Disrupting the Revolution of Cyber-Threats with Revolutionary Security

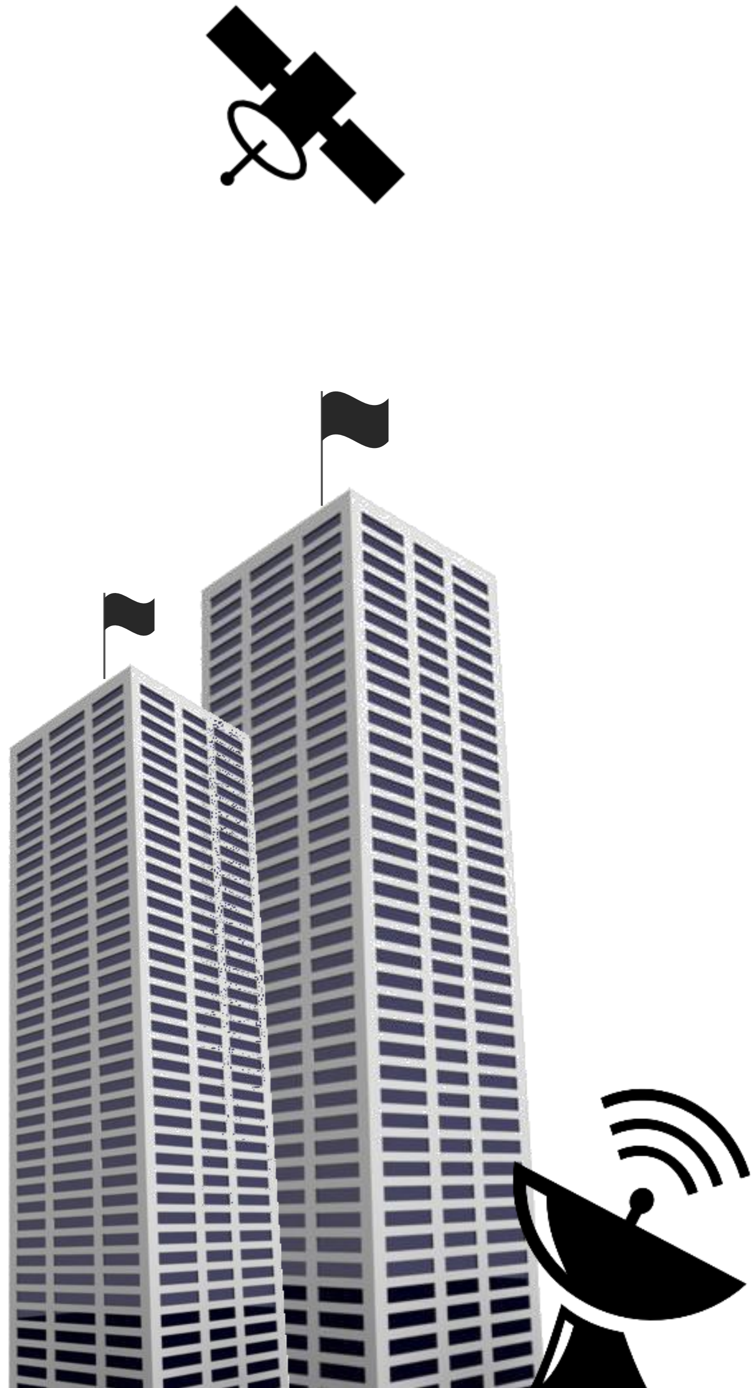
Windows 10

Rick Engle
Principal Windows Technologies Specialist
Microsoft Federal

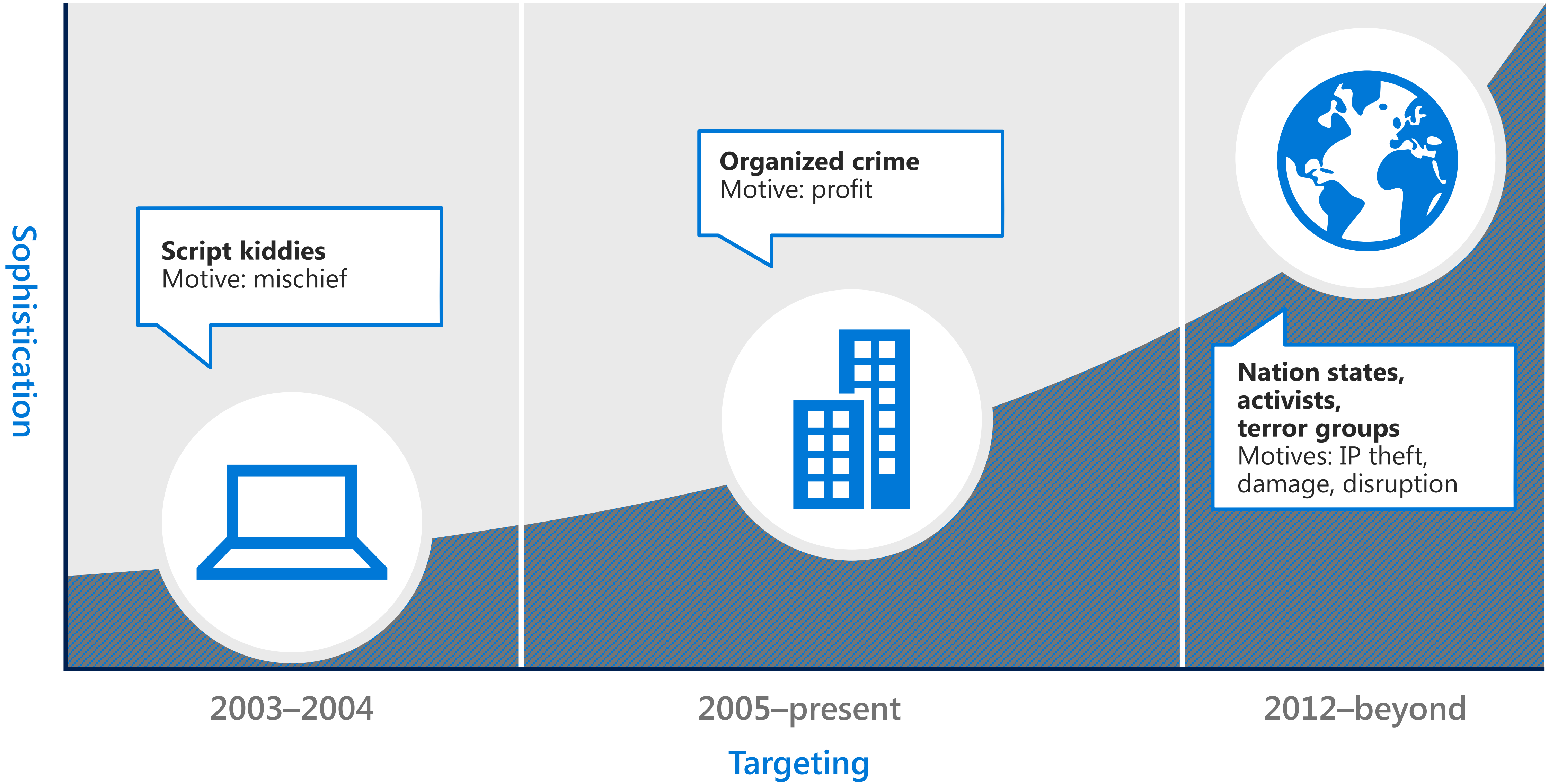
TODAY, YOU ARE EXPERIENCING A

REVOLUTION

OF **CYBER-THREATS**



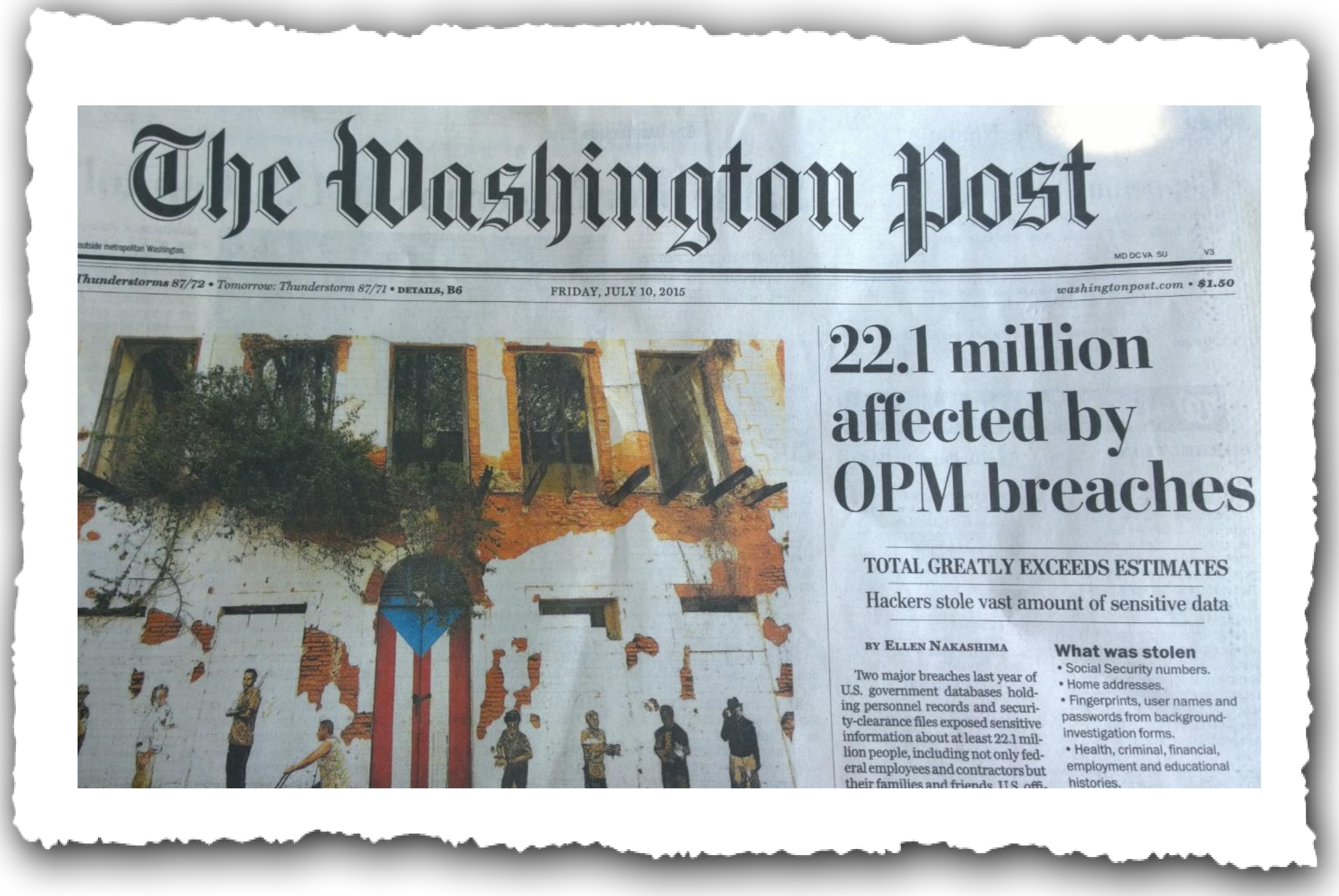
The evolution of attacks



Script kiddies
Motive: mischief

Organized crime
Motive: profit

Nation states, activists, terror groups
Motives: IP theft, damage, disruption



The Washington Post

outside metropolitan Washington.

MD DC VA SU V3

Thunderstorms 87/72 • Tomorrow: Thunderstorm 87/71 • DETAILS, B6

FRIDAY, JULY 10, 2015

washingtonpost.com • $1.50

22.1 million affected by OPM breaches

TOTAL GREATLY EXCEEDS ESTIMATES

Hackers stole vast amount of sensitive data

BY ELLEN NAKASHIMA

Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends. U.S. offi-

What was stolen

- Social Security numbers.
- Home addresses.
- Fingerprints, user names and passwords from background-investigation forms.
- Health, criminal, financial, employment and educational histories.

Addressing the threats requires a new approach:

