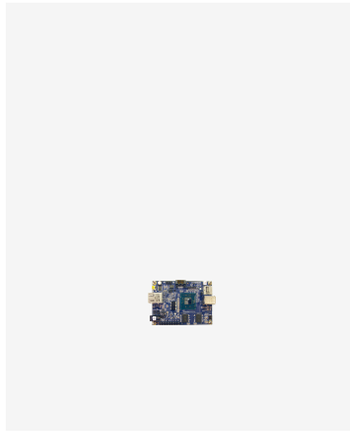
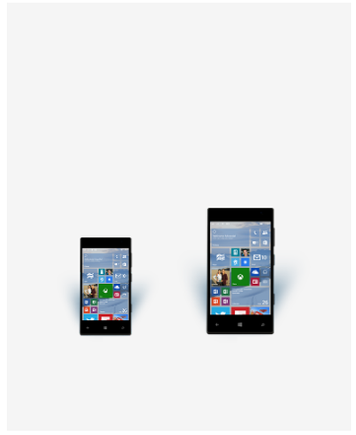
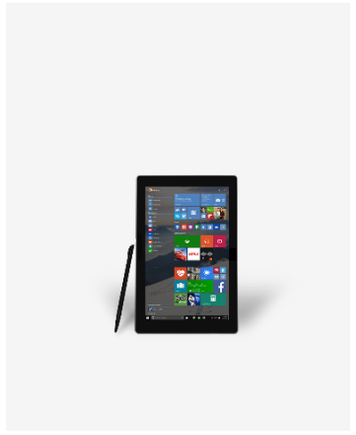
Windows 10

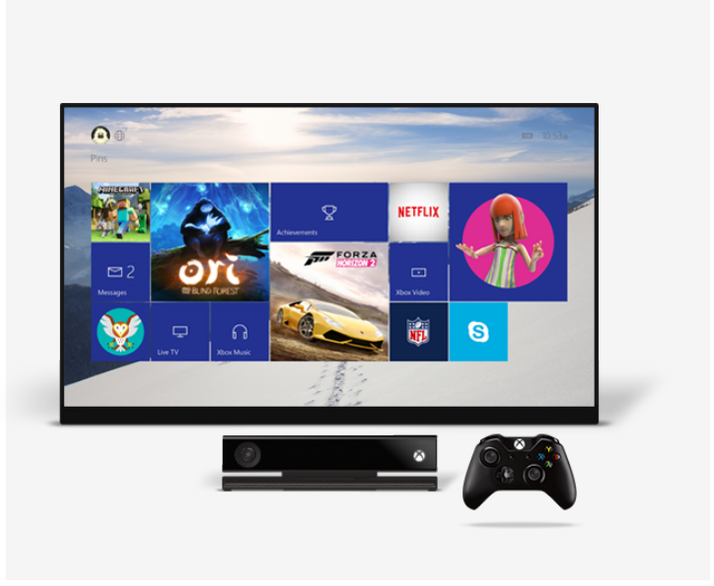
Windows 10 Overview: Security

Ole Tom Seierstad
National Security Officer – Microsoft
oles@Microsoft.com

Microsoft

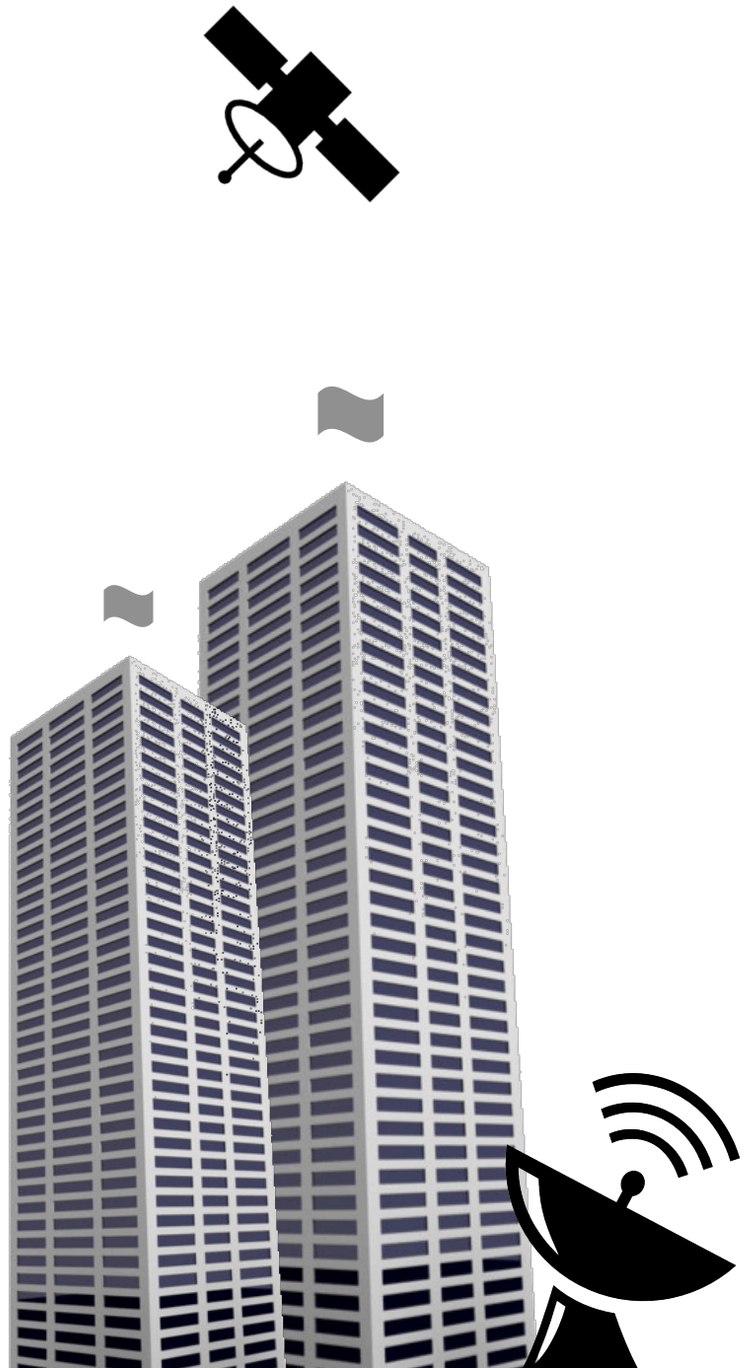

En felles Windows-plattform




You have many of the best security
solutions...


…but the security landscape has changed

TODAY, YOU ARE EXPERIENCING
A
REVOLUTION
OF **CYBER-THREATS**



FAMILIAR THREATS

CYBER-CRIME

THE REVOLUTION

CYBER-ESPIONAGE
CYBER-WARFARE
CYBER-TERROR

FAMILIAR THREATS

ATTACKER FOCUS
ON
FORTUNE 500

THE REVOLUTION

ATTACKERS GO AFTER ANY TARGET:

ALL VERTICALS

SUPPLY CHAINS

SUB CONTRACTORS

LINE LEVEL INDIVIDUALS

SMALL BUSINESSES

FAMILIAR THREATS

MALWARE
VULNERABILITIES

THE REVOLUTION

CREDENTIAL THEFT AT SCALE
ADVANCED PERSISTANT THREATS

Organizations with enormous security budgets and elite security analysts are **struggling** to address these modern threats.

