Microsoft

winhec

2016

Microsoft

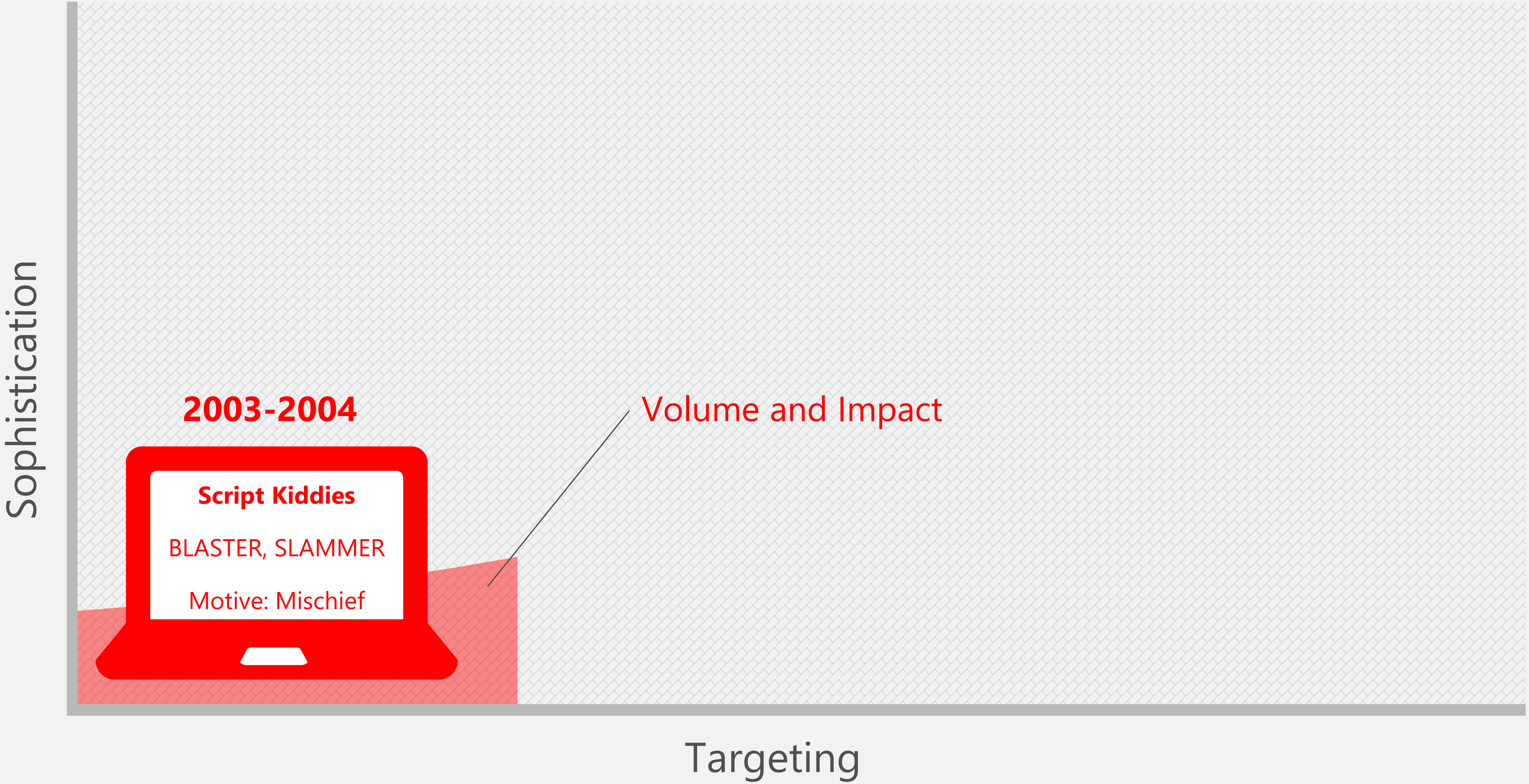
Windows Security

Chris Riggs
Senior Program Manager

winhec

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

THE EVOLUTION OF ATTACKS



2003-2004

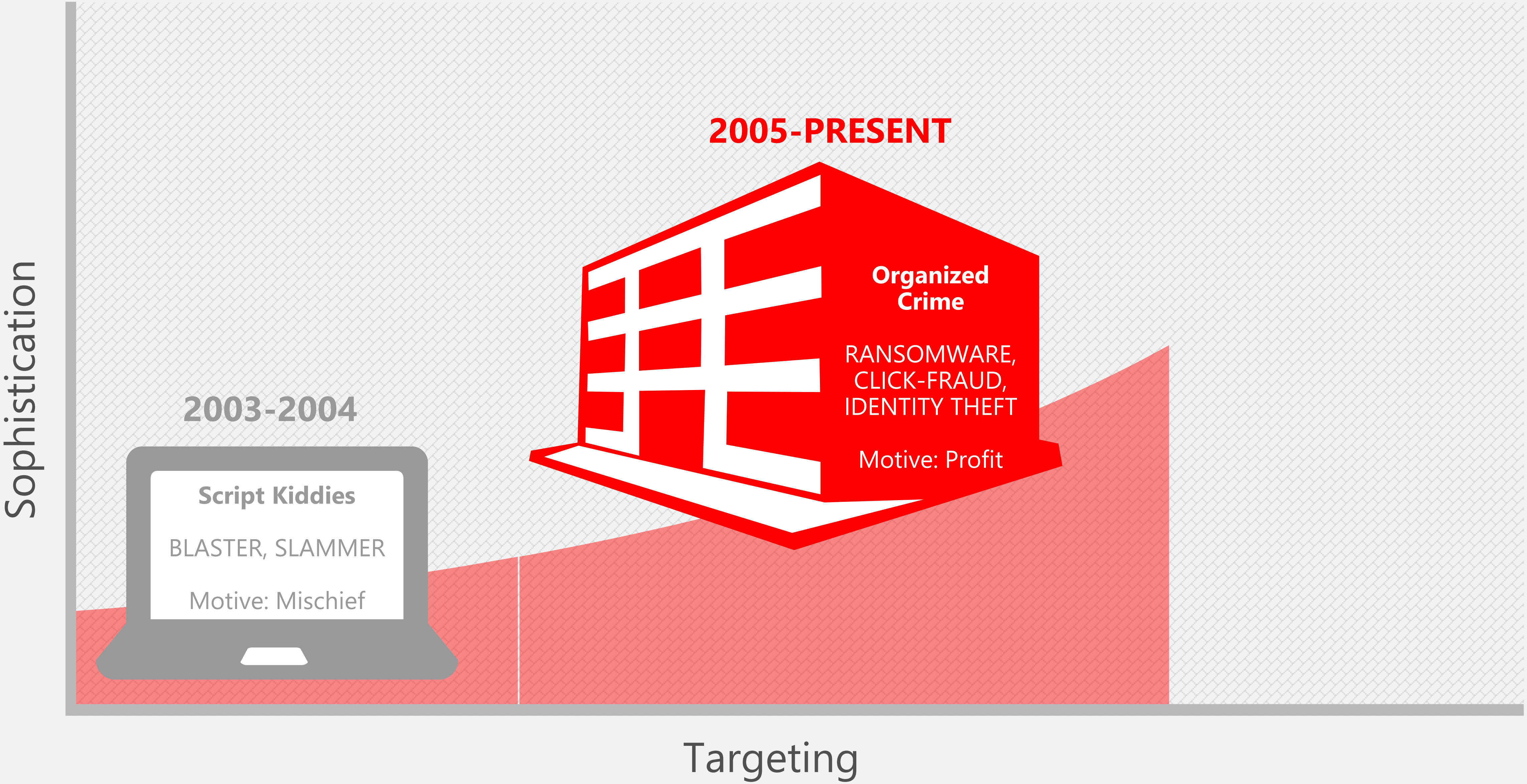
Script Kiddies

BLASTER, SLAMMER

Motive: Mischief

