
Yoda
HUMAN MIND & CLOUD TECHNOLOGY

Agenda

1 **Cos'è Autopilot**
Autopilot permette di semplificare la gestione dei devices, direttamente dal cloud

2 **Offerta Autopilot base**
Un'offerta per configurare una soluzione Autopilot base, per gestire il normale ciclo di vita dei devices

3 **Offerta Autopilot Secure PC**
Un'offerta per proteggere i devices utilizzando le features di Windows 10 principalmente HW-based

4 **Offerta Surface**
È possibile delegare a Yooda il controllo parziale o totale della soluzione

5 **Perché Surface**
La sicurezza, il design, i materiali, la durata: Surface è l'unico device interamente gestibile da cloud

6 **Secure PCs**
Le feature di Windows 10 basate sulla virtualizzazione HW permettono di migliorare la security posture

Yooda


APPS
Identity Protection
INFORMATION PROTECTION
SharePoint
Intune
ATP
Defender
DATA
COS'È
Azure AD
Artificial Intelligence
Operations
AUTOPILOT
Smartworking
Office 365
Device Management

Cos’è Autopilot

In sintesi

Autopilot è un set di funzionalità che permettono di gestire l’intero ciclo di vita di un device, dall’installazione al reset e recover in caso di problemi

Semplifica l’operatività IT

Autopilot riduce l’effort necessario per installare, resettare o riparare i computer degli utenti

Nessuna infrastruttura necessaria

Autopilot è basato interamente sul cloud, non è necessaria alcuna infrastruttura onprem; questo contribuisce a semplificare l’operatività ed ad abbassare i costi di esercizio

Migliora la user experience

L’utente finale riceve direttamente il device dal vendor hardware e dopo un paio di click può già iniziare a lavorare

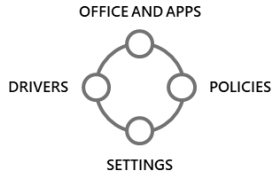
Unbox. Login. Take off

Yooda

Focus on: Windows Autopilot

Unbox e inizia a lavorare, semplicemente!

the old way



Build a custom image, gathering everything else that's necessary to deploy

Deploy image to a new computer, overwriting what was originally on it

Time is money, making this an expensive proposition

the new way (It's a kind of magic)