239

median # of days **attackers are present** on a victim network **before detection**

Security **threats** are more **advanced** & **complex** than ever

Each week, an average company deals with

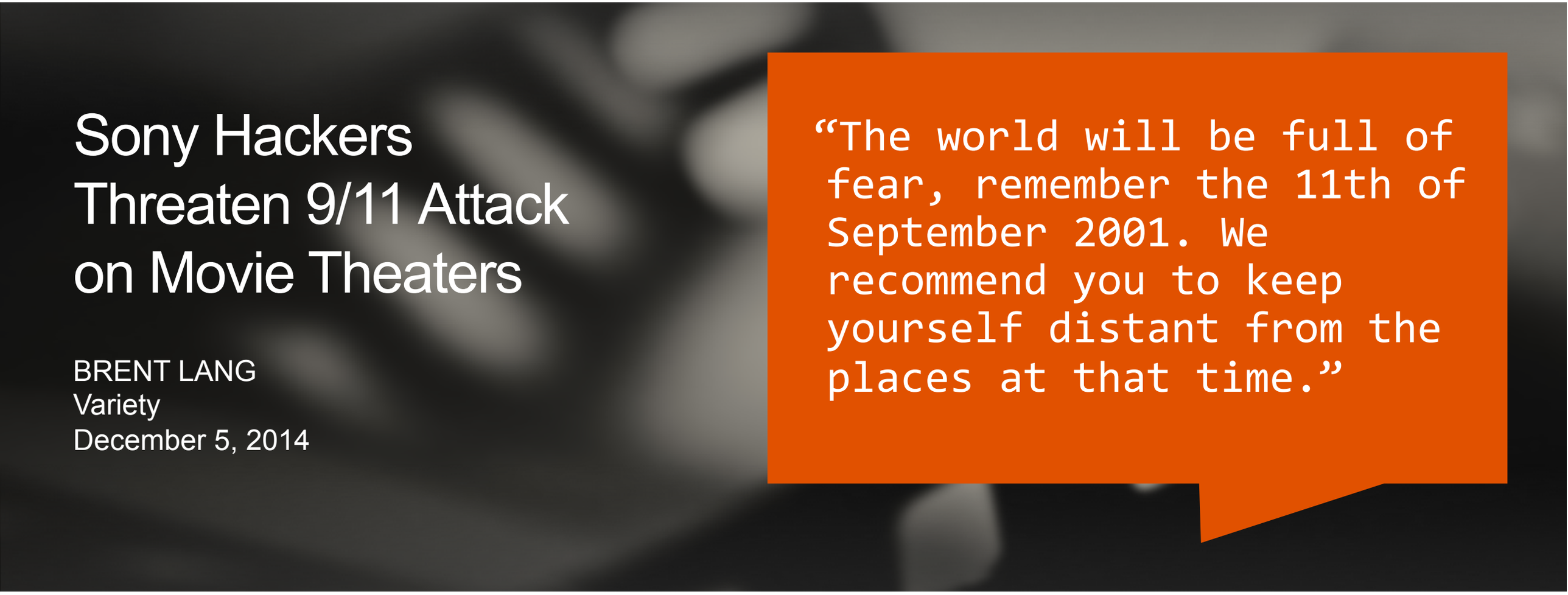
122 **successful** attacks

Up from 102 attacks per week in 2012

Annual cost of cybercrime to a company in the US is **$12M**

(78% increase over 4-years)

Sony Breach – Adding Terror to Playbook



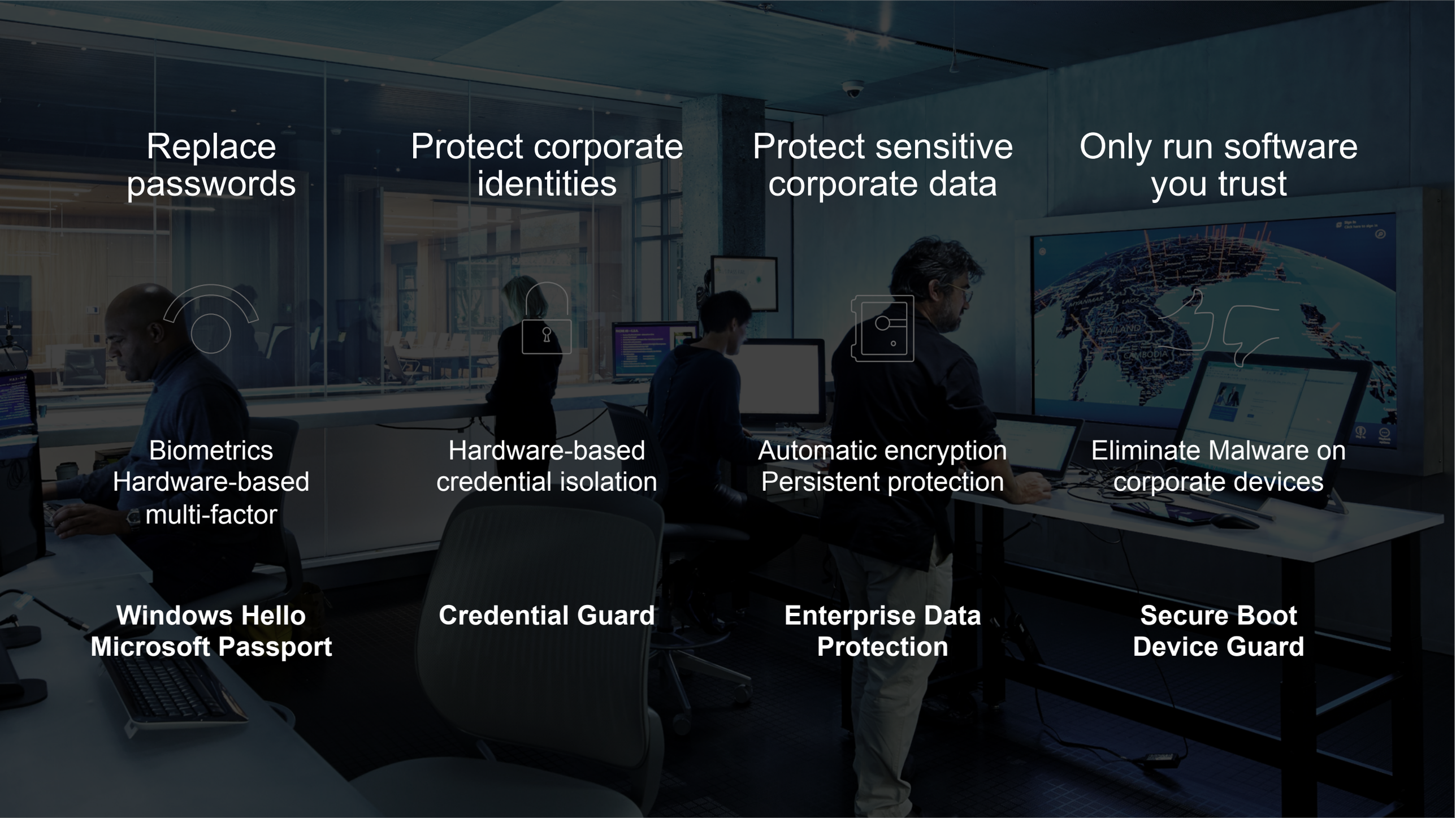
Sony Hackers Threaten 9/11 Attack on Movie Theaters

