Intel® Enterprise Ultra Mobile Security

Presenter:
Marcin Kaczmarski

Date:
October 2013

XIV edycja Seminarium PIU Jakość danych w systemach informacyjnych zakładów ubezpieczeń Warszawa, 29 października 2013 r.

Ultra Mobile Devices Without Compromise:
Enterprise Ready with Enhanced Security

Intel® Technology:
No Compromise for IT

Good

Security Infrastructure Compatibility

- Maintain Existing Management Infrastructure
- Maintain Existing Security Best Practices

Better

Intel® Enhanced Windows 8 Security

- Creates Platform Root and Chain of Trust
- Secure Boot Options:
  Secure Boot/ELAM/Measured Boot

Best

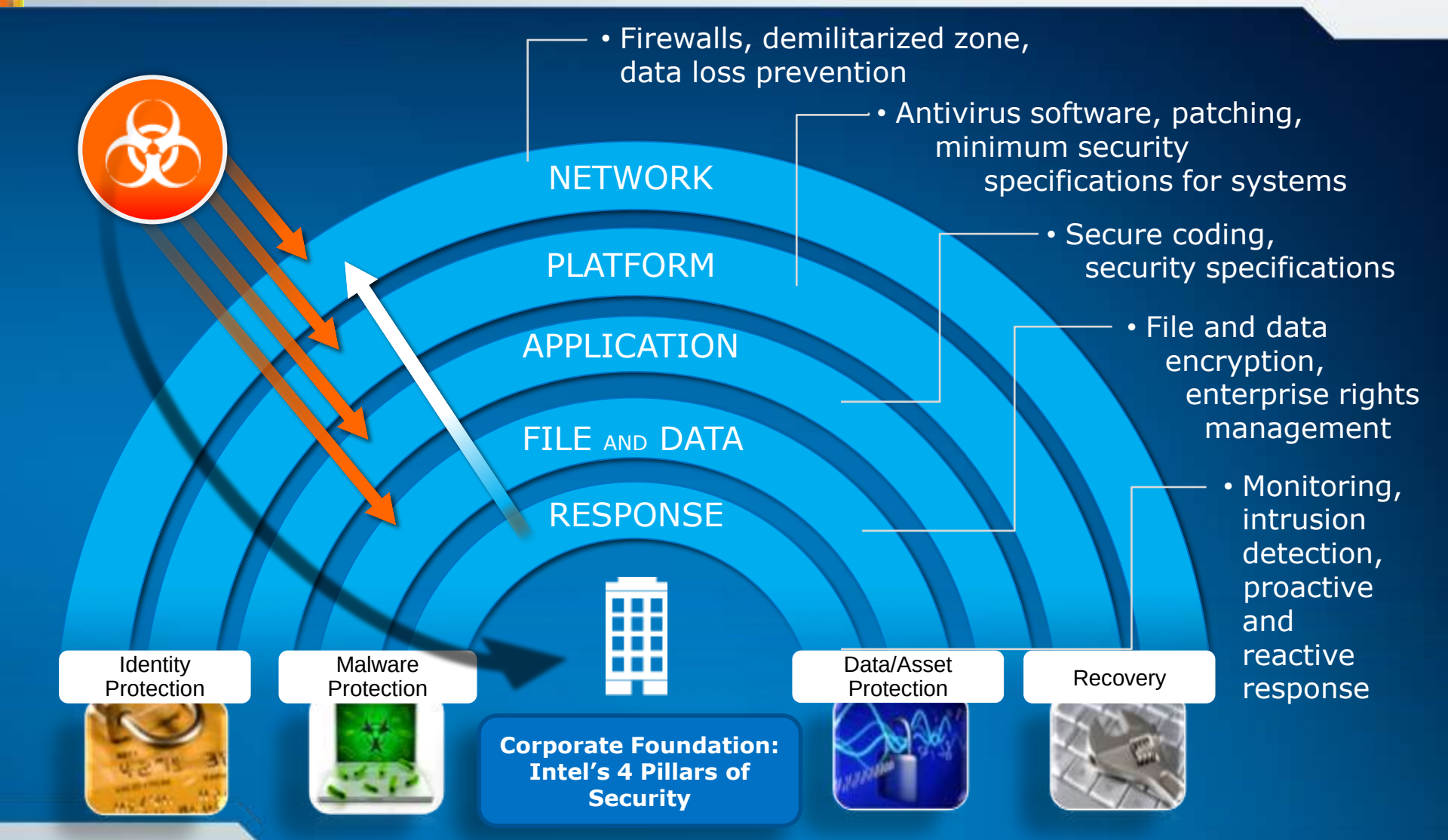
Intel® Hardware-Enhanced Security

- Protection Beyond the OS
- Enabled by McAfee and Other ISVs

Software protection alone is not sufficient AND All Hardware is Not Created Equal

Choose Ultra Mobile Devices with Intel® Technologies

Information Security Best Practice:
Employ Multiple Security Perimeters



Tools of the Modern Hacker

Social Engineering

Manipulating people to divulge data or "click here."

Advanced Persistent Threat (APT)

A long-term, human-directed "campaign" to take control of a specific system or network—all while remaining undetected.

Kernel-Mode Rootkit

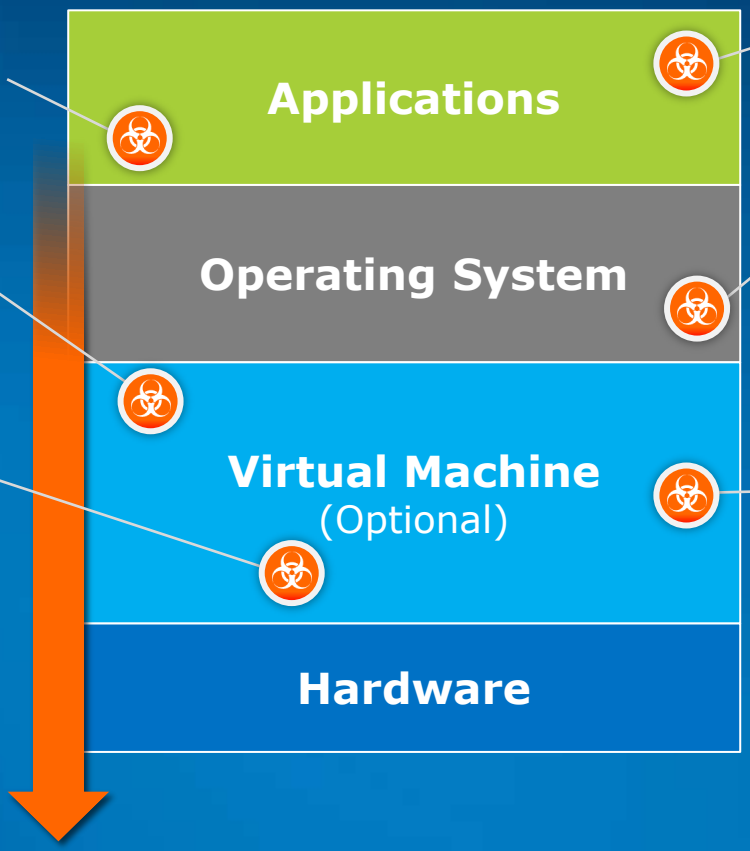
It lives and operates below the operating system to control the OS and evade detection by OS-level security measures. Can cloak other malware, APTs.

Attacks are Moving Down the Stack

Attacks disable security products

Compromise virtual machine

Ultimate APTs: Compromise platform and devices below the OS, using rootkits as cloaks



Traditional attacks: Focused primarily on the application layer

OS infected with APTs: Threats are hidden from security products

New stealth attacks: Embed themselves below the OS and Virtual Machine, so they can evade current solutions

Industry Approaches to Ultra Mobile Security

Intel and McAfee Approach

- Maintain open architecture enhanced by hardware-enhanced security and response
- McAfee and Intel provide unprecedented levels of hardware-enhanced ultra mobile security
- Form factor choice – tablets, Ultrabooks, convertibles

Windows* 8 Enhanced Security

- Enterprise flexibility, leveraging security capabilities to keep threats out
- Unification of platform top to bottom
- Adopting secure app delivery model for touch-based devices

