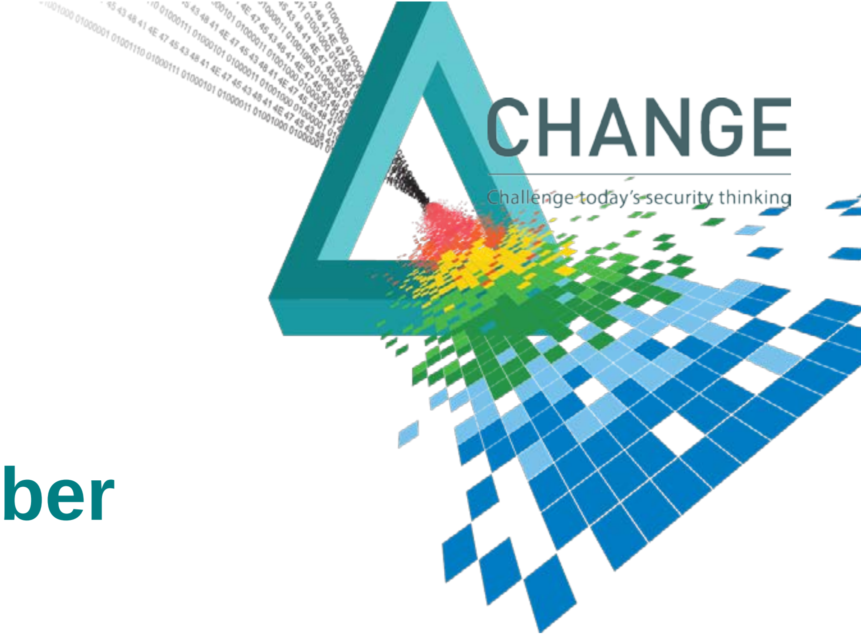
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