RUIN THE ATTACKERS ECONOMIC MODEL

+

BREAK THE ATTACK PLAYBOOK

+

ELIMINATE THE VECTORS OF ATTACK

Security from the inside out – beyond bigger walls

Windows 10 Security Approach

Identity Protection

Information Protection

Device Protection

Identity Protection

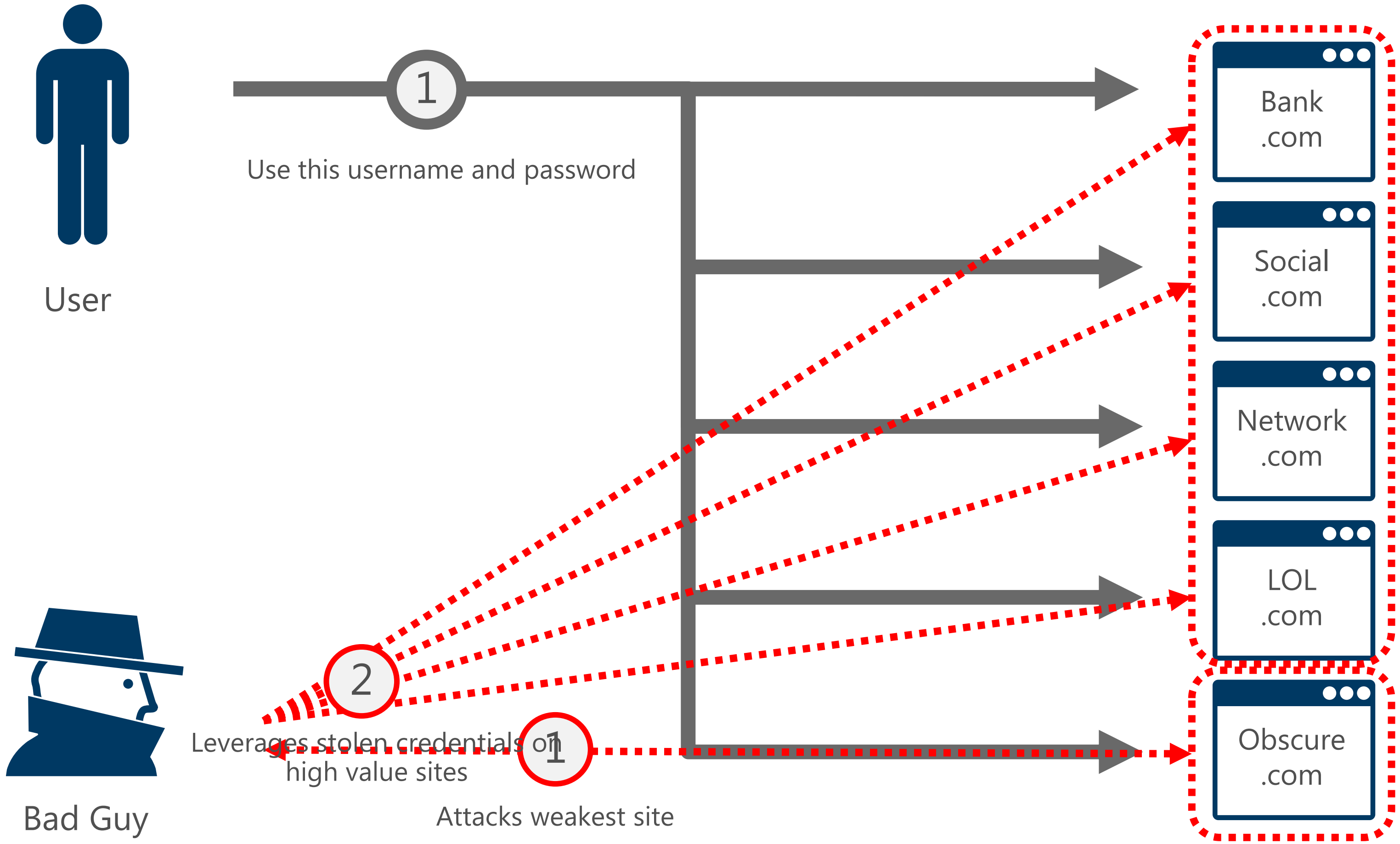
SHARED SECRETS

Easily mishandled or lost

(Hint: The user is the problem)