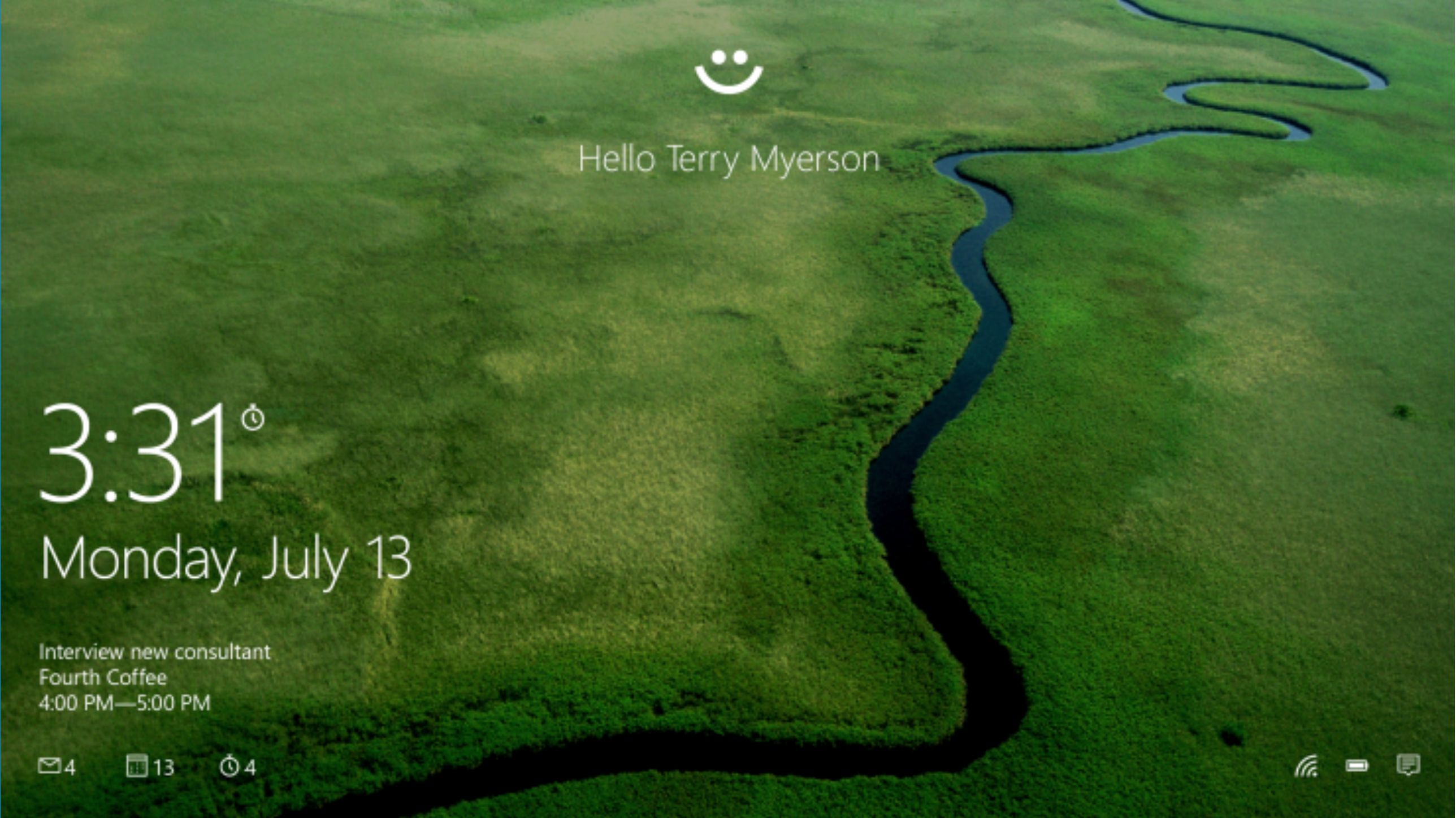
BRENT LANG
Variety
December 5, 2014

> "The world will be full of fear, remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time."

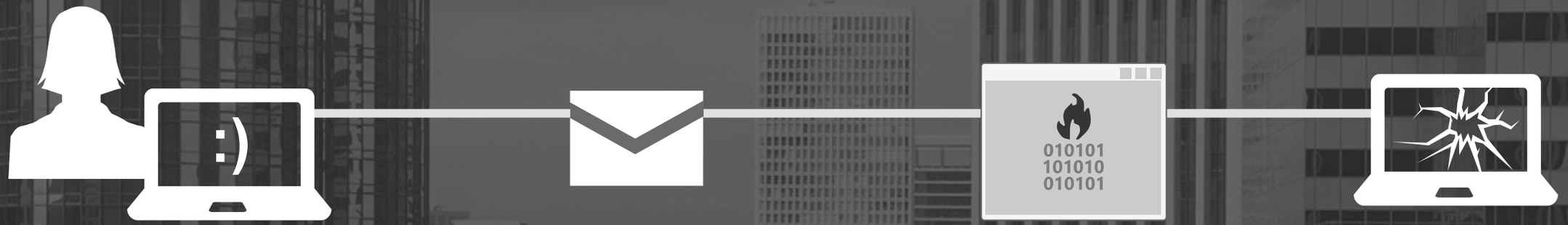
Source: Hackers Threaten Sony Employees in New Email: 'Your Family Will Be in Danger', Dave McNary, MSN, December 5, 2014. Image: G. Hodan

Protection against modern security threats


Replace passwords
Protect corporate identities
Protect sensitive corporate data
Only run software you trust
Biometrics
Hardware-based multi-factor
Hardware-based credential isolation
Automatic encryption
Persistent protection
Eliminate Malware on corporate devices
Windows Hello
Microsoft Passport
Credential Guard
Enterprise Data Protection
Secure Boot
Device Guard


Hello Terry Myerson
3:31
Monday, July 13
Interview new consultant
Fourth Coffee
4:00 PM—5:00 PM
4
13
4

