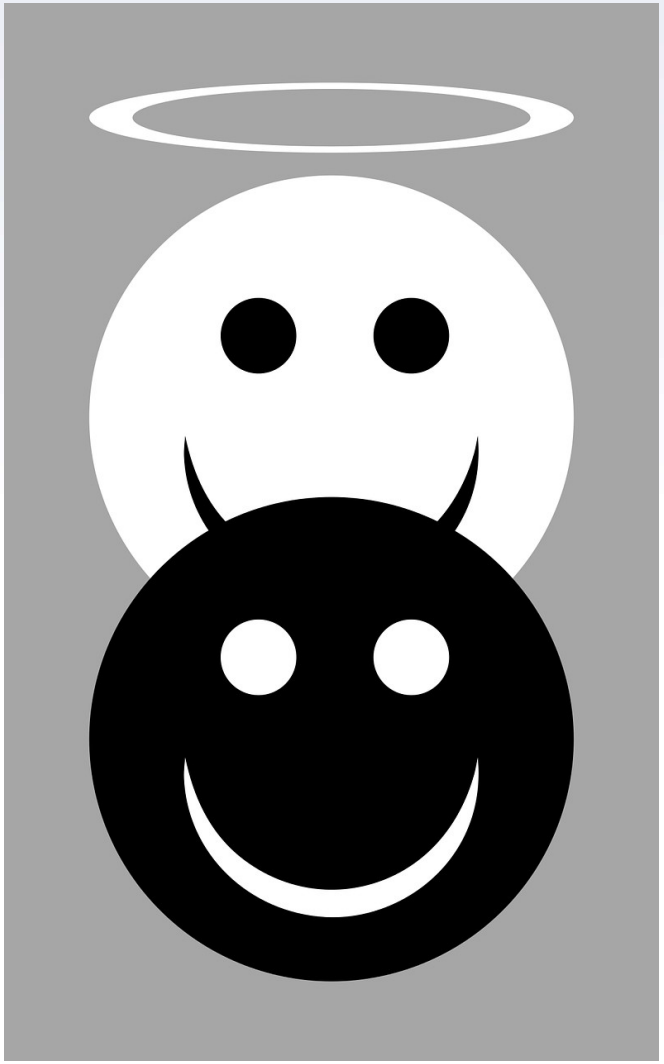
MVP Dagen

Så kom
(sett inn
valgfrittargument)