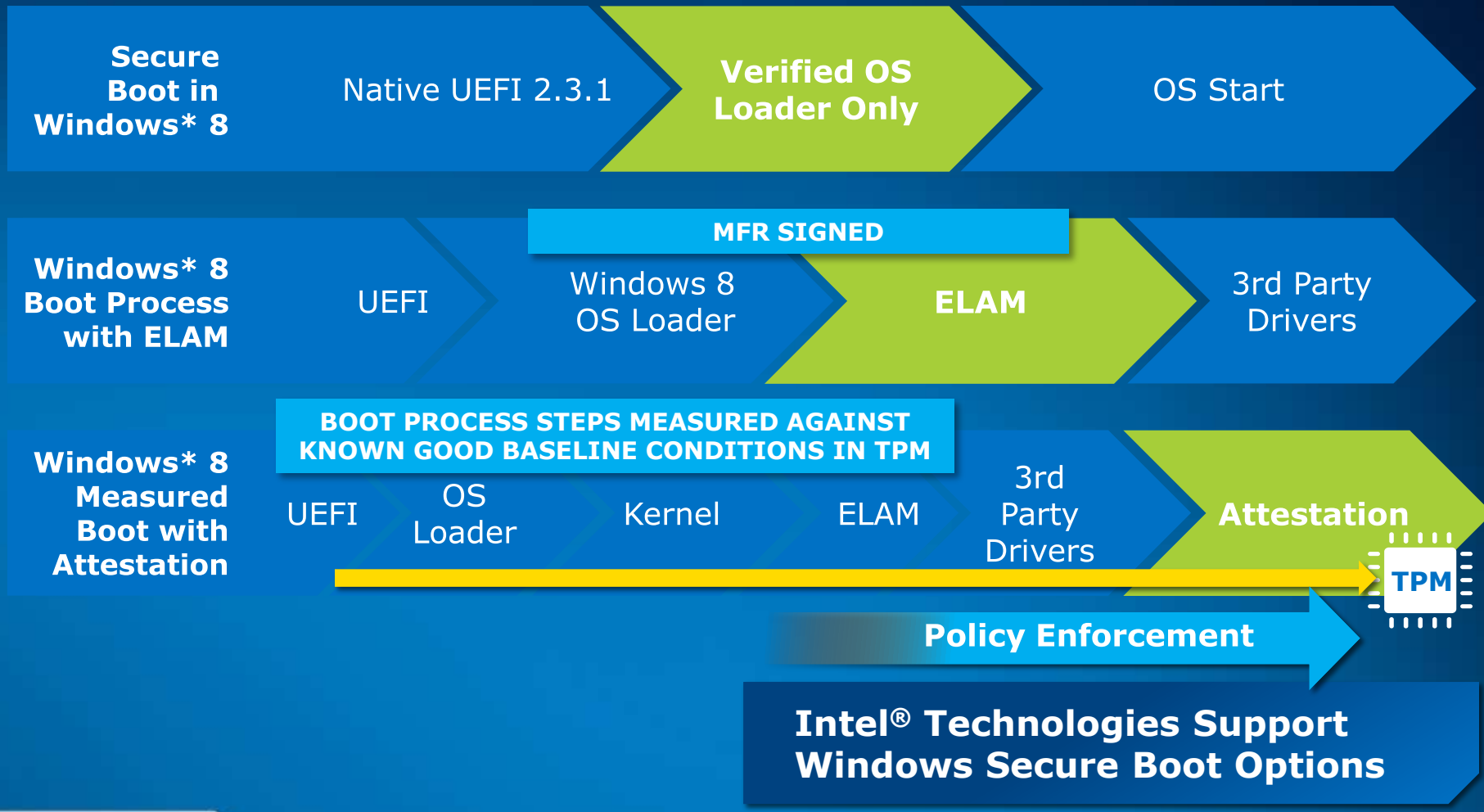
iOS*

- Fundamentally different; closed architecture
- Enterprise legacy compatibility not built-in; requires 3rd party
- Focus on "Good Enough" security with simplified device provisioning

Intel and Windows 8: the best solution for enterprise security

Intel Hardware-Enhanced Security with Windows* 8

Intel® Architecture with Windows* 8 Better Together from Boot to Runtime



Intel® PTT, Anchor Cove and TXT: HW-enhanced Security Choices for Windows 8*

Intel® Platform Trust Technology

- Firmware-based Trust Technology
- Simpler solution compared to TPM hardware
- Supports Windows 8* measured boot
- Meets Windows WQL Connected Standby (CS) requirements
- Notebook/Ultrabook™ option

+

Anchor Cove

- Supports Measured Boot, Verified Boot and Combined Boot
- Protects against boot block level malware execution
- Helps prevent platform repurposing to run malware
- Supports TPM and Intel® PTT

+

Intel® Trusted Execution Technology

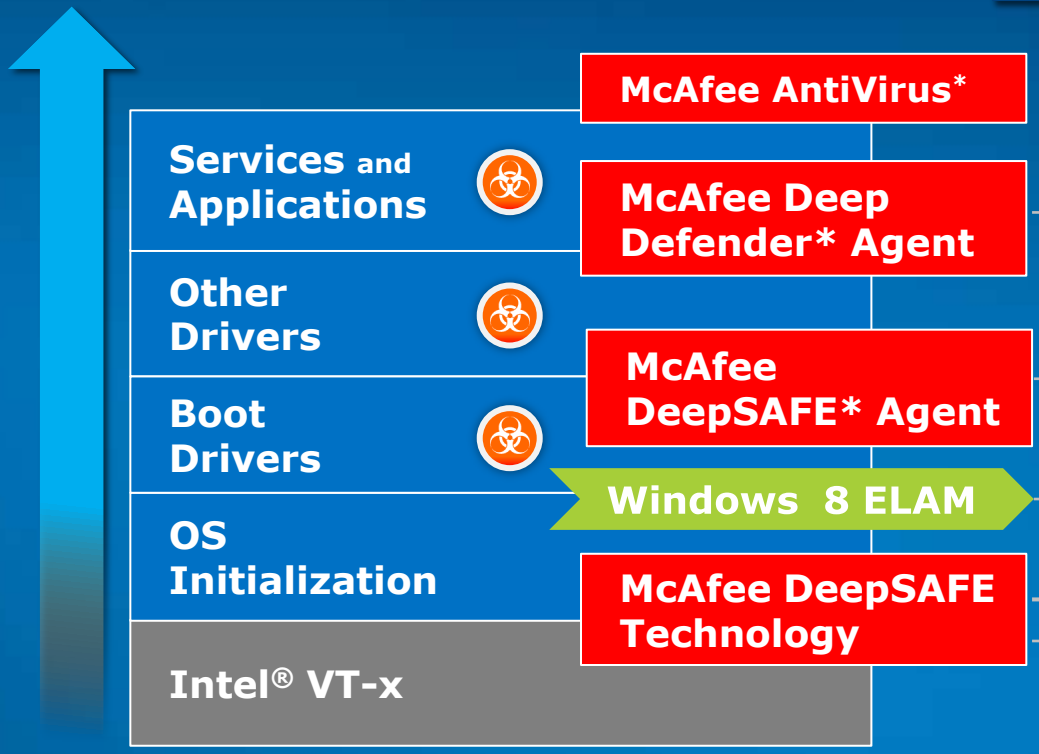
- Protect virtual and physical environment from malware and rootkits
- Validate the behaviors of key components of client system at startup to prevent attacks
- Establish HW based root of trust for measured launch environment
- Hardening the hypervisor with Citrix XenClient* XT

Enabling Hardware-enhanced Windows 8 Boot Security Across A Wider Range of Platforms

McAfee DeepSAFE* Technology/Deep Defender*: Stopping Infection Before it Starts

McAfee DeepSAFE Technology
McAfee Deep Defender
Stopping Stealthy Malware

Next-generation "beyond the OS" security enabled by Intel® Virtualization Technology



- Identifies/stops kernel-mode threats in real-time with out reboot
- DeepSAFE technology loads first for security beyond the OS
- W8 ELAM loads AV early to help detect malware sooner
- Real-time kernel-level memory monitoring using Intel® VT-x hardware assistance
- DeepSAFE loads first before OS

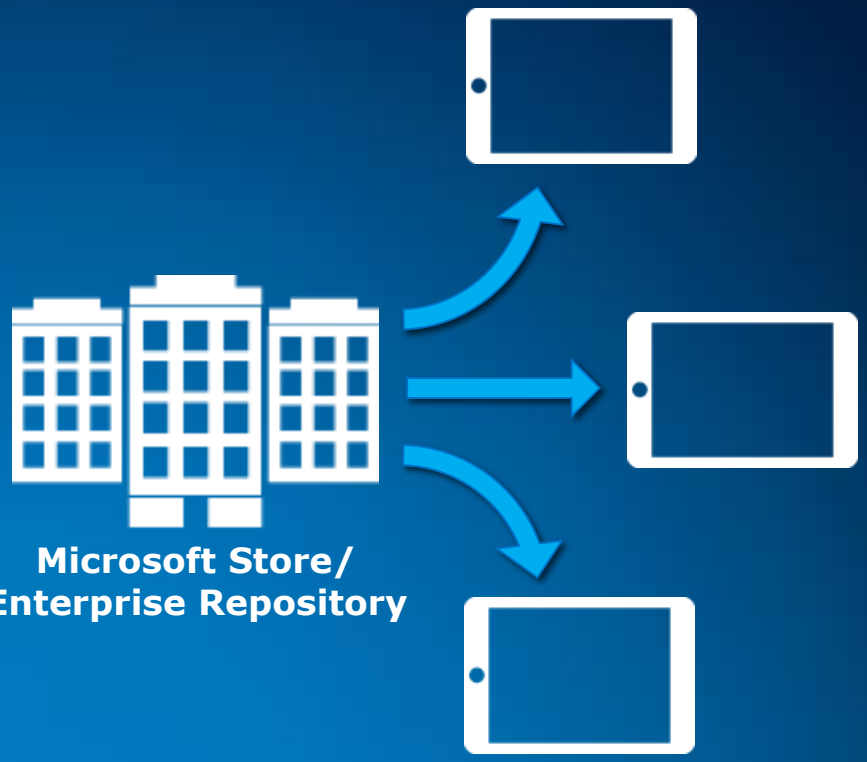
Secure Application Delivery for Touch

App Store Delivery

- Microsoft reviews, tests, and signs application code to meet security for touch
- Users install only vetted code

Sideloading from Enterprise Repository

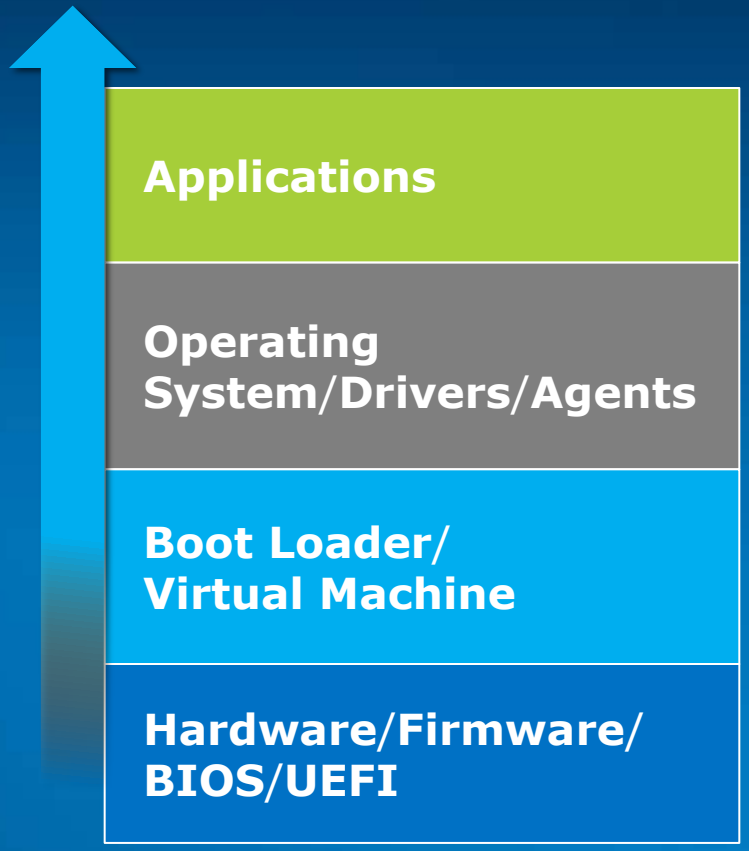
- Develop apps using Microsoft security practices and developer tools
- Enterprise self-certifies and delivers from its own repository