The Anatomy of an Attack

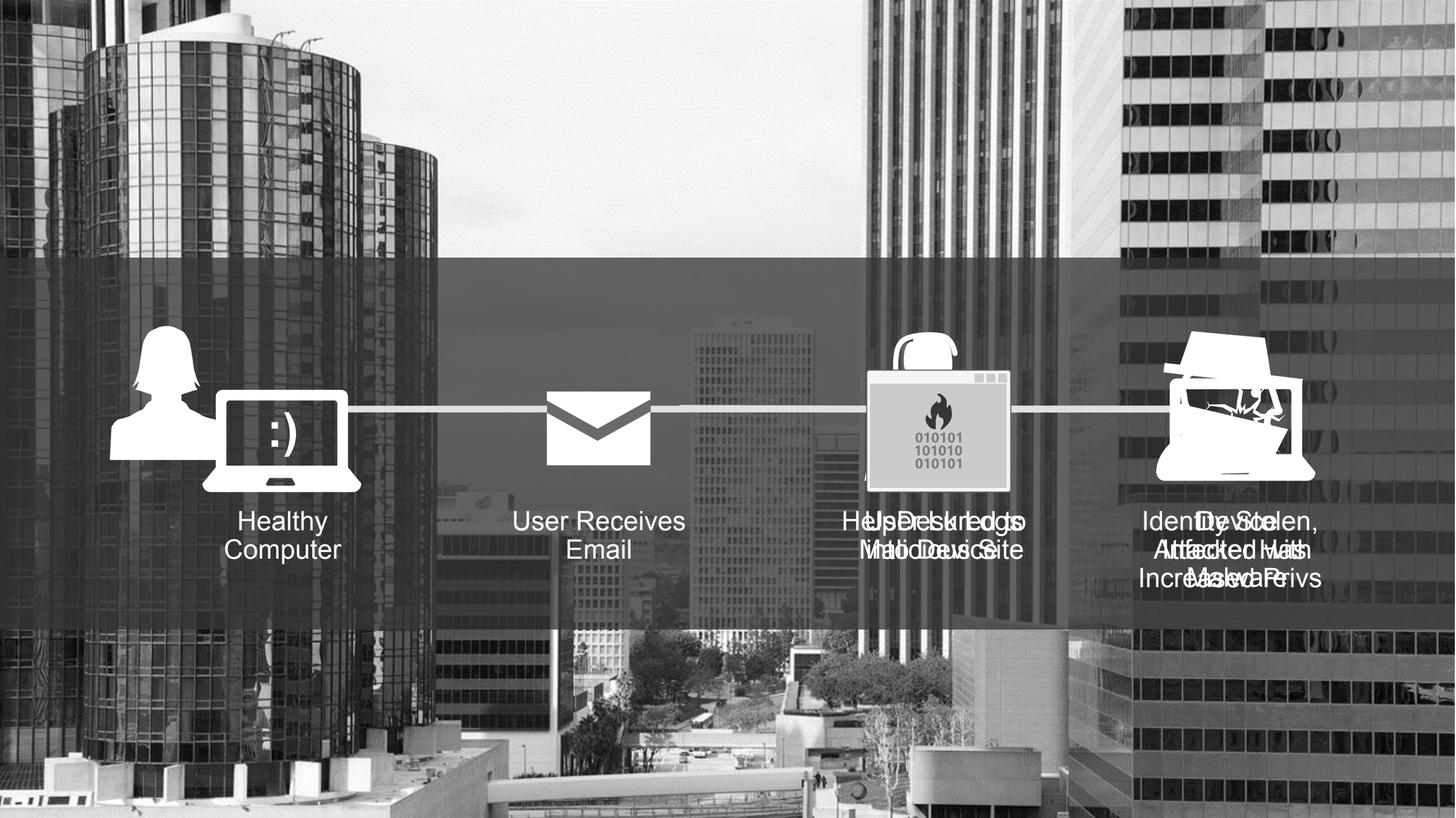


Healthy Computer

User Receives Email

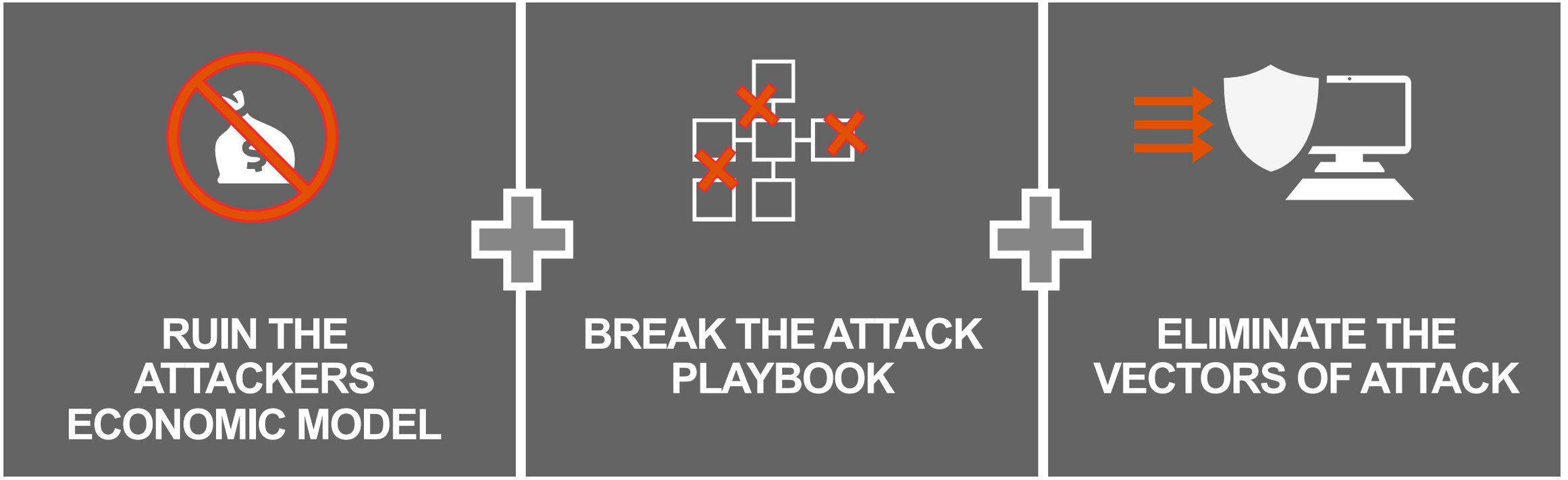
User Lured to Malicious Site

Device Infected with Malware


:)
010101
101010
010101
Healthy Computer
User Receives Email
User Downloads Malicious Site
Identity Stolen, Attacker Increases Privs


eives
il
010101
101010
010101
User Lured to
Malicious Site
Device
Infected with
Malware
HelpDesk Logs
into Device
Identity Stolen,
Attacker Has
Increased Privs

Addressing the Threats Requires a New Approach



Security from the inside out – beyond bigger walls

New challenges require a new platform

	Windows 7	Windows 10
Identity protection	Passwords theft is increasingly successful and today's multi-factor solutions have proven cumbersome and costly to deploy.	Offers an easy to use and deploy multi-factor solution with anti-theft and phishing. Comes with the convenience of a password, but the security of the best multi-factor solutions.
Data protection	Offers optionally configurable disk encryption, but lacks integrated DLP. Use of 3rd party solutions with varying experiences on mobile and desktop.	Market leading disk encryption increasingly enabled OOB and is highly manageable. Data loss prevention and data separation is fully integrated into the experience.
Threat resistance	Apps are trusted until they're determined to be a threat. No realistic way to detect 300K's+ new threats per day. Frequent use of 3rd party.	Mobile level of lockdown possible for desktop machines. Devices able to move trusted app model where untrusted apps are unable to run.
Device security	Platform security built on software alone creates opportunity for malware to hide from security solutions, embedding in the device itself.	Integrated platform and hardware security provides protection from power on to power off and eliminates opportunities to tamper with and hide from the system.