Volume and Impact

THE EVOLUTION OF ATTACKS



Script Kiddies

BLASTER, SLAMMER

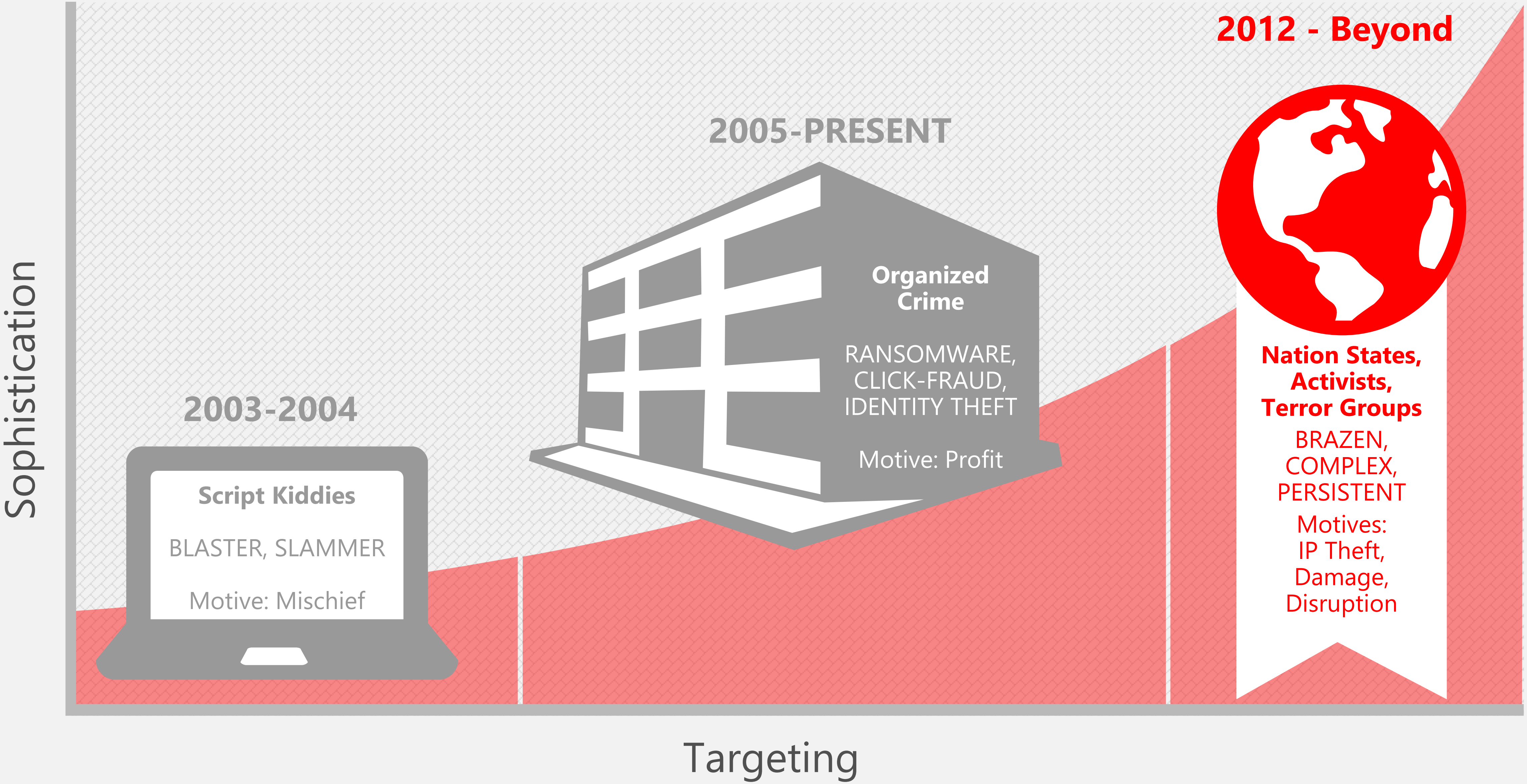
Motive: Mischief

Organized Crime

RANSOMWARE, CLICK-FRAUD, IDENTITY THEFT

Motive: Profit

THE EVOLUTION OF ATTACKS



Sophistication

Targeting

2003-2004

Script Kiddies

BLASTER, SLAMMER

Motive: Mischief