Un-box and turn on off-the-shelf Windows PC

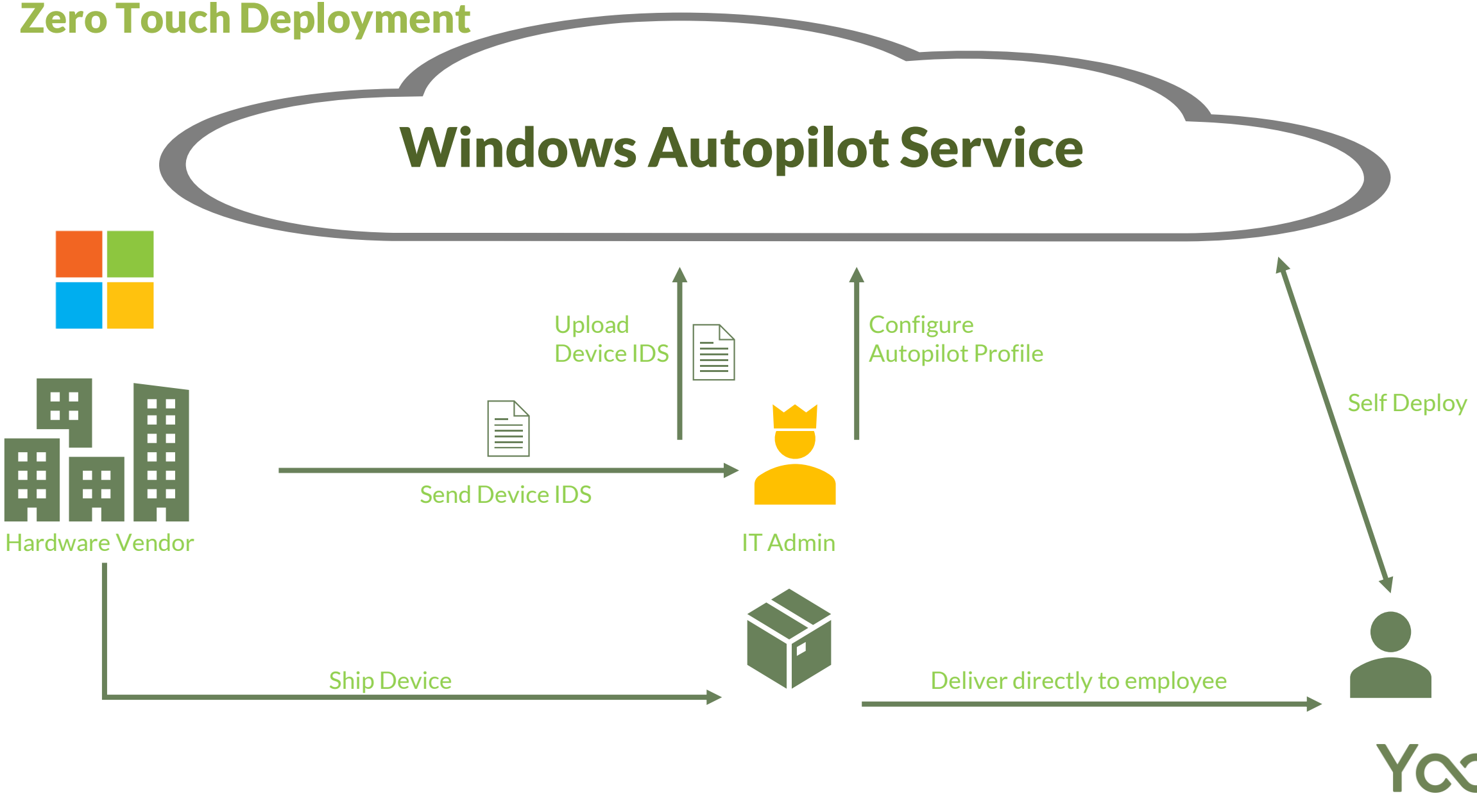
Transform with minimal user interaction

Device is ready for productive use

Yooda

Focus on: Windows Autopilot

Zero Touch Deployment



Yooda

Microsoft Autopilot

Value to customers

Zero Touch Deployment
Il devices viene spedito direttamente all'utente, nessuna attività da parte dell'IT

Integrato con Microsoft management
Nativamente integrato nel Microsoft management stack

Migliore user experience
L'utente riceve un PC già configurato e può contare su un rapido refresh in caso di necessità

Co-management col partner
È possibile delegare a Yooda il controllo parziale o totale della soluzione

No infrastrutture onprem
Nessuna infrastruttura onprem necessaria, soluzione completamente cloud

Reset dei devices
I devices possono essere resettati remotamente e ripartire da una configurazione clean

Yooda


APPS
Identity Protection
Smartworking
INFORMATION PROTECTION
SharePoint
Intune
ATP
Defender
DATA
Azure AD
Device Management
Artificial Intelligence
Operations
AUTOPILOT
Office 365
Offerta base

Microsoft Autopilot

Offerta ambiente pilota

PoC o Pilota
Configurazione di un ambiente pilota su PC personale IT (max 5 PC). I PC saranno messi a disposizione dal cliente

Configurazione ZTD
Configurazione in modalità Self-Driven mode; i devices vengono spediti direttamente all'utente e saranno configurati all'inserimento delle credenziali

Configurazione pre-provisioning (in alternativa a ZTD)
Configurazione di autopilot in modalità pre-provisioning; vengono accorciati i tempi di attesa per l'utente finale

Autopilot Reset
Configurazione della funzionalità Autopilot Reset in modo che sia possibile resettare un device ad uno stato di conformità

Push apps e configurazioni
Autopilot viene configurato affinché, tramite Intune, sia possibile gestire l'installazione di nuove applicazioni e nuove configurazioni

Microsoft Autopilot

Offerta base

Configurazione ZTD
Configurazione in modalità Self-Driven mode; i devices vengono spediti direttamente all'utente e saranno configurati all'inserimento delle credenziali

Configurazione pre-provisioning (in alternativa a ZTD)
Configurazione di autopilot in modalità pre-provisioning; vengono accorciati i tempi di attesa per l'utente finale

Autopilot Reset
Configurazione della funzionalità Autopilot Reset in modo che sia possibile resettare un device ad uno stato di conformità

Push apps e configurazioni*
Autopilot viene configurato affinché, tramite Intune, sia possibile gestire l'installazione di nuove applicazioni e nuove configurazioni

** L'offerta prevede 2 applicazioni standard (es. Office 365, Firefox), configurazione 1 Compliance Profile, 1 Configuration Profile (max 25 PC)*

La nostra offerta

Added value

Co-management

L'utente riceve un PC già configurato e può contare su un rapido refresh in caso di necessità

Solution Delivery

Configurazione di Intune per gestire Windows 10, Android e IOS

Lifecycle management

Nessuna infrastruttura onprem necessaria, soluzione completamente cloud

Protezione

È possibile delegare a Yooda il controllo parziale o totale della soluzione

Yooda


APPS
Identity Protection
Smartworking
INFORMATION PROTECTION
SharePoint
Intune
ATP
Defender
DATA
Azure AD
Device Management
Artificial Intelligence
Operations
AUTOPILOT
Office 365
Offerta Secure PC