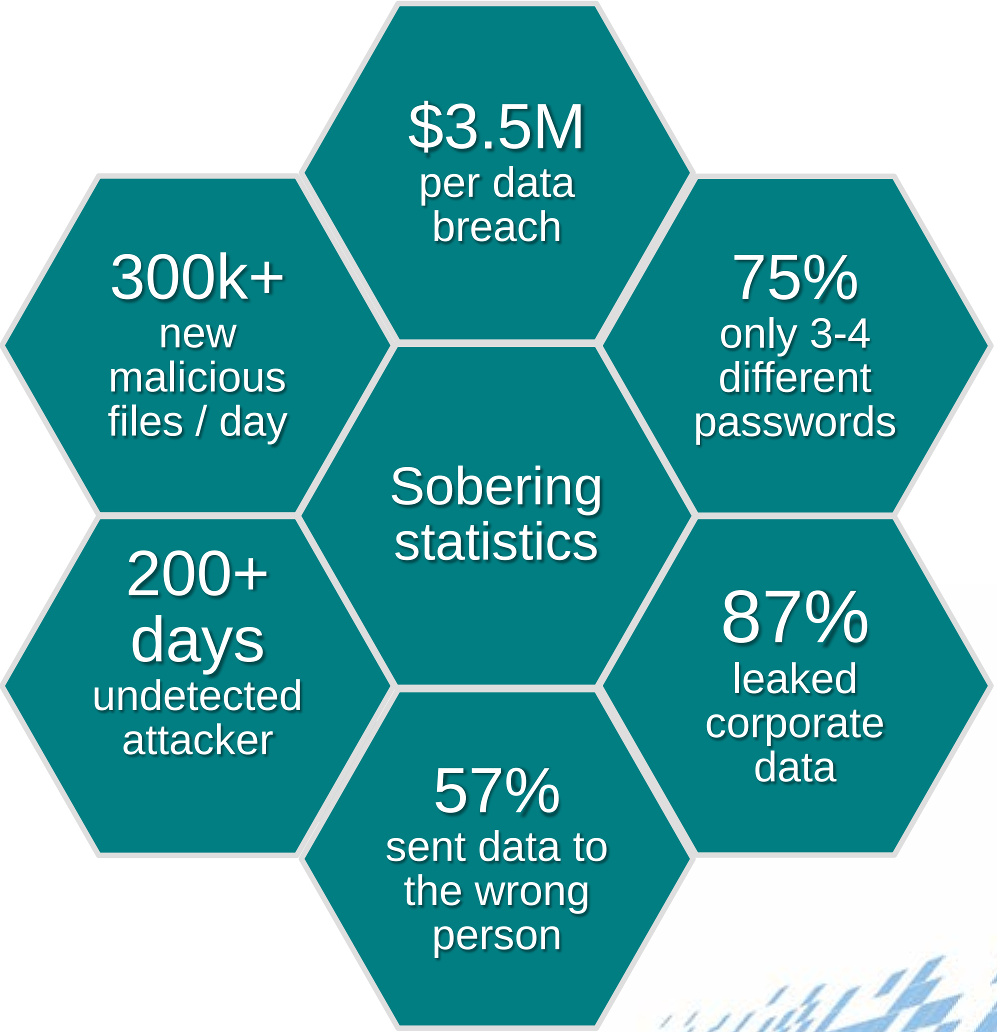


SESSION ID: SPO-W09A

Windows 10: Disrupting Cyber Threats

Cyril Voisin

Chief Security Officer, Middle East and Africa
Microsoft
@cyrilvoisin



Sobering statistics

$3.5M
per data breach

75%
only 3-4 different passwords

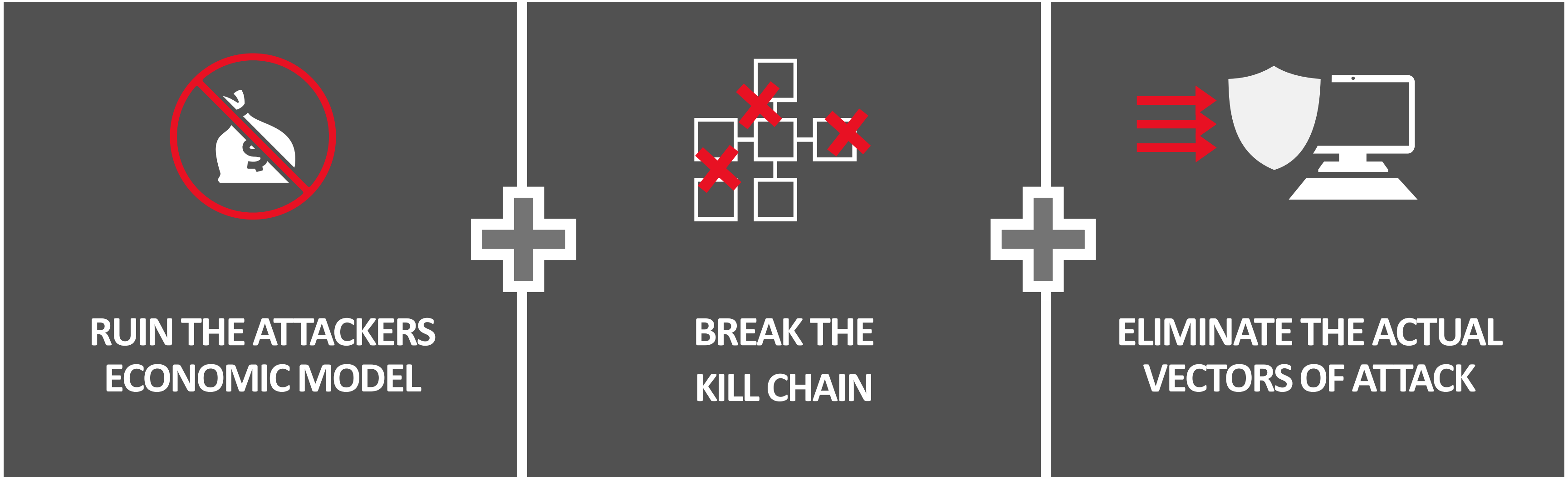
87%
leaked corporate data

57%
