

February 6th-7th

NIC
20/20 VISION

Oslo Spektrum



Some insights



Search Podcast



Sign in

Create Podcast

English Special – Ignite 2019 Interview with Mr Hyper-V Ben Armstrong

Nov 21st, 2019

Ben Armstrong Is the Principal Program Manager with the Hyper-V team. He has more than 20 years working with virtualization a 17 of them at Microsoft. But wait, didn't Hyper-V first arrive in 2008?, yes and that's why he is not only known as Mr. Hyper-V but many know him as the Virtual PC Guy from his old blog. His new blog is <https://american-boffin.com/blog/>. We cover both cool new features and old history, many are not aware that how much virtualization means to security in Windows 10, and Xbox. Xbox you say? Yes already in Xbox 365 virtualization was a key feature. And was Ben invited to go onstage at VMworld?



♥ Like | ↗ Share | ↓ Download(40)



NIC

Xbox 360 & Xbox One



About Hyper-V and how it works

VM

VM

VM

VM

Operating system

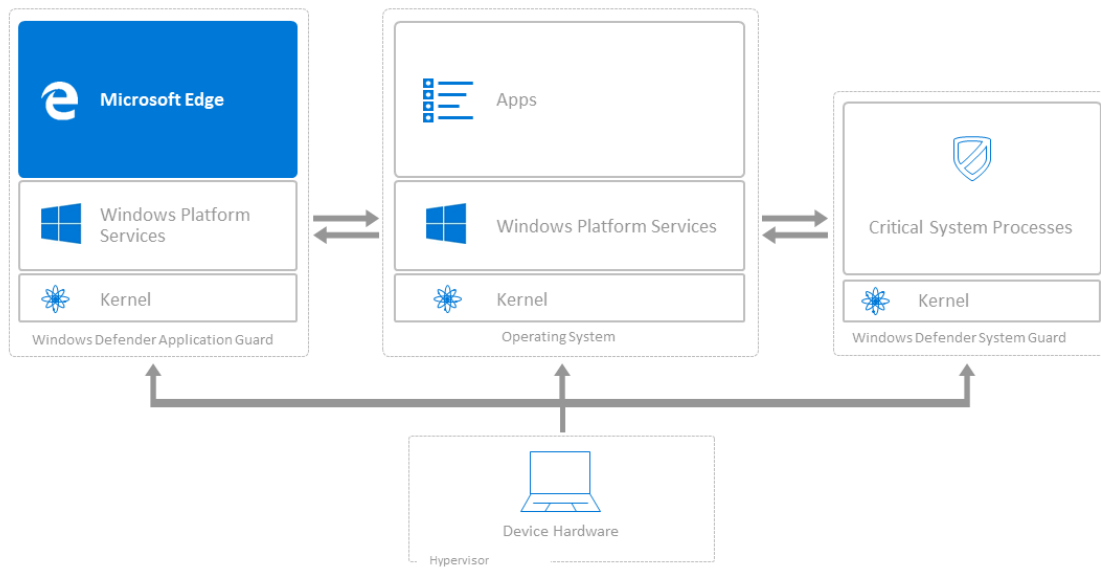
Hardware Abstraction Level (HAL)

Hardware (CPU)

NIC

Windows Defender Application Guard

HARDWARE ISOLATION OF **MICROSOFT EDGE** WITH **WINDOWS DEFENDER APPLICATION GUARD**



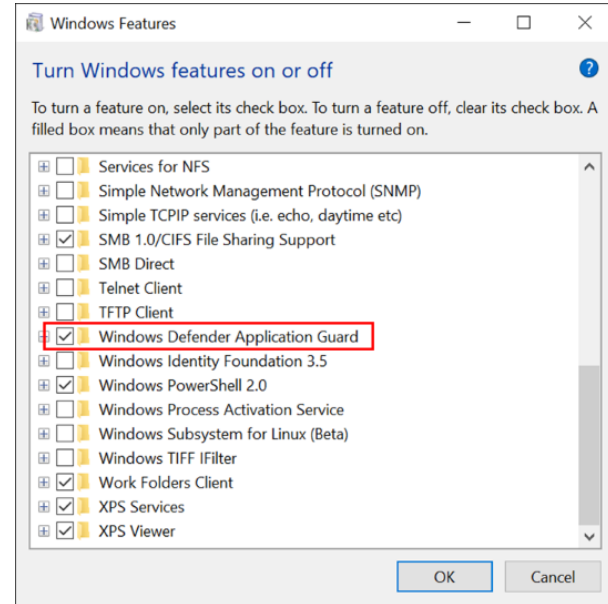
Standalone or Enterprise?