Traditional applications still distributed through Enterprise security and manageability model

Intel® Hardware-Enhanced Security and Response

Intel® Hardware-Enhanced Security Technologies: Raising the Bar on Security



Realtime McAfee antivirus/antimalware scanning

Intel's innovation of UEFI helps ensure Windows* 8 secure boot and chain of trust

Intel® hardware/firmware enables trusted virtual/physical environments

Security features embedded in Intel® silicon enabled by McAfee and other ecosystem ISVs

All Hardware is Not Created Equal

Platform Security Benefits: Intel® Platforms

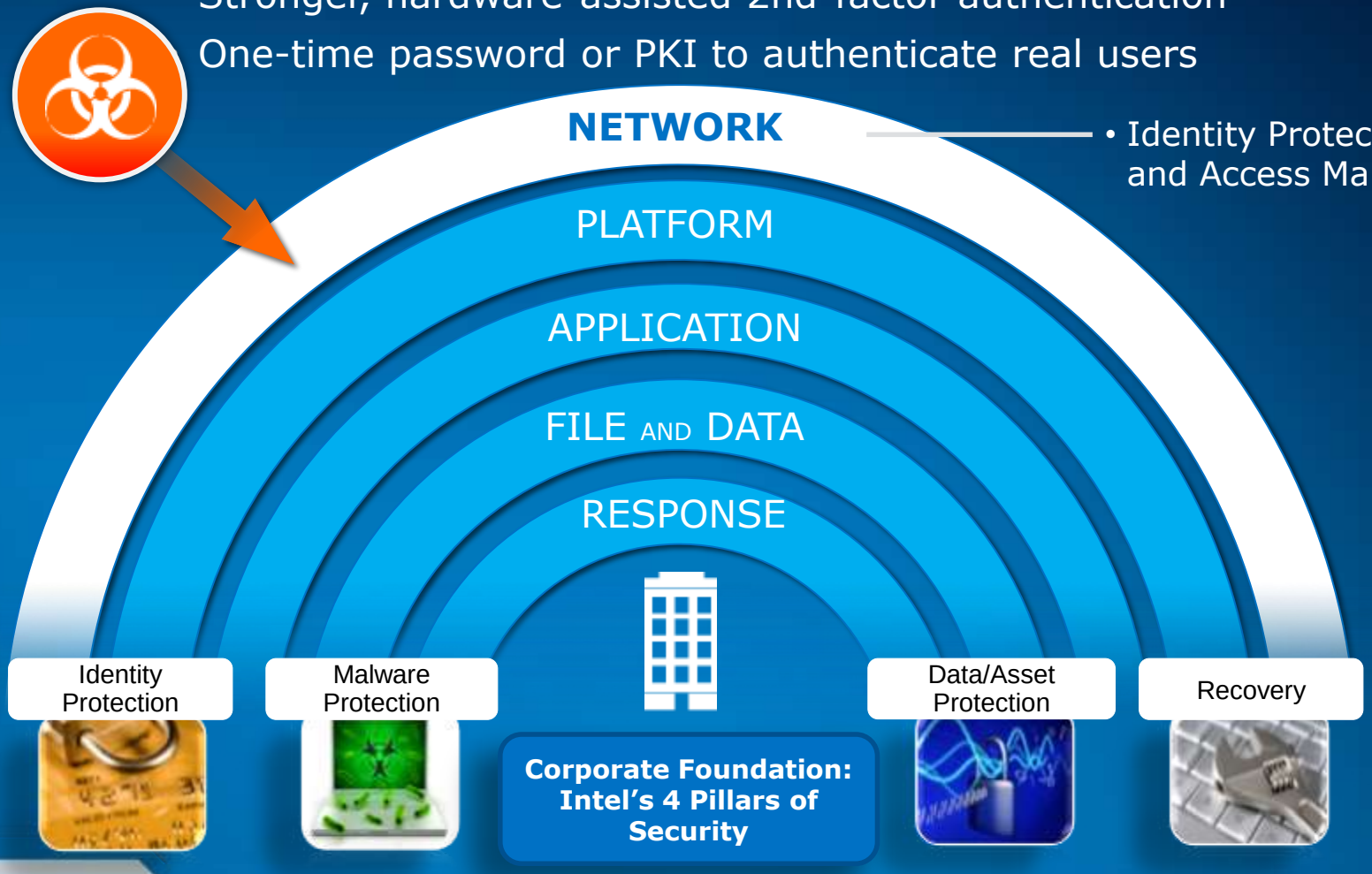
Avoid stealthy threats and guard against rootkits[6]	✓	✓	✓
Protect data with robust encryption[11]	✓	✓	✓
Guard against theft[2]	✓	✓	
Verify a tamper-free environment[1]	✓		
Hardware-based PKI token authentication security[7]	✓		

Hardware-Enhanced Network Security

Intel® Identity Protection Technology[7]

- Stronger, hardware-assisted 2nd-factor authentication

One-time password or PKI to authenticate real users



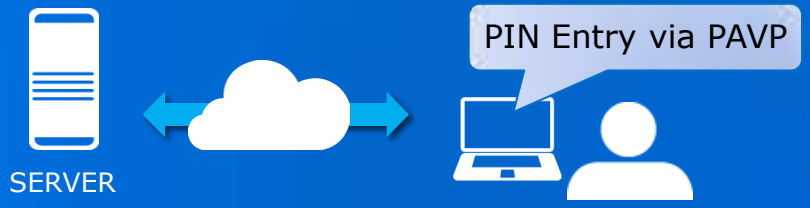
People: The New Network Perimeter
Human Vulnerabilities and Risks

Humans make mistakes: Lost Devices, "Found" USB drives, etc.

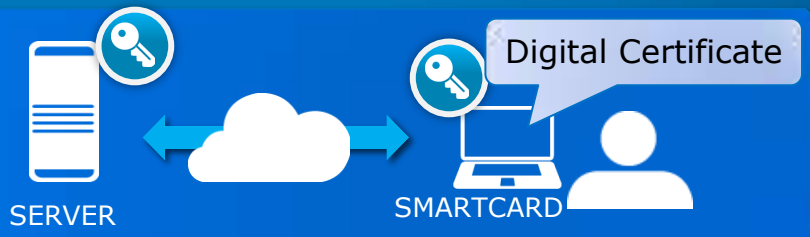
Intel® Identity Protection Technology[7] with 2-factor Authentication

Intel® IPT with **OTP**
Authenticates real Ultra Mobile user

Intel® IPT with **PTD**
Authenticates real user with PIN protected in hardware



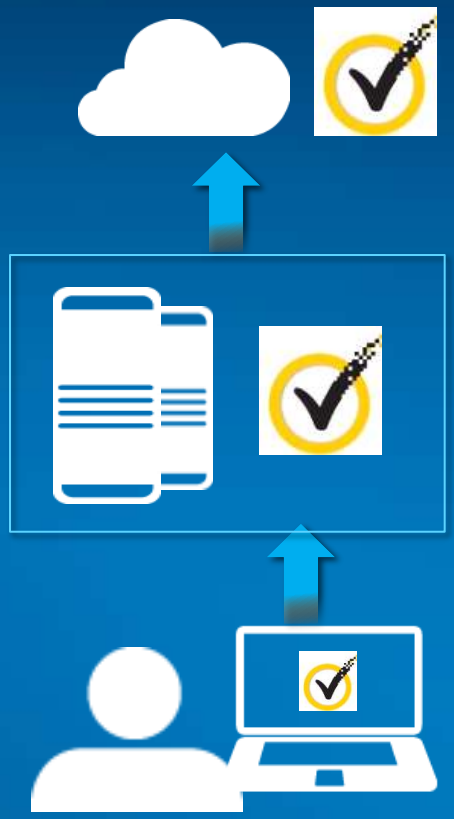
Intel® IPT with **PKI**
Authenticates *real* Ultra Mobile user to your network