sent data to the wrong person

200+ days
undetected attacker

300k+
new malicious files / day

Addressing the Threats Requires a New Approach



RUIN THE ATTACKERS ECONOMIC MODEL

BREAK THE KILL CHAIN

ELIMINATE THE ACTUAL VECTORS OF ATTACK

Security from the inside out – beyond bigger walls

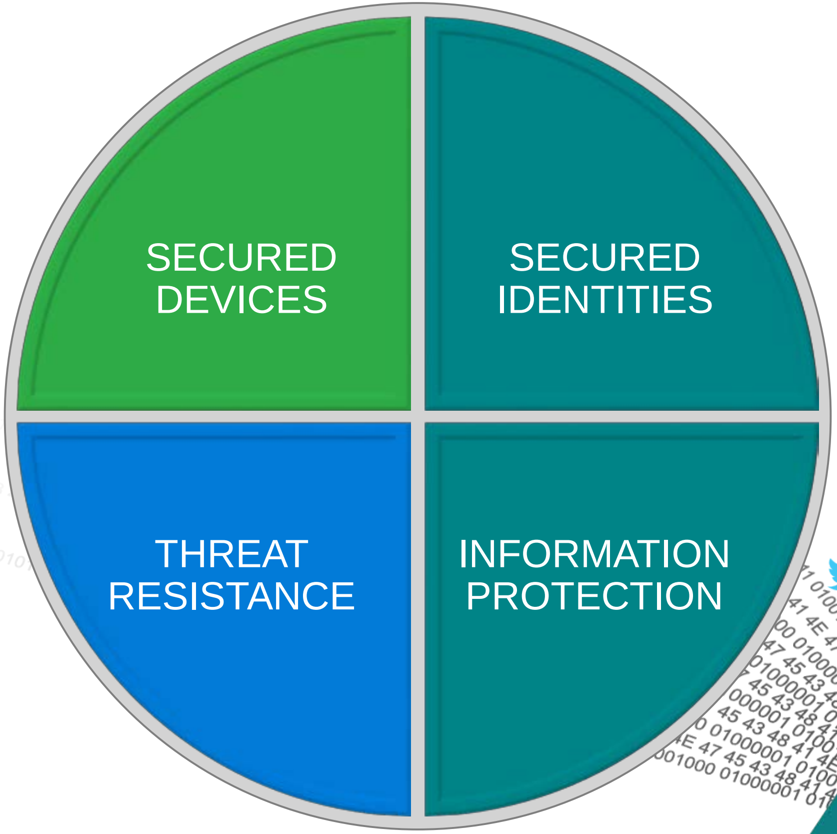
Hardware Rooted Trust