Standalone mode

- Windows 10 Enterprise, 1709 or higher
- Windows 10 Pro, 1803 or higher

Enterprise-managed mode

- Windows 10 Enterprise, 1709 or higher



`Enable-windowsOptionalFeature -online -FeatureName windows-Defender-ApplicationGuard`

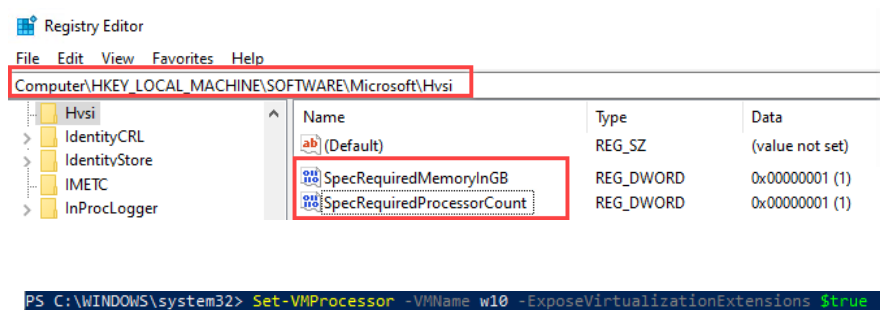


System Requirement

- Second Level Address Translation (SLAT)
- Intel VT-x or AMD-V

And

- 64-bit CPU w. 4 logical cores
- 8 Gigabyte RAM



...Unless

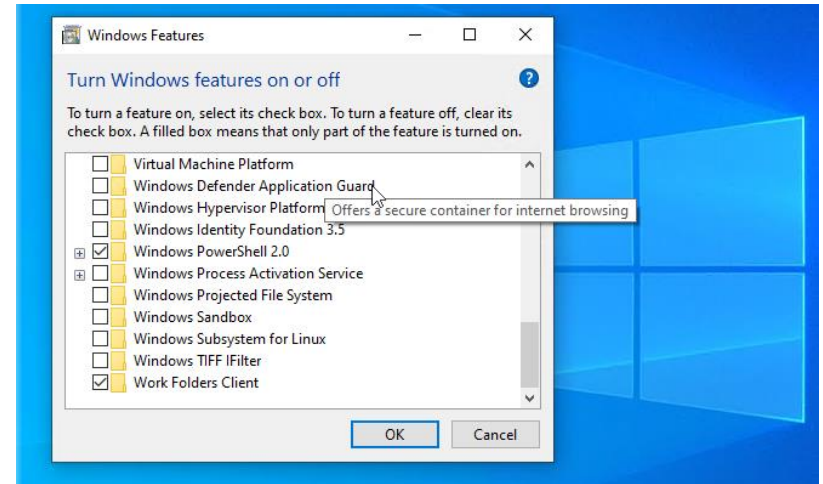
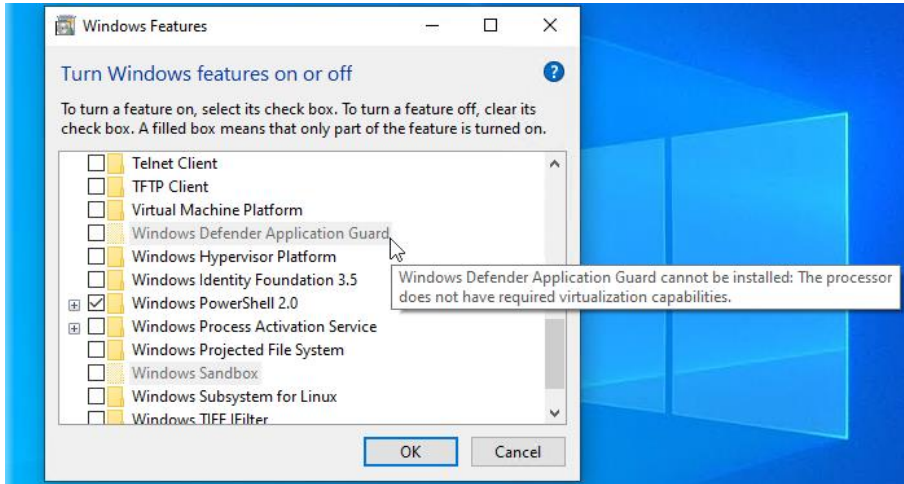
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Hvsi

SpecRequiredMemoryInGB = 1
SpecRequiredProcessorCount = 1

```
Set-VMProcessor -VMName w10 -ExposeVirtualizationExtensions $true
```



System Requirement



Windows Defender Application Guard



nic



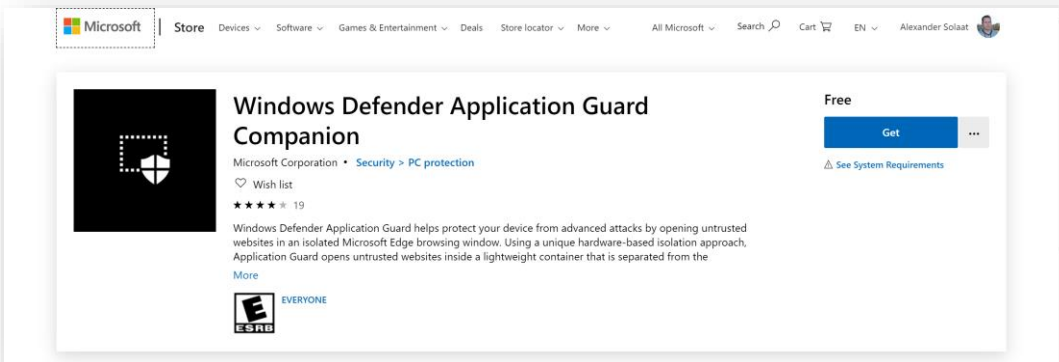
This webpage is trusted.

To help protect your device, Windows Defender Application Guard is checking to see if this is a trusted website.