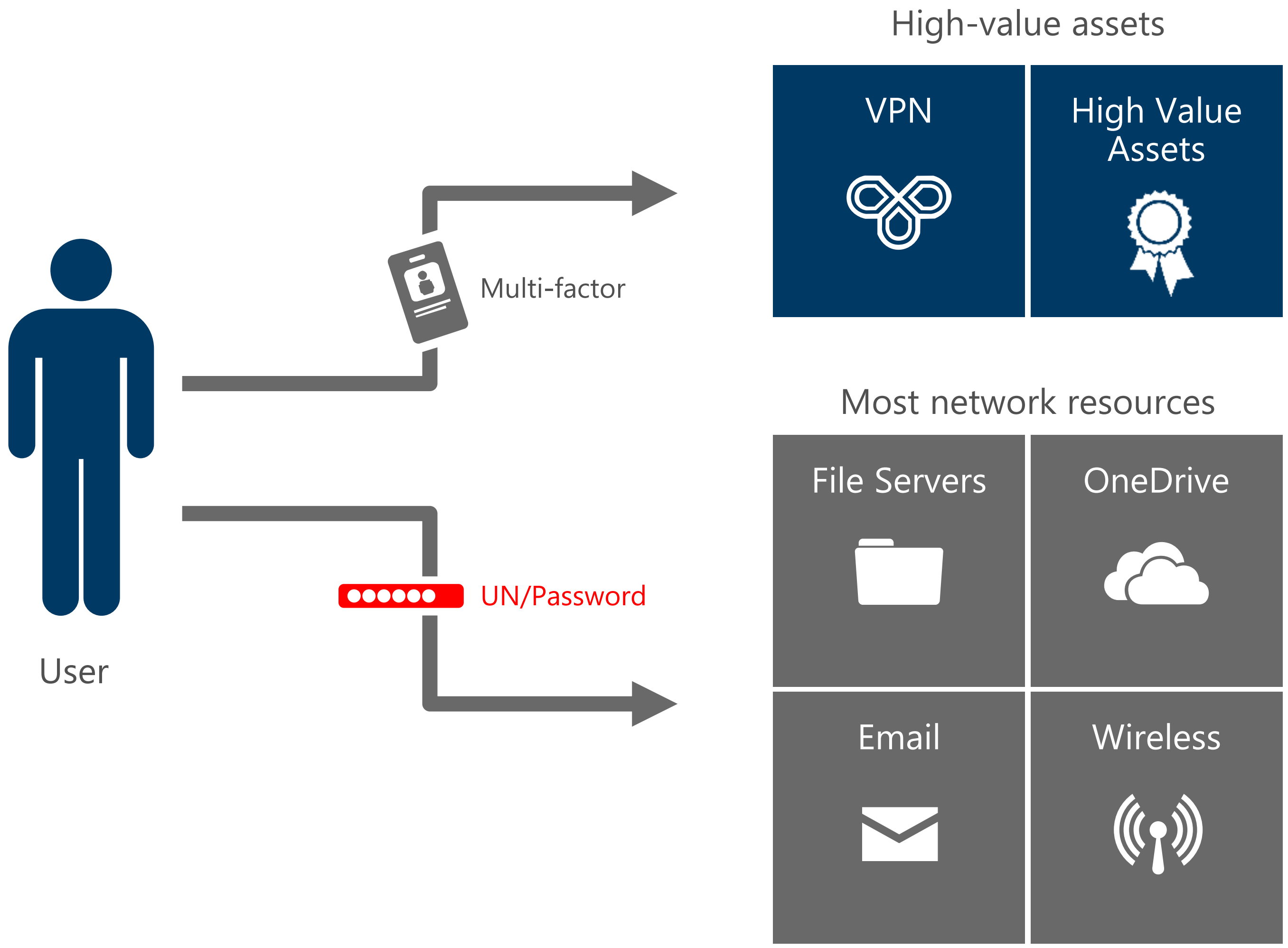
Internet username and password

THE SITES WE USE ARE A WEAK LINK



Typical multi-factor authentication implementations

LIMITED USE OF MFA CREATES WEAK LINKS



High-value assets

VPN

High Value Assets

Multi-factor

User

UN/Password

Most network resources

File Servers

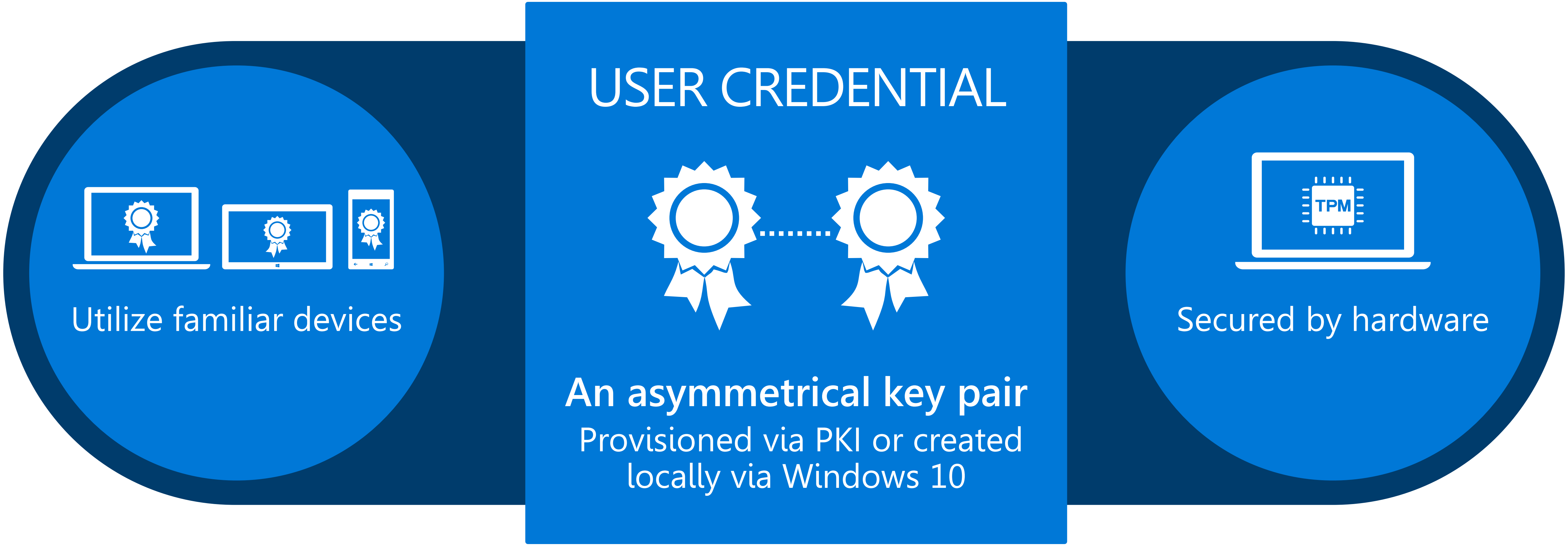
OneDrive

Email

Wireless

Microsoft Passport

Identity protection



Utilize familiar devices

USER CREDENTIAL

An asymmetrical key pair