2005-PRESENT

Organized Crime

RANSOMWARE, CLICK-FRAUD, IDENTITY THEFT

Motive: Profit

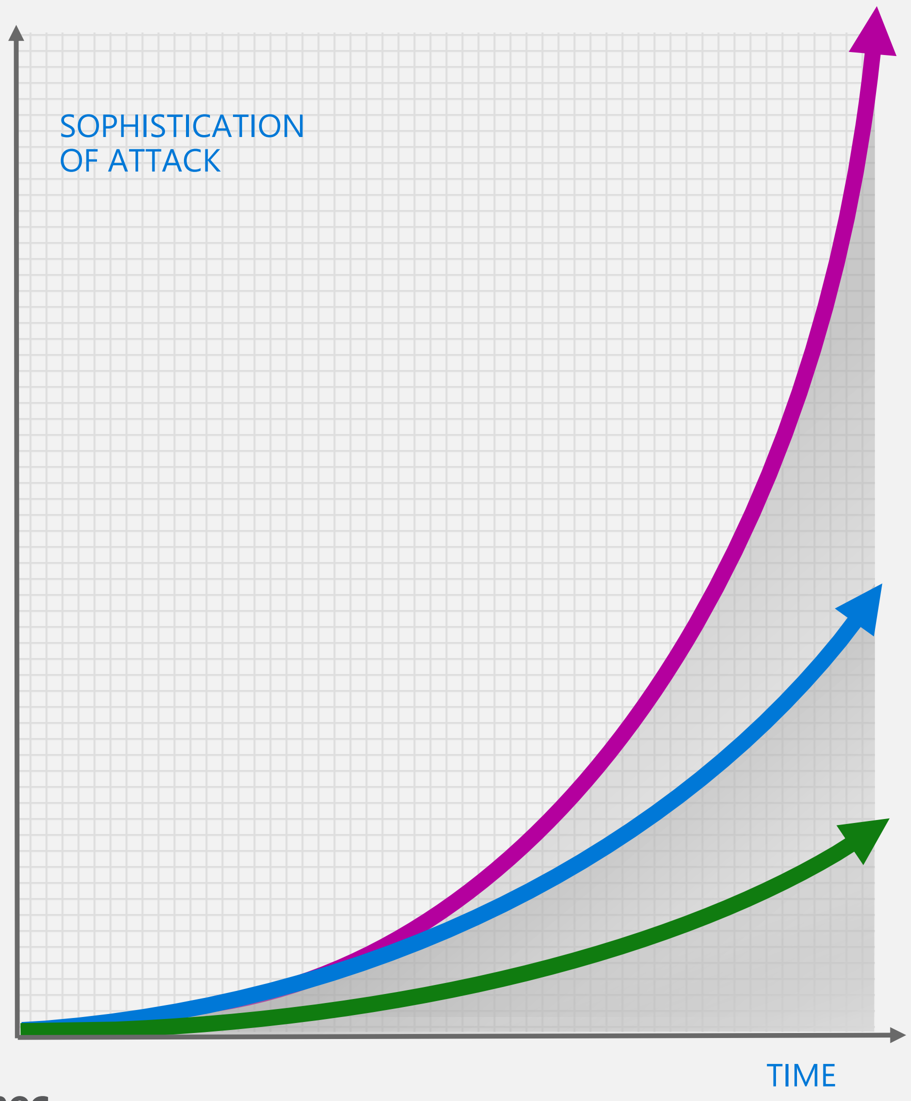
2012 - Beyond

Nation States, Activists, Terror Groups

BRAZEN, COMPLEX, PERSISTENT

Motives: IP Theft, Damage, Disruption

EVOLUTION OF SECURITY THREATS



ADVANCED PERSISTENT ATTACKS (APT)

- **Adversaries**: nation states, mercenaries
- **Goals**: stealing IP, espionage, cyber weapons, hacktivism
- **Targeting**: enterprise, financial, infrastructure, government
- **How**: tailored-made attacks, low degree of automation, leverage system tools
- **Attributes**: attacks last weeks-months, movement across many machines in an org.