Secure PCs

Autopilot and Intune to configure Secured PCs

Infrastructures (optional)

- Enable LAPS
- Configure Windows Update for Business
- Configure Secure AD

Surface Only

- Configure UEFI (DFCI, Surface only)
- Configure Secure Boot (Surface Only)

Hardware Based Security

Enable Credential Guard
- Isolate key system and user secrets

Enable DeviceGuard
- Application Control
- Enable Application Guard and Network Isolation (Network Protection)
- Exploit Protection
- Controlled Folder Access (Protect from ransomware)
- Attack Surface Reduction

Further Security

Enable Bitlocker
- Automatic device encryption during OOBE when
  - Tpm is present
  - Secure boot is enabled

Enable Security Baselines

Enable Windows Hello
- Paired with password or pin during OOBE
- Valid biometric unlock TPM key to access pin and allows login

Enable OneDrive known-folders redirection

Yooda

APPS

Identity Protection

INFORMATION PROTECTION

SharePoint

Intune

ATP

Defender

Smartworking

DATA

Azure AD

Office 365

Artificial Intelligence

Operations

OFFERTA SURFACE

Device Management

Microsoft Endpoint Management

SEMM

UEFI

HVCI

Bundled solutions

Combo Autopilot + Surface

VIP – Smart Working

Surface Device
Surface Pro 7+ I5/8GB/128GB SSD LTE

Accessori
Surface Pen
Surface Type Cover
Travel Hub USB-C
Surface Extended Service Plans 4Y

Servizi
Autopilot *

VIP – Home + Office

Surface Device
Surface Laptop 3 I7/16GB/256GB SSD

Accessori
Surface Extended Service Plans 4Y
Surface Dock2

Servizi
Autopilot *

Office worker

Surface Device
Surface Laptop Go I5/8GB/128 GB SSD

Accessori
Surface USB-C Travel Hub
Surface Extended Service Plans 3Y

Servizi
Autopilot *

*Offerta ambiente pilota

Yooda

APPS

Identity Protection

Smartworking

INFORMATION PROTECTION

SharePoint

Intune

ATP

Defender

Office 365

DATA

Azure AD

Artificial Intelligence

Operations

PERCHÈ SURFACE

Device Management

Microsoft Endpoint Management

SEMM

UEFI

HVCI

Secure Surface

Secured PC

Virtualization Based Security (VBS) e **HVCI** permettono la creazione di una porzione di memoria isolata dal sistema operativo in modo da mitigare gli effetti di tentativi di compromissione; la memoria viene destinata a processi «secured» e ne viene impedita la lettura e scrittura alle applicazioni ed ai normali processi del sistema operativo

VBS e **HVCI** sono abilitati by default in Surface Book 3, Surface Laptop Go, Surface Pro X e Surface Pro 7+

UEFI è scritto e mantenuto direttamente in-house da Microsoft, aggiornato tramite Windows Update for Business e gestito tramite Microsoft Endpoint Manager

Secure Boot è abilitato di default, a protezione dell'integrità del firmware e del sistema operativo e un security processor (TPM 2.0) è abilitato a supporto di Bitlocker e Windows Hello

Yooda

Secure Surface

Secured chip to cloud

Chip

- UEFI w/TPM 2.0
- MDM UEFI Management
- SEMM
- Secure Boot
- BitLocker
- Windows Hello

to

Cloud

- Advanced Windows Security Features
- Conditional Access
- Windows Update for Business
- Microsoft Defender ATP
- Intune Wipe and Retire

Secure supply chain

Surface is secure since the factory
Microsoft reviews every line of code to guard against *supply chain attacks*

Trust chain

Root of Trust anchored in hardware
Boot Guard, Secure Boot
Each stage checks the signature of the next

Security components

SoC security processor—vendor and OEM keys
TPM 2.0—security processor

Secure Surface

Secure Boot and UEFI

UEFI has a "***reduced attack surface***"

- Unnecessary legacy code or unused code has been removed
- Reduced the number of runtime services and System Mode Management drivers