Provisioned via PKI or created locally via Windows 10

Secured by hardware

Accessing credentials

Identity protection

PIN

Simplest implementation option

Works on existing devices

User familiarity

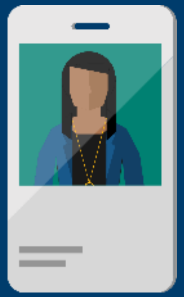
Biometrics

Enables multi-factor

Ease of use

Impossible to forget

Smartcards



Combines multifactor and badge identity

CAC and PIV

Desktop/tablet only

WINDOWS HELLO

Hello Rick

Fingerprint

Iris

Facial

FIDO ALLIANCE

Board level members

Microsoft				
Google	SAMSUNG	lenovo. FOR THOSE WHO DO.	ARM®	BlackBerry.
VISA	MasterCard	PayPal™	Bank of America	DISCOVER
ca technologies	NETFLIX	CrucialTec	yubico Trust the Net.	IdentityX
RSA®	oberthur TECHNOLOGIES THE M COMPANY	Synaptics®	NXP	Nok Nok LABS

Today's security challenge

Identity protection

1.

Single IT Pro's machine is compromised

IT Pro manages kiosks/shared devices on network

Attacker steals IT Pro's access token

2.

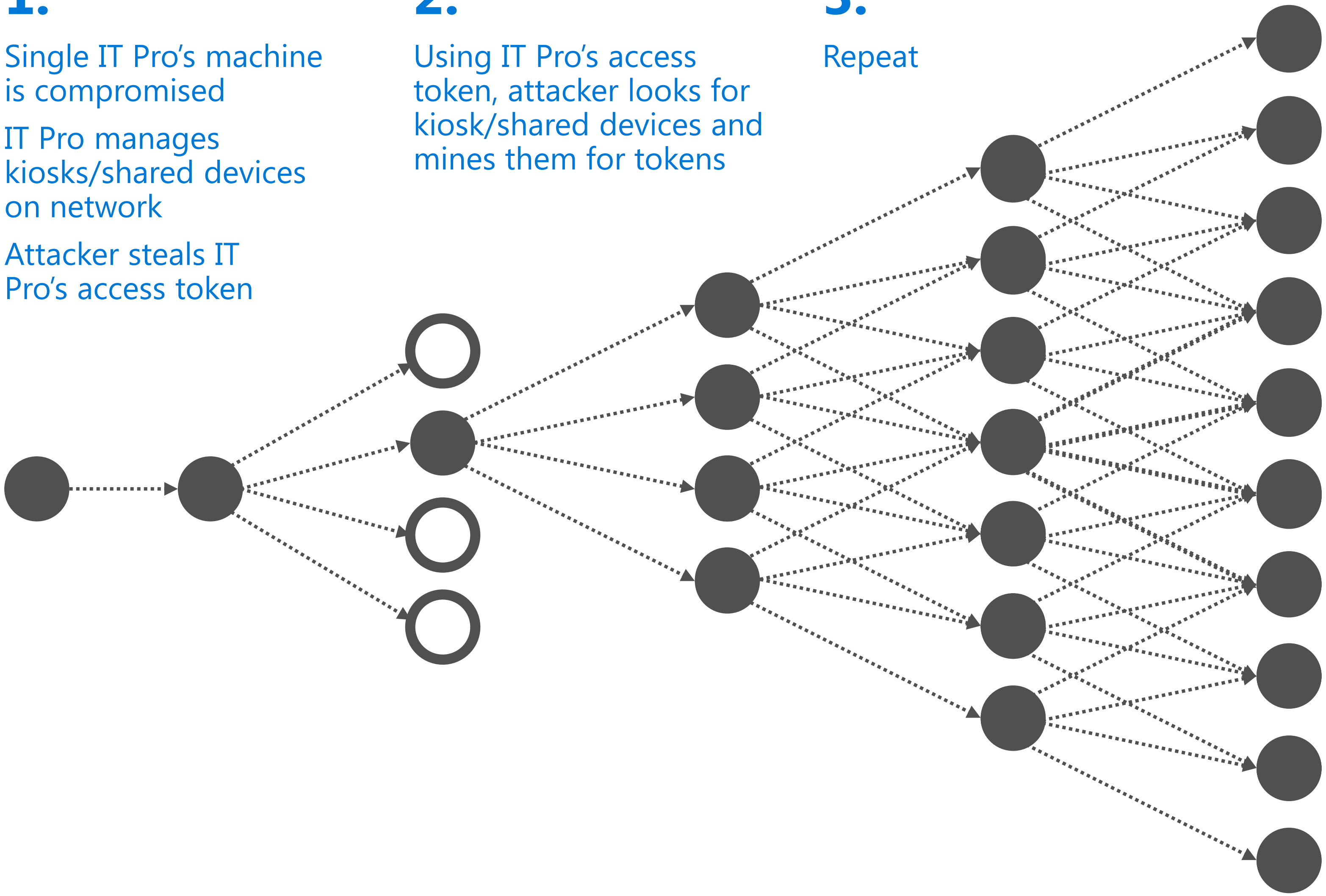
Using IT Pro's access token, attacker looks for kiosk/shared devices and mines them for tokens

3.