MALWARE

- **Adversaries**: crime groups
- **Goals**: monetary revenues through various schemes
- **Targeting**: consumer and enterprise
- **How**: typically machine generated, polymorphic , large scale volumes
- **Attributes**: Attack life can be hrs./days, focus on machine level, across many orgs

UNWANTED SOFTWARE

- **Adversaries**: commercial companies
- **Goals**: monetize user traffic
- **Targeting**: consumers
- **How**: lure users to change browser defaults/install software to generate traffic
- **Attributes**: targeting unsophisticated users, almost impossible to uninstall

"CYBER SECURITY IS A **CXO ISSUE**."

Cyber threats are a material risk to your business

$3 TRILLION

Impact of lost **productivity and growth**

$3.5 MILLION

Average **cost of a data breach** (15% YoY increase)

200+ DAYS

Median number of days attackers are present on a victims network **before detection**

Attacks are fast, efficient, and easier than you think

46%

of compromised systems had **no malware** on them

23%

of recipients **opened** phishing messages

50%

of those who open, click attachments **within the first hour**

Source: McKinsey, Ponemon Institute, Verizon

Protection against modern security threats

Secured hardware

Secured identities

Secured data

Secured from threats

New challenges require a new platform

Windows 7		Windows 10	
Malware starts before Windows, takes control, and evades detection	→	Helps prevent malware from compromising system before OS and defenses can start	Windows Trusted Boot
Passwords are easily stolen Multi Factor authentication too hard	→	Passwords can be replaced with biometrics and easy to use multi-factor authentication	Windows Hello
User credentials are easily stolen on companies networks	→	User credentials are protected using hardware based virtualization/isolation	Credential Guard
Malware can bypass anti-virus and app control solutions	→	Next Gen app control and OS hardening gives IT better control of what runs in their environment	Device Guard
Users and apps can leak business data without restriction	→	Data separation and containment capabilities help prevent accidental data leaks	Enterprise Data Protection
3rd party solutions required to detect targeted attacks on devices	→	Helps detect and respond to breaches with built in behavioral sensors and cloud based analytics	Windows Defender ATP

Attacker Entry Point

ENTER →
(Phase 1)

Browser or Document Exploit Delivery

SmartScreen/ Windows Defender

Phishing

SmartScreen/ Windows Defender

Windows Defender – Advanced Threat Detection

Detect Behaviors

Initial Compromise – single node

ESTABLISH →
(Phase 2)

Internet-Facing Service Compromise

Windows Defender

Browser or Document Exploit Execution

App Container
Control Flow Guard

Stolen Cred Usage

Windows Hello

Windows Defender – Advanced Threat Detection

Detect Behaviors

Escalation – privilege, network ownership, capabilities

EXPAND →
(Phase 3)

Kernel Exploit

Device Guard

Kernel-mode Malware

Device Guard/ Secure Boot

Stolen Cred Usage

Credential Guard

Windows Defender – Advanced Threat Detection

Detect Behaviors

Attacker Goals realized

ENDGAME
(Phase 4)

Alert

Investigate

Windows Defender – Advanced Threat Detection

Securing your hardware

Biometrics

Move from what you know to what you have

Microsoft Hello

Facial recognition

Fingerprint

TPM

Supports Windows 10 security features

Made better in Windows 10 with next gen SOC, TPM 2.0

Virtualization Based Security

Architectural change to address malware threats

Isolates critical Windows components and data from threats

UEFI

Faster and more secure devices

Device is secured from power on to power off

TPM 2.0

Executive Summary

✓ Trusted Platform Mode is a critical component to Windows 10 features and delivering on our security promises to customers

✓ TPM 2.0 firmware or discrete must be enabled by default and is the minimum hardware requirement for Windows 10 (Anniversary Update).

> Exception: This does not apply to OEM systems for special purpose commercial systems, customer orders, and customer images with a custom image

✓ Microsoft recommends working with discrete or firmware TPM suppliers to meet this requirement for Windows 10

TPM Requirements for new Anniversary Update Systems

Windows Desktop

For this Summer, 2016, all new devices and computers, all SKU's, must implement and be in compliance with the International Standard ISO/IEC 11889:2015 or the Trusted Computing Group TPM 2.0 Library, Revision 1.16 (or later) specification and a component which implements the TPM 2.0 must be present and enabled by default.

