Intel® Cyber-Security Briefing:

Trends, Solutions, and Opportunities

John Skinner, Director, Secure Enterprise and Cloud, Intel Americas, Inc.

May 2012

Agenda

- Intel + McAfee: What it means
- Computing trends and security implications
- A new approach to improve cyber-security:
  - ***Hardware-enhanced Security***
- Examples of Hardware-assisted Security
- Opportunity for the *IT Community* to

  Change The Game

Innovation Opportunities by working with Intel and McAfee

- **Change the way we all think** about security problems and solutions
- **Innovate and Deliver** new levels of protection not available with software-only solutions, employing **hardware-enhanced security**
- **Deliver intelligence-in-depth:** Security that is integral to your hardware, network, systems, applications, and databases—and works together to protect your business

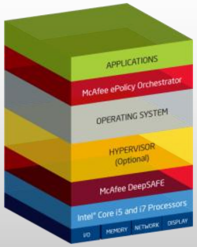
Key Innovation Areas

Next-Gen Endpoint Security

Secure Mobile Devices

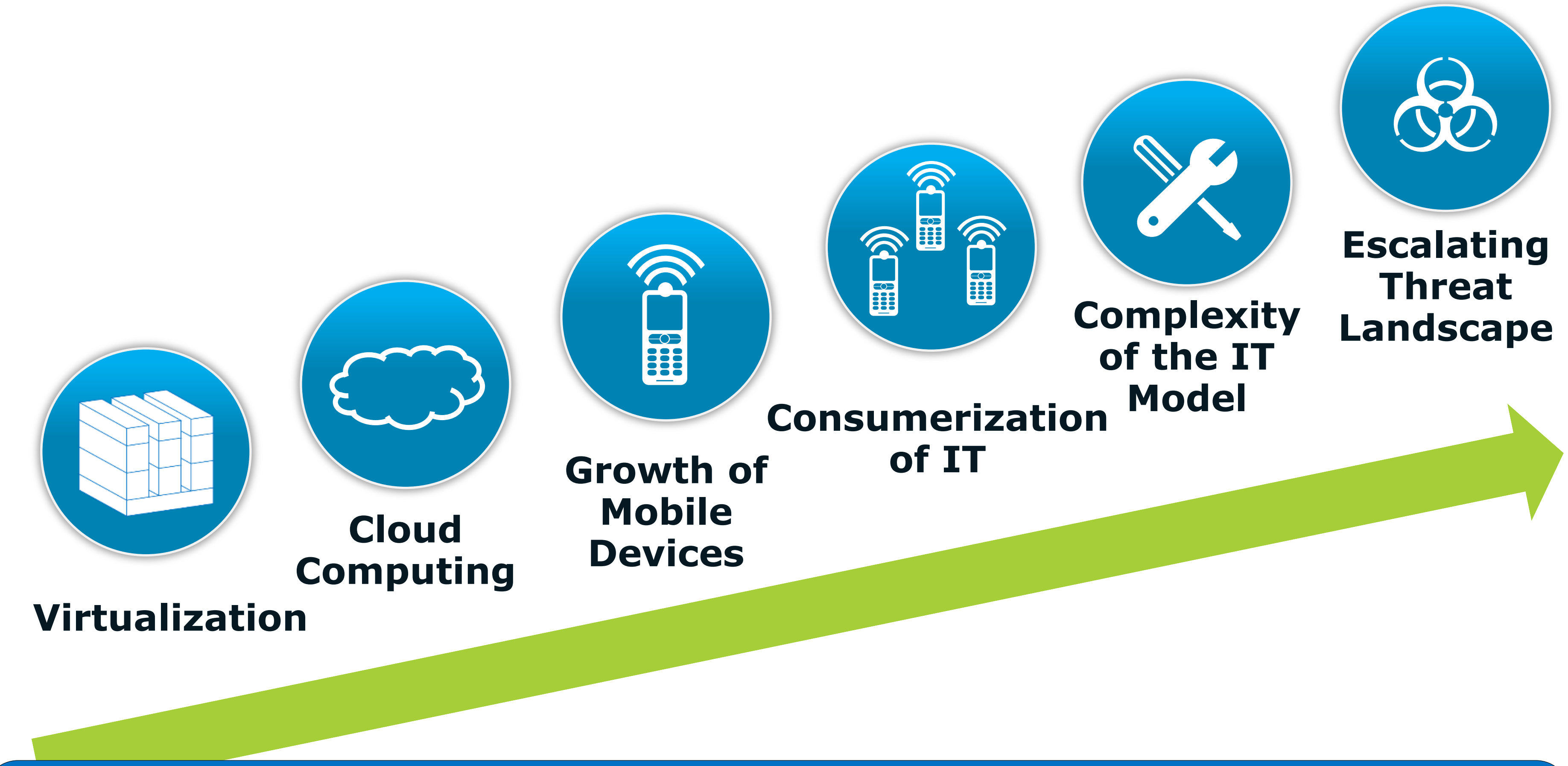
Secure Embedded Devices

Cloud Security Platform



Hardware Enhanced Security

Computing Trends and Security Implications



Virtualization

Cloud Computing

Growth of Mobile Devices

Consumerization of IT

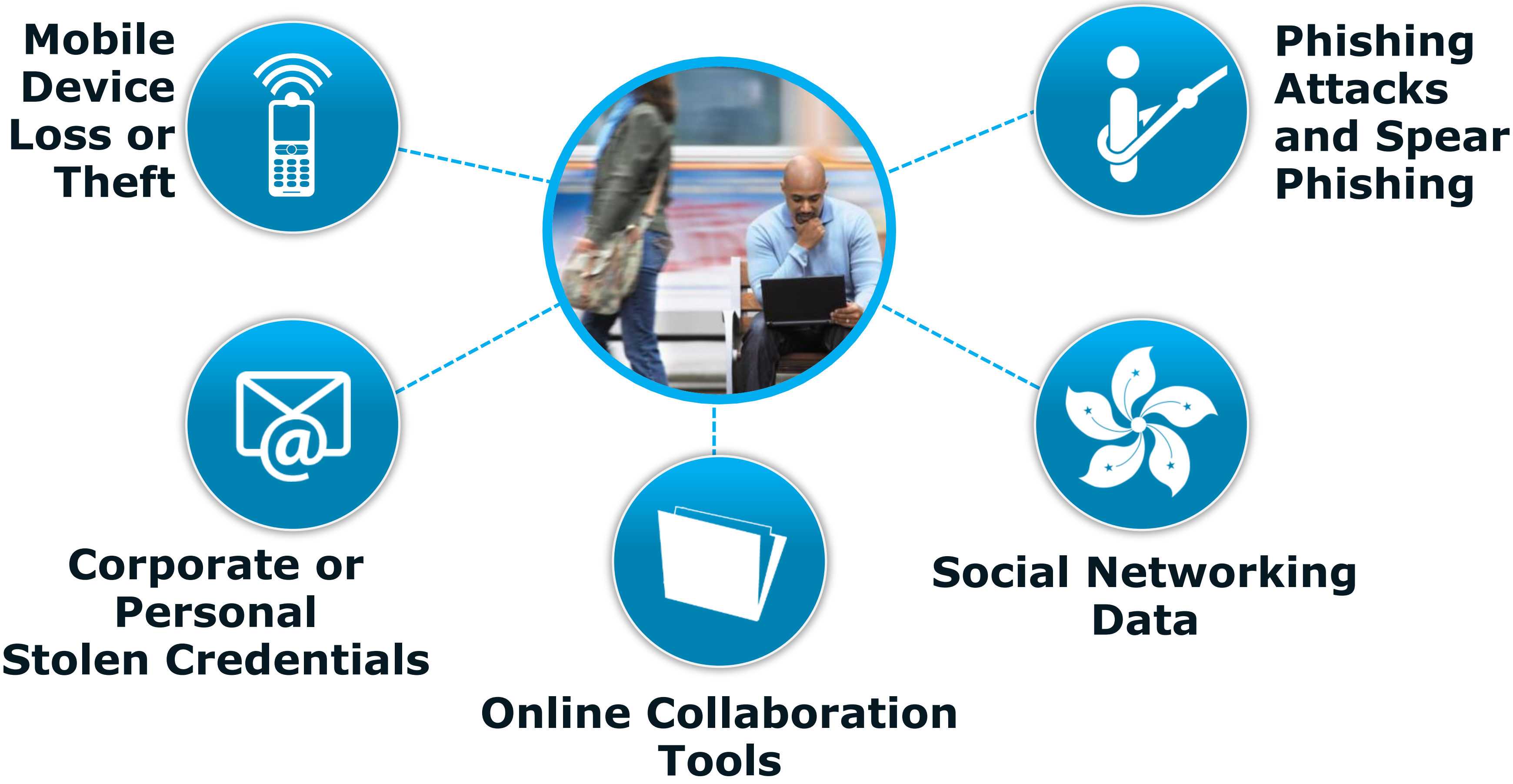
Complexity of the IT Model

Escalating Threat Landscape

As a consequence: The size of the "Attack Surface" and the opportunities for Malicious Entry have expanded.

People: The New Network Perimeter

Human Vulnerabilities and Risks



Mobile Device Loss or Theft

Phishing Attacks and Spear Phishing

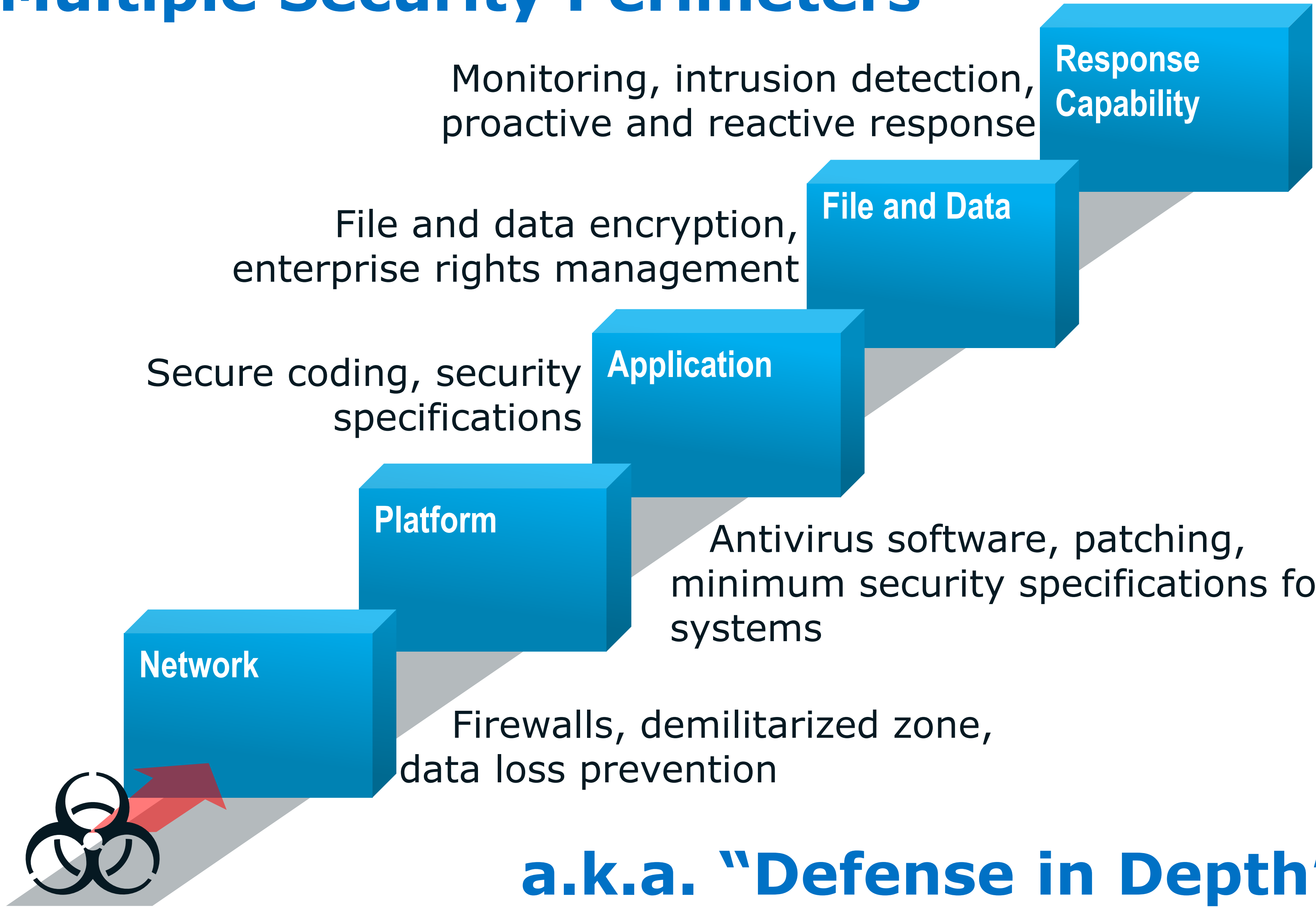
Corporate or Personal Stolen Credentials