Key Threats

- Melissa (1999), Love Letter (2000)
- Mainly leveraging social engineering

2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

Key Threats

- Code Red and Nimda (2001), Blaster (2003), Slammer (2003)
- 9/11
- Mainly exploiting buffer overflows
- Script kiddies
- Time from patch to exploit: Several days to weeks

2004

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

Key Threats

- Zotob (2005)
- Attacks «moving up the stack» (Summer of Office 0-day)
- Rootkits
- Exploitation of Buffer Overflows
- Script Kiddies
- Raise of Phishing
- User running as Admin

2007

Windows Vista

- Bitlocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure “by default” configuration (Windows features and IE)

Key Threats

- Organized Crime
- Botnets
- Identity Theft
- Conficker (2008)
- Time from patch to exploit: days

2009

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPSec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

Key Threats

- Organized Crime, potential state actors
- Sophisticated targeted attacks
- Aurora (2009) and Stuxnet (2010)
- Password and digital identity theft and misuse
- Signatures based AV unable to keep up
- Digital signature tampering
- Browser plug-in exploits
- Data loss on BYOD device

2012

Windows 8

- Firmware Based TPM
- UEFI (Secure Boot)
- Trusted Boot (w/ELAM)
- Measured Boot
- Significant Improvements to ASLR and DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- Device Encryption (All SKU)
- BitLocker improvements and MBAM
- Virtual Smartcards
- Dynamic Access Control
- Built-in AV (Windows Defender)
- Improved Biometrics
- TPM Key Protection and Attestation
- Certificate Reputation
- Provable PC Health
- Remote Business Data Removable

Key Threats

- Nation states active attacking private institutions
- CryptoLocker (2013) and APT’s at scale
- Adding disruption and terror to playbook
- Rampant Passwords theft and abuse
- Pass the Hash becomes part of the default playbook
- AV unable to keep up

2015

Windows 10

- Virtual Secure Mode
- Virtual TPM
- Control Flow Guard
- Microsoft Passport
- Windows Hello
- Biometric Framework Improvements (Iris, Facial)
- Broad OEM support for Biometric enabled devices
- Enterprise Data Protection
- Device Encryption supported on broader range of devices
- DMA Attack Mitigations
- Device Guard
- URL Reputation Improvements
- App Reputation Improvements
- Windows Defender Improvements
- Provable PC Health Improvements

Defending Against Modern Security Threats

Secured Hardware

Secure Roots of Trust

Device integrity

Cryptographic processor

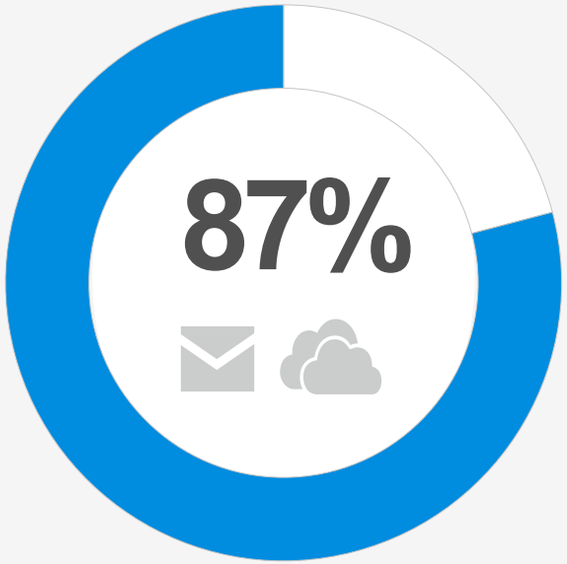
Virtualization

Biometric sensors

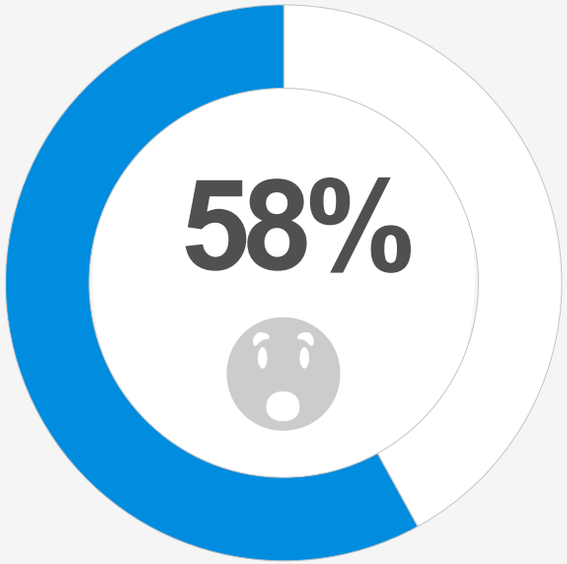
Attack Vectors and Solutions

Device integrity	Cryptographic processor	Virtualization	Biometric sensors
Malware tampers with hardware and corrupts Operating System before it even starts UEFI Secure Boot prevents device tampering and ensures OS starts with integrity	Malware compromises integrity related defenses and gains unauthorized access to sensitive information (e.g.: keys) TPM processor provides tamper proof integrity validation and prevents unauthorized access to sensitive information	Malware gains admin level privilege, gains full access to system, and disables system defenses to evade detection Processor based virtualization isolates critical system components and data and protects even in the event full system compromise	Attacker gains access to users Password/PIN and 2FA device Using a biometric for authentication increases the level of difficult for an attacker to the highest level

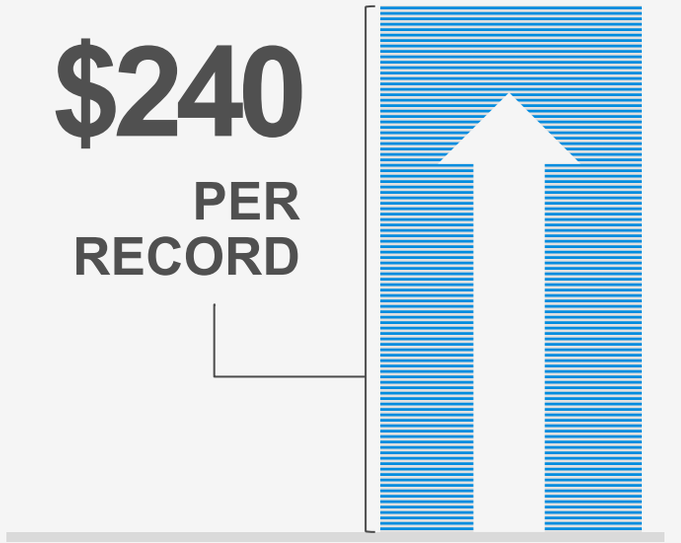
Data Leakage



…of senior managers admit to regularly uploading work files to a personal email or cloud account[1]



Have accidentally sent sensitive information to the wrong person[1]



Average per record cost of a data breach across all industries[2]

[1]Stroz Friedberg, “On The Pulse: Information Security In American Business,” 2013

[2]HIPPA Secure Now, “A look at the cost of healthcare data breaches,” Art Gross, March 30, 2012

Sharing Protection

Rights Management Services

Adding persistent and non-removable protection to data

Significant improvements over Windows 7

Protect all file types, everywhere they go, cloud, email, BYOD, …

Support for all commonly used devices and systems – Windows, OSX, iOS, Android

Can be automatically applied to mail, OneDrive Pro, etc.