Repeat

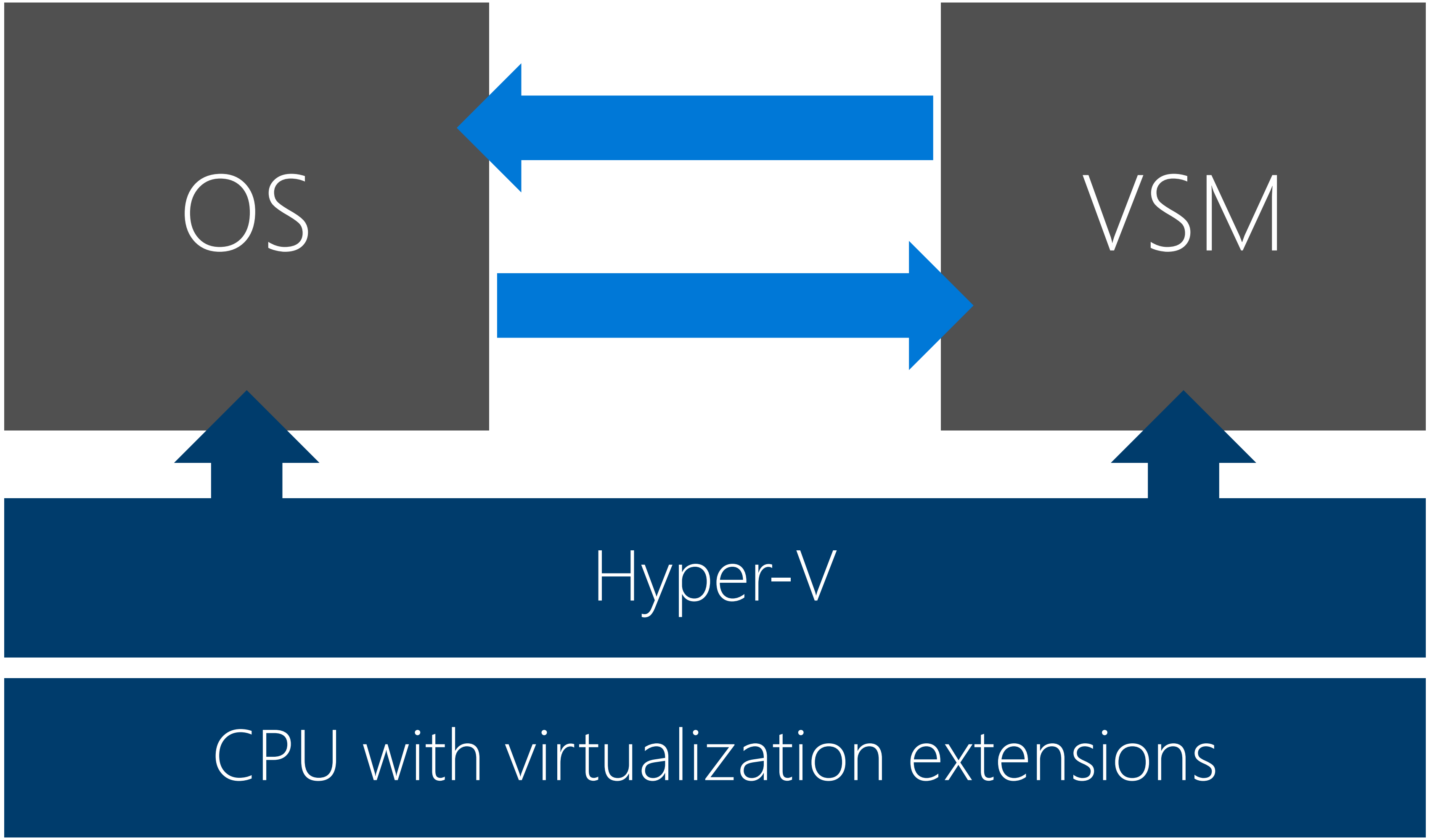
Pass the Hash Attacks

Access to one device can lead to access to many



Virtual secure mode

Identity protection



Information Protection

BitLocker data protection

Protects data when a device is lost or stolen using full disk encryption

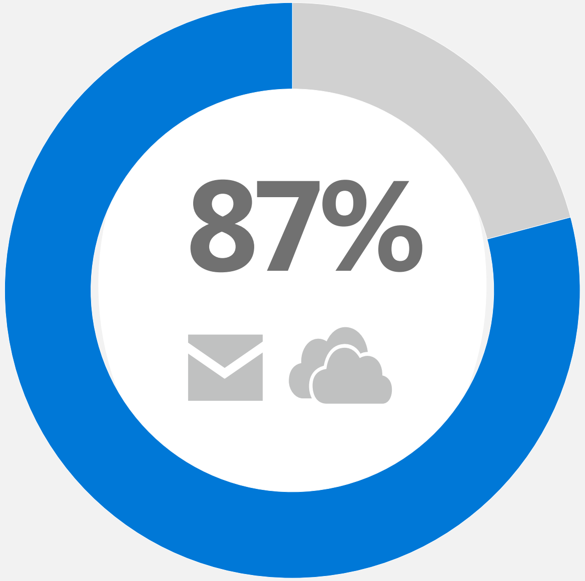
Provides single sign on and protection from cold boot attacks