Surface is the only manufacturer to adopt Project-Mu, an open source code UEFI

- Consistent and transparent across Surface products

UEFI is **built in-house** by Surface team

- Microsoft reviews every line of code to guard against *supply chain attacks*

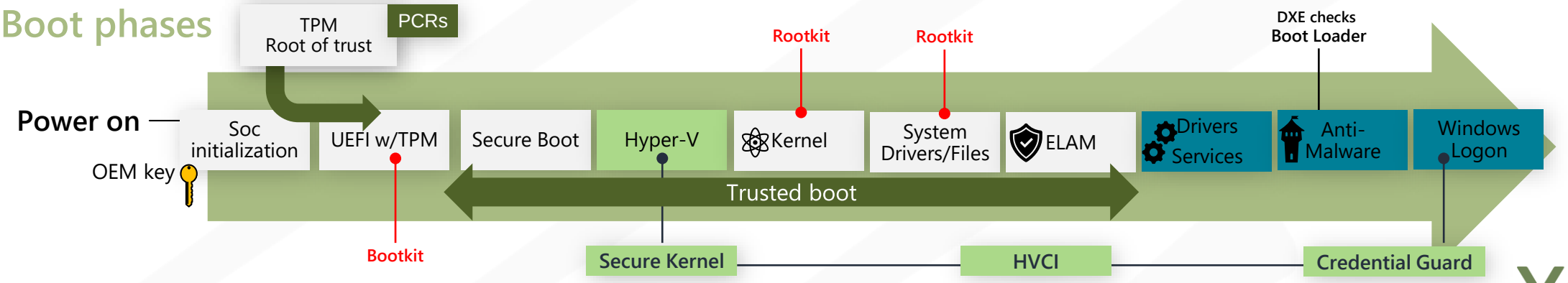
Surface updates **UEFI firmware proactively via Windows Update** for Business

- Customers' devices stay current with the latest fixes and security mitigations
- For example, when Spectre / Meltdown were announced, Surface updated customer devices in the field with mitigations

Managed through Intune

Eliminates BIOS passwords

Provides control of security settings (including boot options and built-in peripherals



Yooda

Secure Surface

Surface Firmware Update

Defense against Supply-chain attacks

- Surface builds UEFI/controllers/sensors/SoC firmware
- Surface UEFI based from Windows' UEFI Project Mu open source
- All code inspected by Surface engineers

A-B update mechanism

- Guard against corrupted updates

Firmware kept current via Windows Update

- Windows signed drivers wrap Capsule Updates
- Surface signed capsule update
- UEFI applies FW update payload
- Color progress bar indicates which FW is updating
- Unique feature to Surface – everything from microcode in the SoC to UEFI to your OS is kept up to date