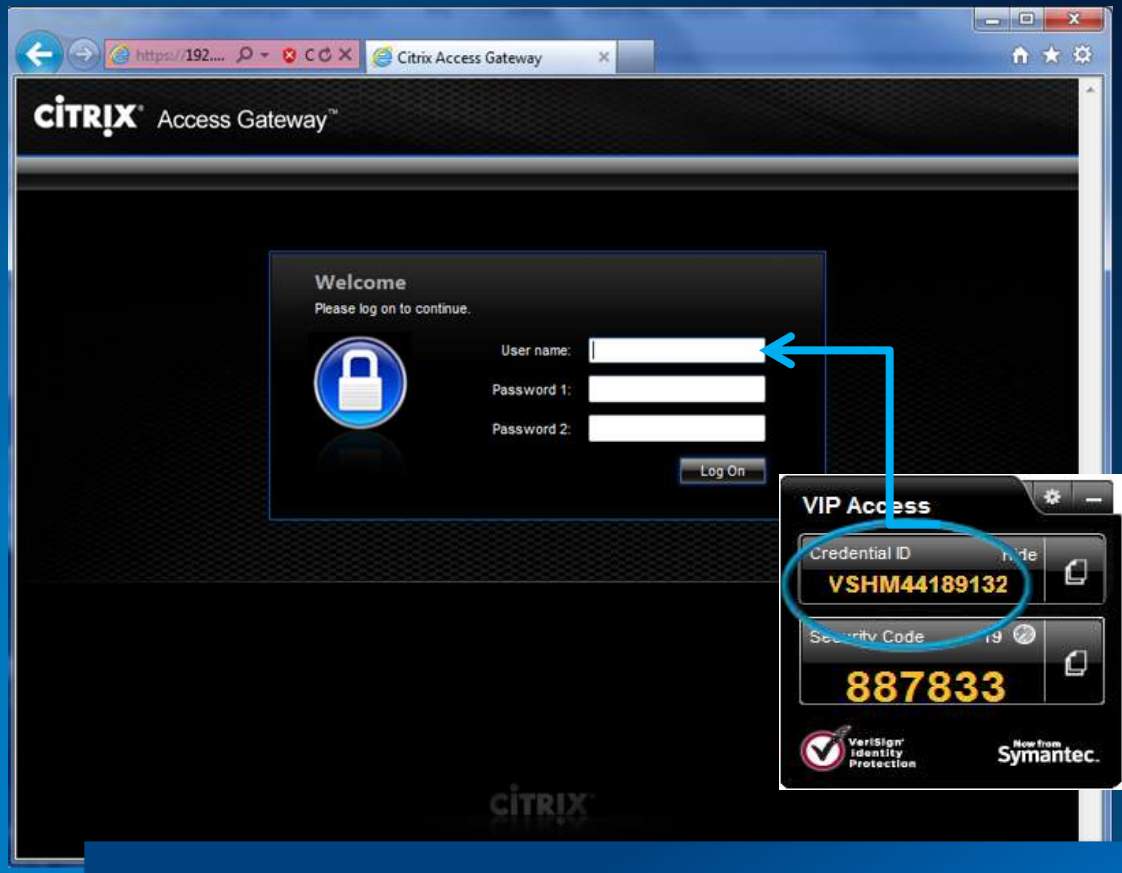
Ecosystem Vendors
- Symantec
- Vasco

IPT Delivers best choice for Network Security

Intel® IPT[7] with One-Time Password



ENTERPRISE



Authenticates Real Users on Their Tablets

Intel® IPT[7] with PKI *with* protected transaction display

Public Key Infrastructure (PKI):

- Private key stored in firmware; used for authentication and encryption
- More secure than Software
- Lower cost and easier to use than smart cards

Now embedded in your PC

Symantec

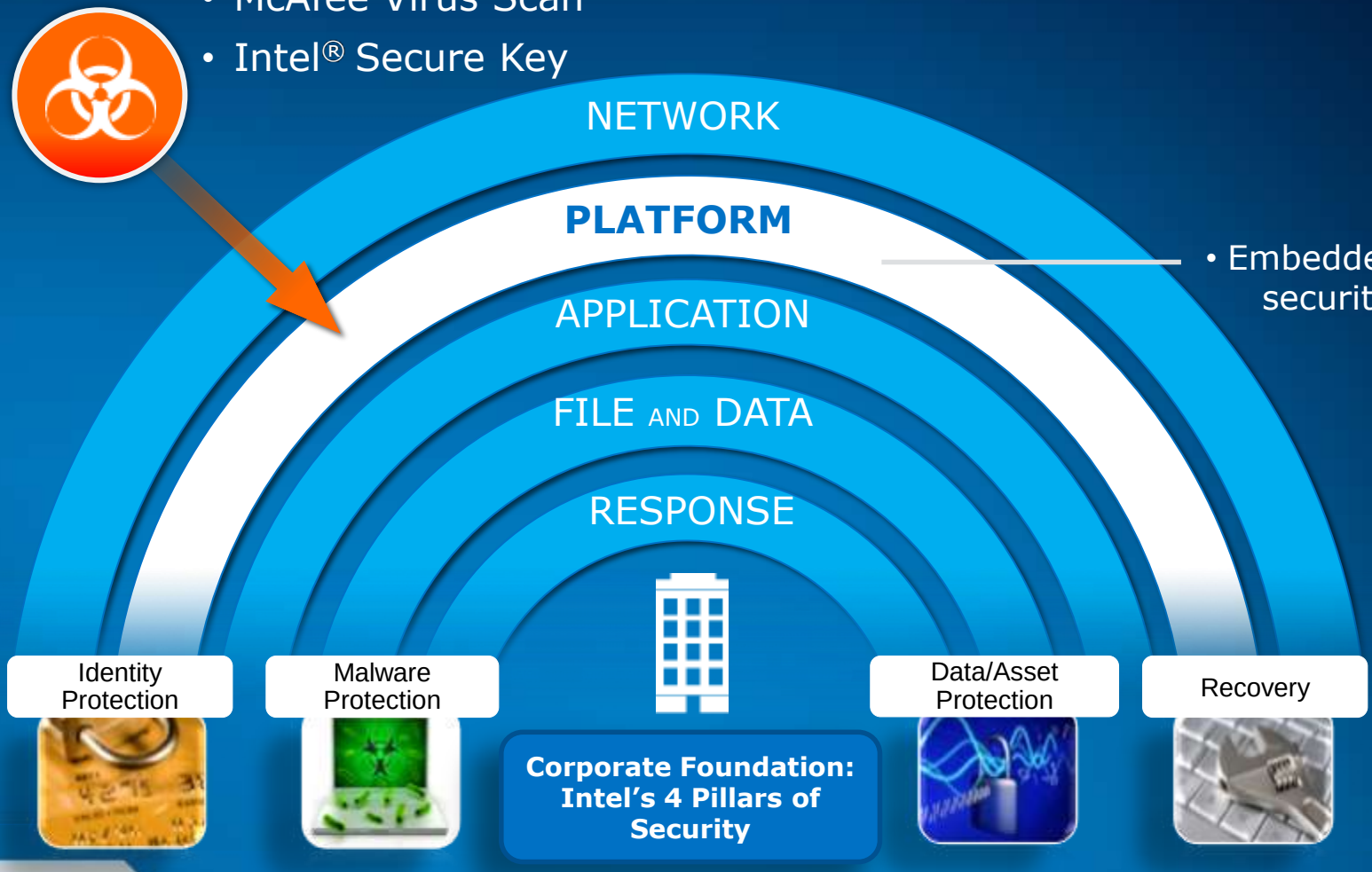
PAVP
protected window, not visible to SW

View seen by malware

Authenticates Real Users on Their Ultra Mobile Devices

Hardware-Enhanced Platform Security

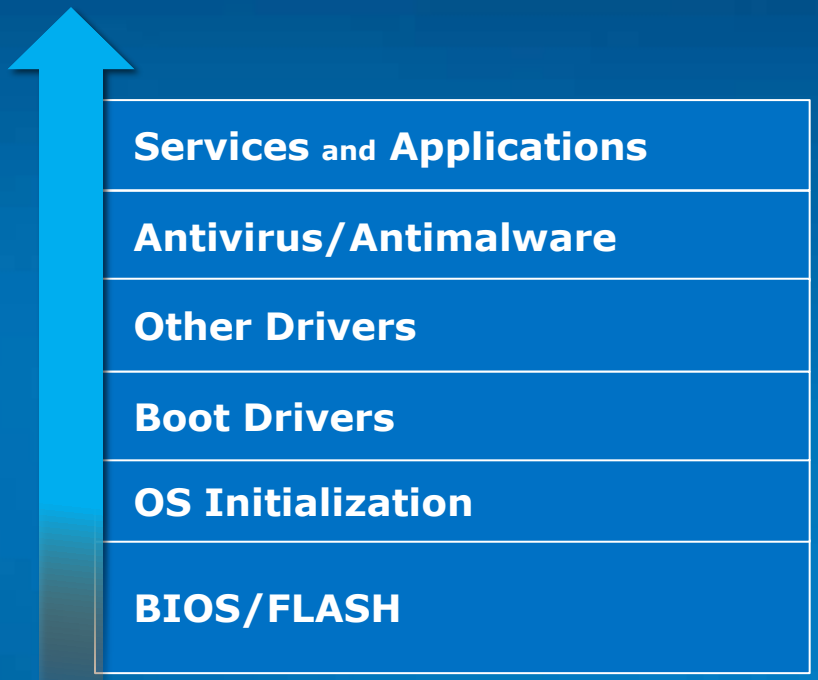
- McAfee DeepSAFE/Deep Defender*
- McAfee Virus Scan*
- Intel® Secure Key



- Embedded system security

Security Threat: Stealth Attacks
Kernel-Mode Rootkits/BIOS/Bootup Attacks

Boot Process



Stealth attacks insert themselves at any platform level

Below visibility of Antivirus/Antimalware

Persistent without detection

EXAMPLES

2011

- Mebromi

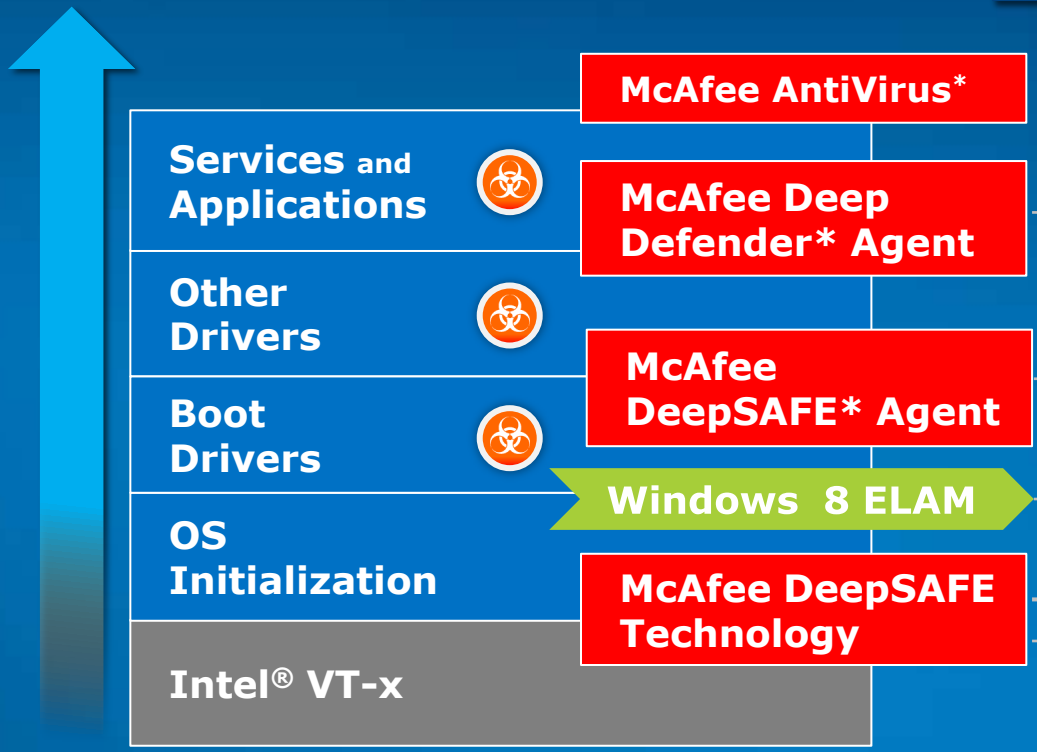
1997

- Chernobyl

McAfee DeepSAFE* Technology/Deep Defender*: Stopping Infection Before it Starts

McAfee DeepSAFE Technology
McAfee Deep Defender
Stopping Stealthy Malware

Next-generation "beyond the OS" security enabled by Intel® Virtualization Technology