Easy to deploy and manageable at scale

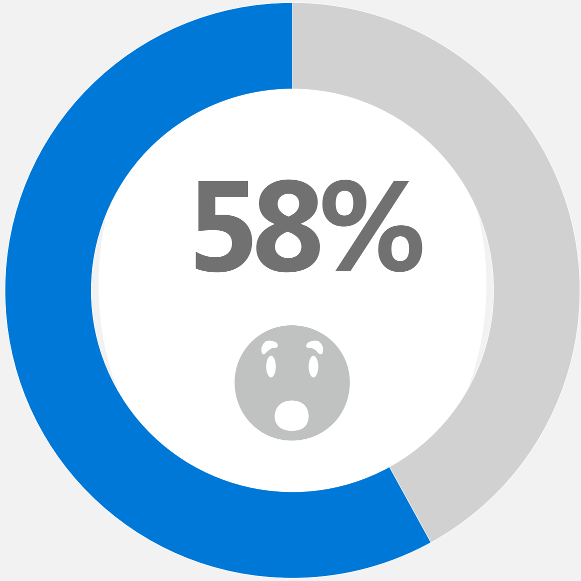
Excellent integration, performance, and reliability

In process for FIPS 140-2 certification

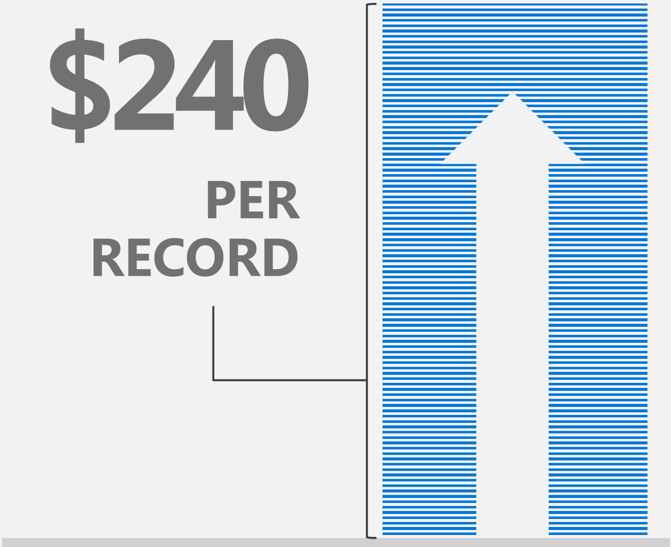
Data Leakage



...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

Information protection needs

DEVICE PROTECTION

DATA SEPARATION

Containment

BYOD separation

LEAK PROTECTION

Prevent unauthorized apps from accessing data

SHARING PROTECTION

HOW OTHERS ARE FILLING THE GAP: PAIN POINTS

Switching modes and between containers

Users change apps to work securely

Experience between mobile and desktop inconsistent

Solutions are expensive

Enterprise data protection

Provides user friendly data separation and containment (corporate versus personal)

Enables data protection wherever your data is

Ensures only trusted apps can access your data

Delivers protection for mobile and the desktop

Device Protection

TODAY'S CHALLENGE

Trusted by default, **until** defined as threat

APPS

Detection-based methods are unable to keep up

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

Threat Analysis

Sobering statistics

200+

The median # of days that attackers reside within a victim's network before detection

76%

of all network intrusions are due to compromised user credentials

$500B

The total potential cost of cybercrime to the global economy

$3.5M

The average cost of a data breach to a company

The frequency and sophistication of cybersecurity attacks are getting worse.

Microsoft Advanced Threat Analytics

Detect threats fast with Behavioral Analytics

No need to create rules or policies, deploy agents or monitoring a flood of security reports. The intelligence needed is ready to analyze and continuously learning.

Adapt as fast as your enemies

ATA continuously learns from the organizational entity behavior (users, devices, and resources) and adjusts itself to reflect the changes in your rapidly-evolving enterprise.

Focus on what is important fast using the simple attack timeline

The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving you the power of perspective on the "who-what-when-and how" of your enterprise. It also provides recommendations for next steps

Reduce the fatigue of false positives

Alerts only happen once suspicious activities are contextually aggregated, not only comparing the entity's behavior to its own behavior, but also to the profiles of other entities in its interaction path.

http://www.microsoft.com/ata

Questions?

Windows 10

Microsoft