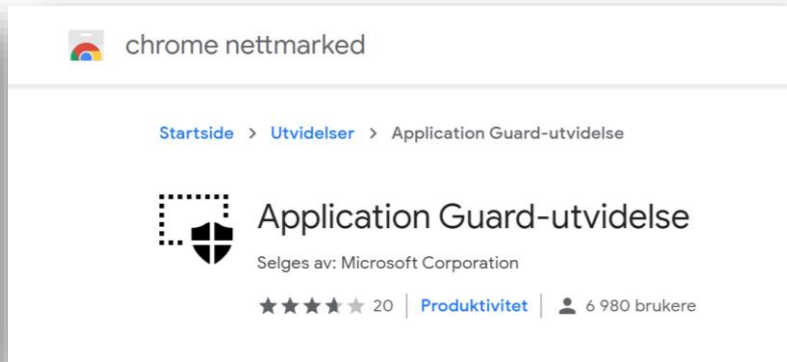


Chromium

- Works with legacy Edge
- Chromium plugin required



The screenshot shows the Microsoft Store page for the 'Windows Defender Application Guard Companion' app. The app is listed as 'Free' and has a 'Get' button. The description states: 'Windows Defender Application Guard helps protect your device from advanced attacks by opening untrusted websites in an isolated Microsoft Edge browsing window. Using a unique hardware-based isolation approach, Application Guard opens untrusted websites inside a lightweight container that is separated from the...'. The app has a rating of 4.5 stars from 19 reviews. The ESRB rating is 'EVERYONE'.



The screenshot shows the Chrome Netmarketed page for the 'Application Guard-utvidelse' extension. The page title is 'chrome nettmarkert'. The breadcrumb trail is 'Startside > Utvidelser > Application Guard-utvidelse'. The extension is developed by 'Selges av: Microsoft Corporation' and has a rating of 4.5 stars from 20 reviews. It is categorized as 'Produktivitet' and has 6 980 brukere.

Standalone vs Managed mode

Welcome to Windows Defender Application Guard

Protect your device from untrusted websites



Windows Defender Application Guard has been successfully configured.

- ✔ This device is compatible
- ✔ Application Guard companion app is installed
- ✔ Application Guard is turned on

Application Guard is configured to run in **standalone mode**. Now you can view untrusted websites in a separate Microsoft Edge browsing window to help protect your device.

[Learn more about enterprise-managed and standalone modes](#)
[Learn more about Windows Defender Application Guard](#)

Welcome to Windows Defender Application Guard

Protect your device from untrusted websites



Windows Defender Application Guard has been successfully configured.

- ✔ This device is compatible
- ✔ Application Guard companion app is installed
- ✔ Application Guard is turned on

Application Guard is configured to run in **enterprise-managed mode**. Now you can view untrusted websites in a separate Microsoft Edge browsing window to help protect your device.

[Learn more about enterprise-managed and standalone modes](#)
[Learn more about Windows Defender Application Guard](#)

Network boundary

Windows 10 and later

Save Discard

***Name**
Cloud Resources ✓

Description
Enter a description... ✓

Platform
Windows 10 and later ✓

Profile type
Network boundary ✓

Settings >
1 configured

Scope (Tags) >
1 scope(s) selected

Applicability Rules >
0 Rule(s) Configured

The network boundary is the list of enterprise resources, such as cloud-hosted domain and IP address ranges for computers that are on the enterprise network. Define network boundaries to apply policies to protect data that resides in these locations.

[Learn more](#) ⓘ

Network boundary ⓘ

Import Export

| Boundary type | Value | Add |
|----------------|----------------|-----|
| Not configured | Not configured | Add |

| Boundary type | Value |
|-----------------|---|
| Cloud resources | .microsoft.com .innofactor.com .protal.a... *** |

Auto detection of other enterprise proxy servers ⓘ
Disable Not configured

Auto detection of other enterprise IP ranges ⓘ
Disable Not configured

OK

Endpoint protection

Windows 10 and later

Select a category to configure settings.

- Microsoft Defender Application G...
3 of 10 settings configured
- Microsoft Defender Firewall
44 settings available
- Microsoft Defender SmartScreen
2 settings available
- Windows Encryption
39 settings available
- Microsoft Defender Exploit Guard
21 settings available
- Microsoft Defender Application C...
2 settings available
- Microsoft Defender Credential Gu...
1 setting available
- Microsoft Defender Security Center
18 settings available
- Local device security options
46 settings available
- Xbox services
5 settings available

Microsoft Defender Application Guard

Windows 10 and later

While using Microsoft Edge, Microsoft Defender Application Guard protects your environment from sites that haven't been defined as trusted by your organization. When users visit sites that aren't listed in your isolated network boundary, the sites will be opened in a virtual browsing session in Hyper-V. Trusted sites are defined by a network boundary, which can be configured in Device Configuration. Note this feature is only available for Windows 10 (64-bit) devices.

i This profile will install a Win32 component to activate Application Guard. End-users will need to restart the targeted devices to complete the successful installation and application of this profile.