Yooda

APPS

Identity Protection

Smartworking

INFORMATION PROTECTION

SharePoint

Intune

ATP

Defender

DATA

Azure AD

Device Management

Artificial Intelligence

Operations

PERCHÈ

Office 365

UEFI

SECURE PC

Secure Boot

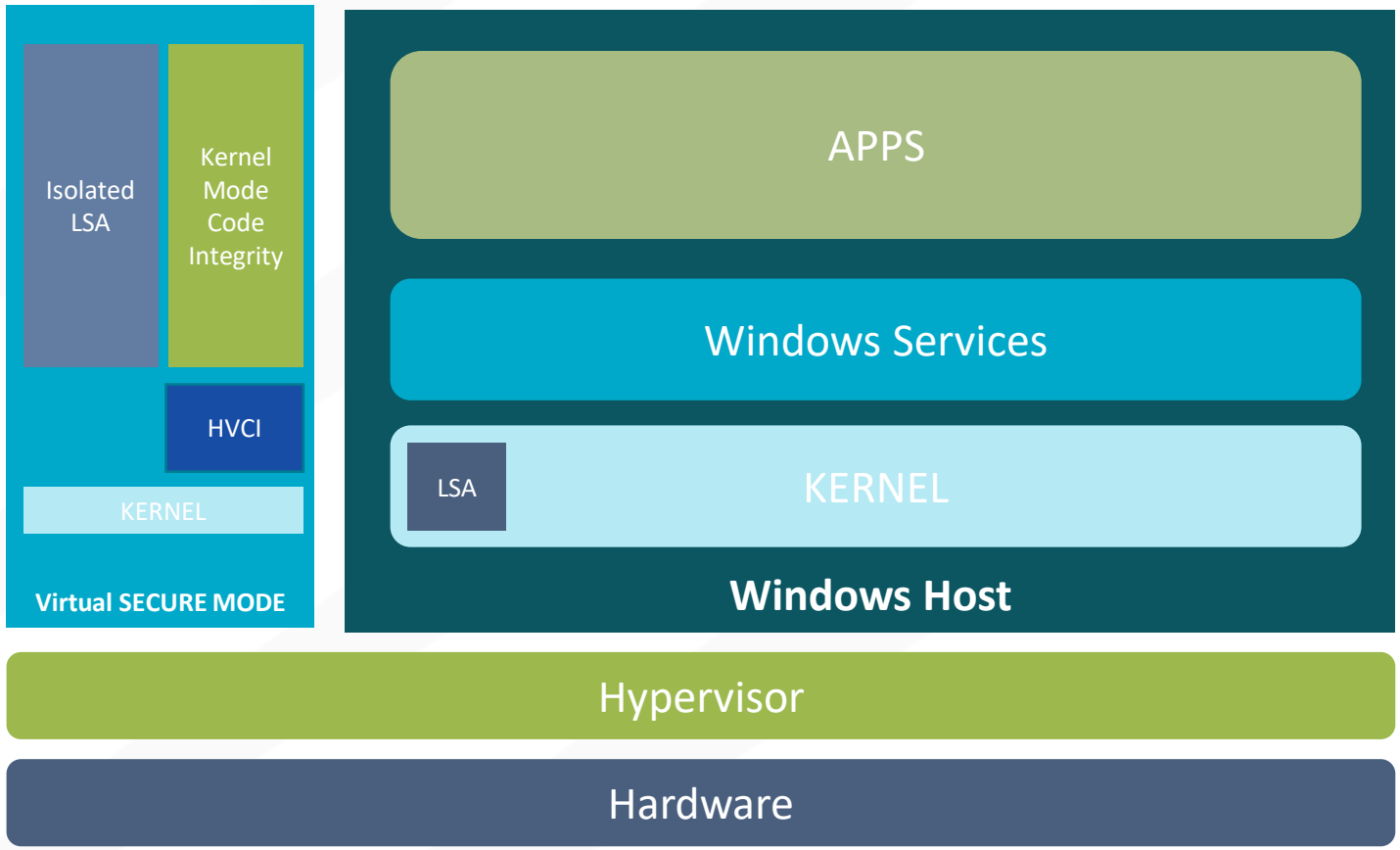
Hardware Based Security

Credential Guard e Device Guard

Virtualization Based Security (VBS) utilizza hardware virtualization per creare una regione di memoria isolata e protetta rispetto il sistema operativo.
Questa porzione di memoria è riservata ai processi che il virtualizzatore riserva allo scopo di separare i normali processi user/kernel dai processi che richiedono una diversa protezione

Credential Guard utilizza una porzione chiamata Isolated LSA per salvarvi user e system secrets

Device Guard utilizza HVCI per la gestione di processi quali Application Control e Application Guard



Yooda

Device Guard (AKA Windows Defender Application Control)

Ulteriori funzionalità di protezione

Exploit Protection

Applica mitigations da tipologie di exploit (ex EMET) quali ad esempio Arbitrary Code Guard, Data Execution Prevention, Code integrity guard e molti altri

Attack Surface Reduction

ASR comprende una serie di policy atte a bloccare la compromissione di sistemi e applicazioni da attacchi basati su malware anche presente all'interno di documenti Office e PDF

È possibile bloccare eseguibili da messaggi email, come l'esecuzione di child processes da documenti Office, o l'esecuzione di obfuscated code etc.

Controlled Folder Access

Controlled Folder Access è fondamentale per la protezione da ransomware. Inibisce l'accesso e la scrittura alle cartelle di Sistema e alle cartelle degli utenti; soltanto le applicazioni e gli script autorizzati possono modificarne il contenuto

