Sami Laiho

Senior Technical Fellow, MVP

Adminize.com / Win-fu.com

sami@adminize.com @samilaiho

BLOG.WIN-FU.COM

What's really new in Windows 10?

Configuration Manager

Forgive my English

- When most get **Administrator** or Spanish get **Administrador**
- we get **JÄRJESTELMÄNVALVOJA**

Sami Laiho

Senior Technical Fellow
adminize.com

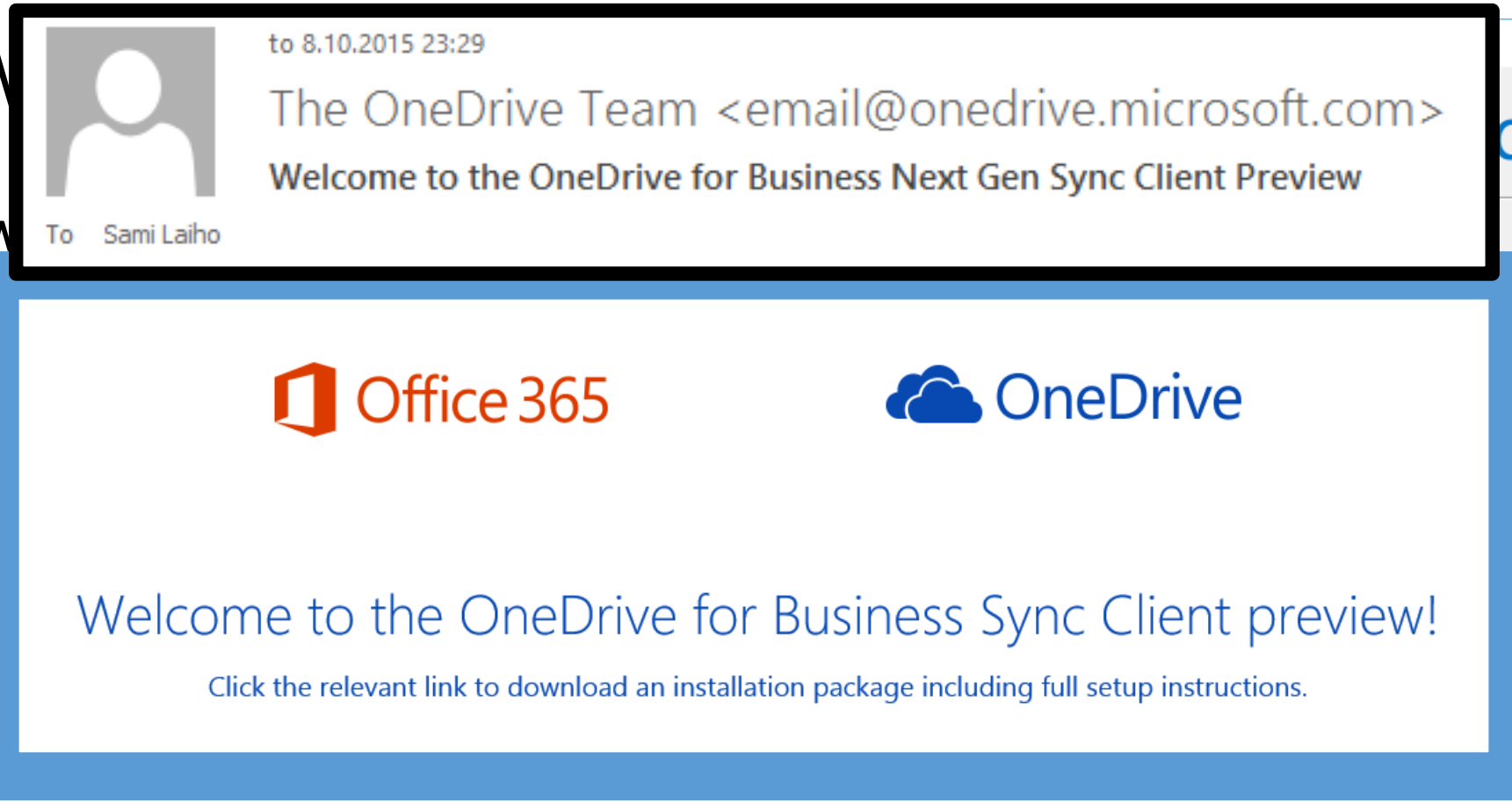
- IT Admin since 1996
- MCT since 2001 (MCT Regional Lead – Finland)
- MVP in Windows OS since 2011
- Specializes in and trains:
  - Troubleshooting
  - Security
  - Centralized Management
  - Active Directory
  - Hacking
  - Penetration testing
  - Social Engineering
- Trophies:
  - Ignite 2015 – Best male presenter ;) (#2 out of 1000 speakers)
  - TechEd Europe 2014 – Best session
  - TechEd North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker
  - TechEd Europe 2013 - Best Session by an external speaker

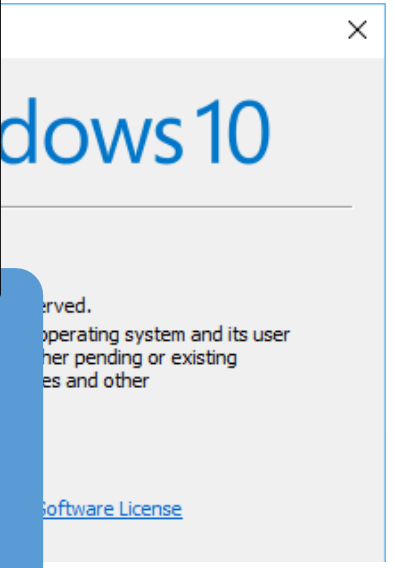
AMAZING!!!!

- A Start-Menu!!! (NOW WITH 2048 things!!)
- Virtual Desktops!!!
- Running applications in Windows!!!
- A transparent Command Prompt!!!

Last W

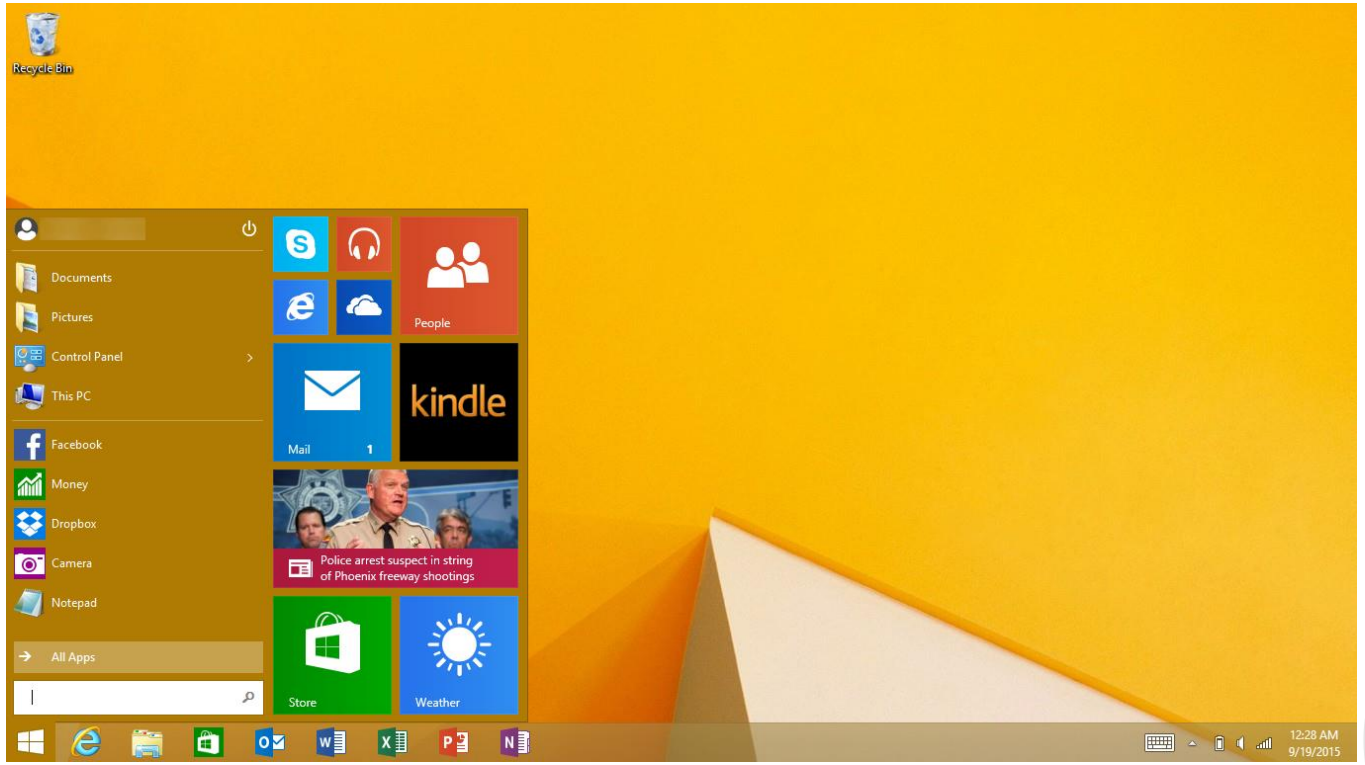
- Windows
- Windo
- Windo
- ”If you
  Windo
- Windows RT?