- Application Guard ⓘ Enabled for Edge ▾
- Clipboard behavior ⓘ Allow copy and paste fr... ▾
- Clipboard content ⓘ Text and images ▾
- External content on enterprise sites ⓘ Block **Not configured**
- Print from virtual browser ⓘ Allow **Not configured**
- * Printing type(s) ⓘ ▾
- Collect logs ⓘ Allow **Not configured**
- Retain user-generated browser data ⓘ Allow **Not configured**
- Graphics acceleration ⓘ Enable **Not configured**
- Download files to host file system ⓘ Enable **Not configured**

I know, I know - how it's like from Intune?



nic

Secured-core PC

Basic integrity protection

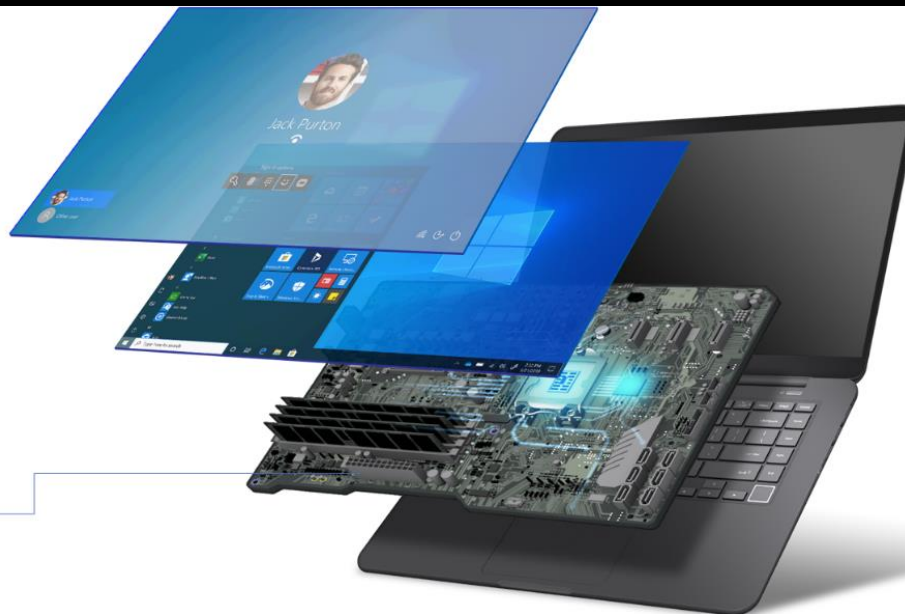
- Secure boot
- TPM2.0
- BitLocker

Protection from kernel attacks

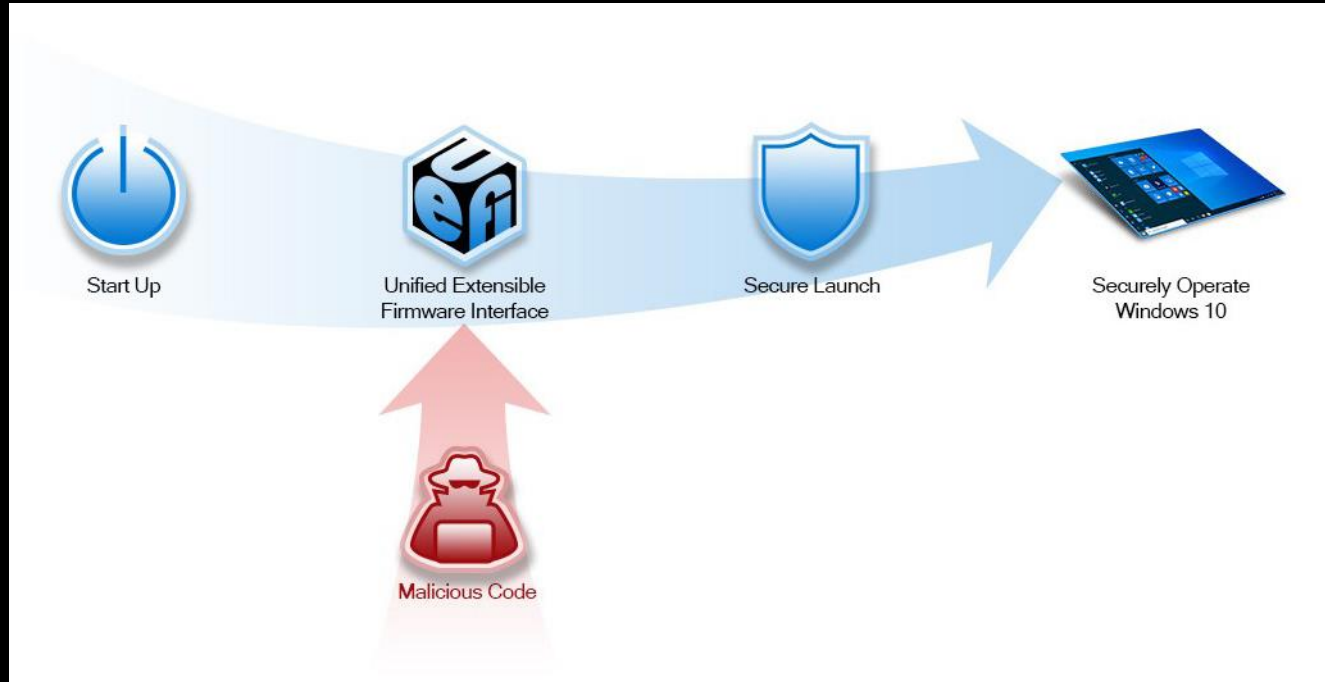
- Virtualization Based Security (VBS)
- Hypervisor protected Code Integrity (HVCI)
- Kernel DMA protection