Support for B2B and B2B via Azure AD

Support for on premise and cloud based scenarios (e.g.: Office 365)

Seamless easy to provision and support for FIPS 140-2 regulation and compliance

Data-at-rest Protection

Risks of unencrypted devices go beyond exposed data

Machine admin credentials can be reset with offline tools

Decommissioned desktops and servers create risk

Device Encryption

BitLocker

Devices can be encrypted out-of-box with BitLocker

Increased global acceptance of TPM
Pervasive on all Windows devices by 2015

Easiest deployment, leading security, reliability, and performance

Single sign-on for modern devices and configurable Windows 7 hardware

Enterprise grade management (MBAM) and compliance (FIPS)

Introducing

Enterprise Data Protection

A Different Approach

Protects data at rest, and wherever it rests or may roam to

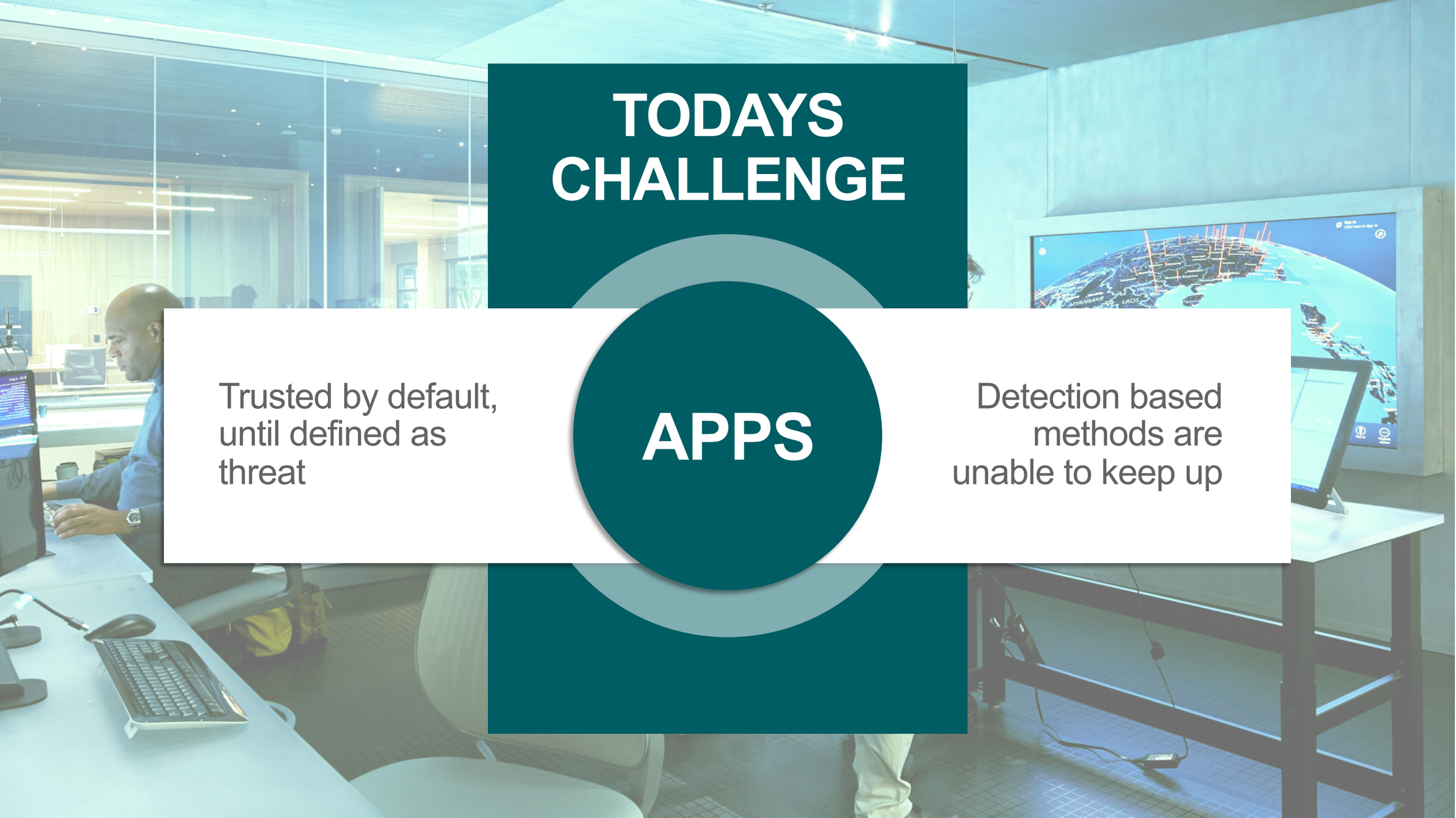
Seamless integration into the platform, No mode switching and use any app