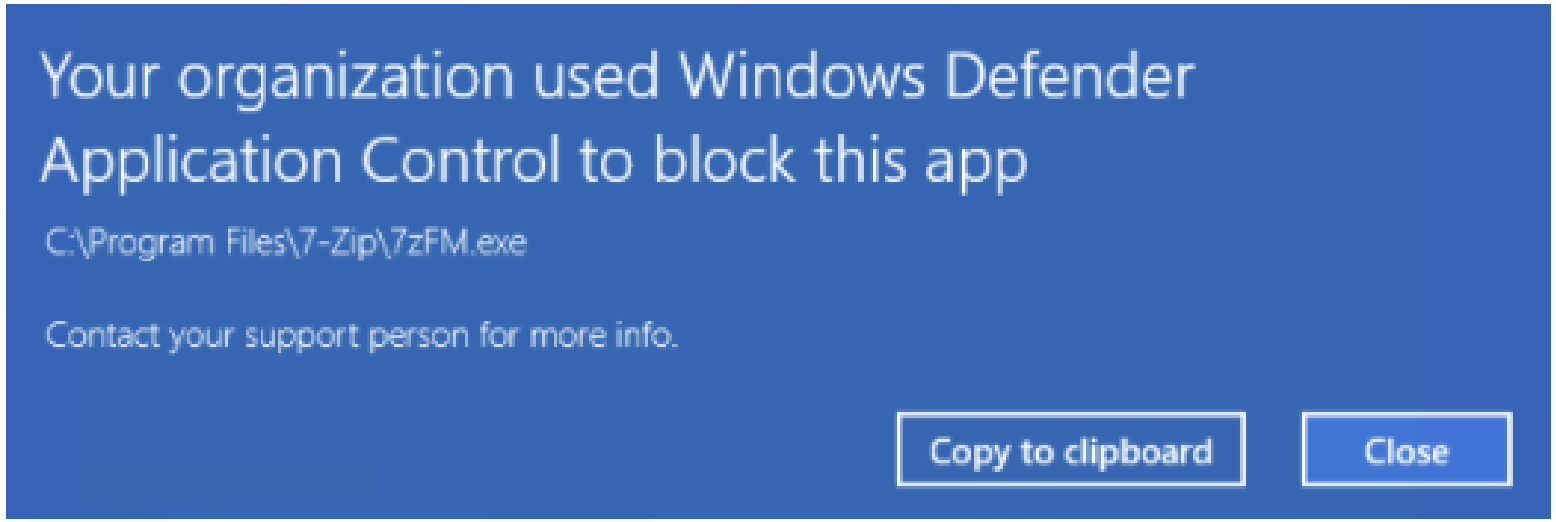
Richiede che la funzionalità di Windows Defender Antivirus real-time protection sia abilitata

Yooda

Application Control

Windows Defender Application Control permette, tramite l'utilizzo di Configurable Code Integrity (CCI), di restringere l'utilizzo di drivers, applicazioni e script; in questo modo si riducono le possibilità per un attaccante di compromettere il sistema.
CCI è avviato a livello kernel e pertanto prima del normale antivirus e delle altre applicazioni di sistema. Inoltre CCI può essere protetto tramite una firma digitale; in questo modo per un attaccante non è sufficiente impadronirsi delle credenziali amministrative per forzare le policy CCI.

Inoltre può essere protetto tramite **HVCI**; in questo modo, anche se un eventuale attaccante riuscisse ad impadronirsi di un processo a livello kernel, non riuscirebbe ancora a superare le policy CCI



Yooda

Application Guard

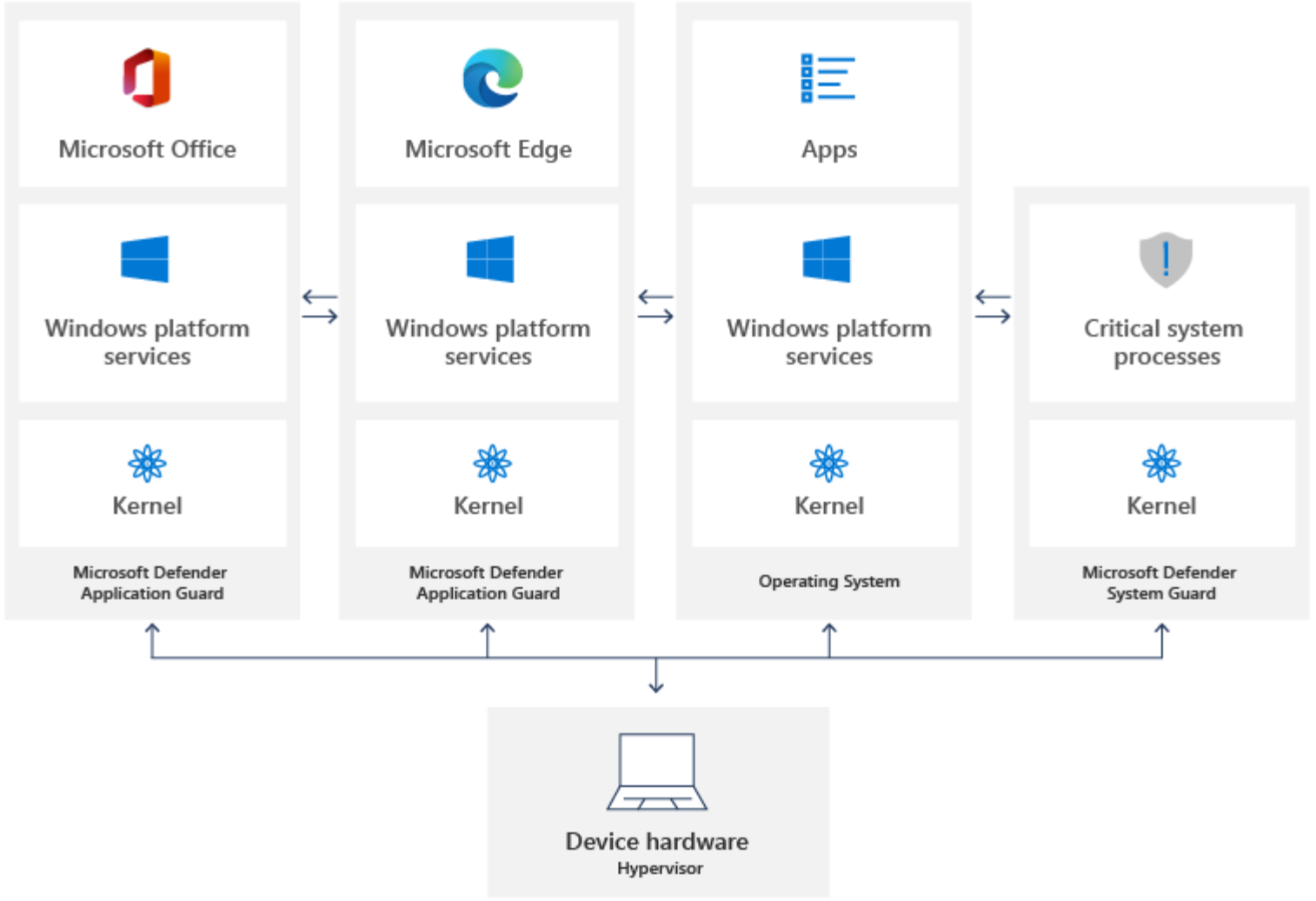
Application Guard permette di proteggere l'utente da attacchi condotti tramite siti web malevoli e documenti Office contenenti codice infetto