Protection from firmware attacks

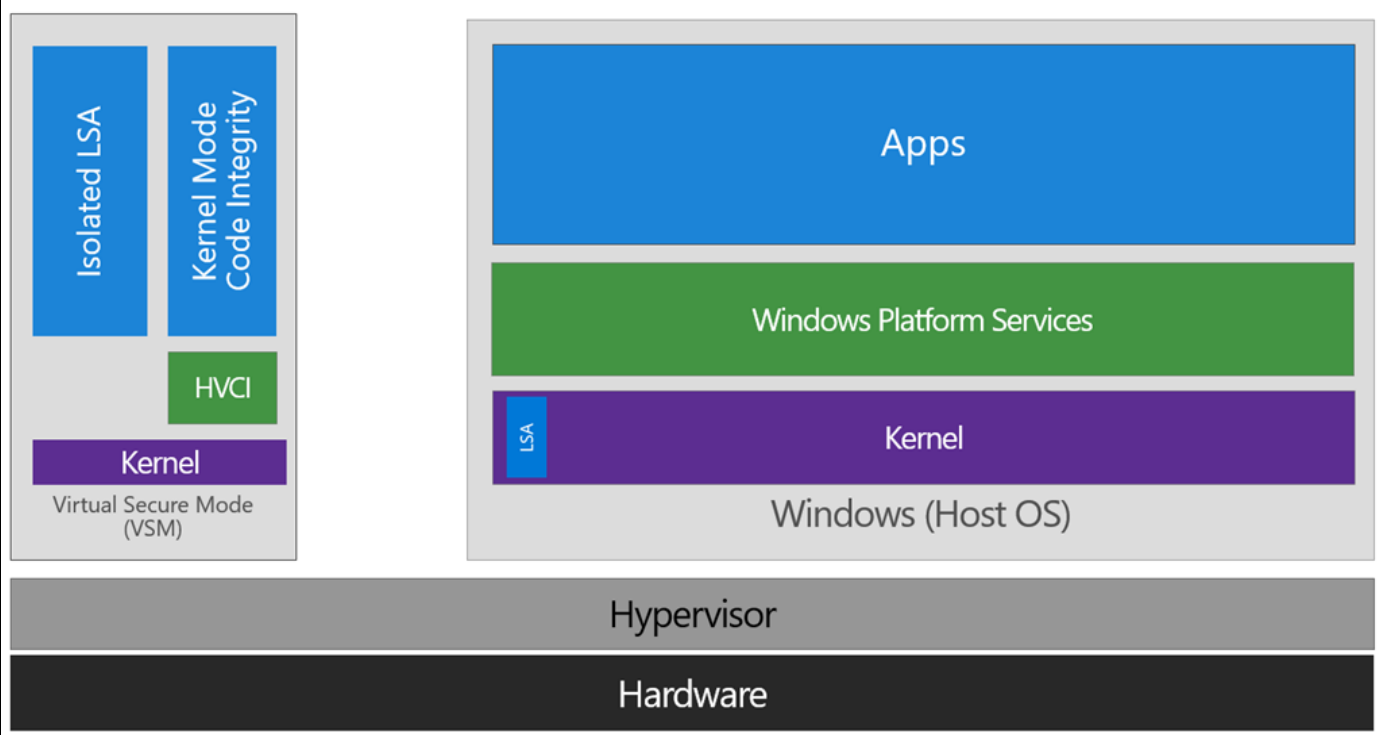
- System Guard Secure Launch
- System Guard SMM Protections