Online Collaboration Tools

Social Networking Data

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

Traditional IT Security Strategy: Multiple Security Perimeters



Response Capability

Monitoring, intrusion detection, proactive and reactive response

File and Data

File and data encryption, enterprise rights management

Application

Secure coding, security specifications

Platform

Antivirus software, patching, minimum security specifications for systems

Network

Firewalls, demilitarized zone, data loss prevention

a.k.a. “Defense in Depth”

A closer look at Hacking:
The *Motivations* Have Expanded….

SLAMMER

ZEUS

AURORA

STUXNET

Hacking for Fun

Organized Crime

State-Sponsored Cyber Espionage

Physical Harm

Hacking Software Tools for Sale:
$11B/year industry with 56% CAGR

“The Malware Tsunami”

There were more malware attacks in 2010-2011 than in the previous 10 years combined!

60,000+ per day
new unique malware pieces

6,000,000 per month
new botnet infections

2,000,000 per month
new malicious web sites

Stealth Attacks
Non-detectable malware and advanced persistent threats

Tools of the Modern Hacker

Candy Drop:

Placing infected USB drives where humans will take them, and later plug them into their PC or other network-connected device.

Social Engineering:

Manipulating people to divulge data or “click here”

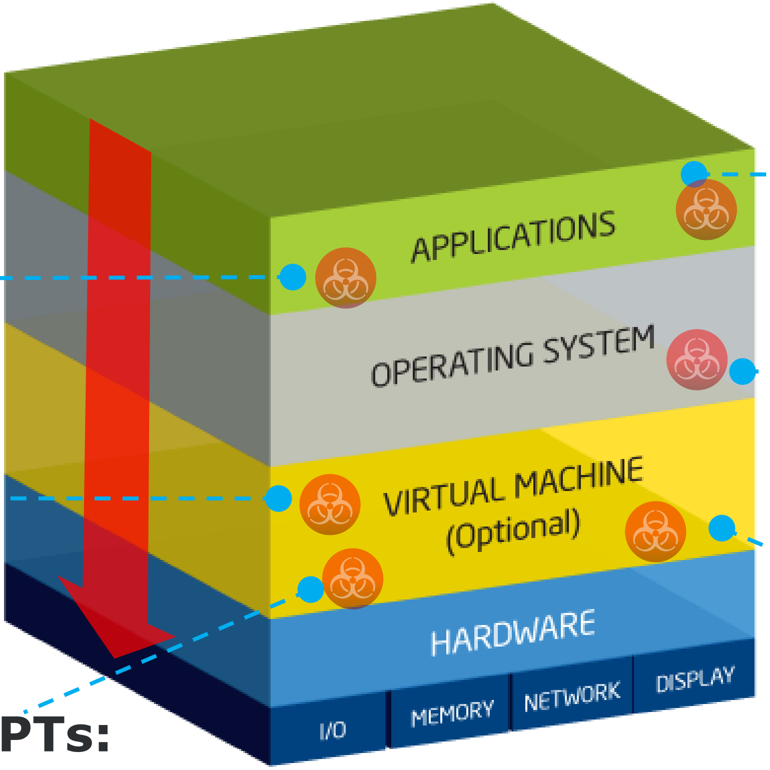
Advanced Persistent Threat (APT):

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, APT’s.

Attacks Are Moving "Down the Stack", to Gain Greater Stealth and System Control



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

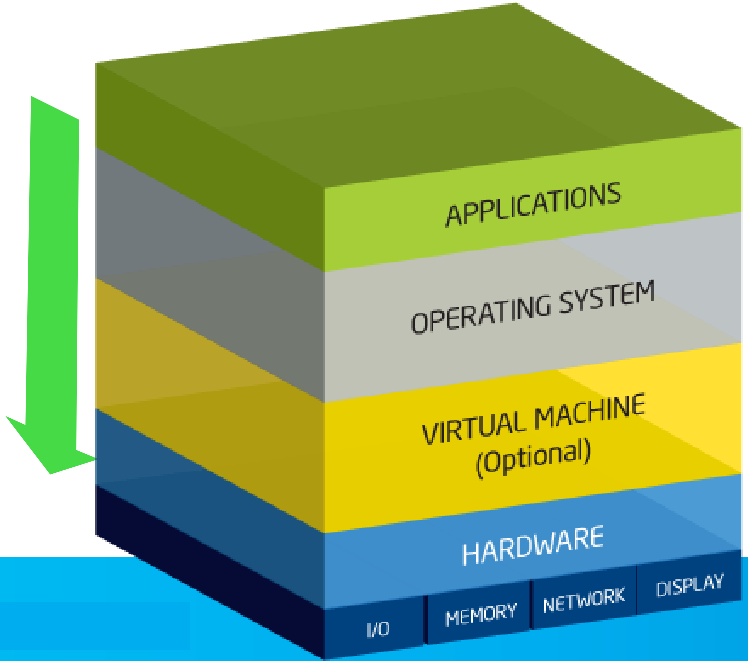
OS infected with APTs: Threats are hidden from security products