I documenti Office provenienti da origini sconosciute (ad esempio un allegato ad una mail) vengono eseguiti all'interno di un ambiente protetto (container); in questo modo se il documento contenesse codice infetto questo non potrebbe infettare il sistema operativo

Parimenti, qualora l'utente navigasse in un sito malevolo protetto tramite Application Guard, il sistema non sarebbe compromesso

Application Guard protegge nativamente Microsoft Edge, ma esistono estensioni per Chrome e Firefox

Application Guard for Office è disponibile con la licenza EMS E5



Further Security

Bitlocker, Security Baselines, Known-Folders

Bitlocker

Permette di cifrare il disco rigido (system e user partition) per rendere inaccessibili I dati in caso di furto o smarrimento del device

È suggerito l'utilizzo di device provvisti di TPM (diversamente occorre una chiavetta USB per eseguire il boot)

Security Baselines

Le Security Baselines sono template preconfigurati che permettono di gestire secondo best-practices di prodotto configurazioni relative a Windows, a Microsoft Edge ed a Windows Defender

Una security baseline può essere composta da più profili, ciascuno relativo a determinate componenti (ad esempio una security baseline può richiedere l'abilitazione di Bitlocker, l'attivazione di Windows Firewall, la richiesta di PIN o password per sbloccare un device, etc.)

Known-Folder Redirection

Known-Folders redirection permette di redirigere le known-folders (Documenti, Desktop, Pictures) in OneDrive; in questo modo si ottiene maggiore flessibilità (work anywhere) e security improvement; infatti, grazie al versioning di OneDrive è possibile mitigare facilmente attacchi di tipo ransomware

Yooda

Windows Hello for Business

I principali **identity breach** sono condotti attraverso tecniche di phishing delle credenziali; Windows Hello for Business, eliminando l'utilizzo di password, rappresenta un notevole miglioramento della **security posture**

Windows Hello for Business può essere utilizzato utilizzando le caratteristiche biometriche degli utenti (fingerprint, riconoscimento facciale) oppure tramite l'utilizzo di security keys (Fido2)