Secured-core PC



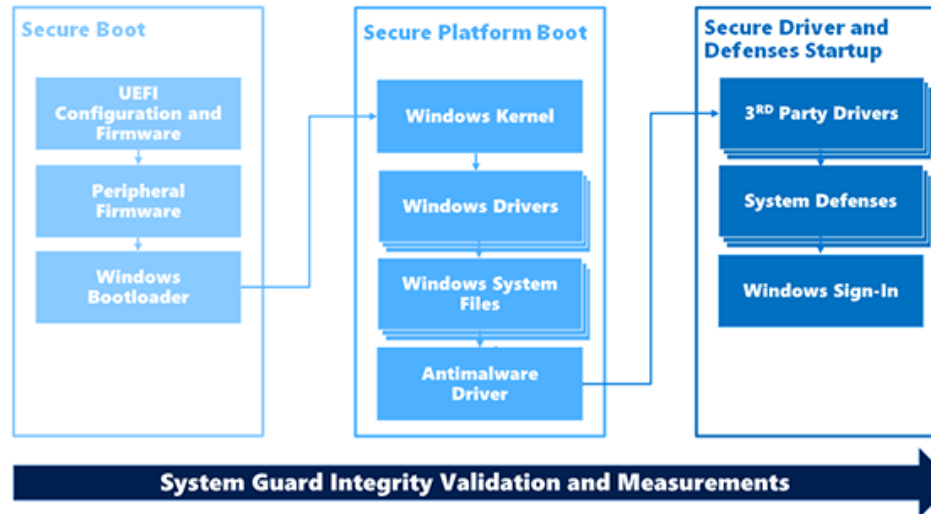
Virtual Secure Mode



Windows Defender System Guard

WINDOWS DEFENDER SYSTEM GUARD

BOOT TIME INTEGRITY PROTECTION



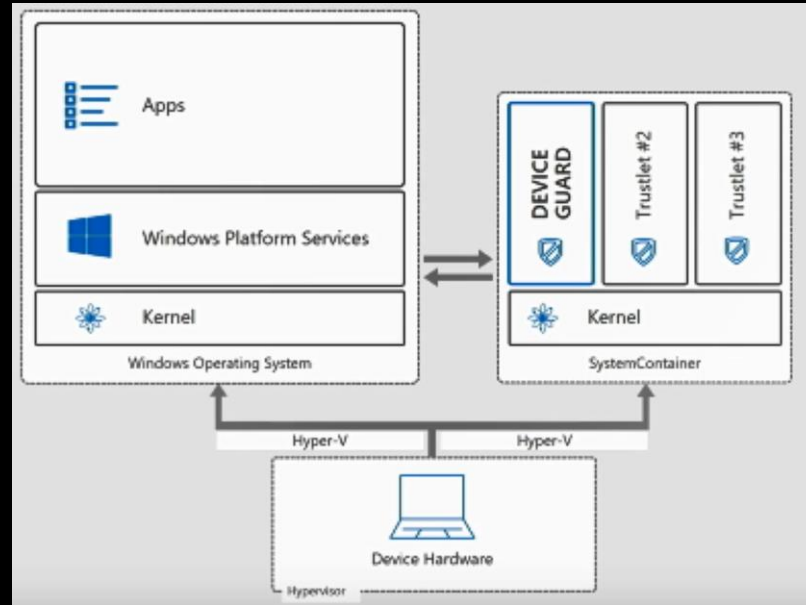
Task Manager

File Options View

Processes Performance App history Startup Users Details Services

| Name | PID | Status | User name | C... | Memo... | Description |
|-------------------------|-------|-----------|-----------|------|-----------|---------------------------------|
| csrss.exe | 464 | Running | SYSTEM | 00 | 572 K | Client Server Runtime Process |
| csrss.exe | 548 | Running | SYSTEM | 00 | 1,124 K | Client Server Runtime Process |
| dwm.exe | 960 | Running | DWM-1 | 02 | 67,632... | Desktop Window Manager |
| explorer.exe | 30... | Running | Arnaud | 00 | 16,512... | Windows Explorer |
| Lsalso.exe | 688 | Running | SYSTEM | 00 | 584 K | Credential Guard |
| lsass.exe | 696 | Running | SYSTEM | 00 | 2,616 K | Local Security Authority Proces |
| msinfo32.exe | 25... | Running | Arnaud | 00 | 1,592 K | System Information |
| MsMpEng.exe | 20... | Running | SYSTEM | 00 | 39,900... | Antimalware Service Executable |
| OneDrive.exe | 26... | Running | Arnaud | 00 | 2,896 K | Microsoft OneDrive |
| RuntimeBroker.exe | 21... | Running | Arnaud | 00 | 3,780 K | Runtime Broker |
| SearchIndexer.exe | 31... | Running | SYSTEM | 00 | 9,168 K | Microsoft Windows Search Ind |
| SearchUI.exe | 38... | Suspended | Arnaud | 00 | 54,492... | Search and Cortana applicator |
| Secure System | 348 | Suspended | SYSTEM | 00 | 16 K | |
| services.exe | 668 | Running | SYSTEM | 00 | 1,920 K | Services and Controller app |
| ShellExperienceHost.exe | 36... | Suspended | Arnaud | 00 | 13,432... | Windows Shell Experience Hos |
| sihost.exe | 27... | Running | Arnaud | 00 | 2,604 K | Shell Infrastructure Host |
| smss.exe | 352 | Running | SYSTEM | 00 | 192 K | Windows Session Manager |
| SnippingTool.exe | 42... | Running | Arnaud | 01 | 2,828 K | Snipping Tool |
| spoolsv.exe | 17... | Running | SYSTEM | 00 | 4,064 K | Spooler SubSystem App |
| sppsvc.exe | 23... | Running | NETWOR... | 00 | 4,076 K | Microsoft Software Protection |
| svchost.exe | 40... | Running | Arnaud | 00 | 1,640 K | Host Process for Windows Ser |
| svchost.exe | 700 | Running | SYSTEM | 00 | 2,222 K | Host Process for Windows Ser |