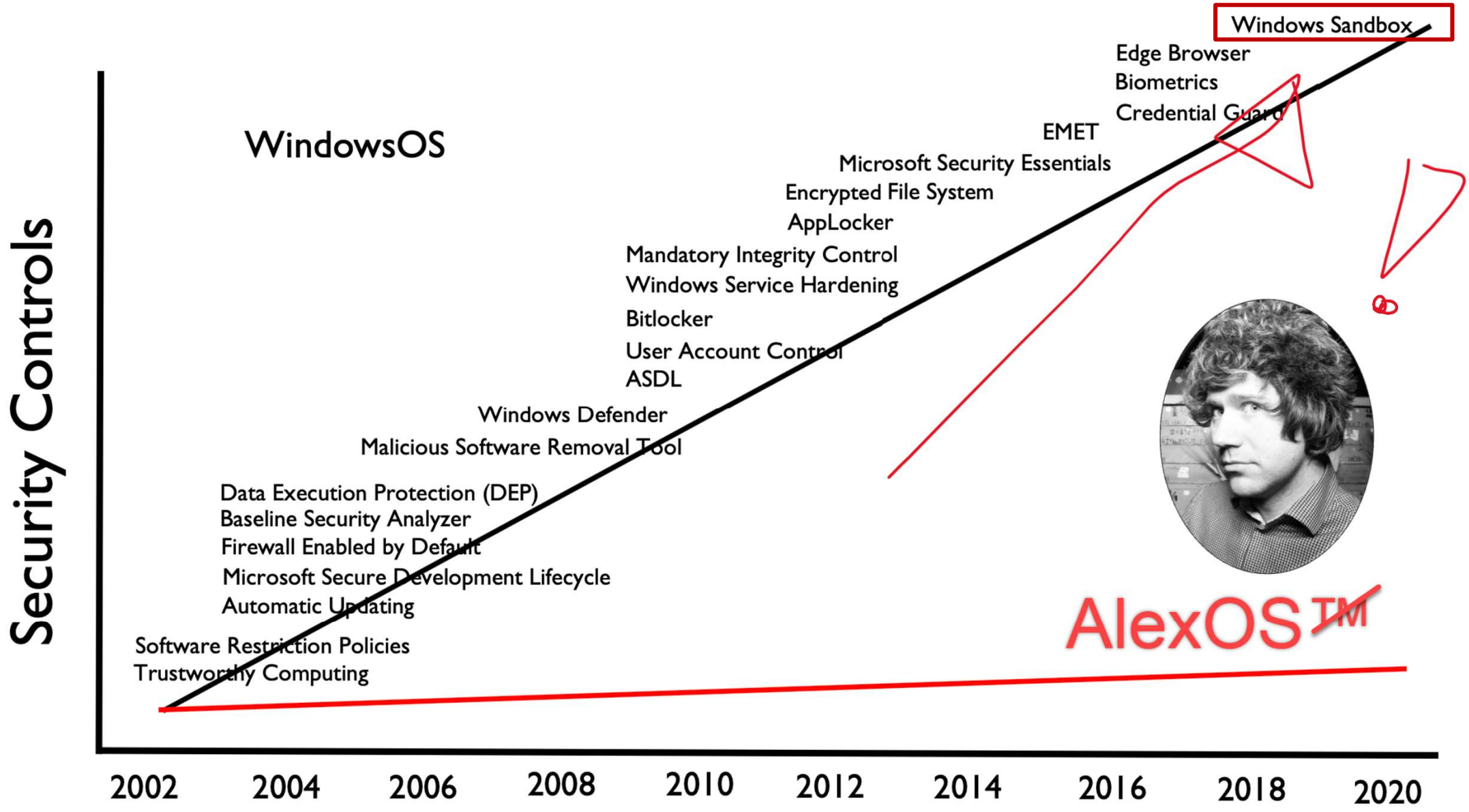
MVP Dagen


Meget sikkert
Lite brukervennlig
Meget brukervennlig
Lite sikkert
Nedlåst maskin
Firmaportal-tjenestetilbud, uten admin
EPM
Macintosh uten (vesentlig) administrasjon
MEJDLA
Permanent lokal admin

Hva galt kan skje, sånn egentlig?



MVP Dagen


Windows Sandbox
Edge Browser
Biometrics
Credential Guard
EMET
Microsoft Security Essentials
Encrypted File System
AppLocker
Mandatory Integrity Control
Windows Service Hardening
Bitlocker
User Account Control
ASDL
Windows Defender
Malicious Software Removal Tool
Data Execution Protection (DEP)
Baseline Security Analyzer
Firewall Enabled by Default
Microsoft Secure Development Lifecycle
Automatic Updating
Software Restriction Policies
Trustworthy Computing
WindowsOS
AlexOS™
Security Controls
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020