Device integrity

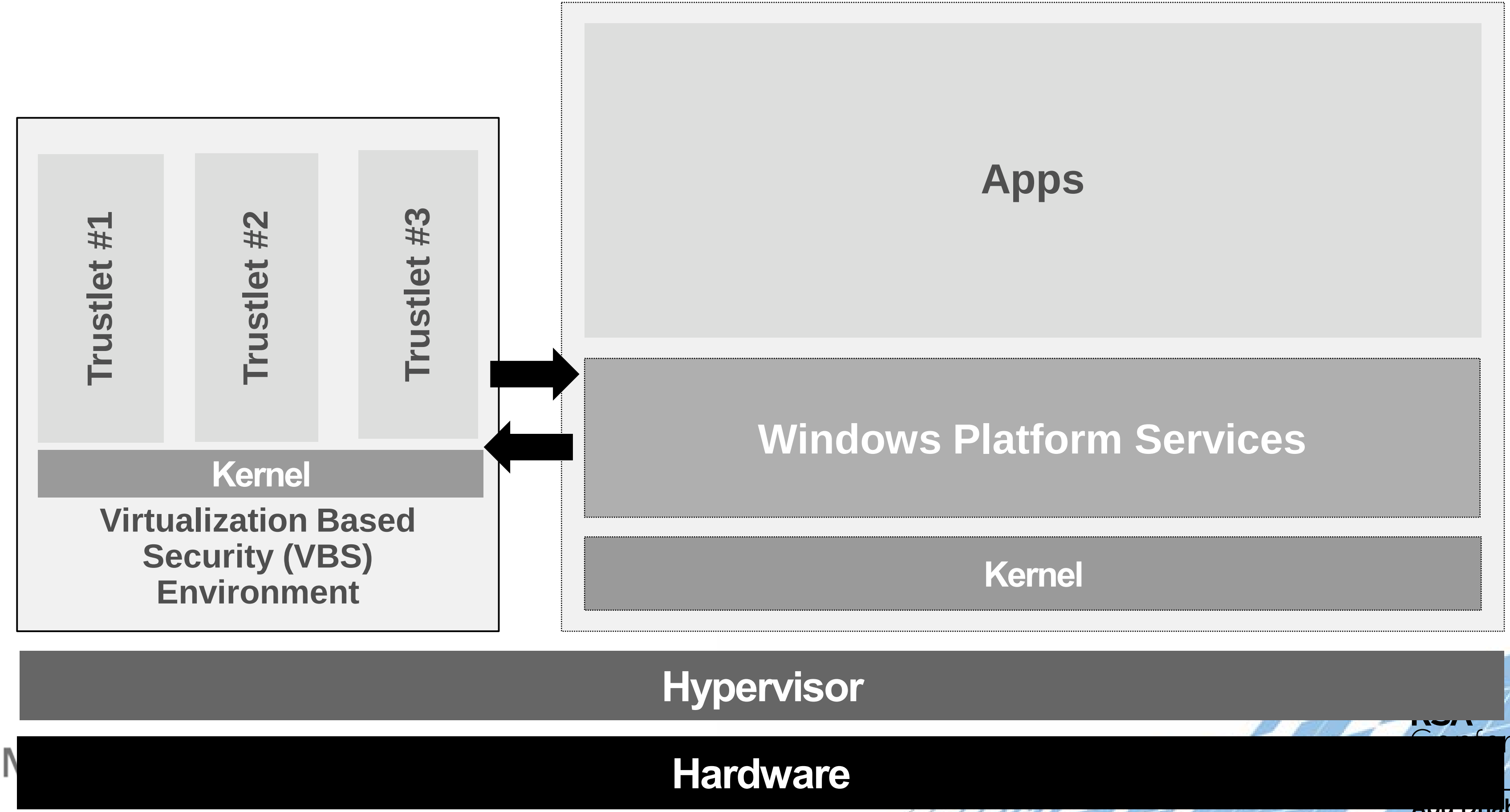
Crypto processing

Biometric sensors

Virtualization



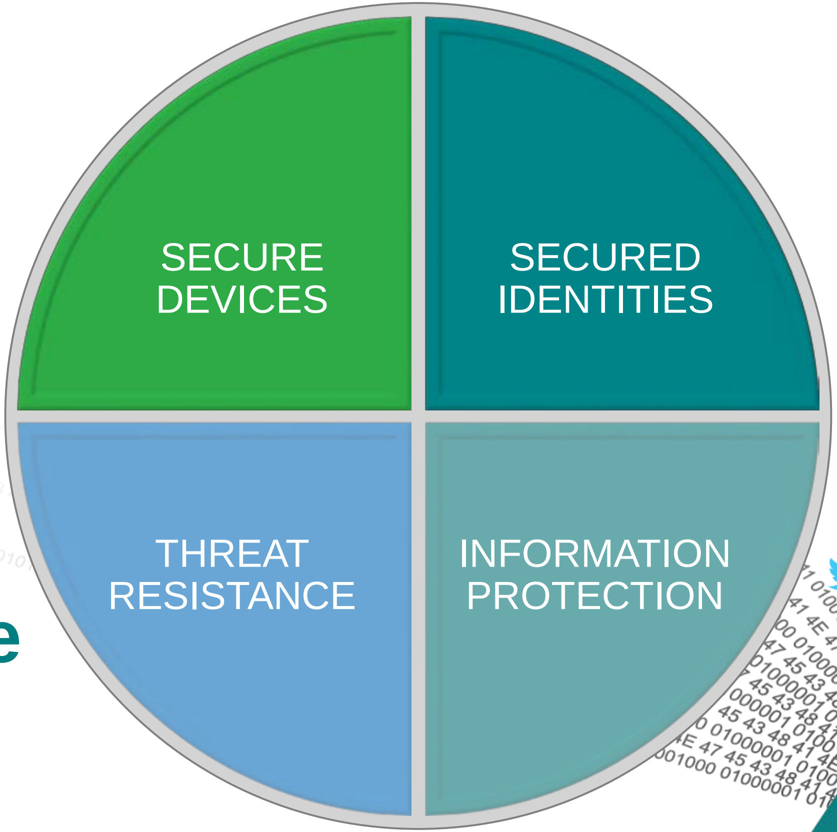
Virtualization Based Security (VBS)


Trustlet #1
Trustlet #2
Trustlet #3
Kernel
Virtualization Based Security (VBS) Environment
Apps
Windows Platform Services
Kernel
Hypervisor
Hardware