Defender Application Control

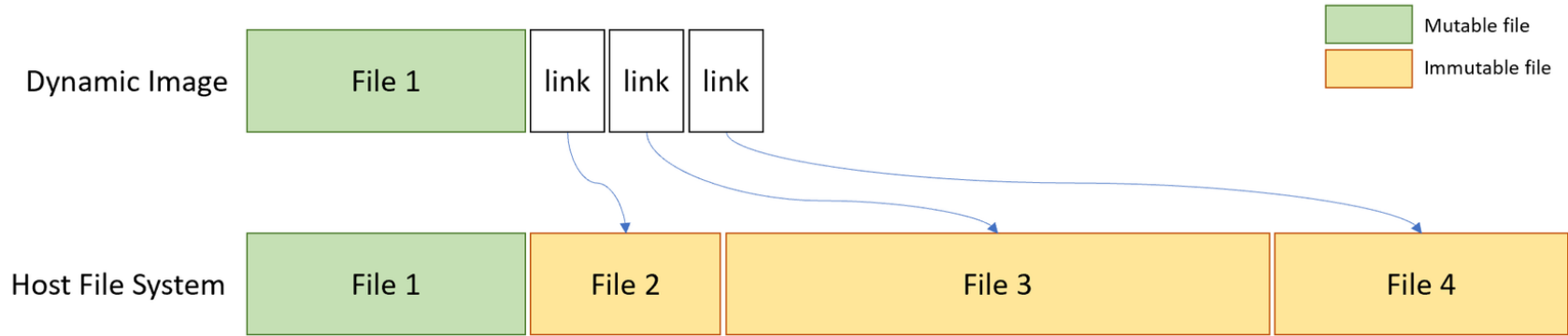


Prerequisites for using the feature

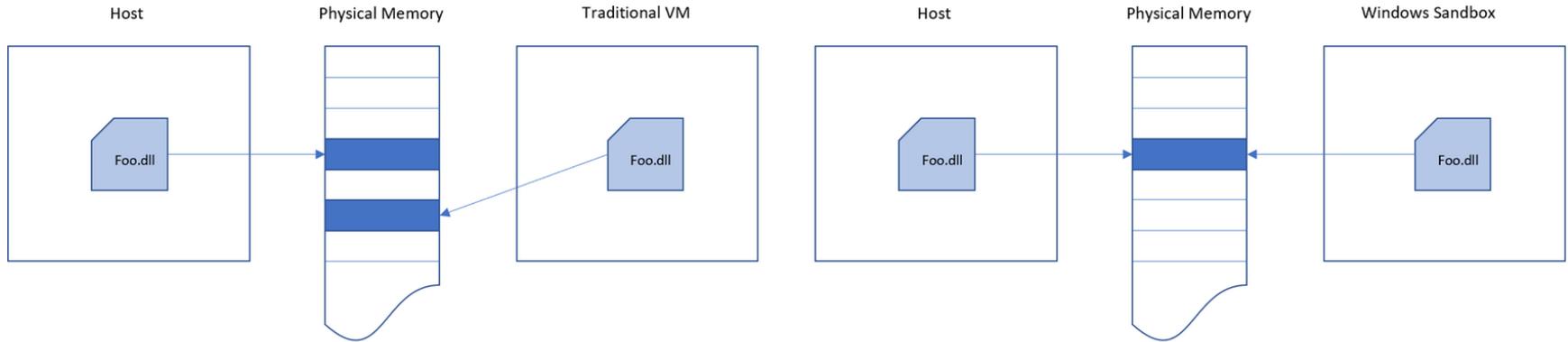
- Windows 10 Pro or Enterprise 1903 or later
- AMD64 architecture
- Virtualization capabilities enabled in BIOS
- At least 4GB of RAM (8GB recommended)
- At least 1 GB of free disk space (SSD recommended)
- At least 2 CPU cores (4 cores with hyperthreading recommended)



VM



Memory



vGPU (virtualized GPU)

- Enable or Disable the virtualized GPU. If vGPU is disabled, Sandbox will use WARP (software rasterizer).

Networking

- Enable or Disable network access to the Sandbox.

Shared folders

- Share folders from the host with read or write permissions. Note that exposing host directories may allow malicious software to affect your system or steal data.

Startup script

- Logon action for the sandbox.

DEMO:


- Original Sandbox
- Sandbox w/simple adjustments

File Explorer window showing the path: This PC > Windows (C:) > Users > c624ot2 > OneDrive > Presentasjoner > 2019 > Ignite > Tools > Sandbox > Simple. The search bar contains "Simple".

The left sidebar shows the following folders:

- Delt med alle
- Dokumenter
- Email attachments
- Notebooks
- Office Lens
- Skrivebord
- Temp
- Tools
- Vedlegg
- Compliance Manager Toolkit 2019-07-02 01
- Microsoft GDPR Discovery Toolkit v1.0 2015
- This PC
 - 3D Objects
 - Desktop
 - Documents
 - Downloads
 - Music
 - Pictures
 - Videos
 - Windows (C:)

The main pane displays a table of files:

| Name | Date modified | Type | Size |
|--|------------------|----------|------|
|  SandBox-ShareConnected.wsb | 31.10.2019 16:21 | WSB File | 1 KB |

1 item

DEMO:
Sandbox w/Chocolatey

Chocolatey

File Home Share View

OneDrive - Personal > Presentasjoner > 2019 > Ignite > Tools > Sandbox > Chocolatey

Search Chocolatey

| Name | Date modified |
|-------------------|------------------|
| WallPaper | 31.10.2019 10:58 |
| Install-Choco.ps1 | 31.10.2019 11:03 |
| Prep.cmd | 04.11.2019 07:08 |
| SandBox-C | 04.11.2019 06:29 |
| Set-WallPa | 21.10.2019 08:35 |

Tools

- Chocolatey
- Pictures
- Podcaster
- Windows Sandbox - Ninite edition

OneDrive - Personal

- ArrowBackup
- Attachments
- Backup
- Bilder
- Blogg og Podcaster
- CV'er
- Delt
- Documents
- Fun
- Gammelt
- Kunder
- Lisenser og nøkkler
- Logo etc
- Music

5 items 1 item selected 410 bytes

Open

- Share
- View online
- View version history
- Choose OneDrive folders to sync
- 7-Zip >
- CRC SHA >
- Edit with Notepad ++
- Share
- Open with...
- Give access to >
- Cisco AMP For Endpoints >
- PowerRename
- Restore previous versions
- Send to >
- Cut
- Copy

Windows Sandbox Links

- <https://github.com/OTvedt/Scripts-For-Sharing/tree/master/Sandbox>
- <https://techcommunity.microsoft.com/t5/Windows-Kernel-Internals/Windows-Sandbox/ba-p/301849>
- <https://techcommunity.microsoft.com/t5/Windows-Kernel-Internals/Windows-Sandbox-Config-Files/ba-p/354902>

OneDrive for Business Malware Protection

- Recover versions of items that pre-date their encryption by ransomware.