Windows RT ”Windows 10 upgrade”

- https://support.microsoft.com/en-us/kb/3033055



Upgrade is recommended

- Until now it has always been a less recommended way to upgrade and has always said to result in poor performance compared to a clean install
- You can opt out or delay the adoption
  - Long Time Servicing Branch
- This is part of a bigger picture:
  - Flight upgrades
  - Home users forced to use Windows Update
  - Windows Update for Business

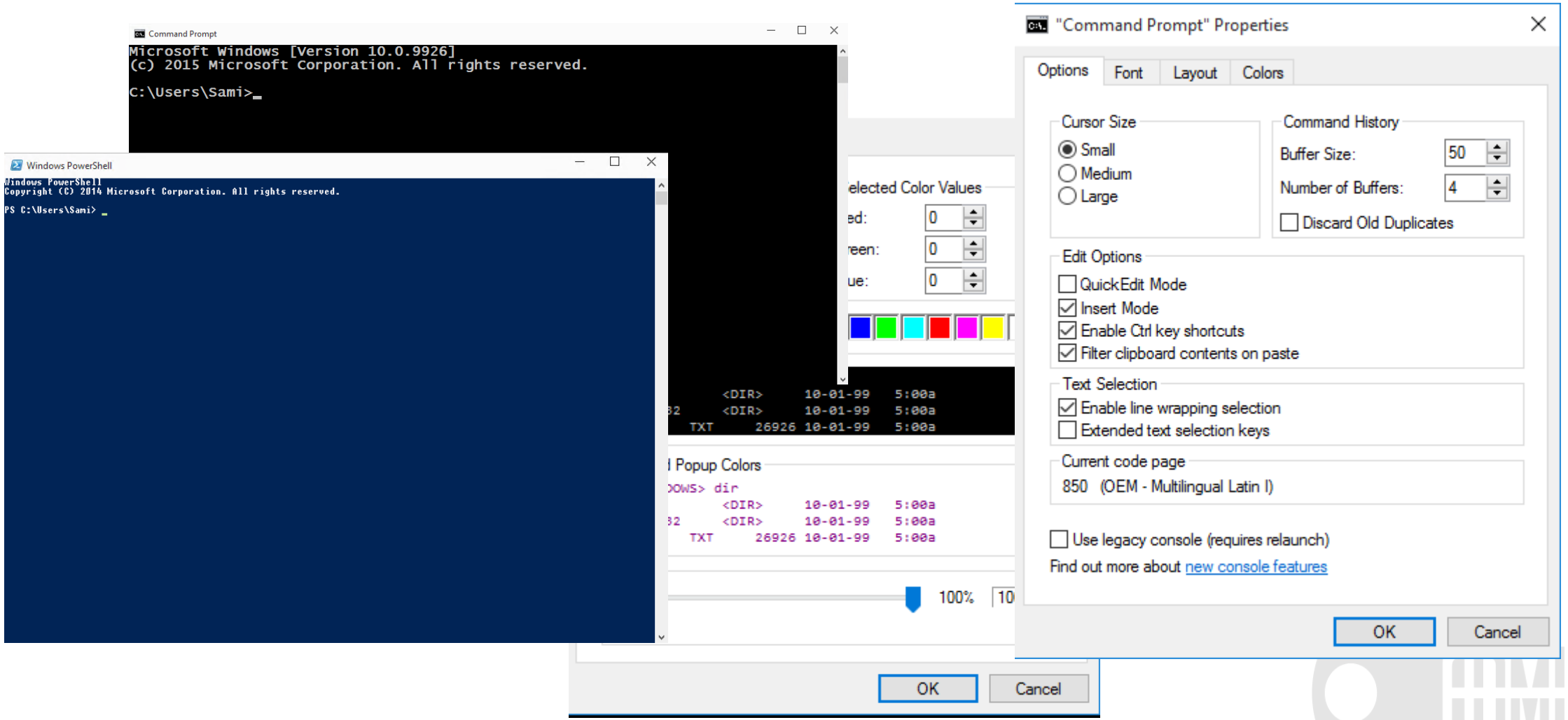
DEMO

Upgrade Settings

Provision packages

- Transform a purchased OEM-installed PC to an Enterprise device
- Trying to make CYOD easier
- Windows ”Phone” has an Enterprise-version so I hope this works…

Fixed ConHost.exe



DEMO

Conhost.exe

Biometrics

- No more passwords!
- Two-factor authentication for everyone!
- First factor to be Biometrics, PIN, face recognition …
- Smartcards and other physical tokens are easily forgotten so let’s use something that’s easier to remember to take with you
  - Your computers TPM
  - Windows 10 phone
- Windows Hello and Windows Passport

DEMO

Windows Hello

account password

this PIN to sign in

I forgot my P

ws Hello

Windows, apps and

Windows Hello setup

New Store and Universal Apps

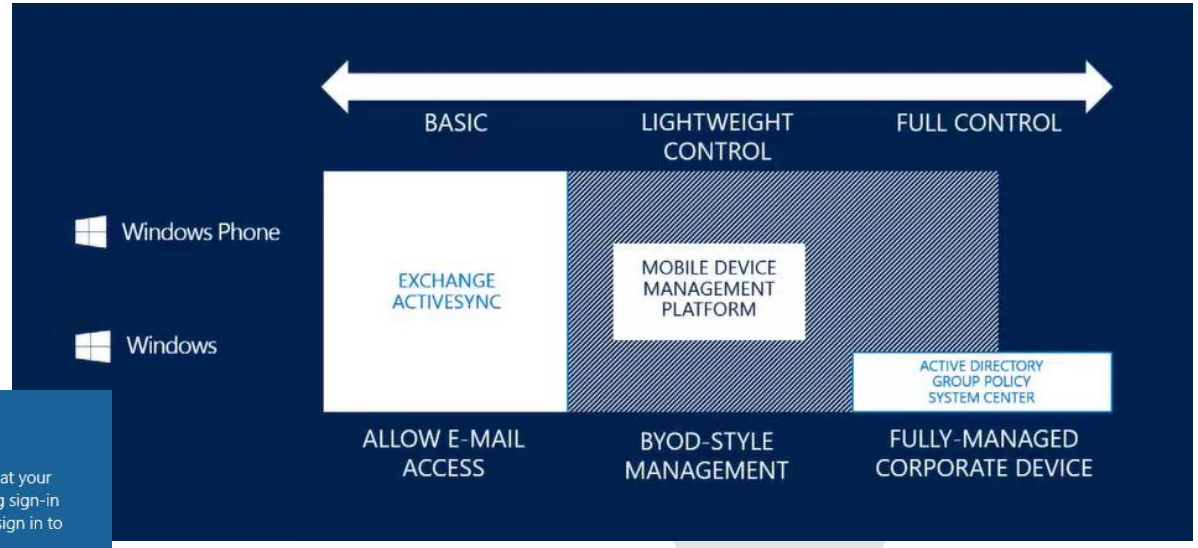
- Only way to make Windows fly in the current world of devices is to make the Store work
- Only way to make the Store work is to make the developers happy with it and get more apps in it
  - Two phases:
    - 1. ”Emulation” for iOS and Android apps, and support for App-V packages
    - 2. Make the store more sexy and appealing to devs – Xbox plays a crucial role in this
- Volume licensing, reusable licenses and Azure AD authentication are a must

Azure AD

- Path to here
  - Windows 7 → Domain
  - Windows 8.1 + Microsoft Account
  - Windows 10 + Azure AD -account
- Windows 10 is the first OS really connected to Azure
- ”AAD should be called Azure Authentication Services (for now at least)” – Sami Laiho

MDM

- InTune, SCCM and 3rd party supported better than before
- Not only for BYOD anymore
- Three scenarios



Hardware features

- Windows Hello and RealSense 3D Cameras
- DirectX 12
- Wireless Charging
- Software Guard Extensions (SGX)
  - https://software.intel.com/sites/default/files/managed/3e/b9/SF15_ISGC003_81_SGX_DL_100_small.pdf
- USB Type C and USB 3.1
- ThunderBolt 3.0 (40Gbps → Two daisy-chained 4K displays)

Hardware features

- Intel Skylake enhancements
  - Keyword spotter algorithm
  - WiGig technology, which can transfer data at 7Gbps
  - DDR4 memory, which will improve internal data transfer between memory, processor and other components
  - SIMD.js for Edge
    - Single Instruction, Multiple Data (SIMD)
  - CPU Speed Shift (30ms→1ms)
  - Sensor Hub
  - Image Signal Processor

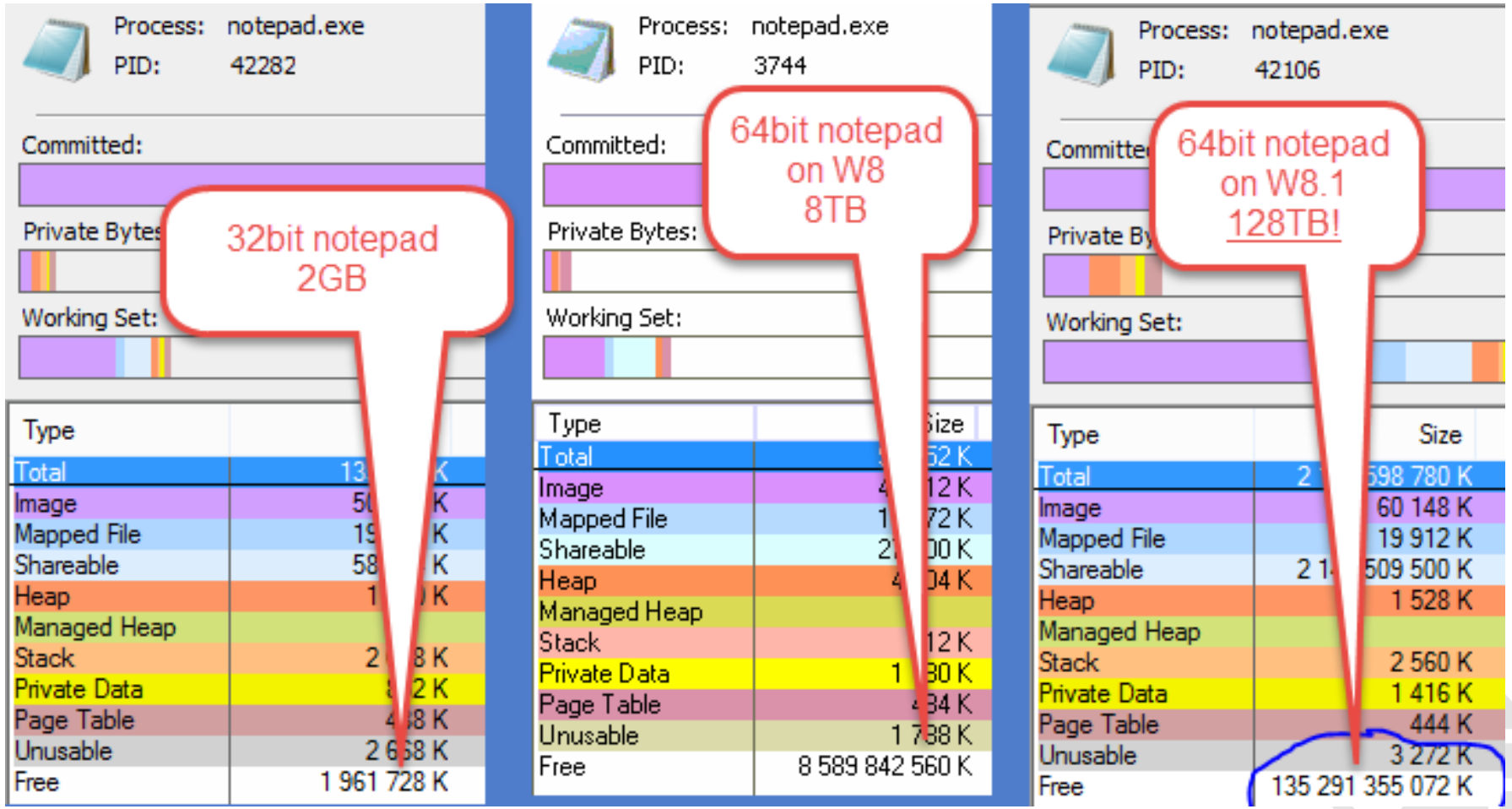
DEMO

CPU Shift

Continuum


Welcome Joe!
Cortana
Up next:
Wednesday 28
Mail
Microsoft Edge
Store
OneNote
Continuum
Music
Video
Xbox
All Apps