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

The End of Passwords, Two-factor for Everyone



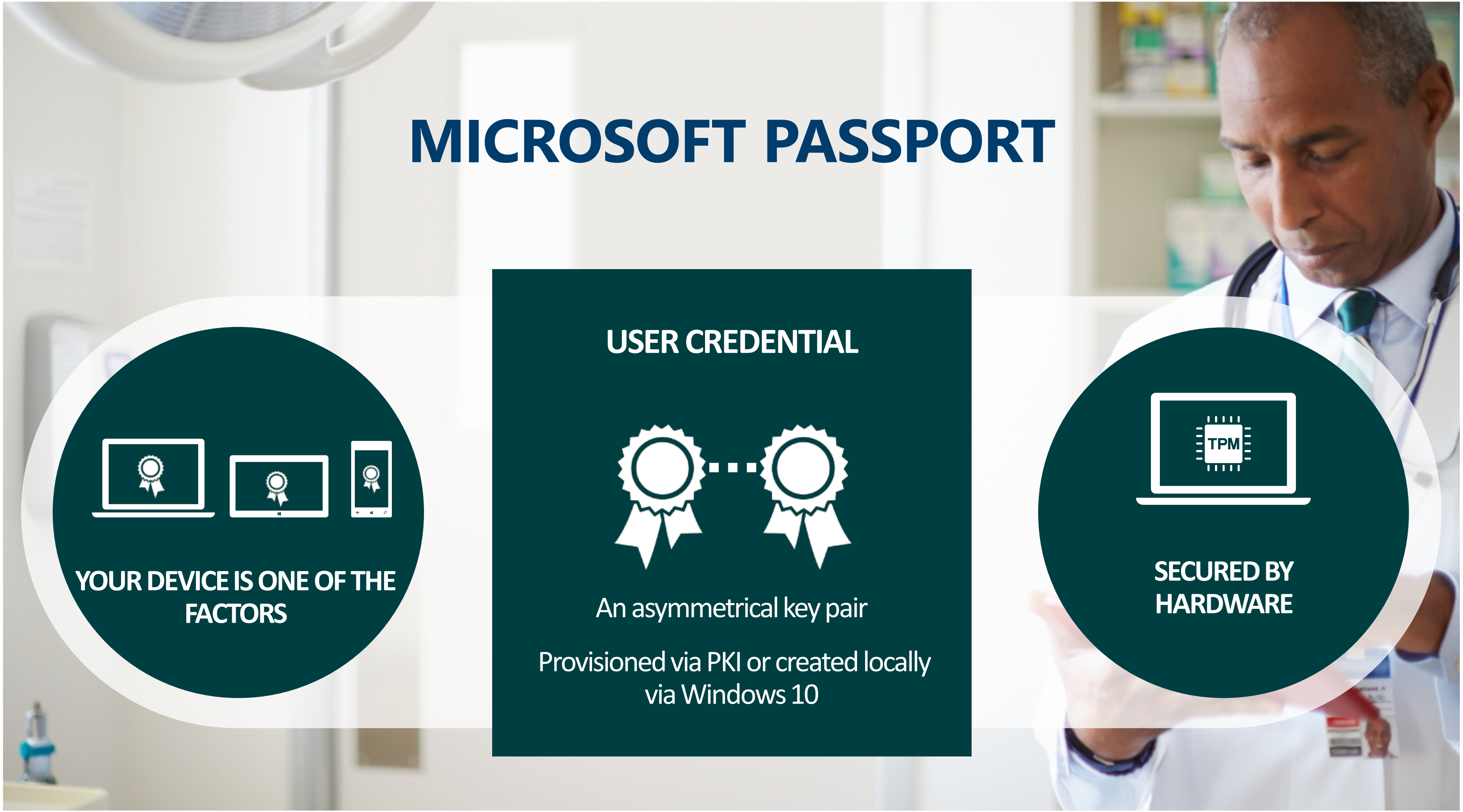
SECURE DEVICES

SECURED IDENTITIES

THREAT RESISTANCE

INFORMATION PROTECTION

#RSAC



MICROSOFT PASSPORT

YOUR DEVICE IS ONE OF THE FACTORS

USER CREDENTIAL

An asymmetrical key pair

Provisioned via PKI or created locally via Windows 10

TPM