Windows Mobile

All Windows Phone devices require TPM 2.0

Windows IOT

TPM remains *optional* on Windows IOT

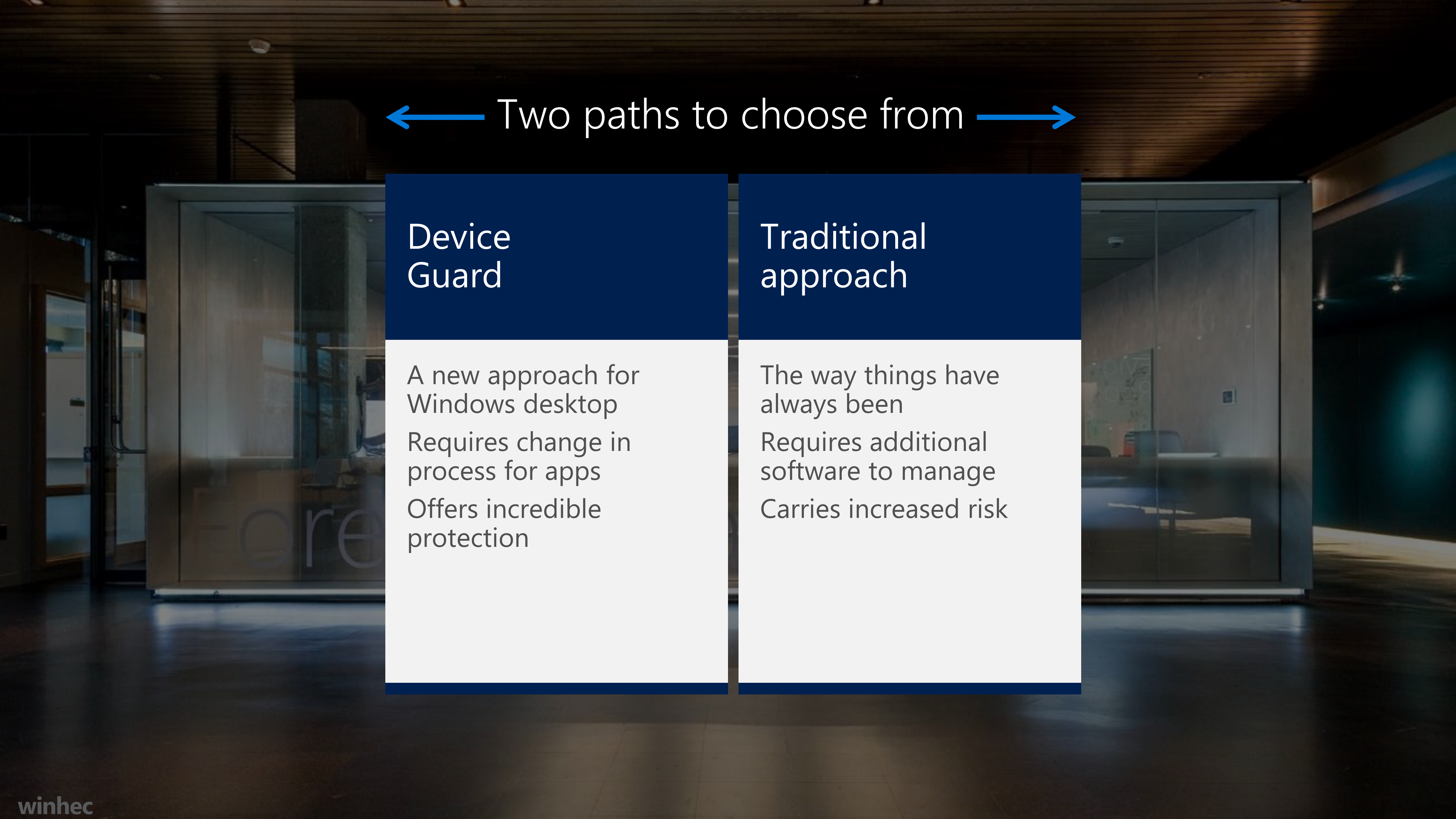
Windows Server

TPM remains *optional* for unless the additional qualification (AQ) criteria for the Host Guardian Services scenario in which case TPM 2.0 is required.