Virtual memory size and ASLR

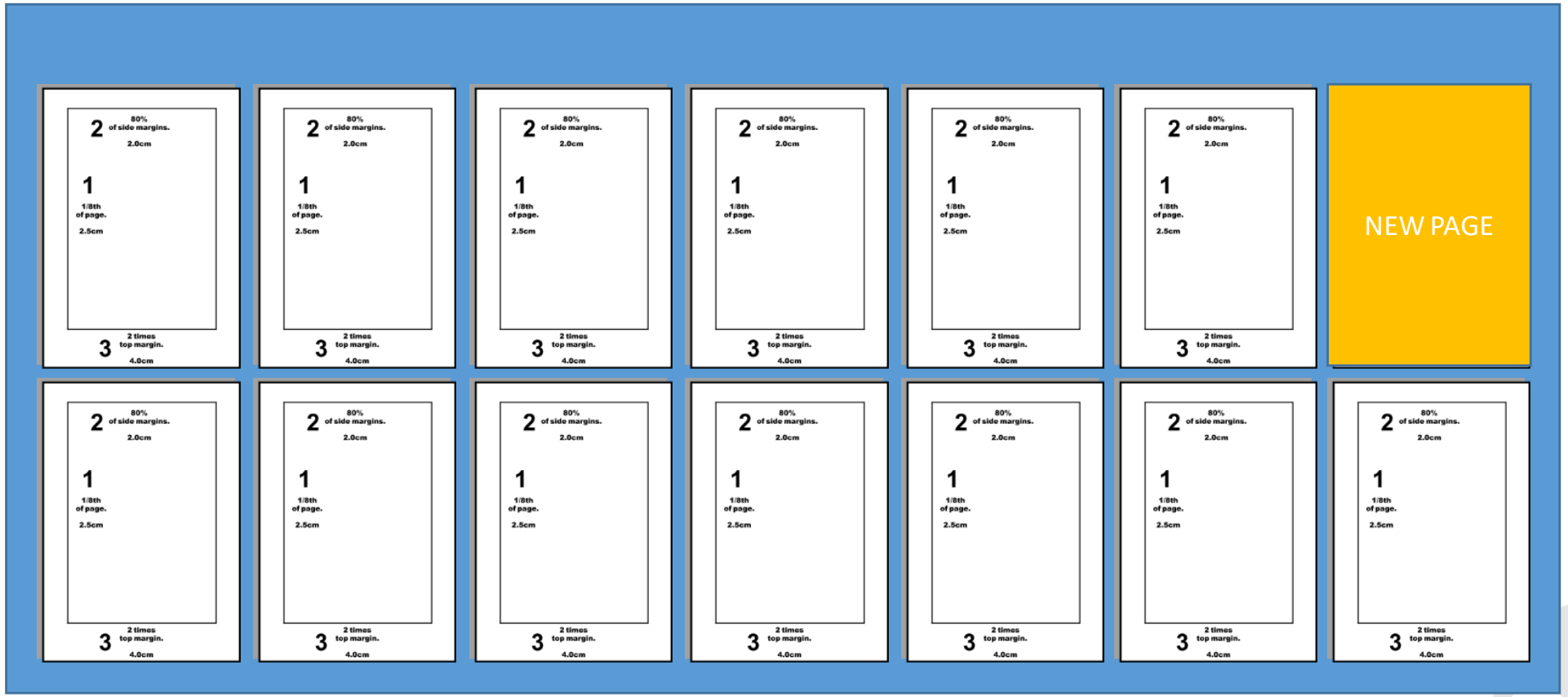


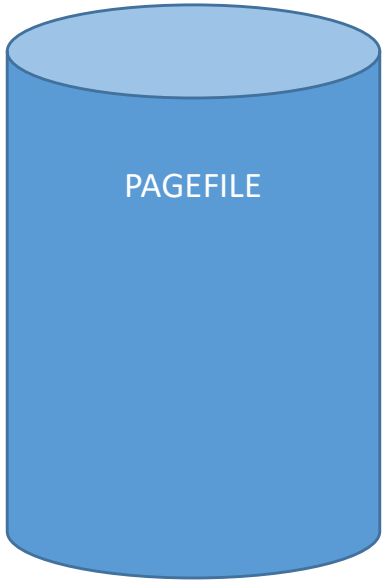
IOMMU

- I/O Memory Management Unit
  - MMU for devices, as opposed to processors
  - Where an MMU translates virtual to physical addresses for a CPU accessing your system's memory, an IOMMU translates virtual to physical addresses for devices
- Hardware based protection against DMA-access
- Protects against buggy drivers and malicious code
- Works with SLAT
- Makes sure a device or VM won’t have access to physical memory addresses not meant for them
- Known as: Intel VT-d / AMD-Vi