Corporate vs personal data identifiable wherever it rests on the device

Prevents unauthorized apps from accessing business data

IT has fully control of keys and data and can remote wipe data on demand

Common experience across all Windows devices with cross platform support

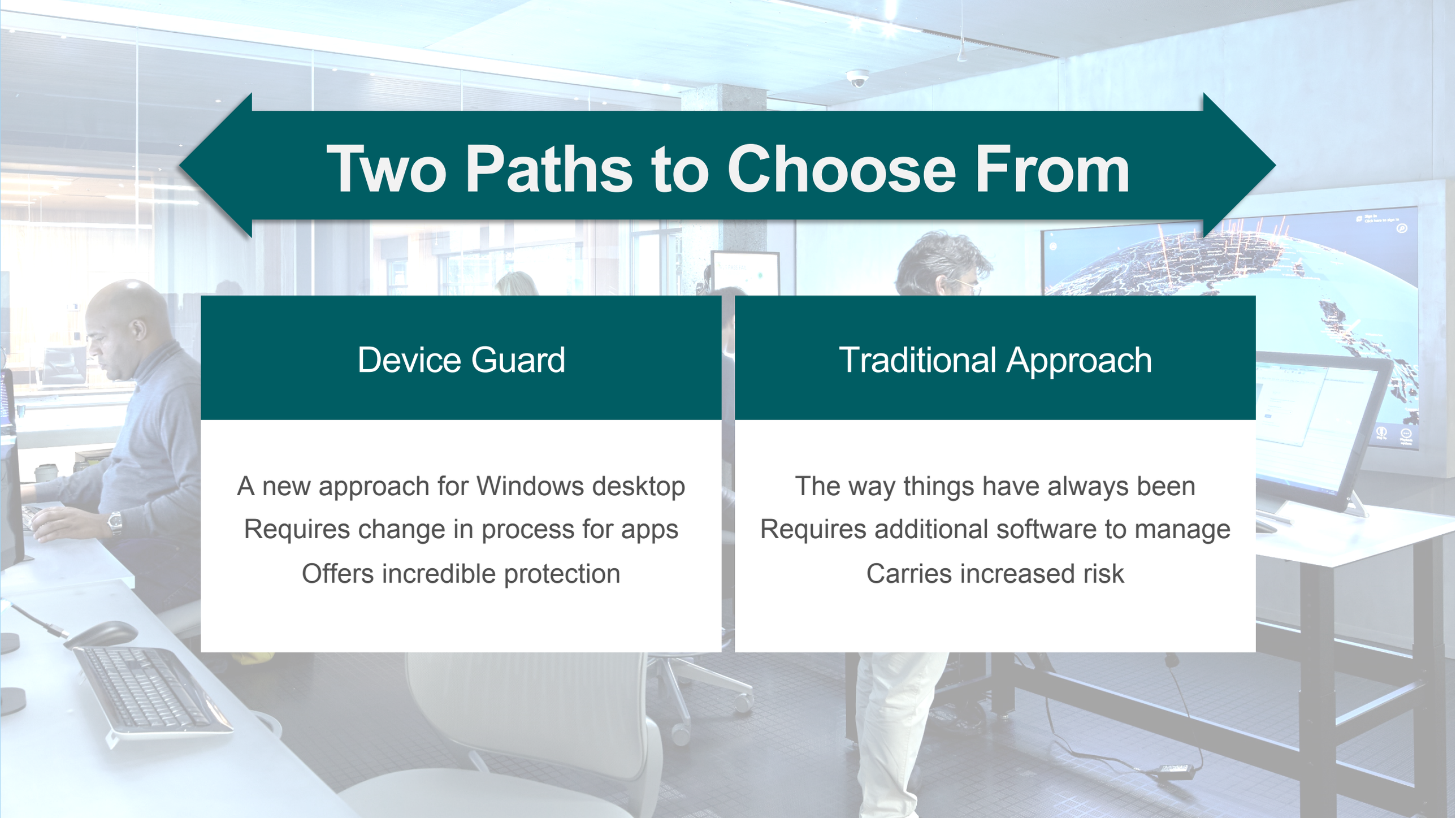


TODAYS CHALLENGE

Trusted by default, until defined as threat

APPS

Detection based methods are unable to keep up



Two Paths to Choose From

Device Guard

A new approach for Windows desktop

Requires change in process for apps

Offers incredible protection

Traditional Approach

The way things have always been

Requires additional software to manage

Carries increased risk

Device Guard

Hardware Rooted
App Control

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

Requires Windows Enterprise edition

Device Guard

Getting Apps into
the Circle of Trust

Supports all apps including Universal and Desktop (Win32).

Trusted apps can be created by IHV, ISV, and Organizations using a Microsoft provided signing service.

Apps must be specially signed using the Microsoft signing service. No additional modification is required.

Signing service will be made available to OEM's, IHV, ISV's, and Enterprises.

Device and Platform Integrity

Ensuring Windows starts on a trustworthy device

UEFI prevents firmware attacks and ensures Windows starts before any malware

TPM enables local and remote verification of system integrity before system start

Windows Trusted Boot prevents malware from starting during boot process and can protects anti-virus solutions

Windows isolates system core and puts sensitive processes into containers – offering protection even with kernel level breach

App Security & Online Safety

Protects system and apps from the most common forms of malware

Windows vulnerability mitigations reduce or eliminate impact of exploits

Windows sandboxes Universal Apps, validates app integrity, and offers app control

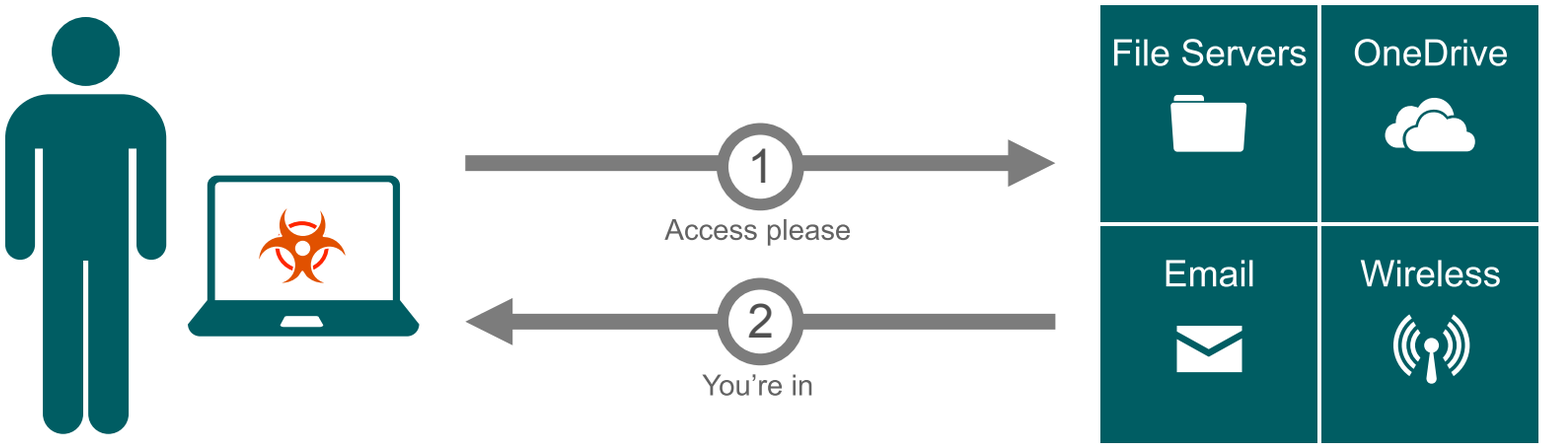
Windows includes Windows Defender, an advanced antivirus and malware solution

Windows and IE SmartScreen blocks malicious websites and apps before they get a chance to impact the device