Windows 10 (Anniversary Update) Feature Dependencies on TPM

Win 10 Feature	TPM 1.2	TPM 2.0	Details
UEFI Secure Boot			• No TPM requirement
Conditional Access			• No TPM requirement
Enterprise Data Protection			• No TPM requirement
Windows Defender - Advanced Threat Detection			• No TPM requirement
Device Guard / Configurable Code Integrity			• No TPM requirement
Windows Hello			• No TPM requirement
Credential Guard	Yes	Yes	• More secure with TPM 2.0
Measured Boot	Yes	Yes	• More secure with TPM 2.0
Device Health Attestation	Yes	Yes	• Requires TPM
Virtual Smart Card	Yes	Yes	• Requires TPM
Passport: Domain AADJ Join	Yes	Yes	• Supports both versions, but requires TPM with HMAC and EK certificate for key attestation support.
Passport: MSA / Local Account	Yes	Yes	• Requires TPM 2.0 for HMAC and EK certificate for key attestation support
BitLocker	Yes	Yes	• TPM 1.2 or later required or a removable USB memory device such as a flash drive
Device Encryption		Yes	• For Modern Standby devices, all require TPM 2.0

Device Guard / Credential Guard



← 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 operating systems (e.g., Windows Phone)

Untrusted apps and executables, such as malware, are unable to run

Protects kernel mode processes and drivers from zero days and vulnerabilities using HVCI

Requires Windows 8 or Windows 10 certified hardware

Getting apps into the circle of trust

Supports all apps including Universal and Desktop (Win32)

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

Signing services are available to OEMs, IHVs, ISVs, and Enterprises

HVCI Readiness

HVCI Compliance

Push for HVCI Compliance on New Devices and Existing Peripherals

- Tied to key enterprise features and security, we require for Windows 10 (Anniversary Update):
- All drivers to meet Hypervisor-Enforced Code Integrity requirements (HVCI) within 90 days of RTM running the HLK
- Validate UEFI firmware support Device Guard enablement
- Move peripherals drivers to HVCI compliance and perform validation

- Windows System Compatibility can be achieved with drivers tested with 1507, 1511 or Anniversary Update HLKs until Windows RS1 RTM, plus 90 days

Device Guard / Credential Guard Requirements

Requirements	Description
Windows 10 Enterprise	The PC must be running Windows 10 Enterprise. (also available on Server '16, Education)
HVCI Compatible Drivers	MUST meet all HVCI Compatible Driver requirements as described in "Filter.Driver.DeviceGuard.DriverCompatibility". "Device.DevFund.DeviceGuard.DriverCompatibility"
A VT-D or AMD-Vi IOMMU[1]	IOMMU enhances system resiliency against memory attacks.
x64 architecture	The Windows hypervisor only supports 64-bit PC
Virtualization extensions	Virtualization extensions are required to support virtualization-based security: • Either Intel VT-X or AMD-V • CPU supports Second Level Address Translation

Device Guard / Credential Guard Requirements

Requirements	Description
Secure firmware update process	UEFI firmware must support secure firmware update following section System.Fundamentals.Firmware.UEFISecureBoot in Windows Hardware Compatibility Program requirement.
Firmware support for SMM protection	Firmware SMM code must be reviewed and hardened to prevent memory attacks. This will provide a strong platform security foundation for VSM (Virtual Secure Mode). 1. System MUST implement the ACPI WSMT table, as described in the "Windows SMM Security Mitigation Table" document. All non-reserved WSMT protection flags field MUST be set indicating that the documented mitigations are implemented. 2. SMM must not execute code from memory that is writable by the OS.
UEFI NX Protections	UEFI RunTime Services 1. Must implement UEFI 2.6 specification's EFI_MEMORY_ATTRIBUTES_TABLE. The entire UEFI runtime must be described by this table. 2. All entries must include attributes EFI_MEMORY_RO, EFI_MEMORY_XP, or both 3. No entries must be left with neither of the above attribute, indicating memory that is both executable and writable. Memory MUST be either readable and executable OR writeable and non-executable.
Firmware security patch for Secure MOR Implementation	Secure MOR bit prevents certain memory attacks thus necessary for Credential Guard. This will further enhance security of Credential Guard.
Trusted Platform Module (TPM) version 1.2 or 2.0	TPM 1.2 and 2.0 provides protection for encryption keys that are stored in the firmware. TPMs, either discrete or firmware will suffice, but this is a must have requirement for Credential Guard.
Intel TXT / SGX	Intel TXT is not supported with the Microsoft hypervisor. TXT must be disabled in the firmware. Intel SGX is not utilized by the Microsoft hypervisor, VBS, or guest VMs. SGX applications may run in the Windows root when Device Guard is enabled.