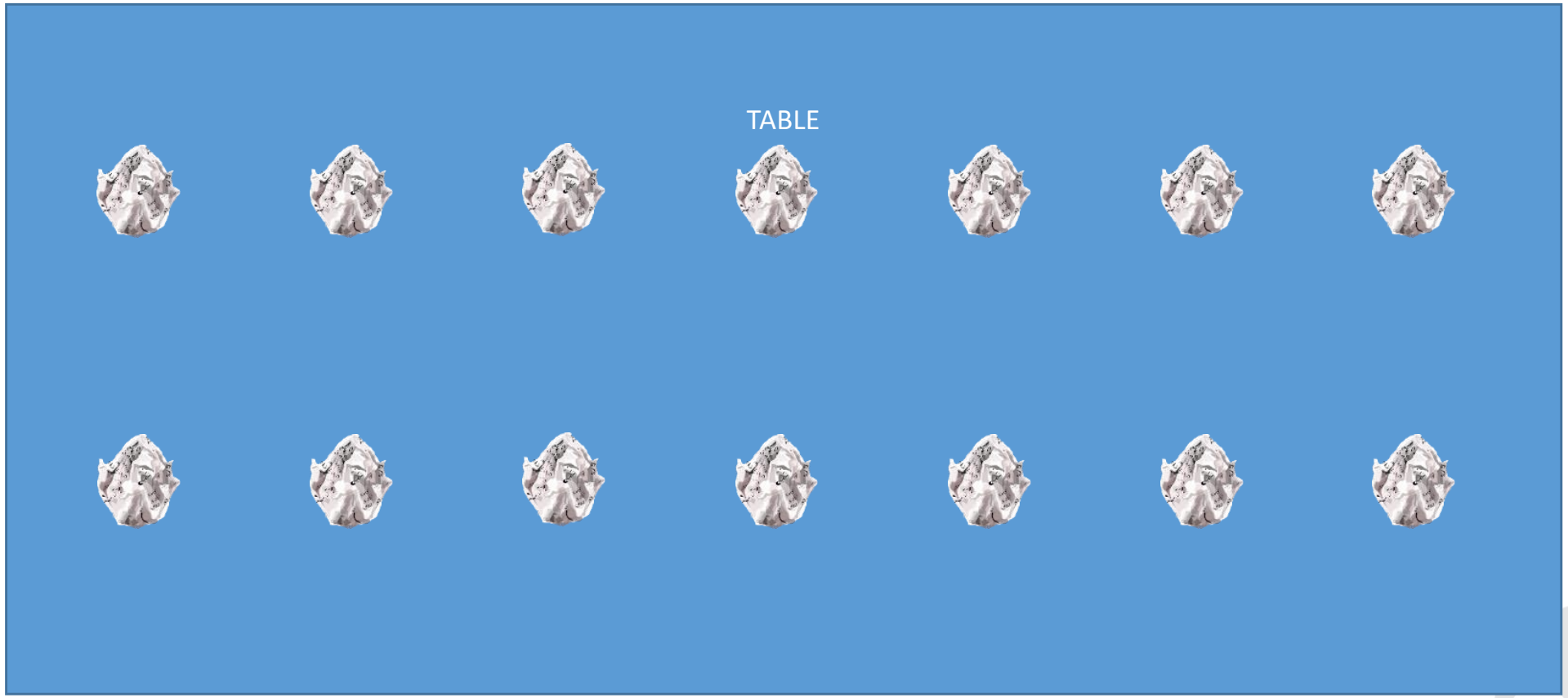
Memory Compression

To fit a new page old might need to be paged out…

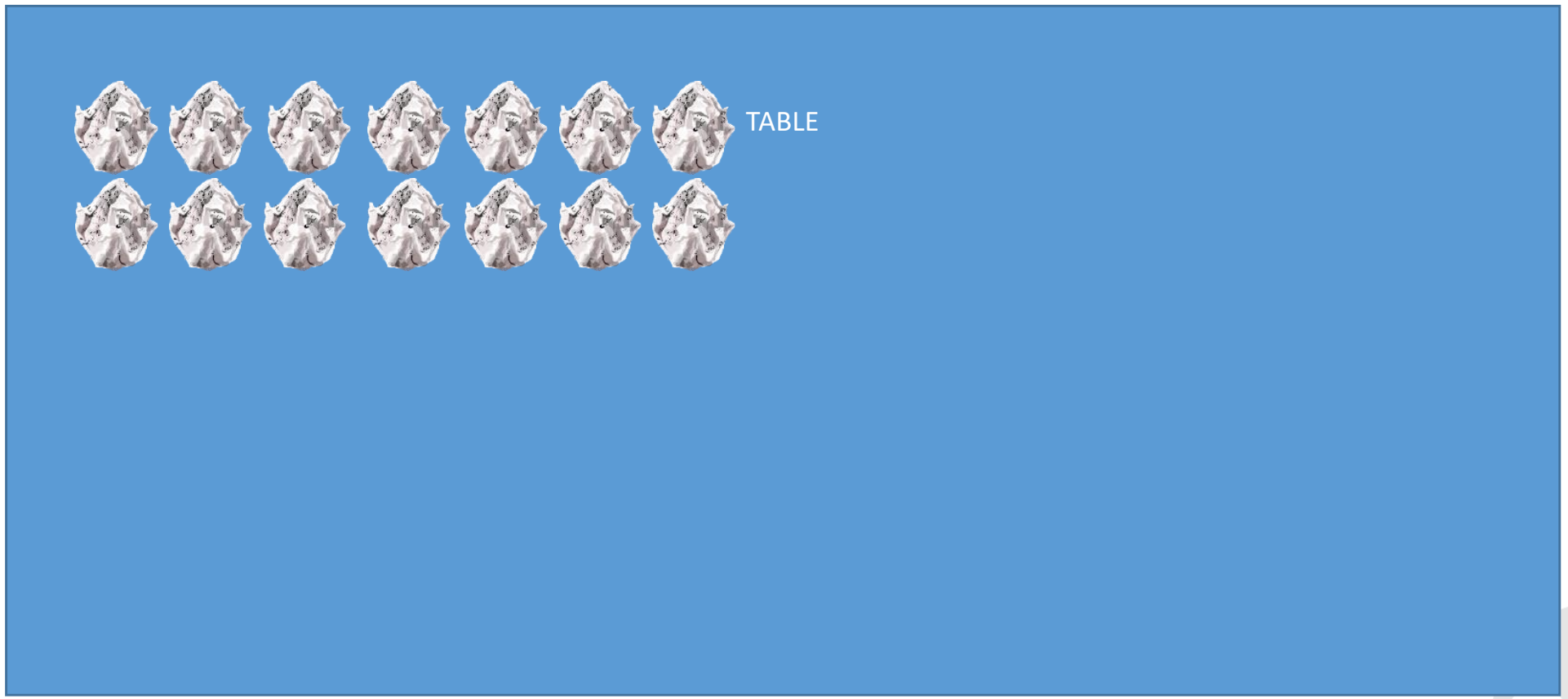




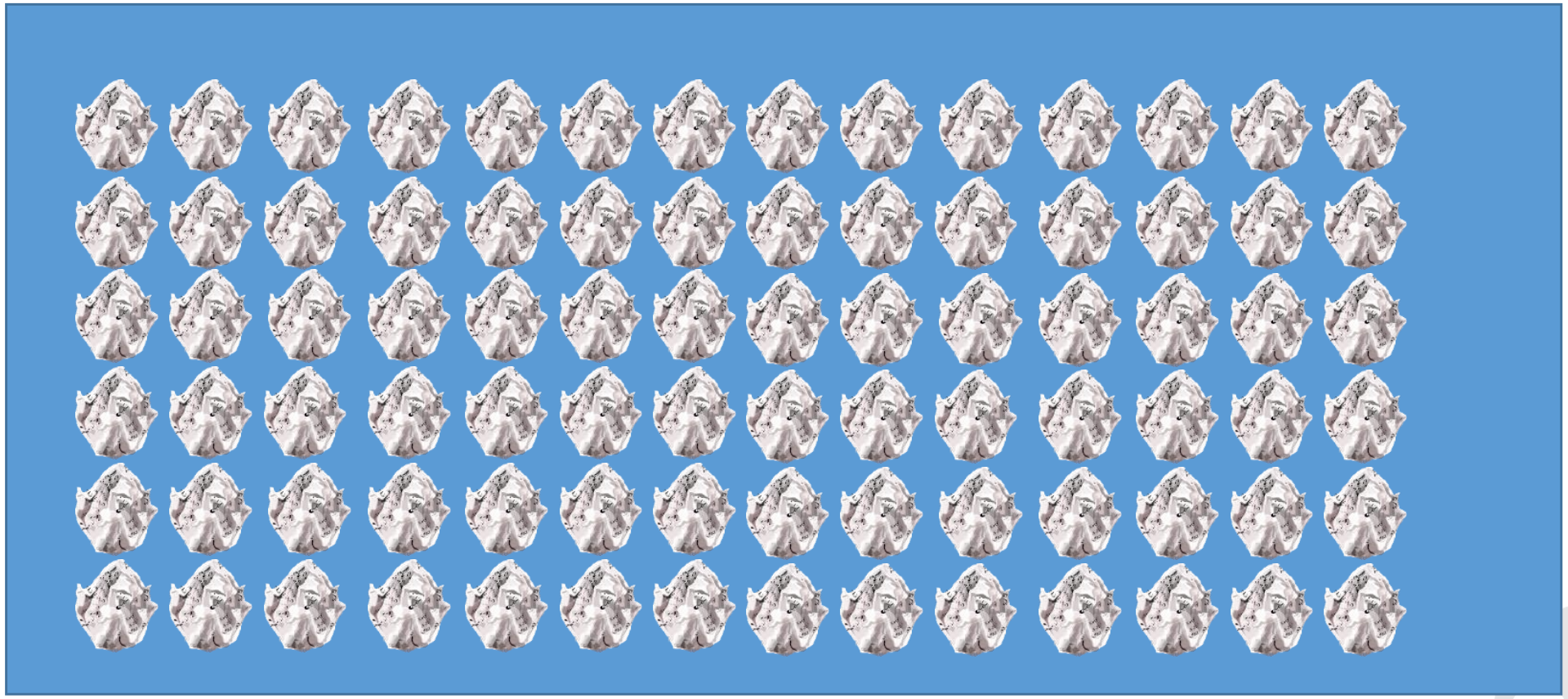
Compress the pages



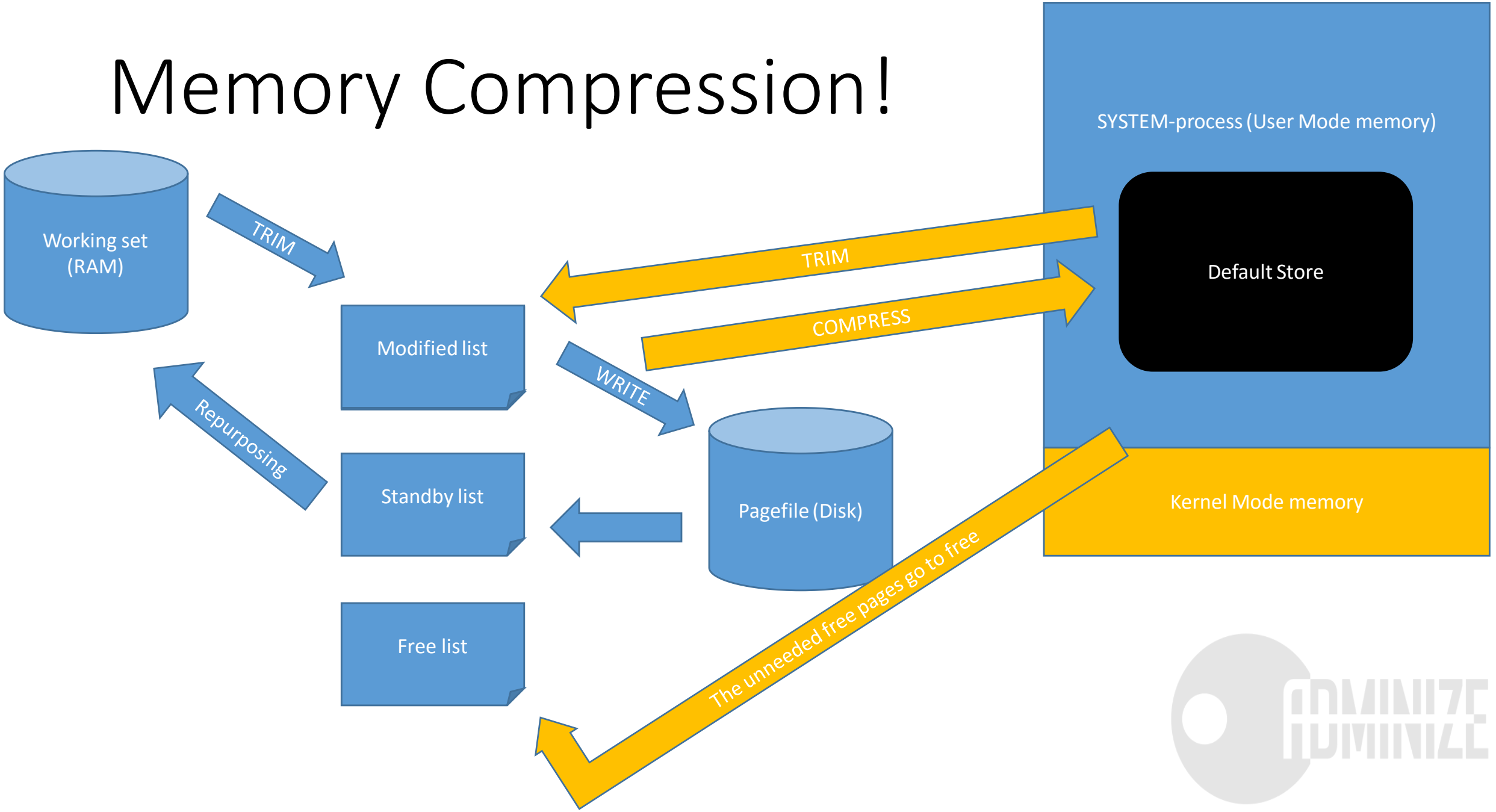
Compressed pages on a table



Compressed pages on a table



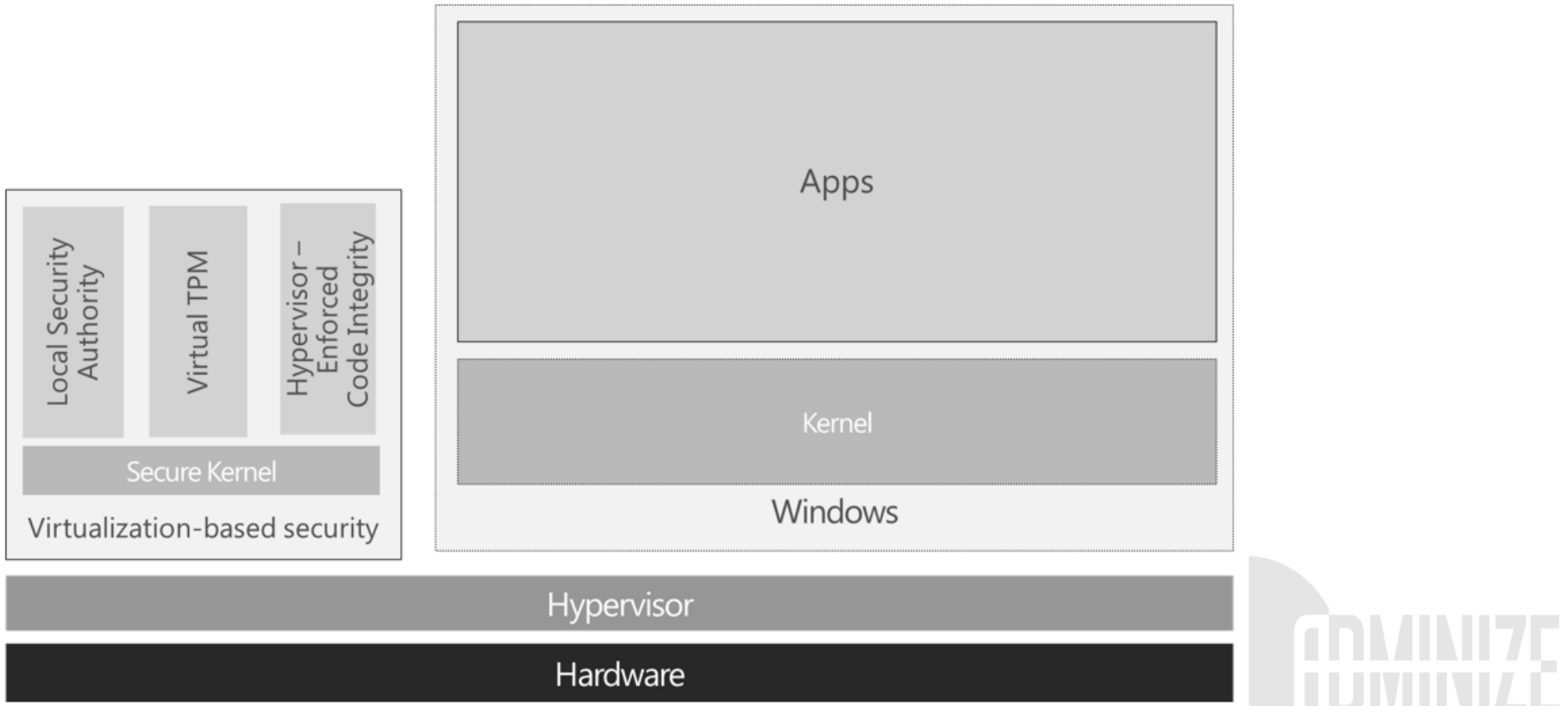
Memory Compression!



Device Drivers

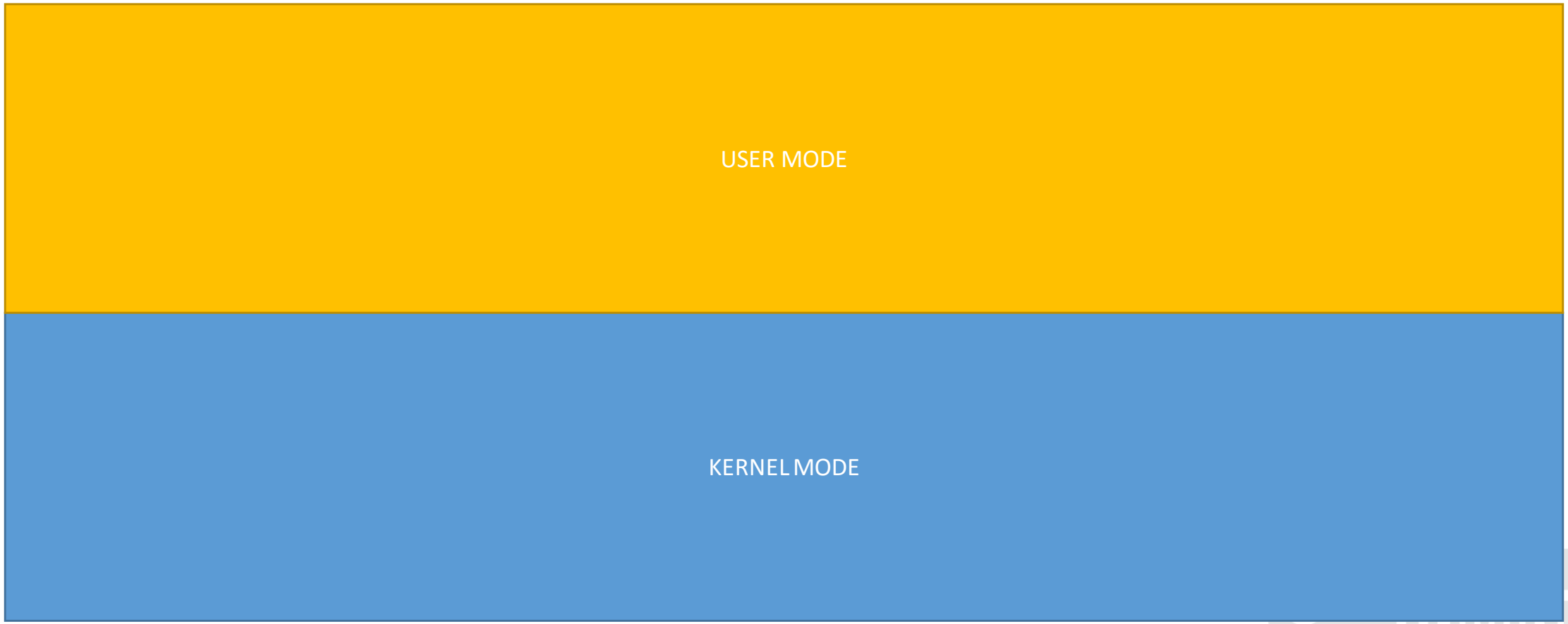
- Microsoft Signatures to be REQUIRED for Windows 10 Kernel-Mode Drivers
- To distribute you will have to:
  - Sign your driver package with your company's code signing certificate
  - Login to the Microsoft Hardware Developer Portal