SECURED BY HARDWARE

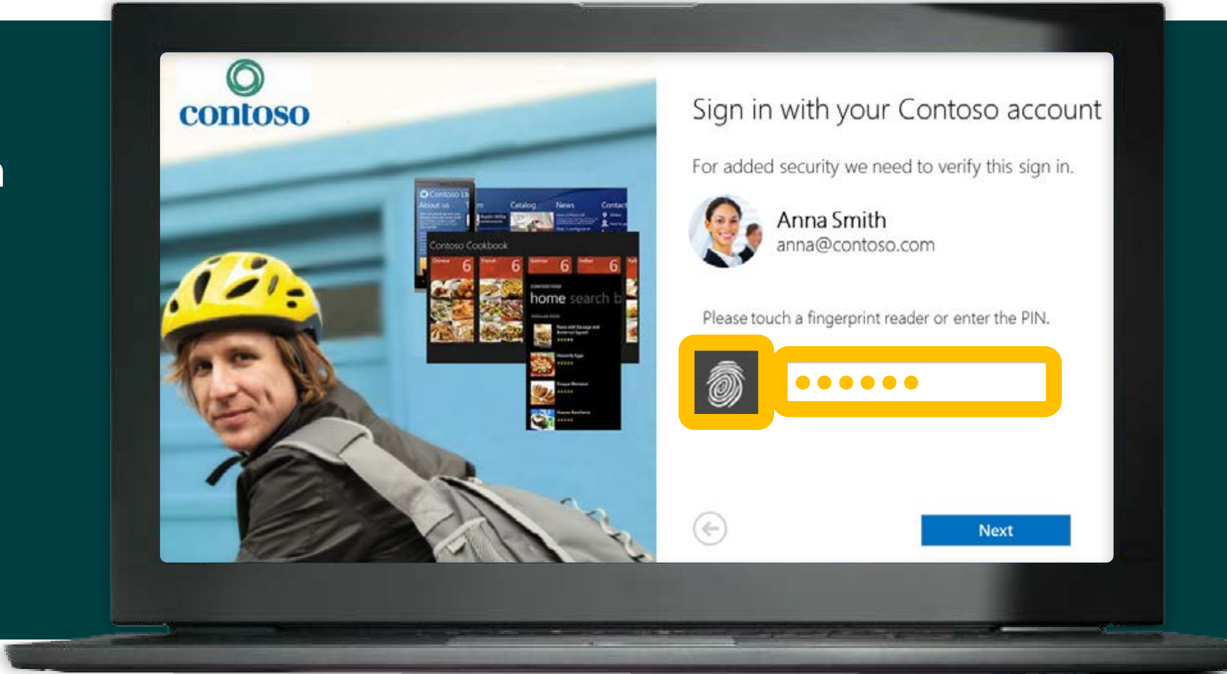
ACCESSING CREDENTIALS

PIN

Simplest implementation option
No hardware dependencies
User familiarity

Windows Hello

Improved security
Ease of use
Impossible to forget



Sign in with your Contoso account

For added security we need to verify this sign in.

Anna Smith
anna@contoso.com

Please touch a fingerprint reader or enter the PIN.