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

APT: Advanced Persistent Threat

A New Approach Is Required: "Hardware-enhanced Security"

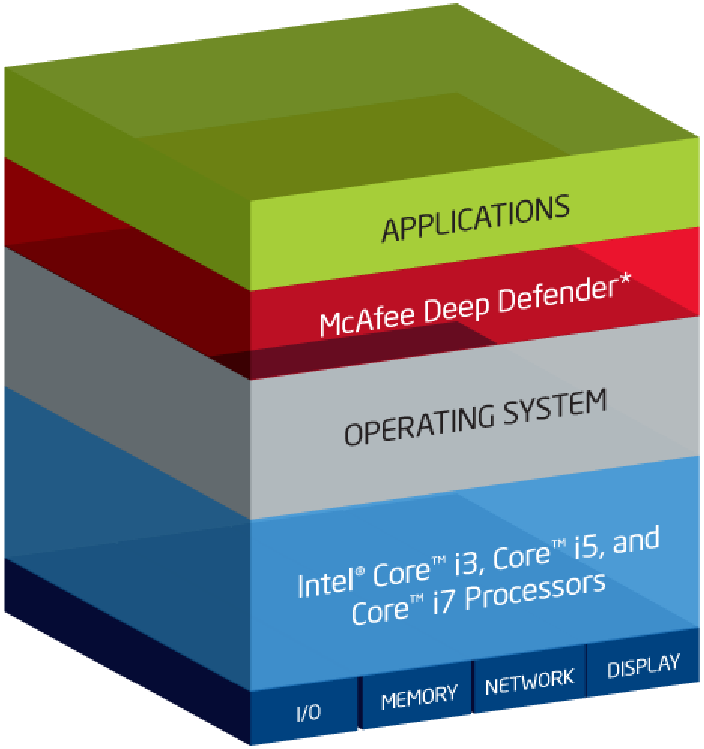
- **Move critical security processes *down into the hardware***
  - Encryption, Authentication, Manageability, and Platform Cleansing
  - Hardware is inherently less vulnerable to modification or corruption
- Establish **a security perimeter from the hardware layer up**
- **Isolate** the security services from the host OS (often the target)
- Build in capability to **monitor, maintain, repair, and recover**



Added Protection against:

- Viruses and worms
- Malware
- Disabled software
- ***Rootkits***

Example of Hardware-enhanced Security: The DeepSAFE* Security Platform



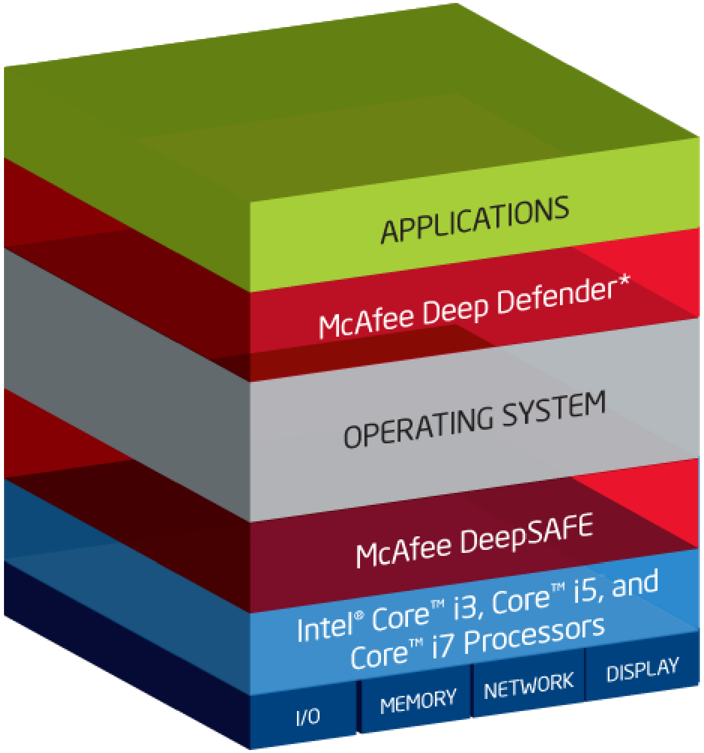
DeepSAFE is the first hardware-assisted security platform from Intel and McAfee. Platform capabilities include:

- McAfee Deep Defender* product
  - Utilizes the isolation capabilities of Intel Virtualization Technology
  - Works "beyond" the OS, so it can't be corrupted by OS or malware
  - Detects, blocks, and removes stealthy advanced persistent threats and malware
- Foundation for future solutions from McAfee and Intel

Next-generation "beyond the OS" security enabled by Intel® processor technology

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

Example of Hardware-enhanced Security: The DeepSAFE* Security Platform

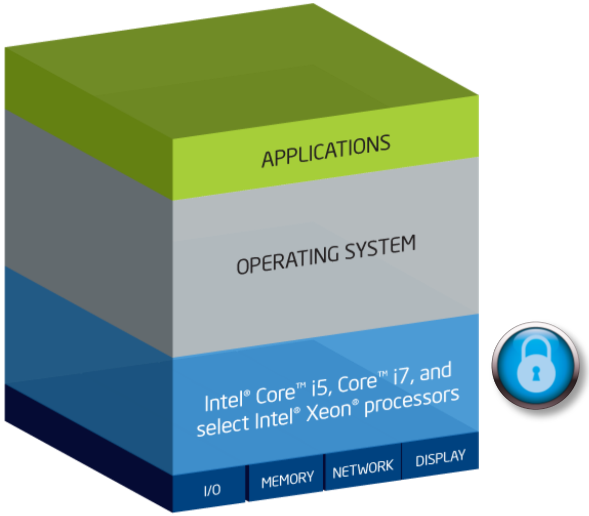


DeepSAFE is the first hardware-assisted security platform from Intel and McAfee. Platform capabilities include:

- McAfee Deep Defender* product
  - Utilizes the isolation capabilities of Intel Virtualization Technology
  - Works “beyond” the OS, so it can’t be corrupted by OS or malware
  - Detects, blocks, and removes stealthy advanced persistent threats and malware
- Foundation for future solutions from McAfee and Intel

Next-generation “beyond the OS” security enabled by Intel® processor technology

Hardware-enhanced Security: Faster Encryption on PCs and Servers


APPLICATIONS
OPERATING SYSTEM
Intel® Core™ i5, Core™ i7, and select Intel® Xeon® processors
I/O
MEMORY
NETWORK
DISPLAY

Intel® Core™ i5, Core™ i7, and
select Intel® Xeon® processors, with
Intel® Advanced Encryption Standard
New Instructions (Intel® AES-NI)

> *"There's a definite benefit to…*
> *Intel® AES-NI instructions… this is huge*
> *for corporate desktops/notebooks."*
>
> —Anandtech[1]

Whole-disk Encryption

Internet Security

File Storage Encryption

Intel® AES-NI increases encryption operations up to 4x by using hardware and software together.[2]

[1] The Clarkdale Review: Intel® Core™ i5 processor 661, Core™ i3 processor 540, and Core i3 processor 530, Anand Lal Shimpi, Anandtech, January 2010. http://www.anandtech.com/show/2901/5 .

[2] Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) requires a computer system with an Intel AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. See full disclaimer at http://www.intel.com/performance

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

Example of Hardware-enhanced Security: Intel® Identity Protection Technology

Now built into
your PC with Intel® IPT

Traditional hardware token

PC with Intel® IPT embedded tokens

1. **Utilize PCs with Intel® IPT support**

2. **Choose a security software vendor[1]**

   Used for remote authorized users (VPN) and/or for the public web

End Users

Add security that is easy to use

Web Sites

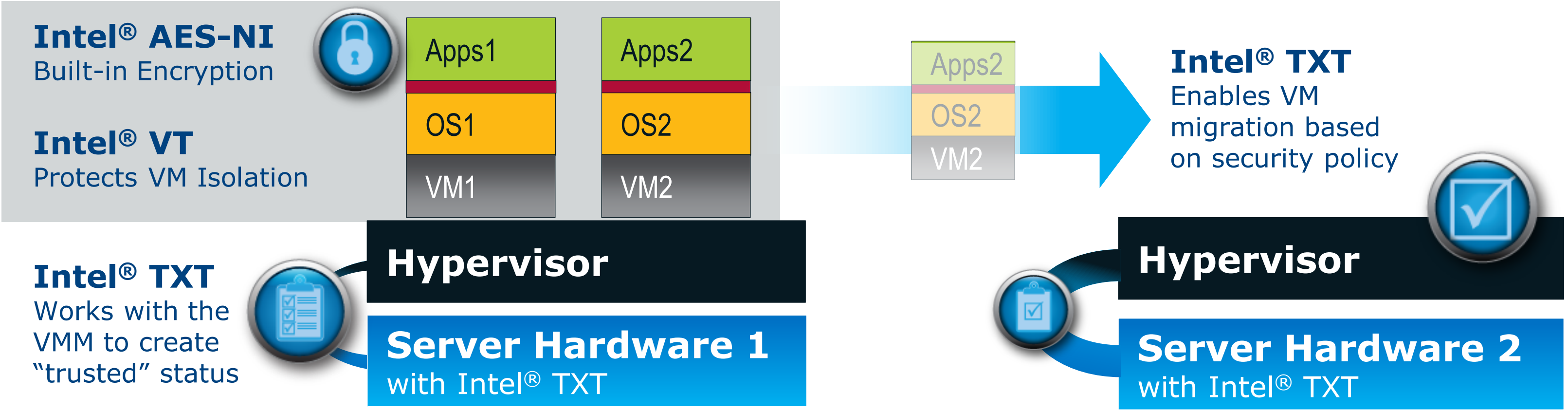
Protect user accounts and limit losses

Organizations

Secure method for authorized users to remotely log in

[1] Embedded tokens work with all Symantec VIP protected web sites as well as enabled VASCO protected sites.

Example of Hardware-enhanced Security for Virtualized Servers and Clouds



Intel® AES-NI
Built-in Encryption

Intel® VT
Protects VM Isolation

Intel® TXT
Works with the VMM to create "trusted" status

Intel® TXT
Enables VM migration based on security policy

Encrypt

Intel® AES-NI
delivers built-in encryption acceleration for better data protection

Isolate

Intel® VT and Intel® TXT
protects VM isolation and provides a more secure platform

Comply

Intel® TXT
establishes "trusted" status to enable migration based on security policy

Establishing the foundation for more secure data centers

Intel® AES-NI – Intel® Advanced Encryption Standard New Instructions; **Intel® TXT** – Intel® Trusted Execution Technology; **Intel® VT** – Intel® Virtualization Technology