  - Upload your signed driver package
  - Agree to a few particulars
  - Download the Microsoft signed files (within minutes)
- Why?
  - driver signing is vulnerable to exploitation
  - Bad guys have managed to steal certificates
  - some have even managed to acquire code signing certs on their own

Device Guard

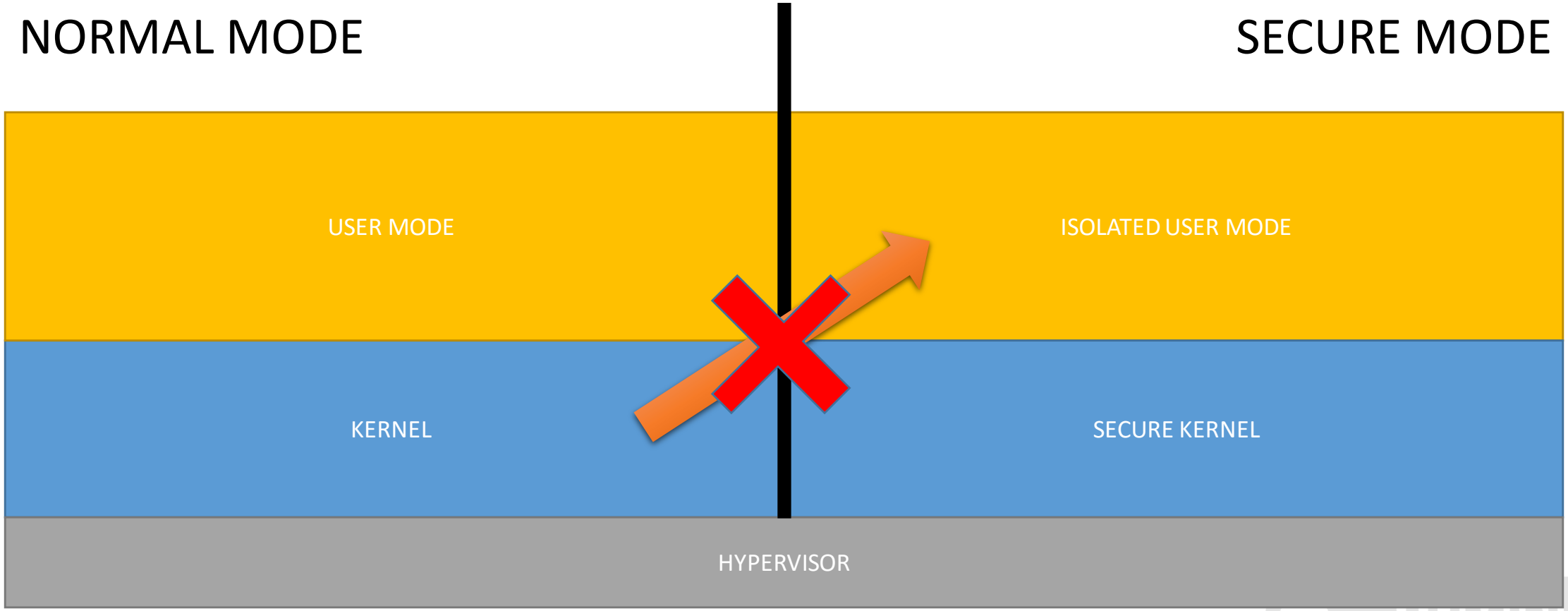


Isolated User Mode

Traditional Kernel Mode vs User Mode



Normal and Secure mode



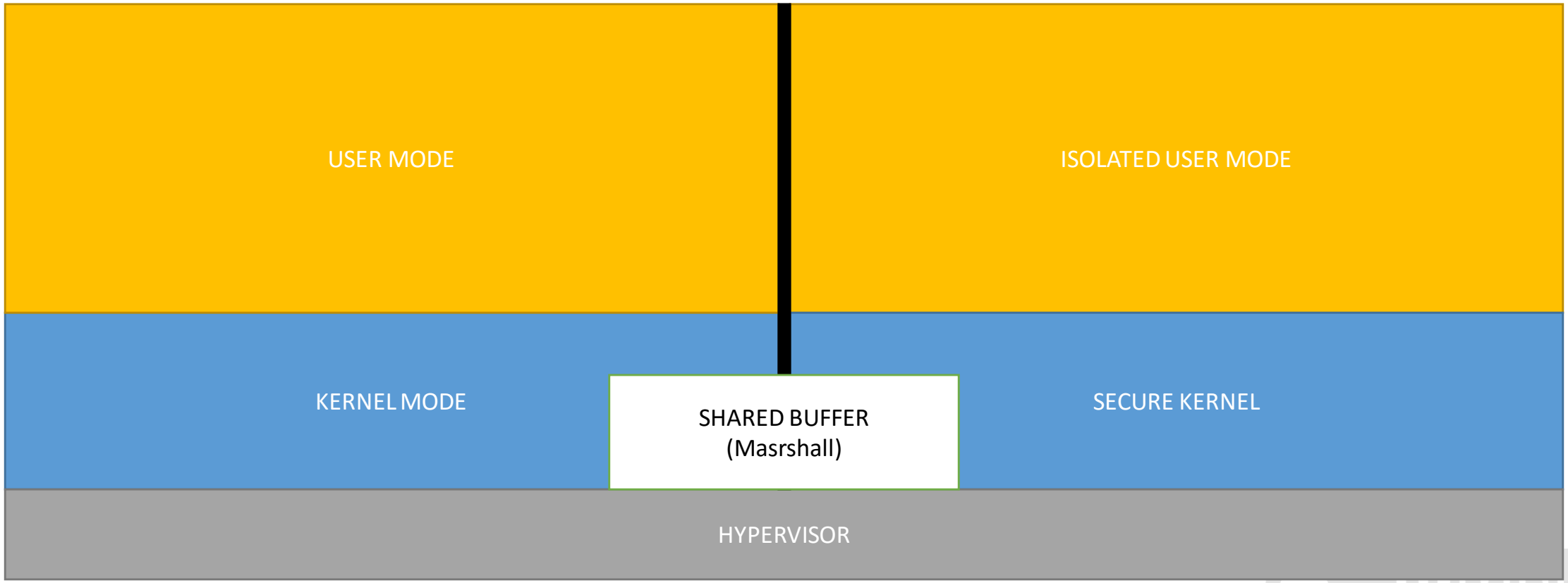
Isolated User Mode

- Protects User Mode from the code in the Kernel Mode
  - Normally Kernel has full visibility to User Mode processes' memory