●●●●●●

Next

Hello Cyril

WINDOWS HELLO

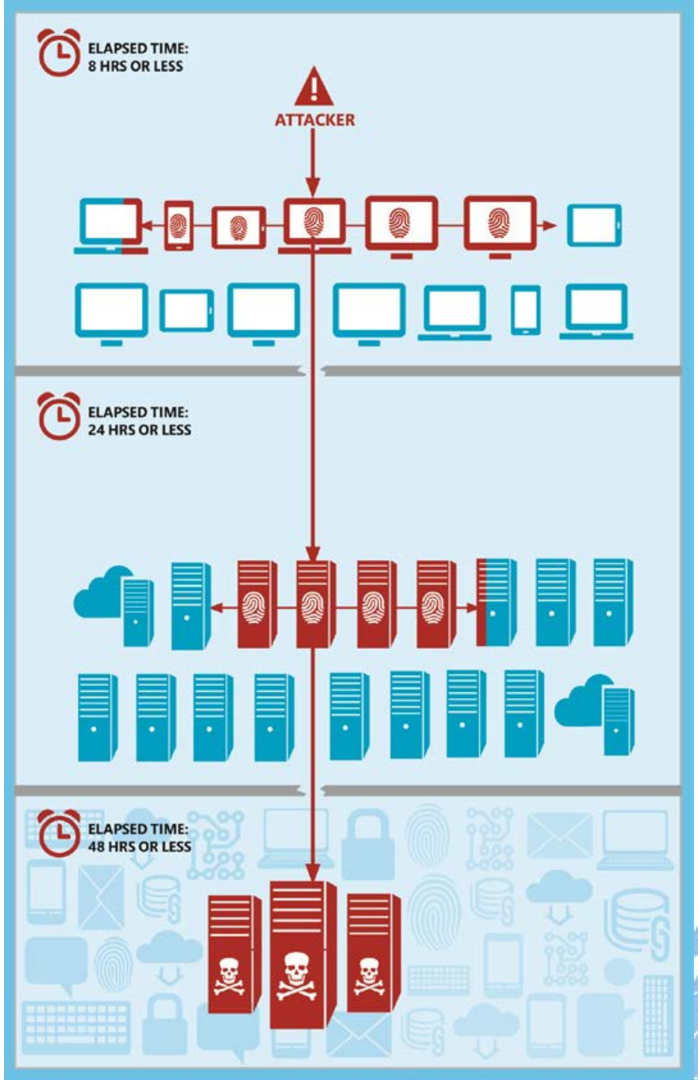
Fingerprint

Iris

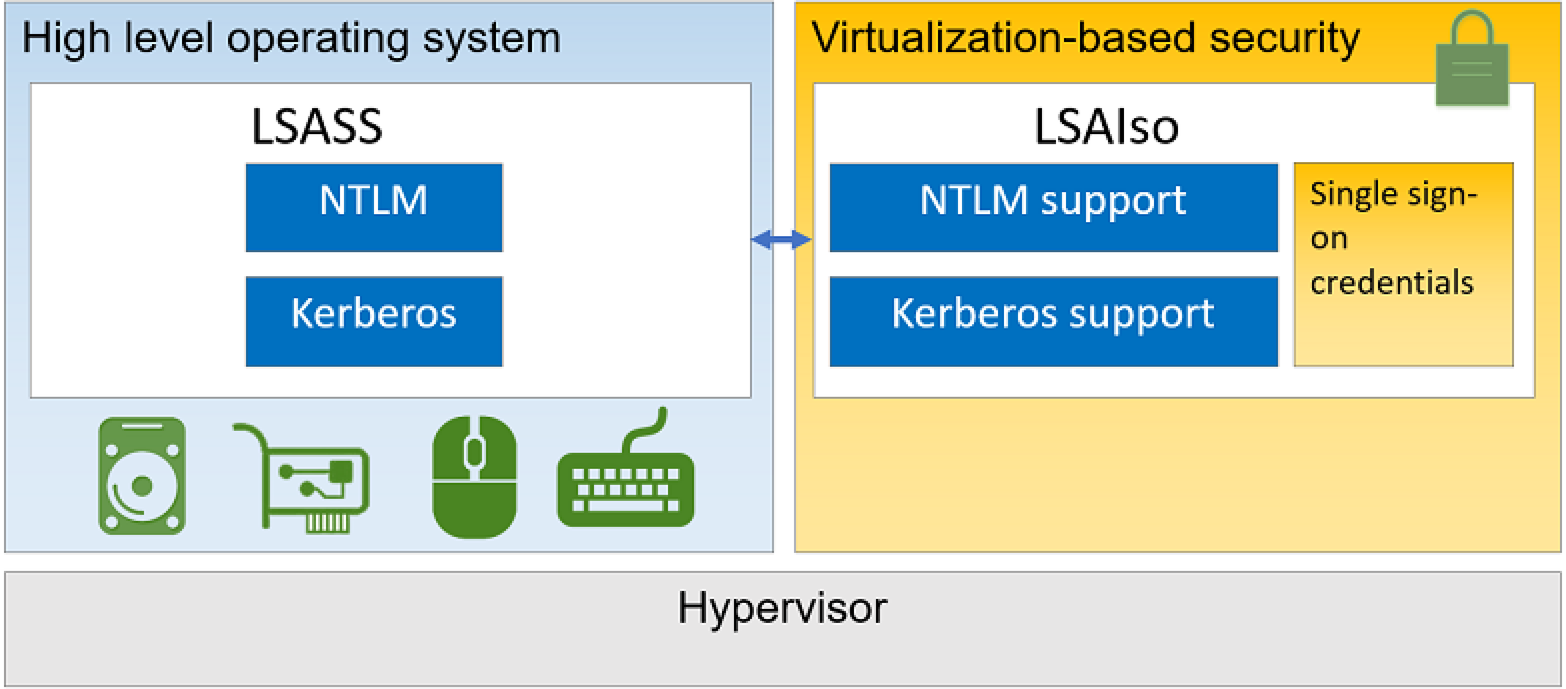
Facial

Credentials Theft

With Pass-The-Hash attack and other credential theft techniques, access to one device can lead to access to many