Identifies/stops kernel-mode threats in real-time with out reboot

DeepSAFE technology loads first for security beyond the OS

W8 ELAM loads AV early to help detect malware sooner

Real-time kernel-level memory monitoring using Intel® VT-x hardware assistance

DeepSAFE loads first before OS

Security Threat: Token Theft/Key Guessing

PSEUDO RANDOM NUMBER GENERATOR

EXAMPLES

2010

- Sony Playstation 3* jailbreak
- Weak PRNG in PHP session leads to hijacking

2008

- Debian/OpenSSL Fiasco

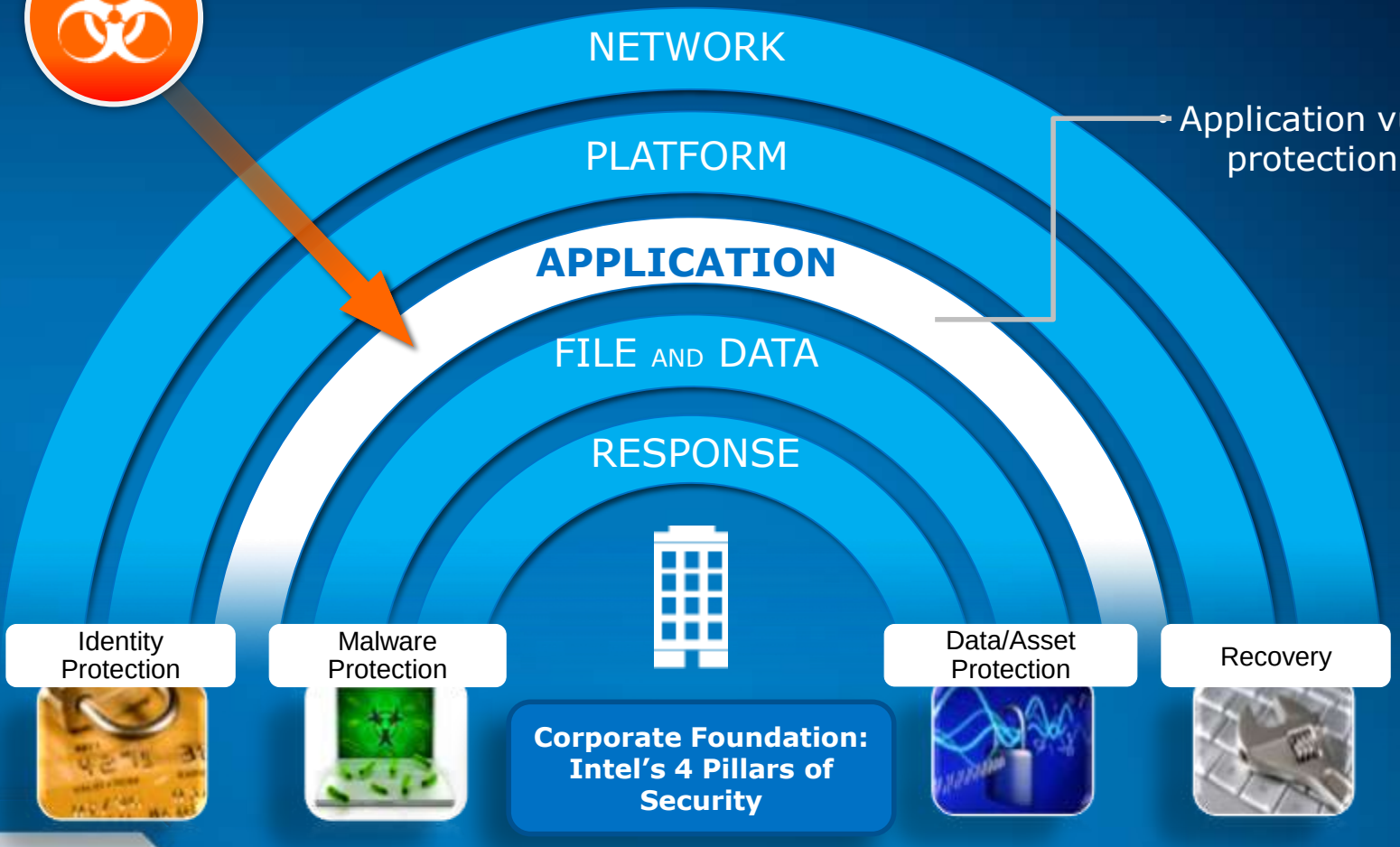
Intel® Secure Key: Strong Security from True Random Numbers[12]

- Entropy source delivers truly random, nondeterministic seed
- Delivers high quality, truly random numbers for key generation
- Extremely fast performance
- "Standards" compliant (NIST SP 800-90) and NIST FIPS 140-2 Level 2 certified
- Hardware implementation isolates Entropy Source from software attacks
- In 3rd generation Intel® Core™ processors

Ecosystem Vendors
- McAfee
- Microsoft
- Symantec
- RSA
- Open SSL and more

Hardware-Enhanced for Application Security

- McAfee Deep Defender*
- Intel® OS Guard



* Other names and brands may be claimed as the property of others.

Security Threat: Social Engineering
You can't resist what you are unaware of

"Mobile Pwn2Own*: iPhone* 4S hacked by Dutch team"

iPhone and iPad* both run iOS

- Exploit using web browser/ plugin vulnerabilities
- Irresistible links result in un-resistible attack
- Key vector for malware installation/ jailbreaking
- Over 3 million drive-by URLs discovered by Google in 2007[1]

AFFECTED DEVICES:

- Smartphones
- Tablets
- Notebooks
- Desktops

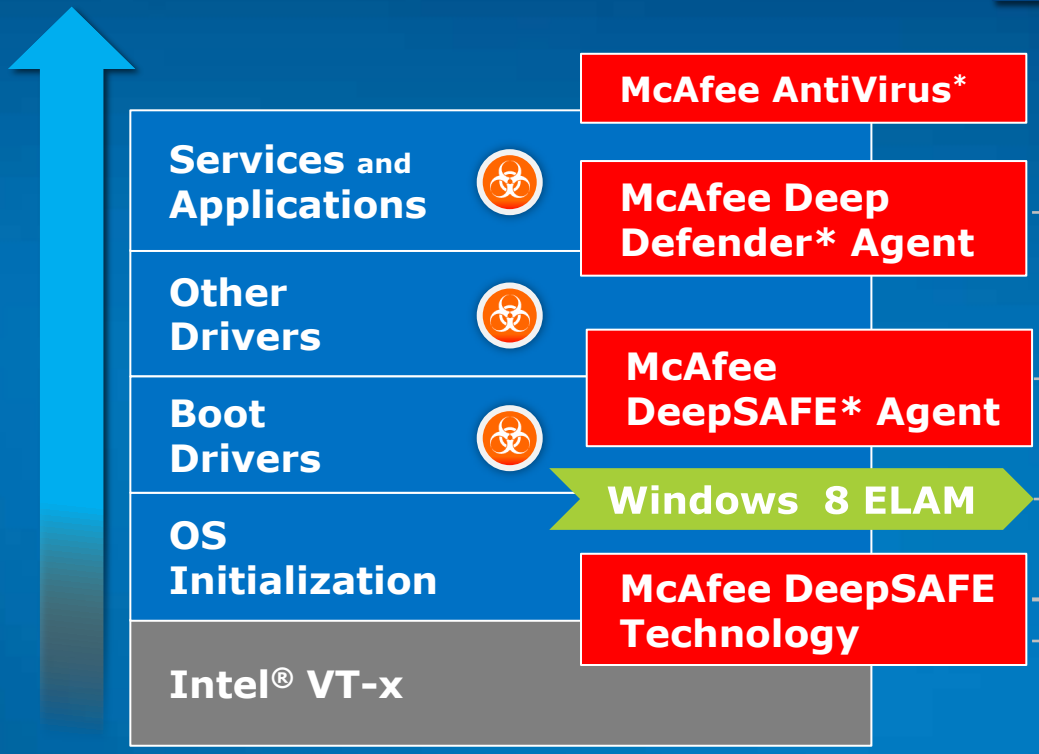
1. N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The Ghost In The Browser - Analysis of Web-based Malware." In Proceedings of HotBots 2007, Usenix, April 2007.