Secure Kernel

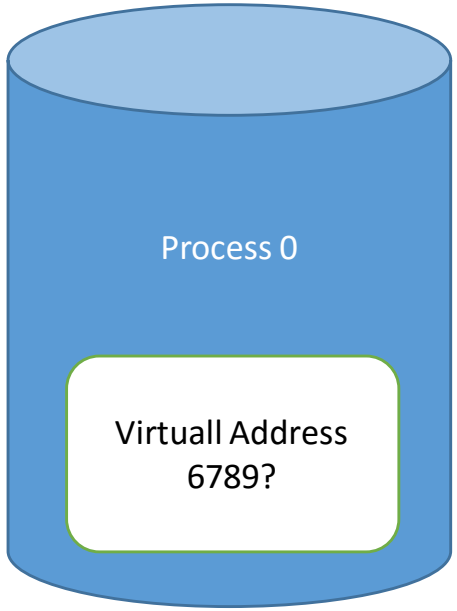
- IUM is on top of Secure Kernel (Secure System)
- Not a real Kernel but more a proxy that talks to the real Kernel but marshalls the transactions and does sanity checks
- Does not implement stuff that the normal kernel already does
- Secure Kernel cannot be extended like the normal
  - Only accessible by Microsoft not 3rd party
- All CryptoCode, Challenge/Response is here so it stays private to the Virtual Secure Mode

Traditional Kernel Mode vs User Mode

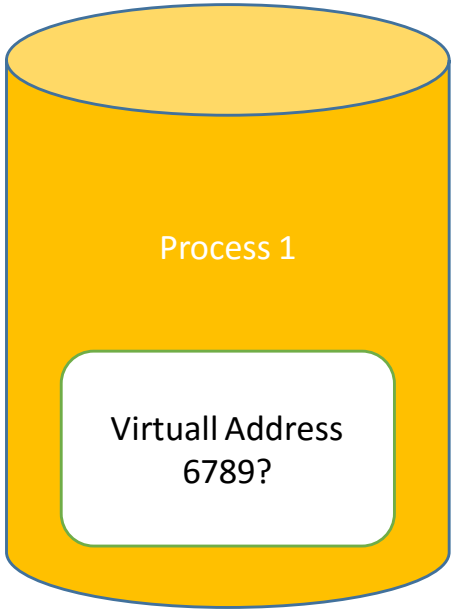


How come the Kernel is not able to access the memory of the Secure Kernel?

Traditional Virtual memory



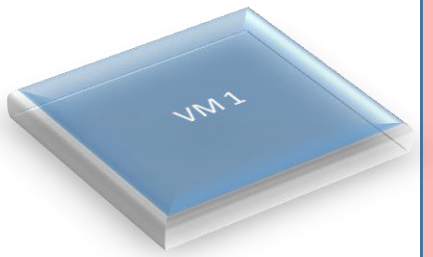
PAGETABLE	PROCESS 0	
V-Address	P-Address	ACCESSMASK
xxxx	yyyy	z-z-z
6789	0x7777777	R-X

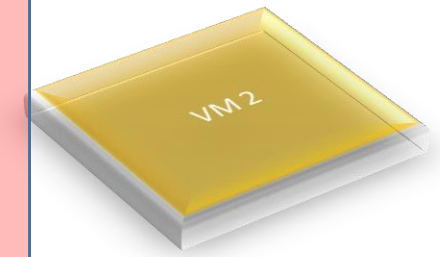


PAGETABLE	PROCESS 0	
V-Address	P-Address	ACCESSMASK
xxxx	yyyy	z-z-z
6789	0x7778888	RW-

Kernel has access to the Page Table so why wouldn’t it have access to the memory?

Hypervisors and VMs





PAGETABLE	VM 1	
GPA	SPA	ACCESSMASK
xxxx	yyyy	z-z-z
67890	0x7777777	R-X

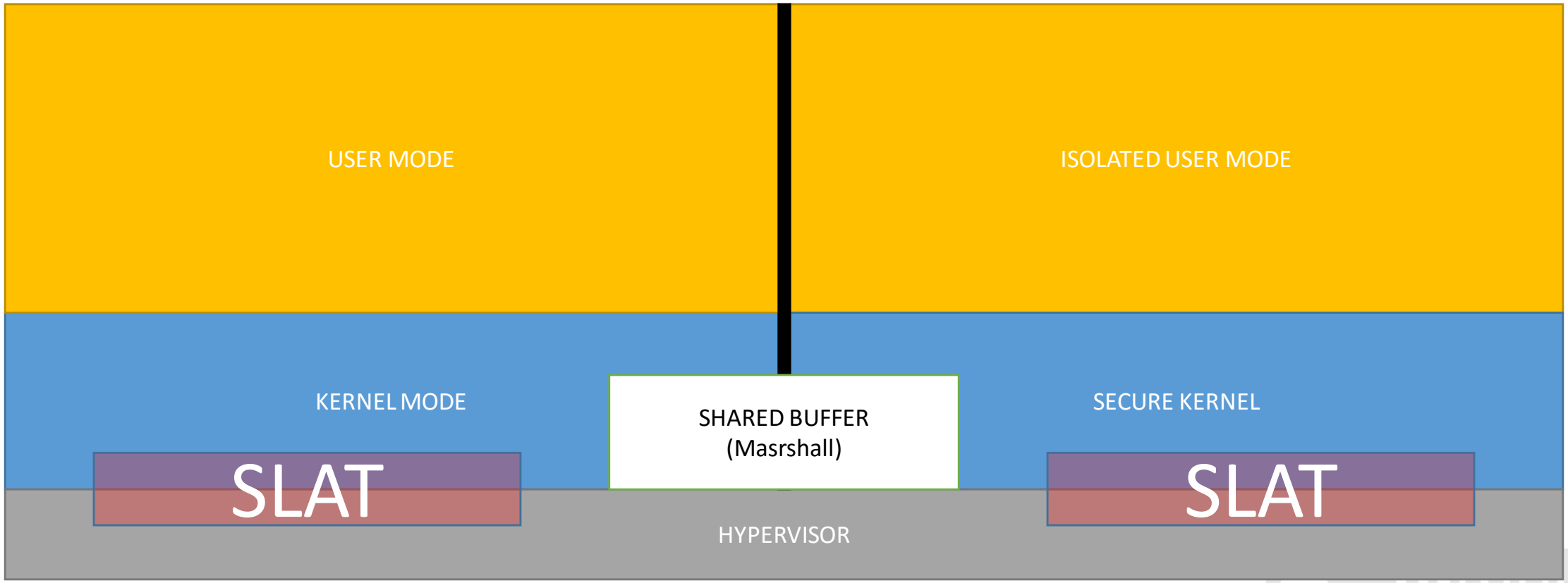
PAGETABLE	VM 2	
GPA	SPA	ACCESSMASK
xxxx	yyyy	z-z-z
67890	0x7778888	R-X

VIRTUAL RAM
Physical
Address?

VIRTUAL RAM
Physical
Address?