Hardware-enhanced Security: Other Applications

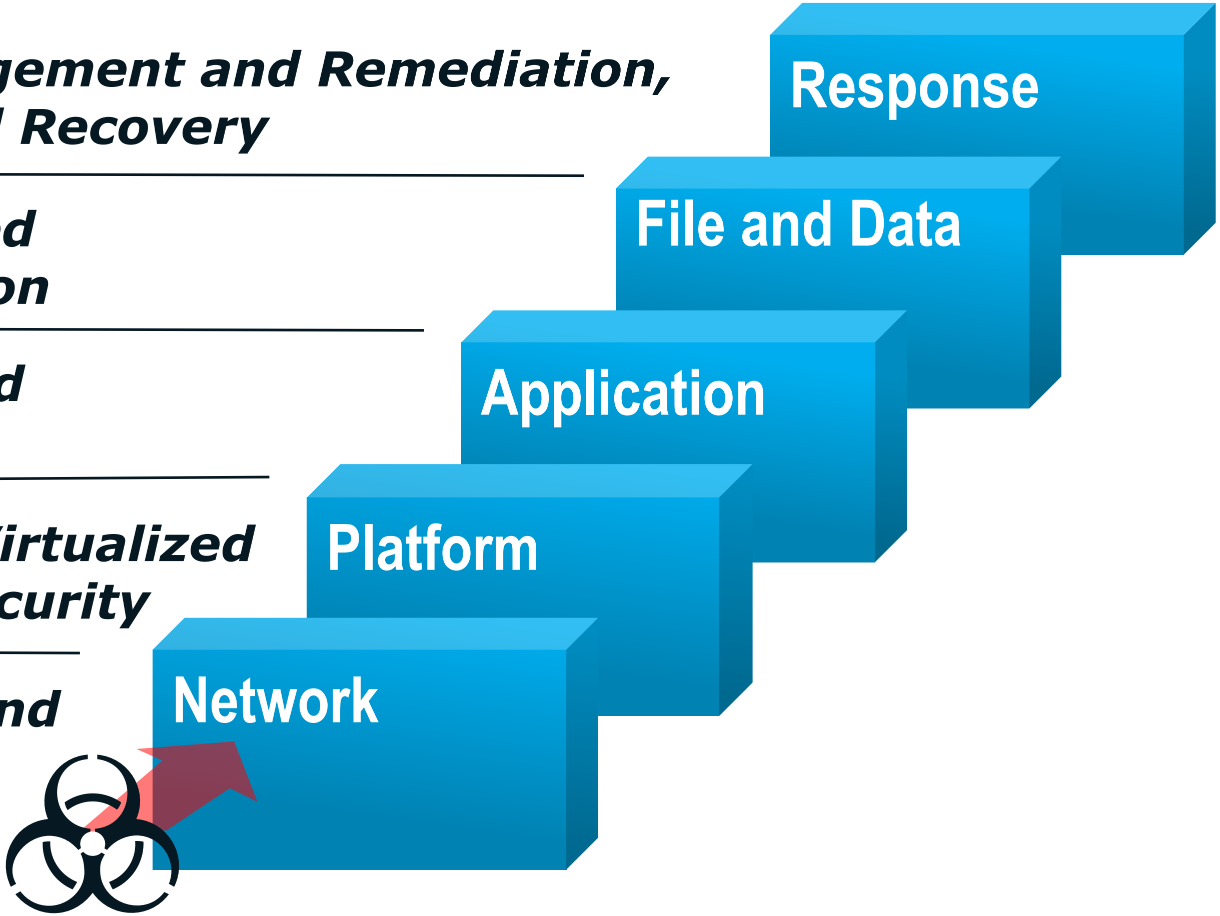
Remote Client Management and Remediation, Client Anti-Theft and Recovery

Hardware-accelerated Whole-Disk Encryption

Hardware-accelerated Data Encryption

Embedded System, Virtualized Server, and Cloud Security

Identity Protection and Access Management



Intel and its partners are applying Hardware-enhanced Security to “harden” each perimeter of defense.