McAfee DeepSAFE* Technology/Deep Defender*: Stopping Infection Before it Starts

McAfee DeepSAFE Technology
McAfee Deep Defender*

Stopping Stealthy Malware

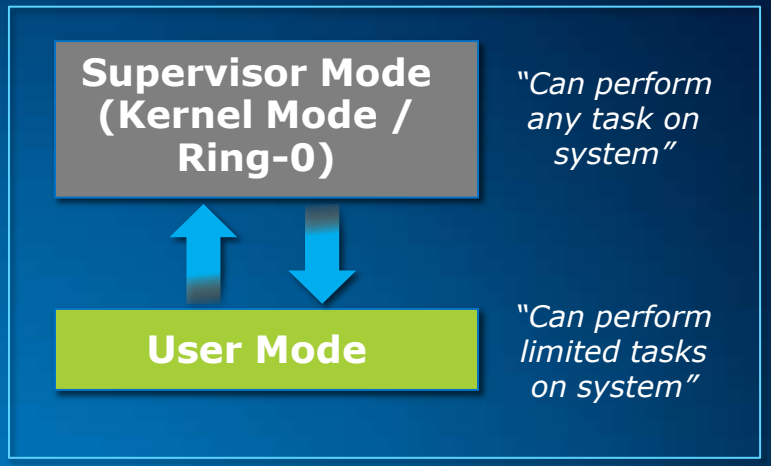
Next-generation "beyond the OS" security enabled by Intel® Virtualization Technology



- Identifies/stops kernel-mode threats in real-time with out reboot
- DeepSAFE technology loads first for security beyond the OS
- W8 ELAM loads AV early to help detect malware sooner
- Real-time kernel-level memory monitoring using Intel® VT-x hardware assistance
- DeepSAFE loads first before OS

Security Threat: OS EoP/Vulnerability Chaining Attacks

- How modern web browsers are being broken
- Up to 17 vulnerabilities chained
  - Attacker gains Ring-0 level execution privileges through vulnerability
  - System calls malicious code
- Sophisticated attacks; used by APTs



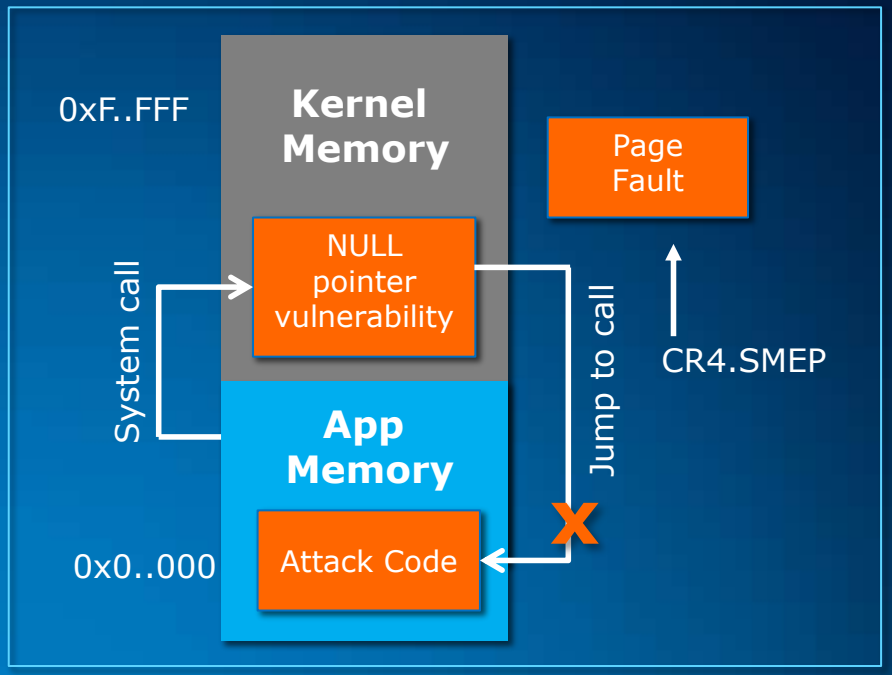
EXAMPLE

2010

- Stuxnet

Intel® OS Guard: Contain Code in User Space[6]

- Helps prevent user code executing in Ring 0
- Next-generation Intel® Execute Disable bit
- Used by Windows* 8
- In 3rd generation Intel® Core™ processors

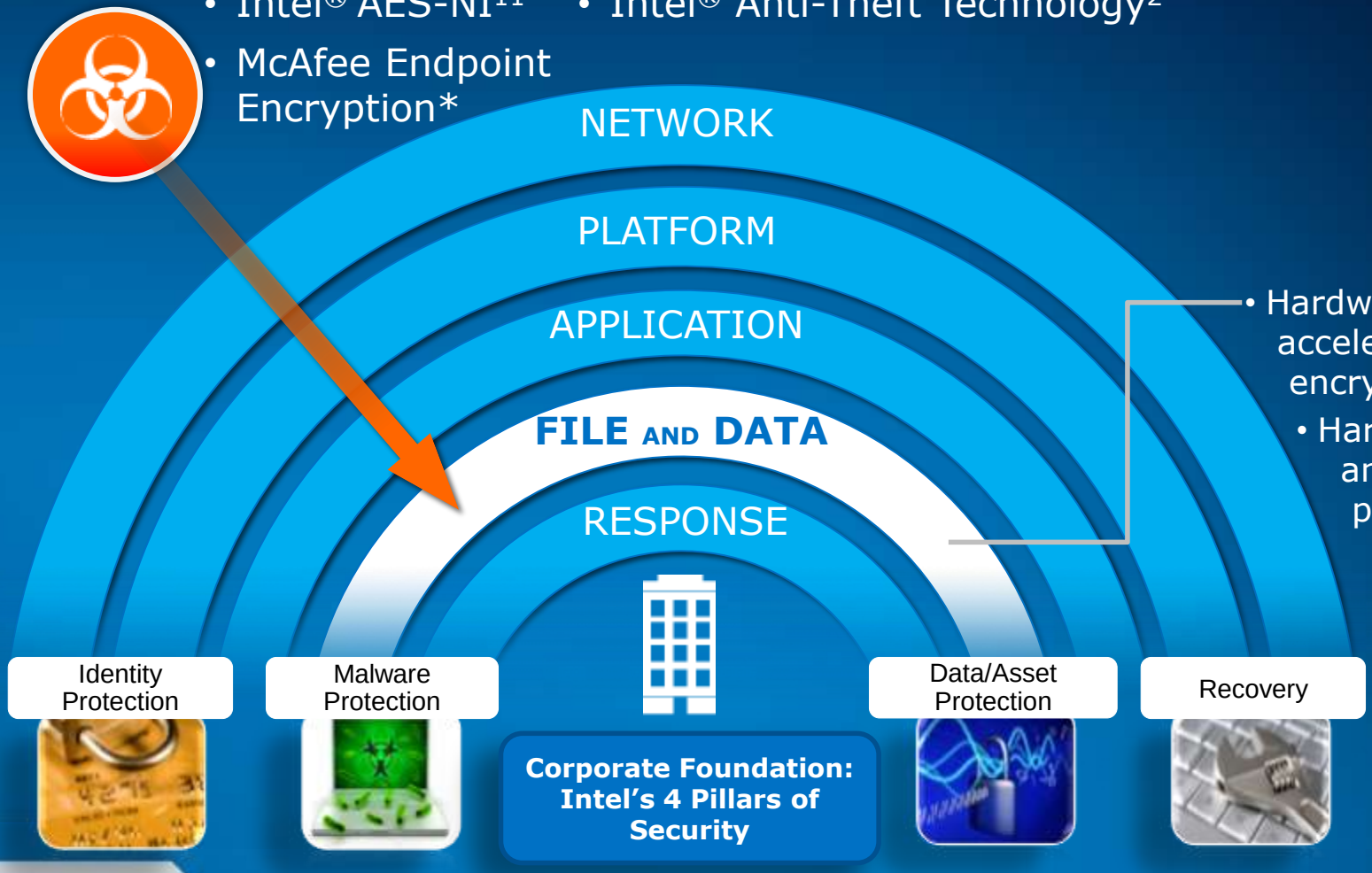


"PRIVILEGE ESCALATION ATTACK"

Application strengthening will continue to be a focus for future technologies

Hardware-Enhanced File and Data Security

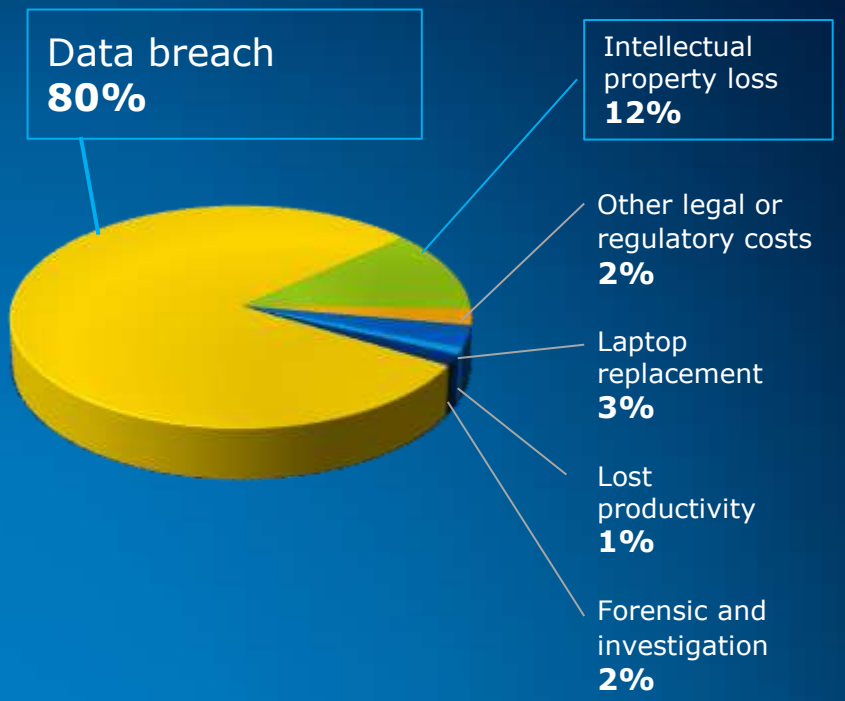
- Cost of Loss
- Intel® AES-NI[11]
- McAfee Endpoint Encryption*
- Intel® SSD Pro
- Intel® Anti-Theft Technology[2]



- Hardware-accelerated encryption
- Hardware-based anti-theft protection

Security Threat: Cost of Data and Asset Loss

- Every **49.3 seconds**, a laptop is lost or stolen in a U.S. airport
- 3 out of 4 lost laptops result in a **data breach**
- The average **cost** to a business of a missing laptop is **$49,246** due to loss of IP
- And of all lost laptops, **46% had confidential data** and no encryption+



Data breach and Intellectual property loss are two biggest costs of asset loss

+ Source: The Cost of a Lost Laptop, Ponemon Institute, 2009.