SLAT

Kernel and Secure Kernel have their own SLAT's

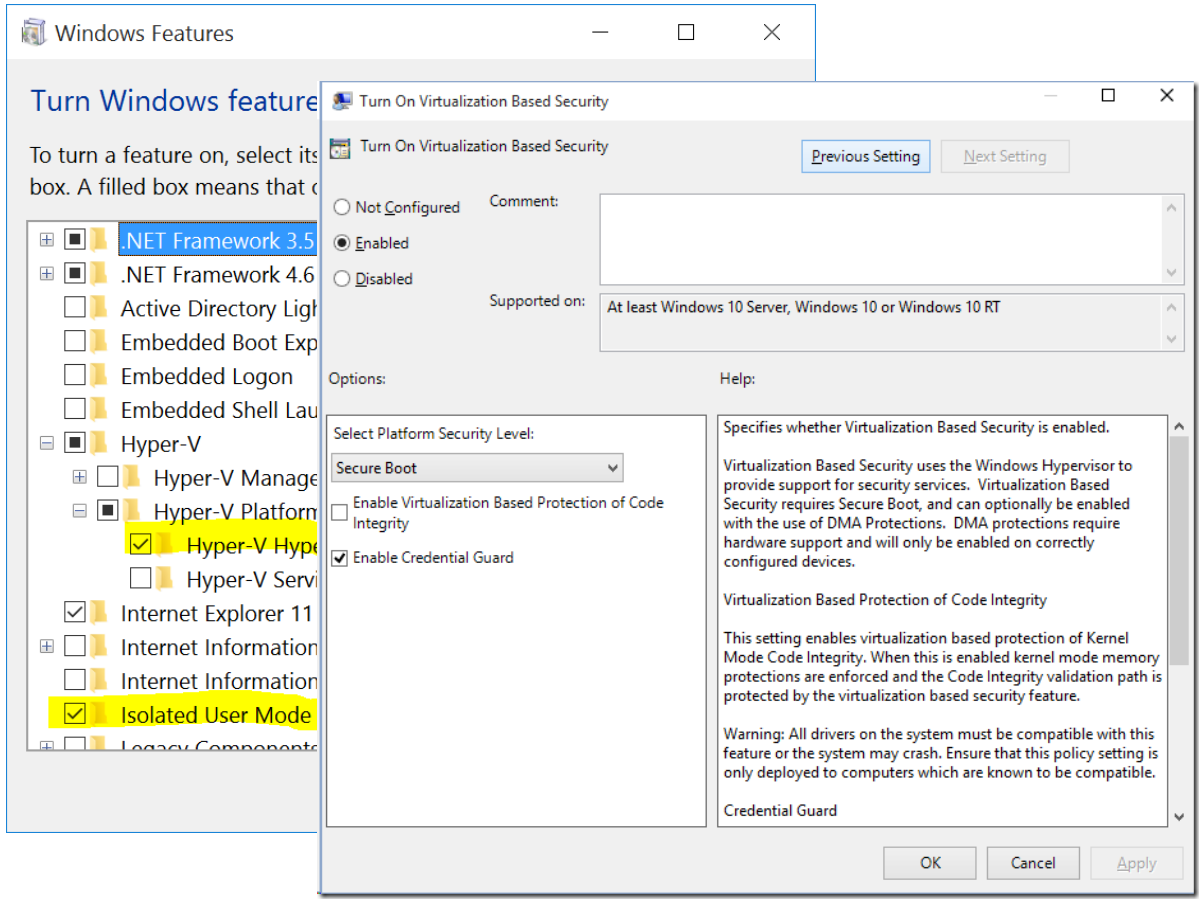


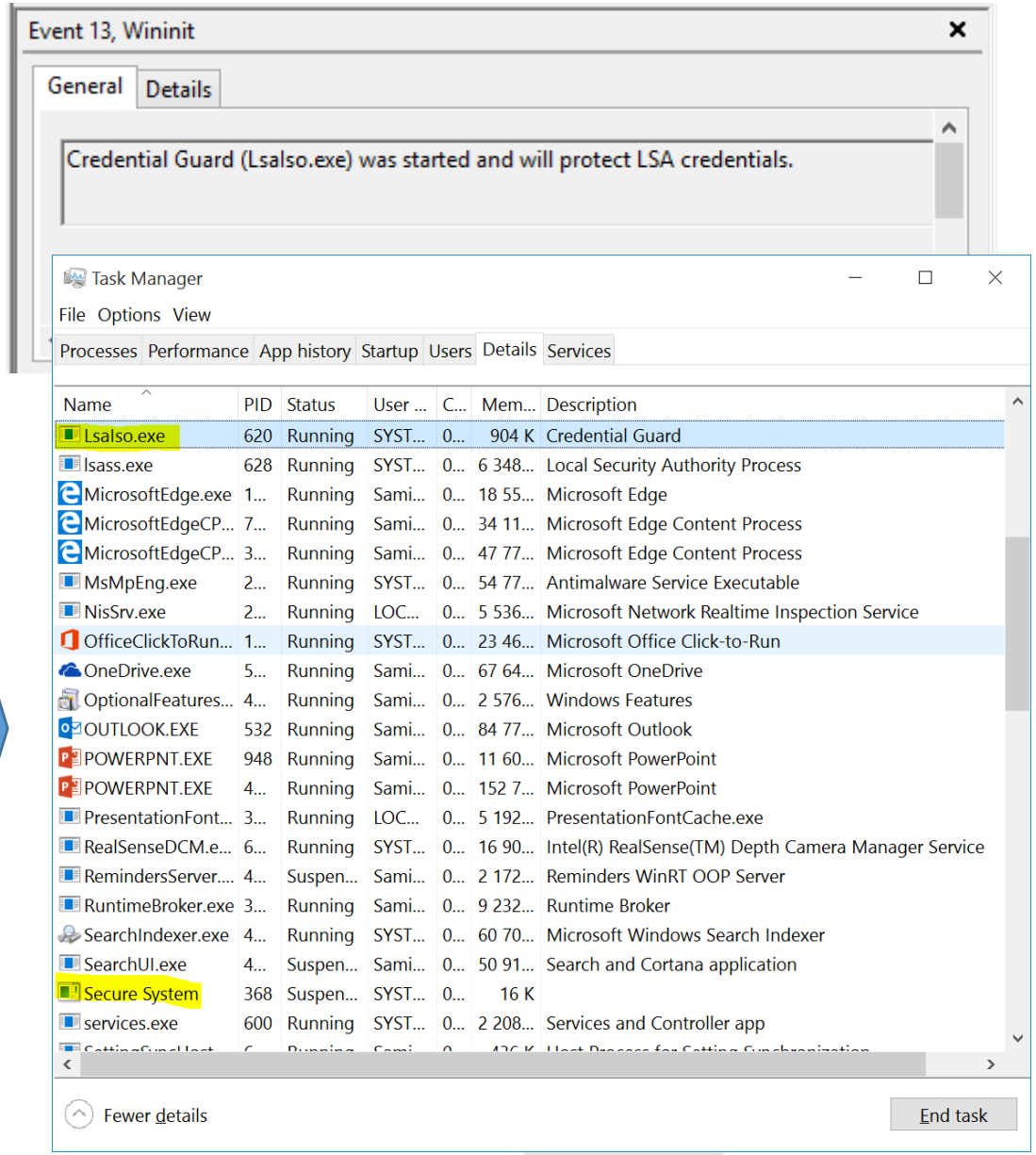
Hypervisors and VMs

So what is VSM? Really?

- It’s not really a VM but a functionality possible because of virtualization technology (Kind-Of-Semi-Almost-VM)
- This could be multiplied easily to many VMs

Enabling VSM





- **bcdedit /set vsmlaunchtype auto**

Trustlets

- Processes running in Virtual Secure Mode
  - Currently not available for developers
  - In the future anything that needs Secrets to stay secret
- Currently three trustlets
  - LSAISO = Credential Guard
  - vTPM = Virtual TPM
  - HVCI = Kernel Mode Code Integrity
- If a trustlet shuts down all keys are gone and the secrets are safe

Device Guard

- Device Guard requires:
  - UEFI Secure Boot with non-Microsoft UEFI CA removed from the UEFI database.
  - TPM 1.2
  - Virtualization support enabled by default in the system firmware (BIOS):
    - Virtualization extensions (e.g., Intel VT-x, AMD RVI)
    - SLAT (e.g., Intel EPT, AMD RVI)
    - IOMMU (e.g., Intel VT-d, AMD-Vi)
  - UEFI BIOS configured to prevent an unauthorized user from disabling Device Guard hardware security features.
  - Kernel mode drivers must be Microsoft signed and compatible with hypervisor-enforced code integrity.
  - Windows 10 Enterprise only