Defense-in-Depth enhanced by Hardware-assisted Security

Intel® vPro™ Technology

McAfee® DEEP COMMAND

intel® ANTI-THEFT TECHNOLOGY

Intel® AES-NI
Intel® AES New Instructions

McAfee EEPC

Intel® AES-NI
Intel® AES New Instructions

McAfee EEPC

Intel® VT

Intel® vPro™ Technology

McAfee® DEEP DEFENDER

McAfee® DEEP COMMAND

Intel® TXT
Intel® Trusted Execution Technology

Intel® IPT
Intel® Protection Technology

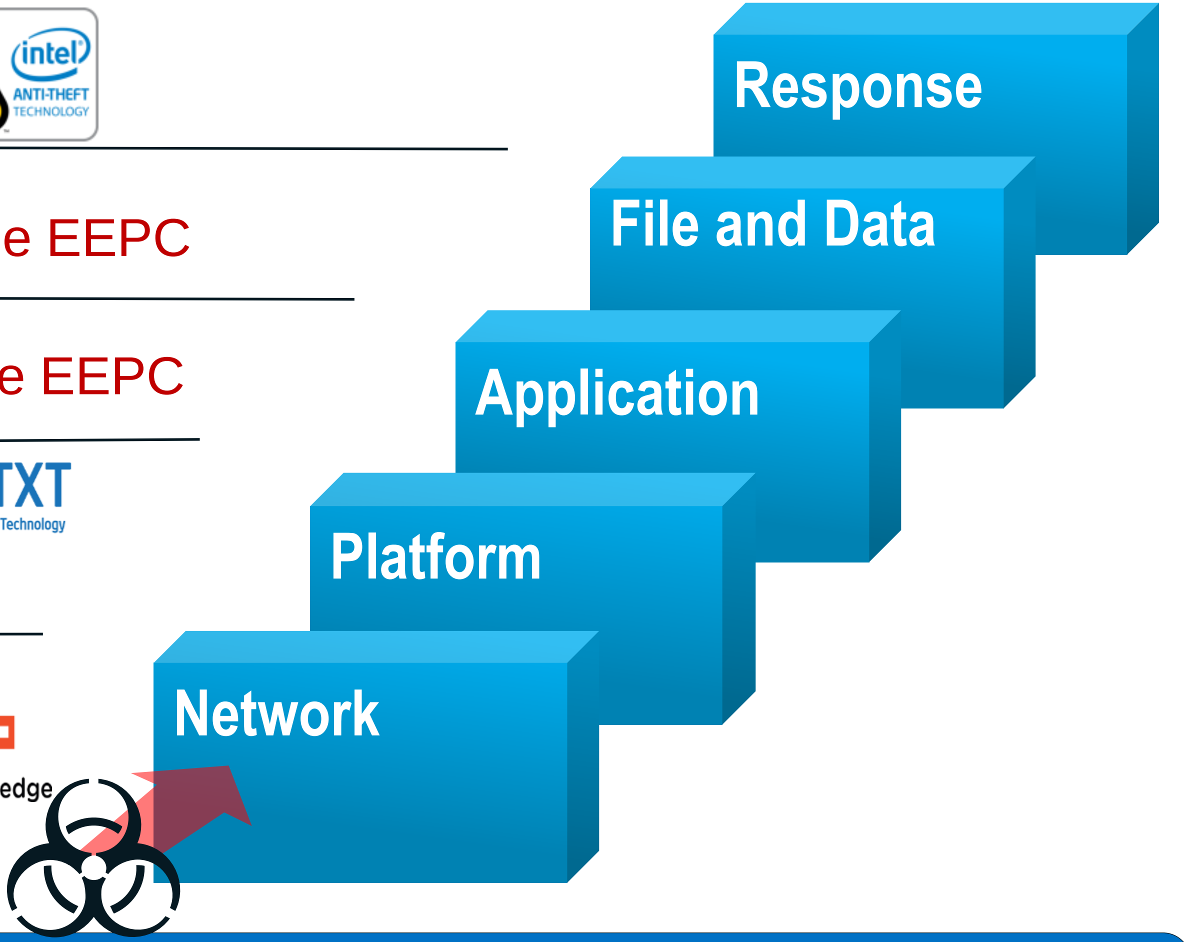
Intel® Expressway Cloud Access 360

Intel® Expressway Service Gateway

OTC

Log In

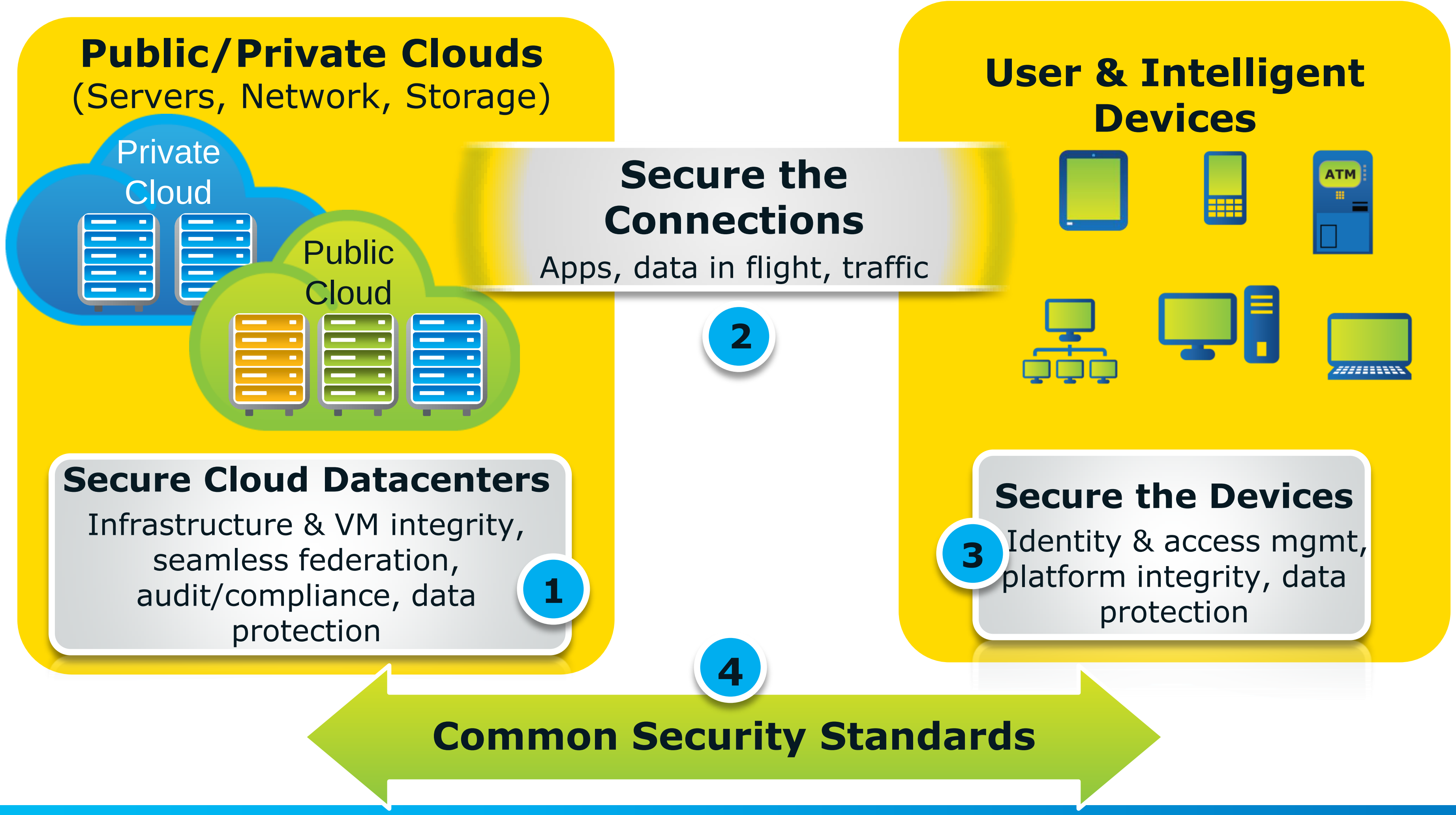
nordic edge



Intel and its partners are applying Hardware-enhanced Security to “harden” each perimeter of defense.