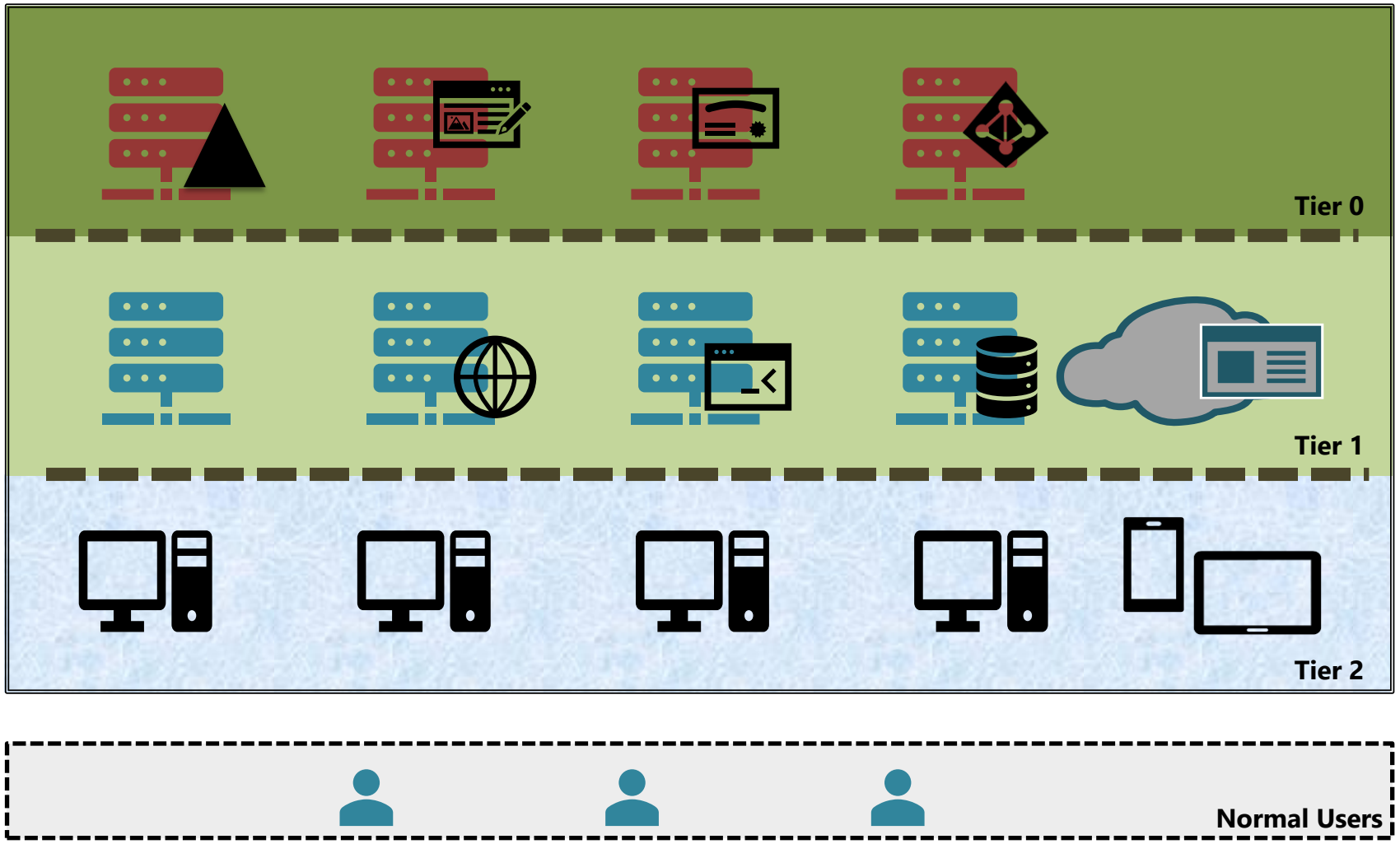
Vengono create delle chiavi asimmetriche che vengono utilizzate per l'autenticazione. La chiave privata non lascia mai il device e non è possibile risalire alle caratteristiche biometriche a partire dalla chiavi generate e conservate sul device (TPM 2.0 se disponibile)

Requirements

- Windows 10 versione 1511 o later
- Azure Active Directory in hybrid mode
- Estensione dello schema a Windows 2016
- Domain/Forest level Windows 2008 R2 o superiore
- Domain Controller Windows 2016 o superiore
- Certificate Authority Windows 2012 o superiore
- Azure MFA tenant
- Licenza Azure AD Premium

Yooda

Securing Privileged Access
AD Tiering



Active Directory tiering acts as a **containment** zone

The idea is to **harden the environment** making it harder for the attacker to escalate its position

Implementation of technical controls that **prevent privileged credentials** from intentionally or accidentally crossing tier boundaries

The primary focus is **controlling credential exposure. You never want higher tier credentials exposed at a lower tier.** Exposing a lower tier to a higher tier is allowed

Stefano Cerasa
Direzione Commerciale

A long career in Unified Communications, now tries to manage the company (good luck old fellow ☺)

s.cerasa@yooda.tech
+39 335 5611 764

Pacho Baratta
Marketing Manager

A UC guy for a very long time, focused on Exchange and OCS/S4B, now exploring new topics…

p.baratta@yooda.tech
+39 335 5715 630

Francesco Bragantini
CTO

Many, many years spent designing architectures and planning voice solutions. He's the yoda master, may the fourth be with us!

f.bragantini@yooda.tech
+39 334 6509 768

Yooda
HUMAN MIND & CLOUD TECHNOLOGY

Powered by
Yooda
HUMAN MIND & CLOUD TECHNOLOGY