DEMO

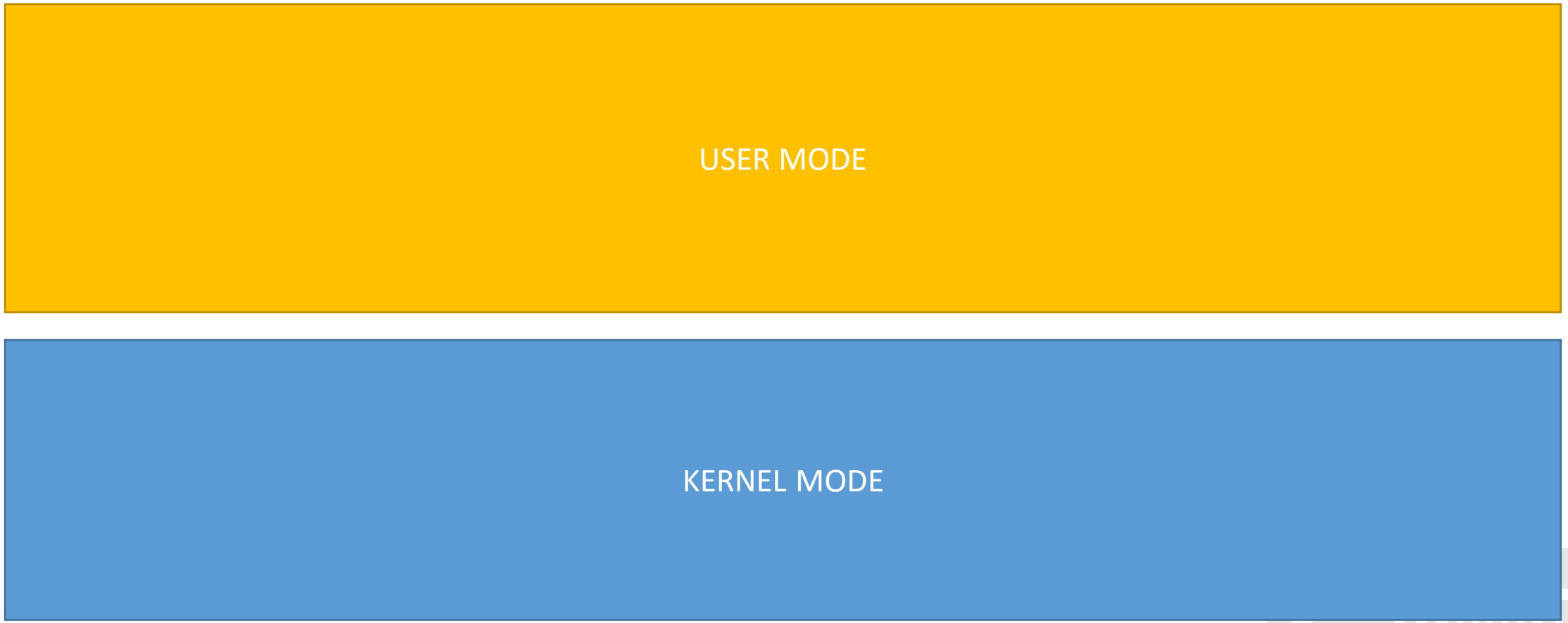
Process Dump

Nested Virtualization

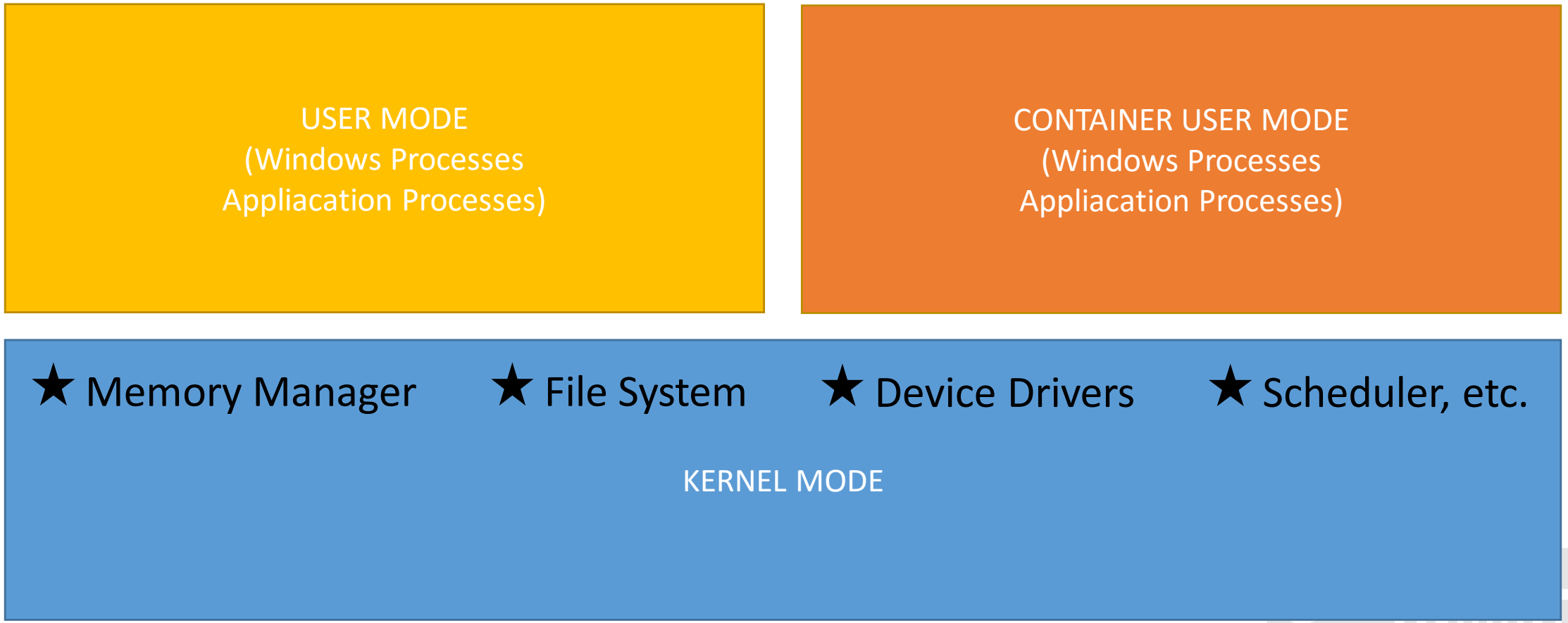
Containers

- Containers are a new level of virtualization
- I see it like App-V for Operating Systems
- Two different levels: **Server Containers** and **Hyper-V Containers**
- More info:
  - http://blogs.technet.com/b/virtualization/archive/2015/10/13/windows-insider-preview-nested-virtualization.aspx
  - https://channel9.msdn.com/Events/Build/2015/2-704

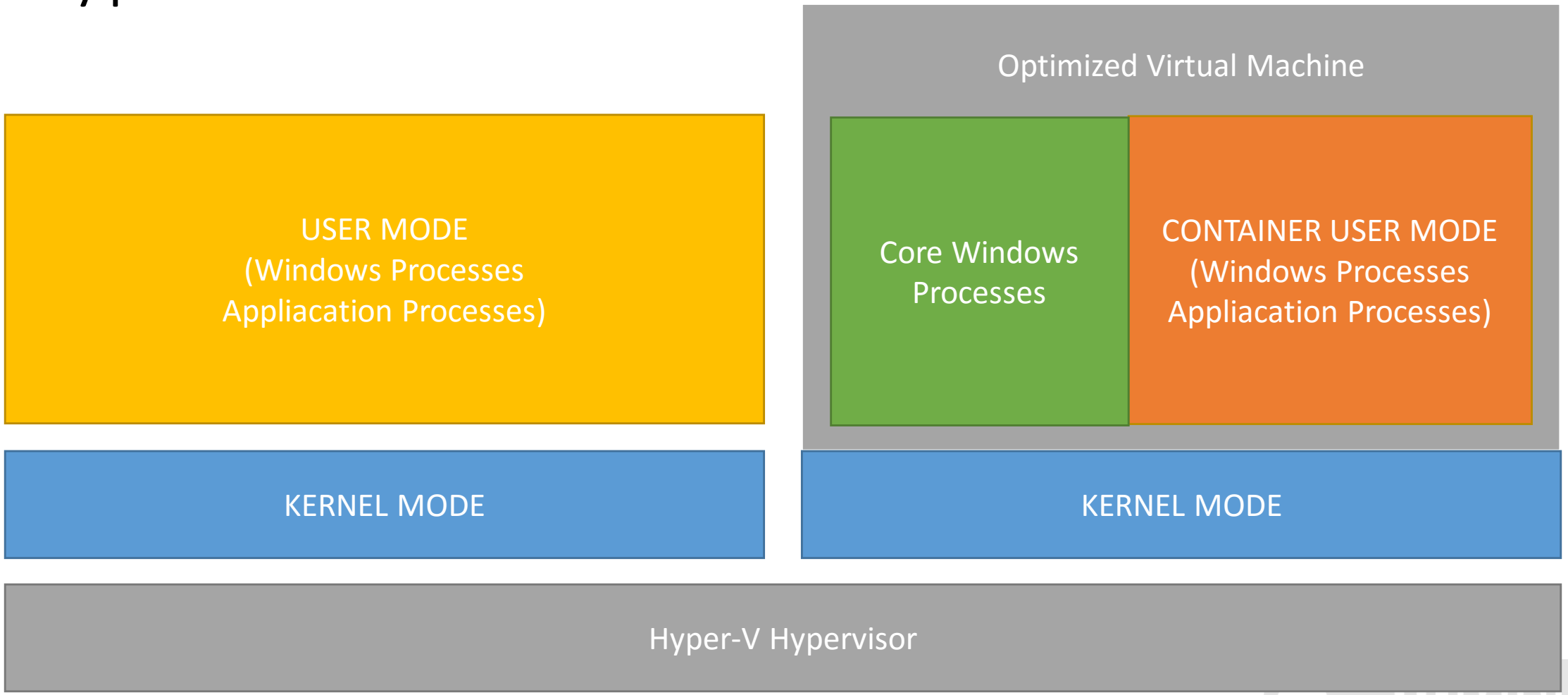
Server Containers



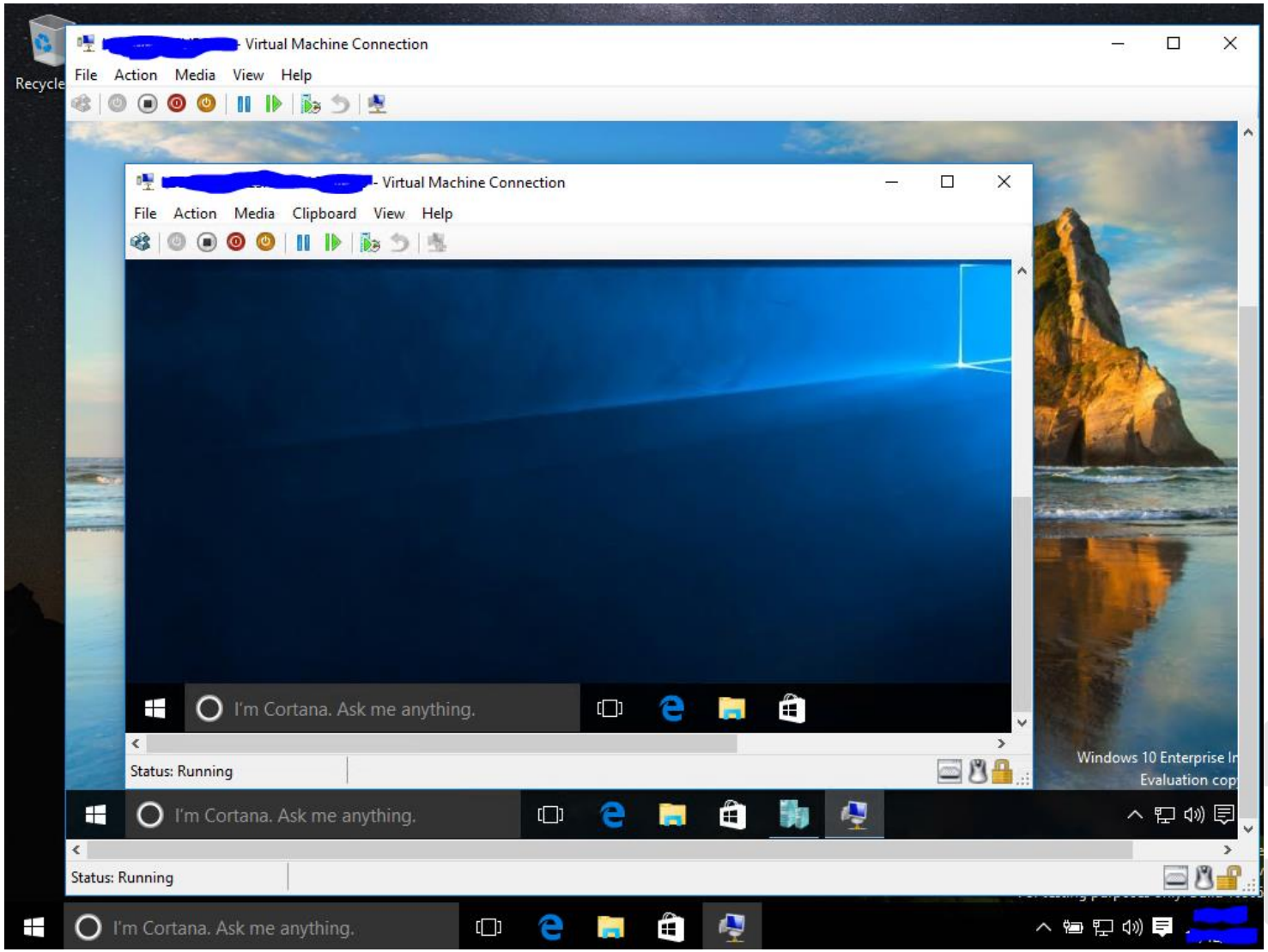
Server Containers



Hyper-V Containers



Hyper-V inside of Hyper-V



Contact

- sami@adminize.com
- Twitter: @samilaiho
- Blog: http://blog.win-fu.com/
- Free newsletter: http://eepurl.com/F-GOj
- Websites:
  - www.adminize.com
  - www.win-fu.com
  - www.wioski.com
  - www.samilaiho.com
- Video-based training:
  - Later: http://www.pluralsight.com/
  - NOW: http://dojo.win-fu.com/

Nächster Event: Freitag 17. Juni Digicomp Bern
(begrenzte Anzahl Teilnehmer möglich)