Restore your OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Select a date preset or use the slider to find a date with unusual activity in the chart. Then select the changes that you want to undo.

Select a date

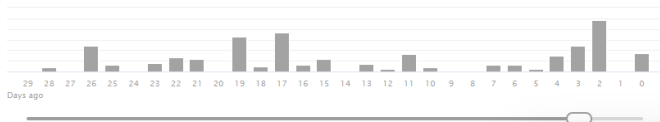
Custom date and time

All changes after 1/29/2020, 12:01:14 AM will be rolled back

Restore

Cancel

Move the slider to quickly scroll the list to a day.



Select a change in the list below to highlight it and all the changes before it. Then select the Restore button to restore your OneDrive to the highlighted changes.

| | | | | |
|-------------------------------------|--|---|--|---------------------------------------|
| <input checked="" type="checkbox"/> | | Updated by Alexander Solaat Rødland 12:01:14 AM | | Config and Clipboard demo cu... |
| ∨ | | 4 days ago - 1/28/2020 (21) | | |
| | | Updated by Alexander Solaat Rødland 11:19:29 PM | | Config and Clipboard demo cu... |
| + | | Added by Alexander Solaat Rødland 11:19:28 PM | | Config and Clipboard demo cut.tscproj |
| | | Updated by Alexander Solaat Rødland 11:10:39 PM | | Configuration from Intune cut.tscproj |
| + | | Added by Alexander Solaat Rødland 11:10:38 PM | | Configuration from Intune cut.tscproj |
| | | Updated by Alexander Solaat Rødland 8:47:10 AM | | Configuration from Intune.tscproj |
| + | | Added by Alexander Solaat Rødland 8:47:09 AM | | Configuration from Intune.tscproj |
| + | | Added by Alexander Solaat Rødland 8:07:47 AM | | GPO.msc |
| | | Updated by Alexander Solaat Rødland 8:07:47 AM | | Networksolation.reg |
| | | Updated by Alexander Solaat Rødland 8:07:47 AM | | Registry.reg |
| + | | Added by Alexander Solaat Rødland 8:07:47 AM | | IntuneCloudStuff.reg |
| + | | Added by Alexander Solaat Rødland 8:07:47 AM | | Registry.reg |
| + | | Added by Alexander Solaat Rødland 8:07:47 AM | | Networksolation.reg |
| | | Updated by Alexander Solaat Rødland 8:07:47 AM | | GPO.msc |
| | | Updated by Alexander Solaat Rødland 8:07:47 AM | | IntuneCloudStuff.reg |

Are you sure you want to restore your OneDrive?

All changes after 1/29/2020, 12:01:14 AM will be rolled back








Restore

Cancel

NIC

Microsoft Cloud App Security

- Block / Lock users when multiple files are edited

| Policy type icon | Policy type | Use |
|---|--|---|
|  | Access policy | Access policies provide you with real-time monitoring and control over user logins to your cloud apps. |
|  | Activity policy | Activity policies allow you to enforce a wide range of automated processes using the app provider's APIs. These policies enable you to monitor specific activities carried out by various users, or follow unexpectedly high rates of a certain type of activity. |
|  | Anomaly detection policy | Anomaly detection policies enable you to look for unusual activities on your cloud. Detection is based on the risk factors you set to alert you when something happens that is different from the baseline of your organization or from the user's regular activity. |
|  | App discovery policy | App discovery policies enable you to set alerts that notify you when new apps are detected within your organization. |
|  | Cloud Discovery anomaly detection policy | Cloud Discovery anomaly detection policies look at the logs you use for discovering cloud apps and search for unusual occurrences. For example, when a user who never used Dropbox before suddenly uploads 600 GB to Dropbox, or when there are a lot more transactions than usual on a particular app. |
|  | File policy | File policies enable you to scan your cloud apps for specified files or file types (shared, shared with external domains), data (proprietary information, personal data, credit card information, and other types of data) and apply governance actions to the files (governance actions are cloud-app specific). |
|  | Session policy | Session policies provide you with real-time monitoring and control over user activity in your cloud apps. |

Olav Tvedt

IT Dude



Twitter: @olavtwitt

**Blog: <https://olavtvedt.blogspot.com>
<https://www.linkedin.com/in/otvedt>**

Alexander S. Rødland

Not IT Dude

INNOFACTOR®



Twitter: @alexsoaat

**Blog: <https://solaat.no>
<https://www.linkedin.com/in/alexsoaat>**

Slides and demos from the conference will be available at

<https://github.com/nordicinfrastructureconference/2020>