Enhancing End to End Cloud Security

Build Foundation of Integrity: From Client to Network to Cloud



Public/Private Clouds
(Servers, Network, Storage)

User & Intelligent Devices

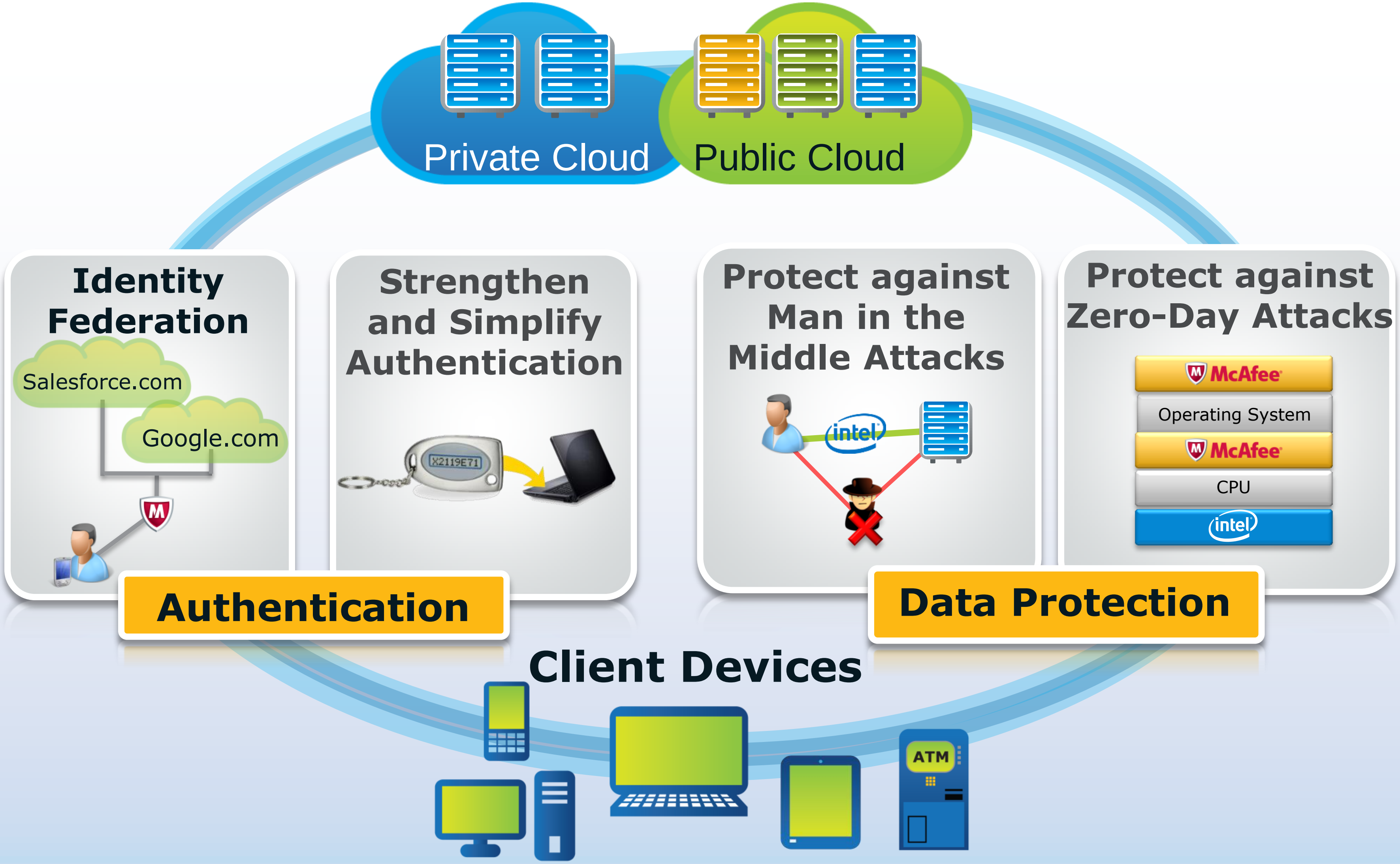
2 **Secure the Connections**
Apps, data in flight, traffic

1 **Secure Cloud Datacenters**
Infrastructure & VM integrity, seamless federation, audit/compliance, data protection

3 **Secure the Devices**
Identity & access mgmt, platform integrity, data protection

4 **Common Security Standards**

Example of How Hardware-enhanced PC Security can enhance Cloud Security

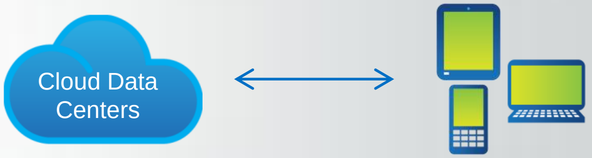


Enhancing End to End Cloud Security

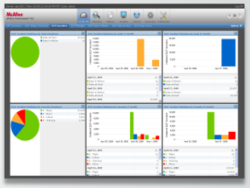
intel McAfee

Intel + McAfee: Toward Worry-Free Cloud Computing

Deliver hardware-enhanced security to better protect data, users, & traffic from client to cloud



Tools to aggregate security information across clouds to automate & simplify policy setting & improve audit/compliance reporting



nitrosecurity

New capabilities to automate client to cloud security and service levels, such as identity as a service

Intel® Cloud SSO

salesforce platform

Industry collaboration to accelerate broad adoption of security standards so IT can easily adopt cloud

OPEN DATA CENTER ALLIANCE

NIST National Institute of Standards and Technology U.S. Department of Commerce

CSA cloud security alliance℠

TRUSTED COMPUTING GROUP

Summary and Opportunity

The info security challenge is escalating.

Hardware-assisted Security is solving a variety of problems, many unsolvable by software-only.

We all have opportunity to *Change The Game:*

Intel/McAfee + Partners + Customers

Thank You!

Legal Notices and Disclaimers

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.

Intel may make changes to specifications and product descriptions at any time, without notice.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to http://www.intel.com/performance

Intel, Intel Inside, the Intel logo, Intel Core, and Xeon are trademarks of Intel Corporation in the United States and other countries.

Security features enabled by Intel® AMT require an enabled chipset, network hardware and software and a corporate network connection.   Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Setup requires configuration and may require scripting with the management console or further integration into existing security frameworks, and modifications or implementation of new business processes. For more information, see http://www.intel.com/technology/manage/iamt.

No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a subscription with a capable Service Provider. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro

The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/

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