WinRE integration helps remediate when the OS or other defenses are inoperable

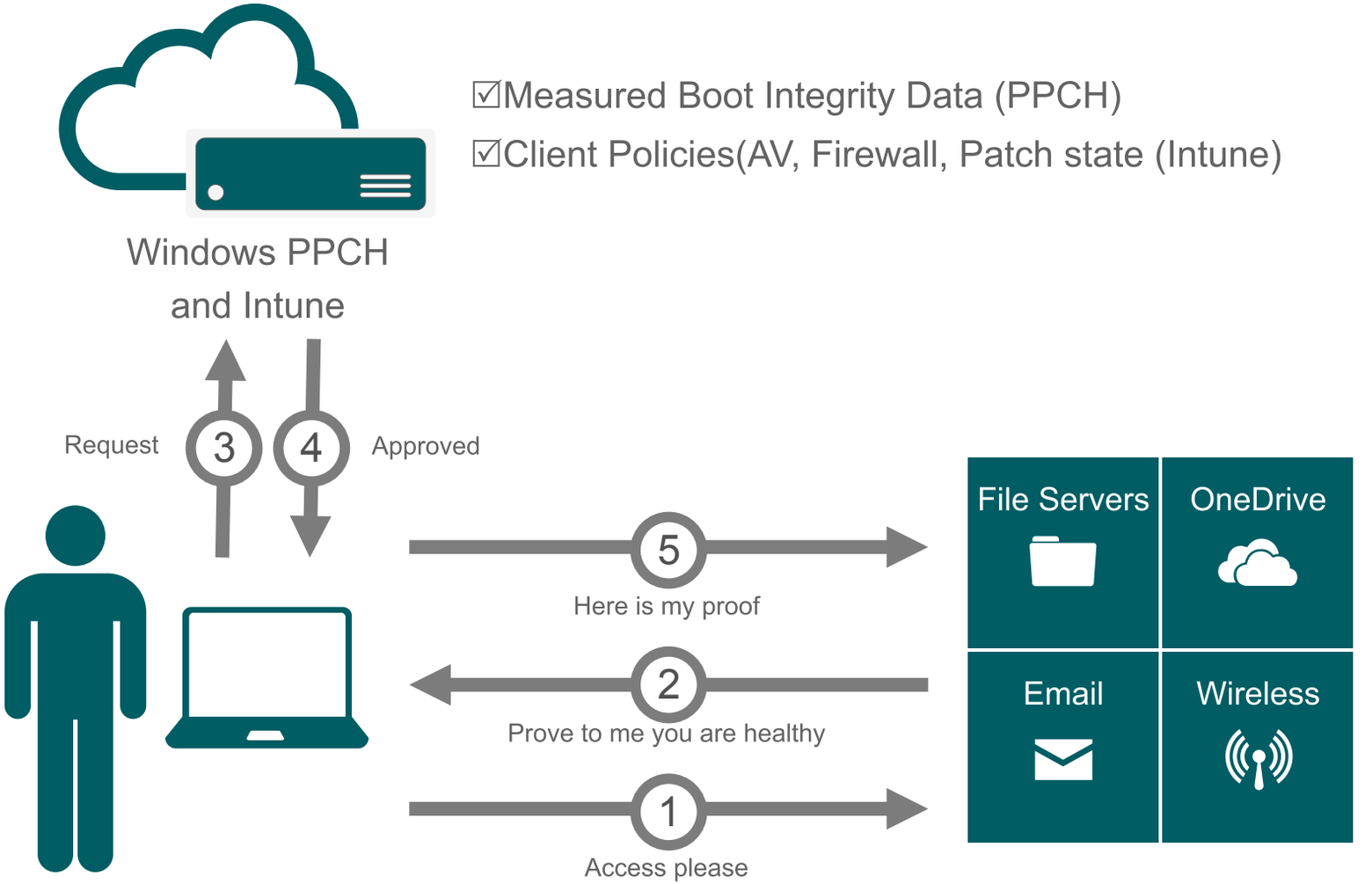
Unknown PC Health

Health is assumed

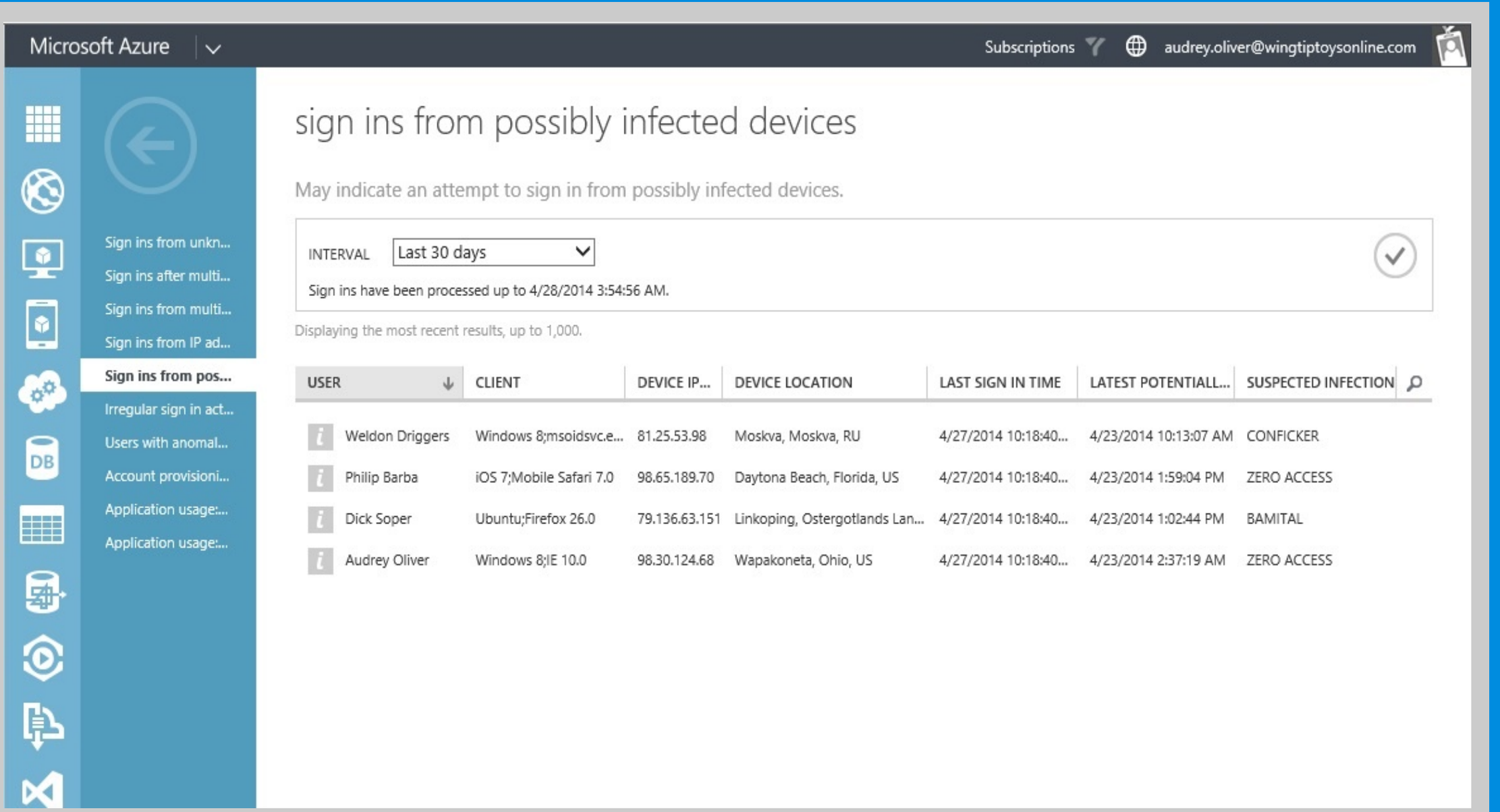


Provable PC Health Enables

PPCH provides health intel to MDMS



Microsoft Azure Security Control



Active threat protection