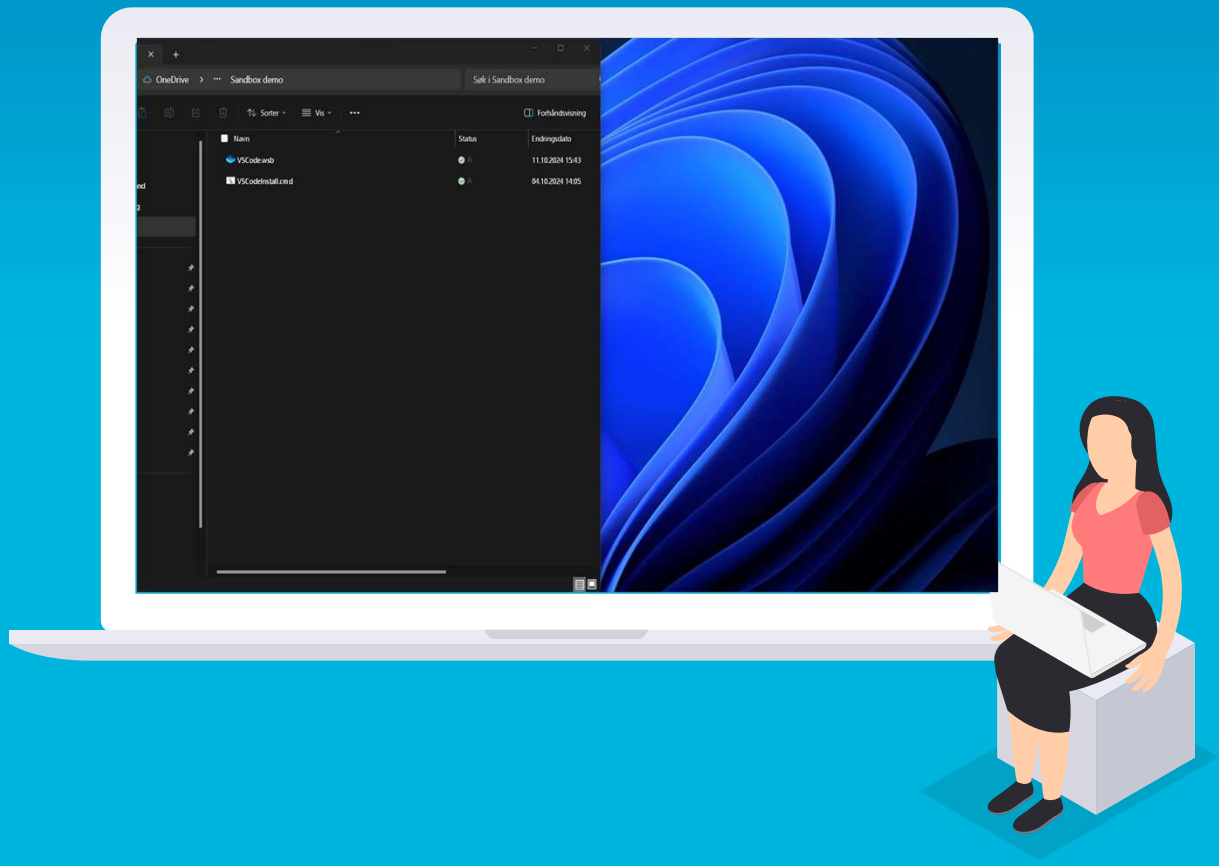
Stol ikke på Arkerne


Windows-sandkasse
Papirkurv
SafeAttachment.docx
Username
password
FRAUD
ALERT
Søk
4:41 PM
10/14/2024
Alexander Solaat R...
Denne PCen
Papirkurv
7°C
Delvis sol
NOB
16:41
14.10.2024

MVP Dagen

Sandbox

What if v2...



MVP Dagen


Det er når presentasjonen slutter, arbeidet begynner!
Takk for oss!
BEGIN.

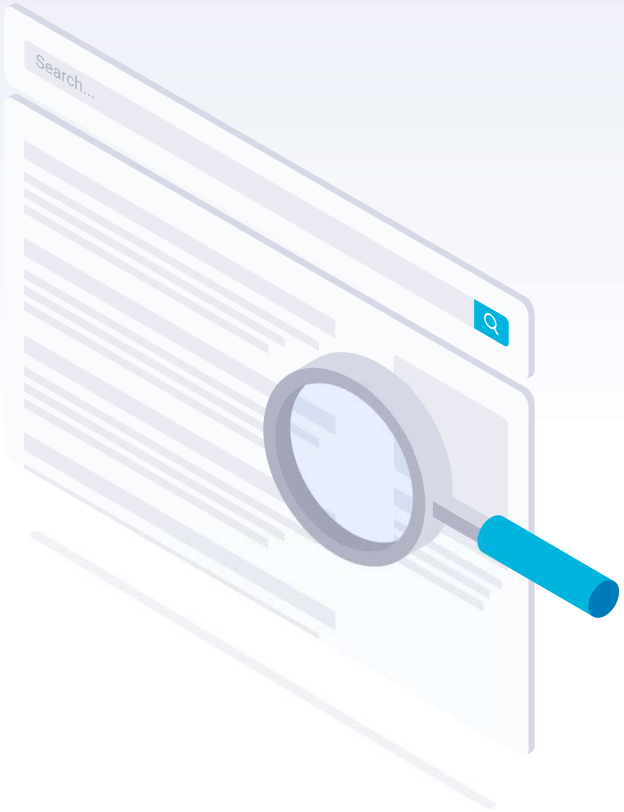
MVP Dagen

Takk!

Spørsmål?

Du finner meg på i gangen eller på

- @alexsolaat



MVP Dagen