++ Source: The Cost of a Lost Laptop, Ponemon Institute, 2009.

Intel® AES-NI: Productivity & Security[11]

The Challenge: **Encryption slows productivity**

The Answer: **Intel® AES-NI accelerates encryption**

- Intel® AES-NI hardware accelerates encryption, enabling ubiquitous encryption and productivity
- McAfee Endpoint Encryption* uses Intel AES-NI for near native performance
- In select 2nd generation Intel® Core™ processors and 3rd generation Intel® Core™ processors

Intel AES-NI

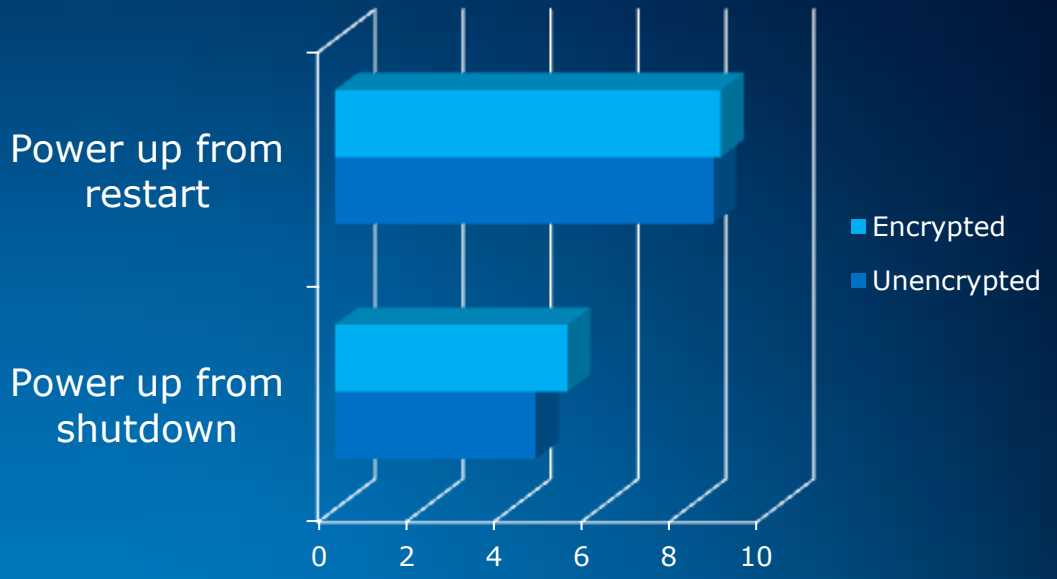
= Up to **4x** Faster Encryption[3]

Other Ecosystem Vendors

- Cisco
- Microsoft
- Symantec
- Check Point
- Winzip
- VMware View
- BitDefender and more

Intel® AES-NI[11] and McAfee EEPC*: Enabling Productive Users Without Sacrificing Security

- Accelerates Encryption Operations By Up To 3.5x
- Near native performance on SSDs using AES-NI technology (v7.0,Q4'12)
- Near-native performance for network and local file encryption (EEFF v4.1 Q4, 2012)



Accelerate Encryption Operations

Whole-Disk Encryption

File Storage Encryption

Intel® SSD Pro: Accelerated Whole-Disk Encryption

- Integrated full-disk encryption
- Hardware-based, on-disk acceleration
- Protects data at rest
- Remotely manageable
- Easy deployment using Intel® Setup & Configuration Software (SCS)

DATA SECURITY
WITH ENCRYPTION

- Self encryption drives with 256 bit AES Encryption Technology[1]
- Improve performance; reduces software license costs

DATA INTEGRITY
WITH END-TO-END DATA PROTECTION

- Protects data while in transit from host to SSE and back
- Improves reliability

DATA PROTECTION
WITH SECURE ERASE

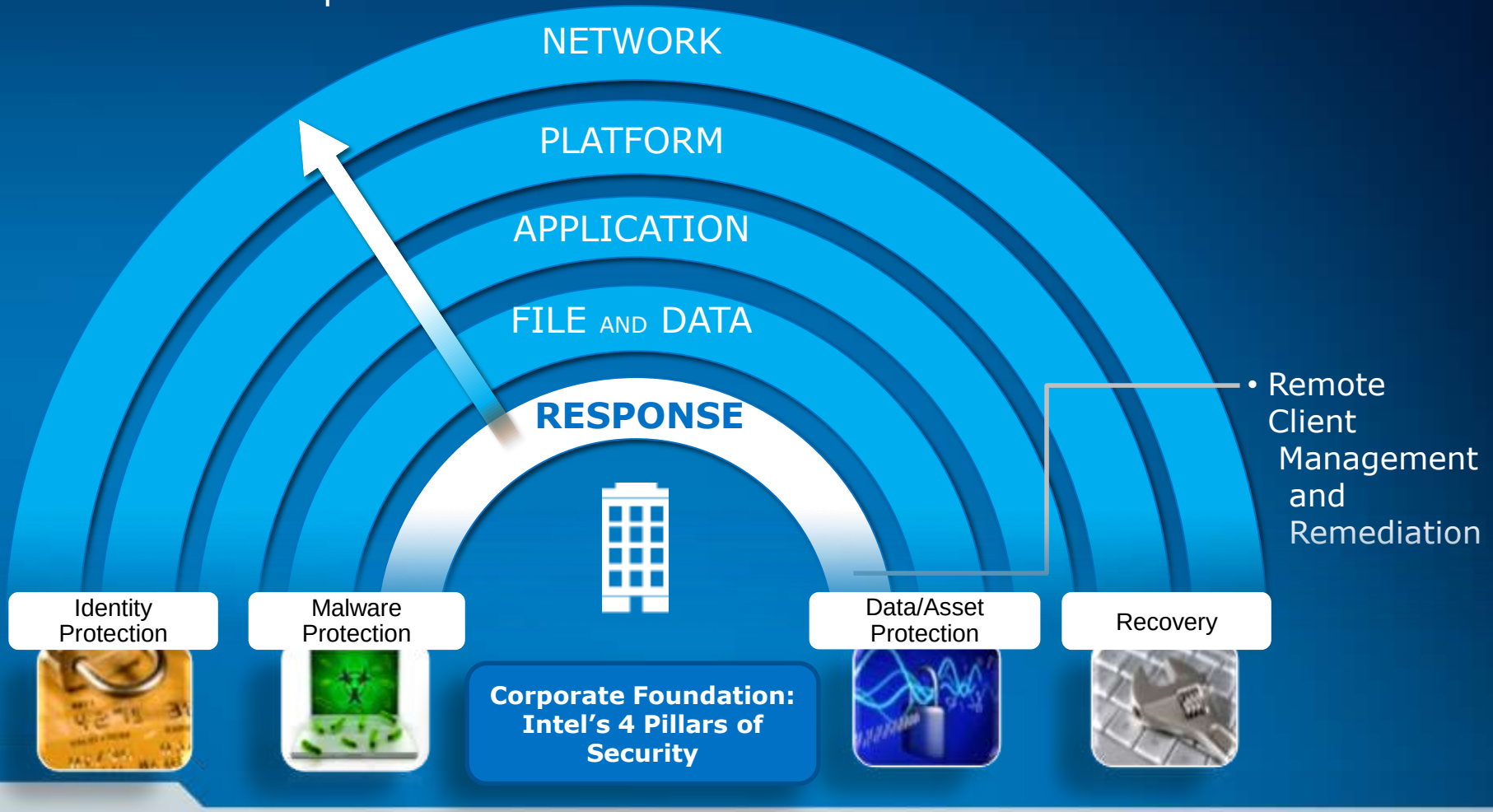
- Executes secure erase command for user data, SSD reserved data, and retired block areas
- Improves protection, reduce, re-use, or disposal costs

1. Not available on 60 GB and 120 GB SKUs

Response & Recovery

Intel® vPro™ Security: IT Tablet Support Without Compromise

- Intel® AMT with Remote Encryption Management
- McAfee ePO Deep Command*



IT Challenge: Proliferation of New Device Types Increases Security Management Complexity and Risk

Ultra Mobile Devices Without Compromise: Enterprise-ready Security and Manageability

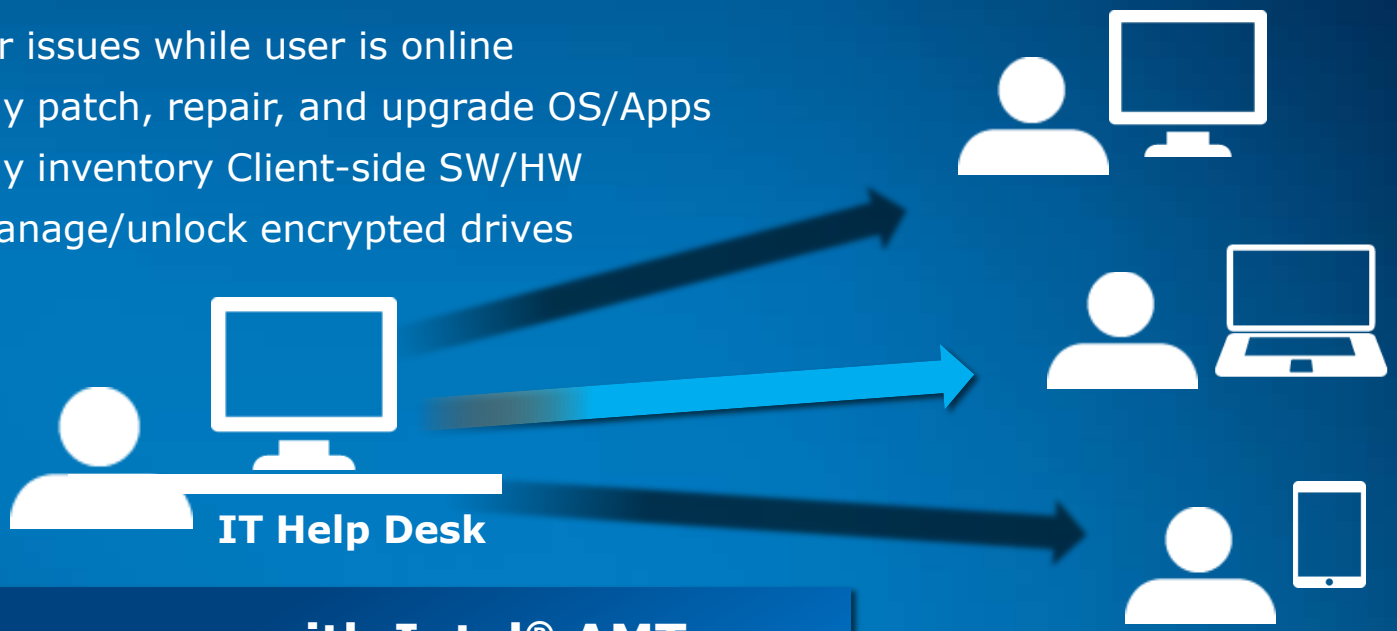
- **Intel® vPro™ Technology-based Enterprise Ultra Mobile devices Enable[9]**
  - Fine-grained Security, Manageability, and Visibility
  - Remote, Secure, OOB Access
  - Remote Repair
  - Remote Security Management
- **Windows* 8 on Desktop and Touch Devices**
  - Traditional and App Store Application Delivery
  - Windows 8 Security Features + Hardware-assistance
- **Unified Windows-based Security Management**
  - McAfee ePolicy Orchestrator*
  - Proven, Scalable Architecture
  - Lower Cost and Optimized Security