System Management Mode (SMM) Mitigations:

- ✓ Firmware must consider attacks from kernel malware
- ✓ It must protect itself from security compromise
- ✓ It must NOT facilitate bypass of a hypervisor

System Management Mode Mitigations

- Virtualized Based Security seeks to create a secure environment
  - Platform firmware, including SMM, must play a key role in providing a secure foundation
  - SMM is opaque to the OS, and the OS must assume SMM is within the same trust domain as the OS itself
- Exploits may be mounted via SMM
- To protect against these threats, changes to SMM programming practices and assumptions must be introduced
- The OS must be able to determine what SMM security mitigations have been implemented on a specific platform
- The OS must rely on SMM firmware to accurately self-report which of the Microsoft recommended security best practices it has implemented
- To accomplish this, Microsoft has defined the ACPI static table Windows SMM Security Mitigations Table (WSMT)

Resource

Windows SMM Security Mitigations Table (WSMT)

https://msdn.microsoft.com/en-us/library/windows/hardware/dn495660(v=vs.85).aspx#wsmt

Device Security Best Practices

Protecting our customers requires an ecosystem effort

Window 10 security features rooted in hardware

- BitLocker, Secure Boot, Health Attestation, Device Guard, Credential Guard, Windows Hello, Microsoft Passport

Researcher & attacker interest follows

- 37 unique publicly disclosed firmware issues in the last ~2 years according to Intel Security ATR
- Exploits can lead to security control bypass

Not letting up on software vulnerabilities though

- Antivirus, System Utilities, Certificates

Targeted Security Promises

1. My device’s software & firmware are developed according the **Security Development Lifecycle**. *(or equivalent, ISO/IEC 27034)*

2. Security issues are monitored, investigated and resolved by a formal security **response process**.

3. My device’s software & firmware can **be updated in the field** when future issues are discovered.

4. My device has the proper hardware to **take advantage of Window security features.**

5. Firmware security **best practices** are followed.

6. My device is **not vulnerable** to publically known UEFI vulnerabilities at the time of release.

7. Security Certificates added to my device are documented and **justified**, with a pre-defined security response plan.

Device Security for OEMs

- Firmware is software…
  - ✓ Follow industry best practices (*e.g. NIST 800-147, ISO/IEC 19678:2015*)
  - ✓ Conduct security reviews on your firmware
  - ✓ Plan to regularly address reported vulnerabilities going forward and in the field with updates.
- Proper implementations provide opportunity to demonstrate security benefits of modern hardware
- Follow best practice checklists in ChipSec, HSTI & HLK

Security Checklist for OEMs	Tool Method
1. UEFI/BIOS lock down configs	HSTI / ChipSec
2. UEFI/BIOS vulnerability assessment	ChipSec (fix all warnings and errors)
3. UEFI/BIOS updated	Via UEFI Firmware Update Capsule
4. Secure MOR enabled	HSTI
5. Platform Secure Boot enabled	HSTI
6. Boot Guard / Hardware Verified Boot	HSTI
7. Confirm enabled TPM 2.0	HLK
8. Static DBX updated	HLK
9. HVCI driver compliance	HLK / WHQL

Tools:

Run ChipSec: https://github.com/chipsec/chipsec
Run HSTI: http://aka.ms/hsti
Run HLK: https://msdn.microsoft.com/en-us/windows/hardware/dn913721.aspx

Call To Action

1. Be ready to enable and support our existing and new security features in Windows 10
2. Update firmware regularly
3. Leverage our security best practices
4. Run tools, including HSTI, ChipSec, & HLK
5. Provide feedback to us: winhec@microsoft.com