Credential Guard



High level operating system

LSASS

NTLM

Kerberos

Virtualization-based security

LSAIso

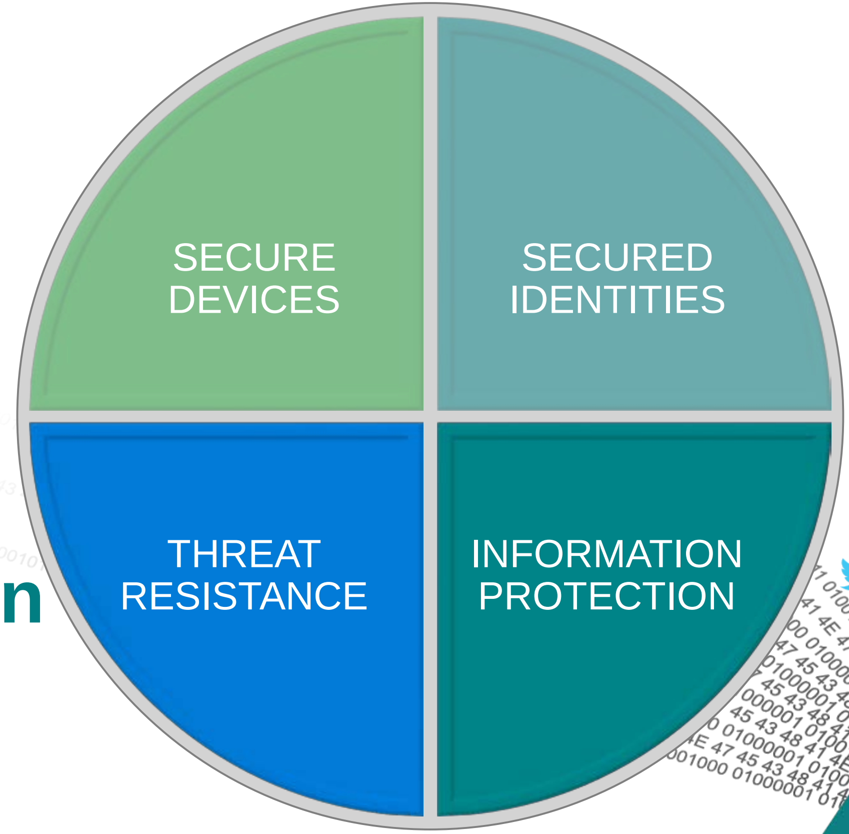
NTLM support

Kerberos support

Single sign-on credentials

Hypervisor

Active Threat Protection


SECURE DEVICES

SECURED IDENTITIES

THREAT RESISTANCE

INFORMATION PROTECTION

Device Guard

- Hardware rooted system core protection and app control
- Zero day and vulnerability protection for system core (kernel mode)
- Windows desktop can be locked down to only run trusted apps, just like many mobile OS's (e.g.: Windows Phone)
- Untrusted apps and executables, such as malware, are unable to run
- Resistant to tampering by an administrator or malware
- Requires devices specially configured by either the OEM or IT, and Windows 10 Enterprise
- Apps must be specially signed using the Microsoft signing service.

There’s more…

- Enterprise data protection: democratizing Data Loss Prevention
- Hardware rooted trust
- Conditional access and provable health
- Manageable hard disk encryption
- Device and platform integrity
- Platform and apps security improvements
- Control Flow Guard (CFG)
- IE improvements

Windows 10 Security In a Nutshell

- Virtualization Based Security (**VBS**) is the **game changing hardware based innovation** that **changes security forever** in Windows
- **Windows 10 Enterprise Protections:**
  - **Identity** protection: Microsoft Passport and Windows Hello provide an **alternative to passwords**
  - **Online** protection: **Device Guard protects the system core from vulnerability exploits and locks down your device**, so you can run only trusted applications, scripts, and more
  - **Information** protection: **Enterprise Data Protection** help ensure your corporate **data isn’t** accidentally or intentionally **leaked** to unauthorized users or locations
  - **Device** protection: **UEFI Secure Boot** and **Windows Trusted Boot** help ensure that a genuine version of Windows starts first on your device, preventing attackers from evading detection

Deploy Windows 10 Enterprise

- Next week
  - Download Windows 10 Enterprise and install on a few test machines
  - Procure Windows 10 hardware that supports Windows Hello
- Within 3 months
  - Approve Microsoft Passport/Windows Hello/Credential Guard and Device Guard
  - Start looking at Enterprise Data Protection
- In 3 months
  - Deploy Windows 10 on your PCs and tablets to help you be more secure!