Intel® AMT: Enabling Comprehensive Fine-Grained Security and Manageability[4]

Save Time, Stay Compliant and Secure with Fewer Deskside Visits

Remotely Access Clients Through Secure Channel

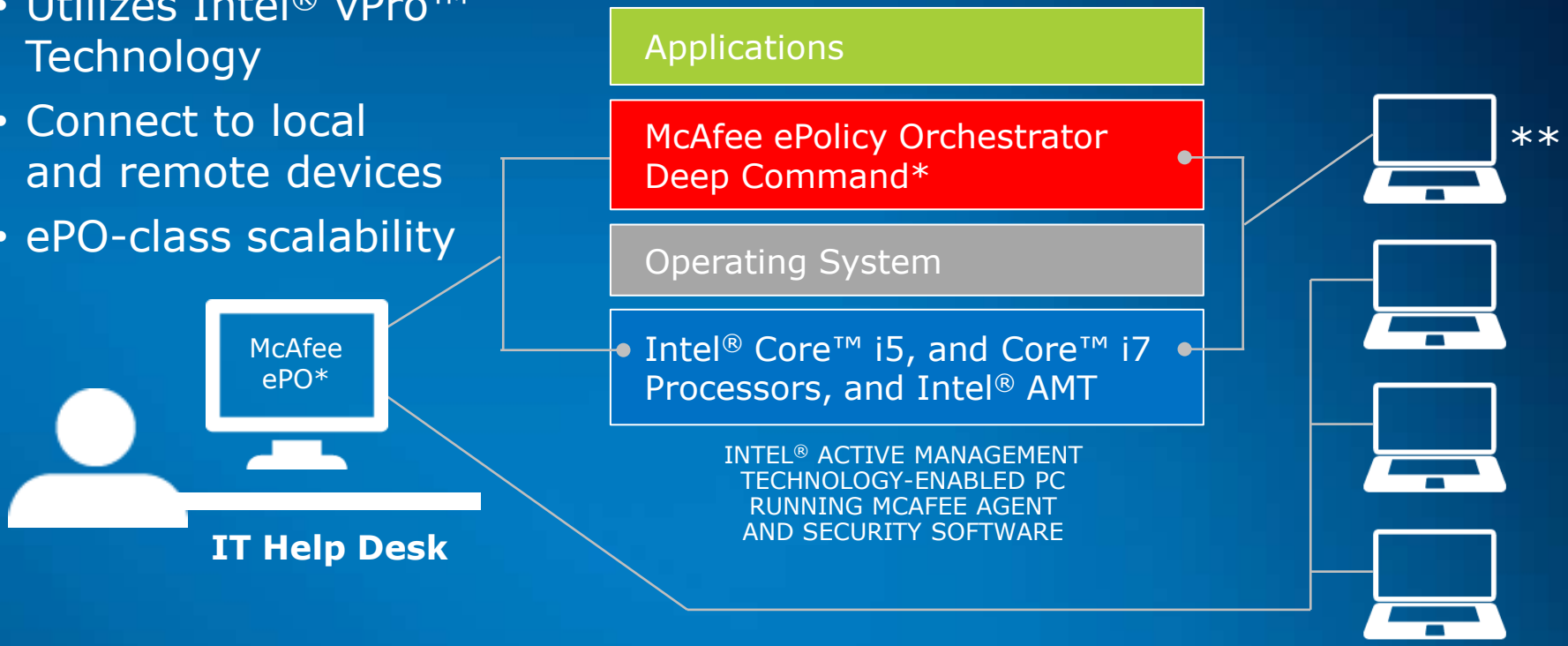
- Irrespective of Power or OS state
- Address user issues while user is online
- Automatically patch, repair, and upgrade OS/Apps
- Automatically inventory Client-side SW/HW
- Remotely manage/unlock encrypted drives



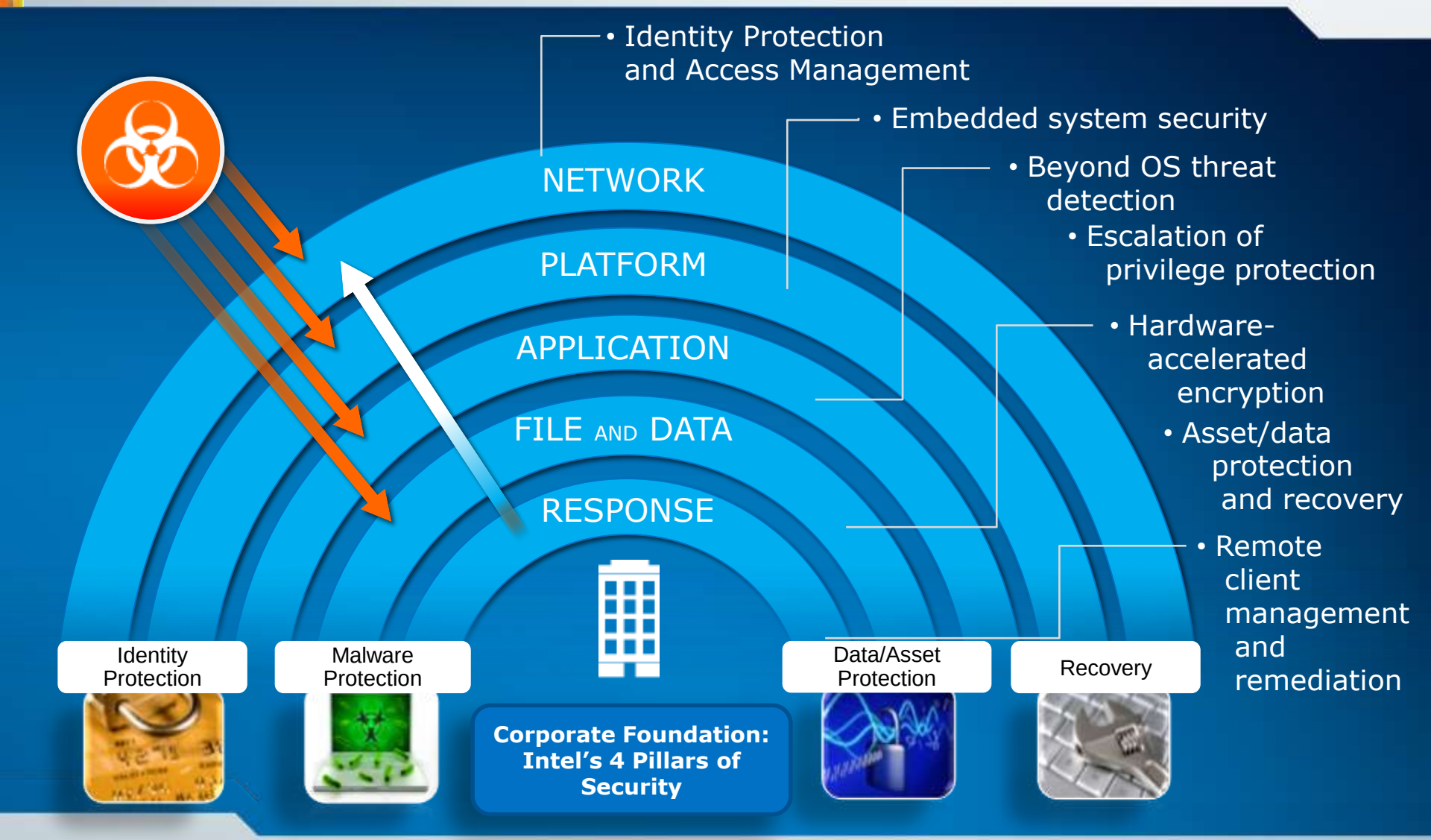
Remote recovery with Intel® AMT

McAfee ePO Deep Command*: Comprehensive Security Management

- Reduce cost of security operations
- Improve security to powered-off PCs
- Maintain security access while lowering energy use
- Utilizes Intel® vPro™ Technology
- Connect to local and remote devices
- ePO-class scalability



Intel® Technologies: Hardware-Enhanced Security at Every Level



References/Where to Go for More Information

- Security in Computing Strategy
  - Includes Intel® OS Guard[6], DRNG, Granite City
- Intel® Identity Protection Technology[7]
  - http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/granular-trust-model-improves-enterprise-security.html
- McAfee DeepSAFE* Platform
- McAfee Deep Defender*
- McAfee ePO Deep Command*
- McAfee Endpoint Encryption*
- Cloudbuilder
- NTG Security & Manageability

Thank you