

# Preventing Stealthy Threats: A Proactive approach from Intel and McAfee

## Speakers

*John Skinner, Director of Secure Enterprise and Cloud, Intel*

*Ed Metcalf, Director of Product Marketing for Intel solutions, McAfee*

# Today's Discussion

- The Evolving Threat Landscape
- Computing Trends, Security Implications
- Why a New Approach is Required
- Hardware-Assisted Security Technology
- McAfee Deep Defender
- McAfee Deep Command
- Q & A



# Today's Threat Landscape: Hacker *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**

# Industry Problems

- Current security solutions provide **protection within the OS**
- Cyber criminals are **circumventing this protection** with advanced stealthy threats
- Current security solutions are **ineffective at preventing** these threats



- **Advanced Persistent Threat (APT):**

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

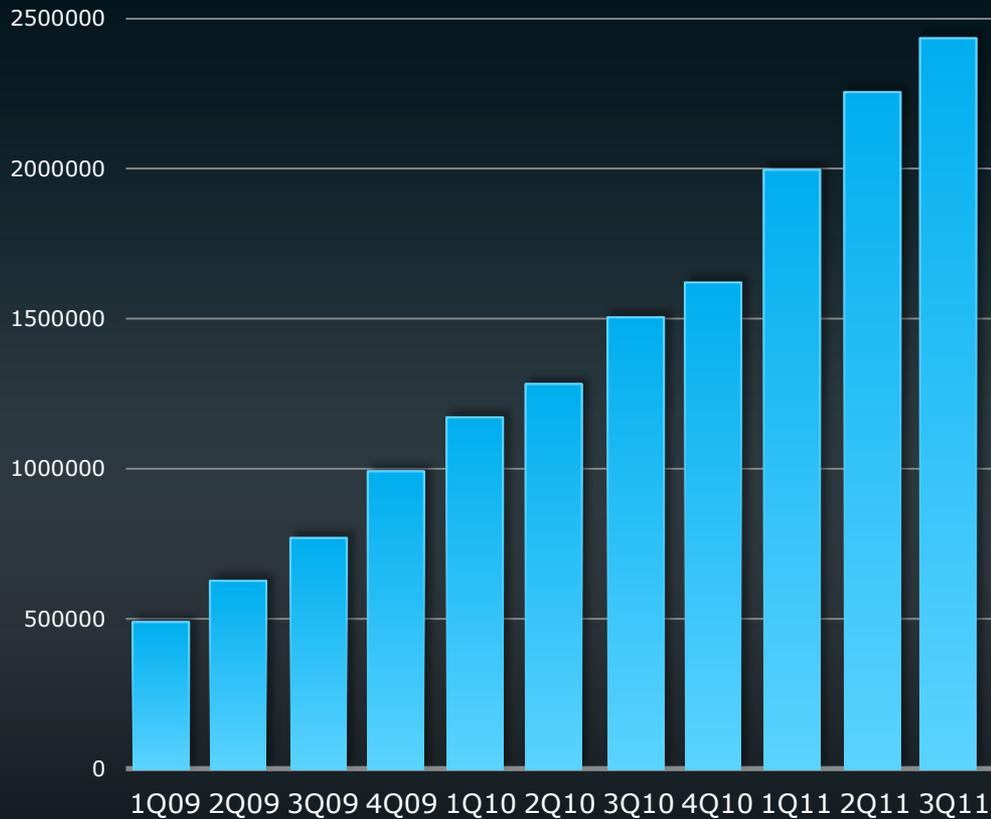
- **Kernel-mode Rootkit:**

Lives and operates below the operating system, and evades detection by OS-level security measures. Cloaks other malware & APT's.



# Stealth Malware Explosion

UNIQUE ROOTKITS  
Cumulative



- Stealth techniques drive proliferation of malware
- Designed to evade traditional security measures
- Cyber criminals using more stealth to hide data-stealing malware
  - 110,000 new rootkits each quarter
  - 1,200 new rootkits per day
- More malware using rootkits to evade detection
  - Stuxnet
  - Koobface
  - SpyEye
  - TDSS

# Stealth Techniques Increases Risk Exposure

Slow system performance from hidden threats decreases employee productivity

Stealth techniques to spread malware across your enterprise i.e. Zeus

"Re-imaging" endpoints to remove hidden malware infections

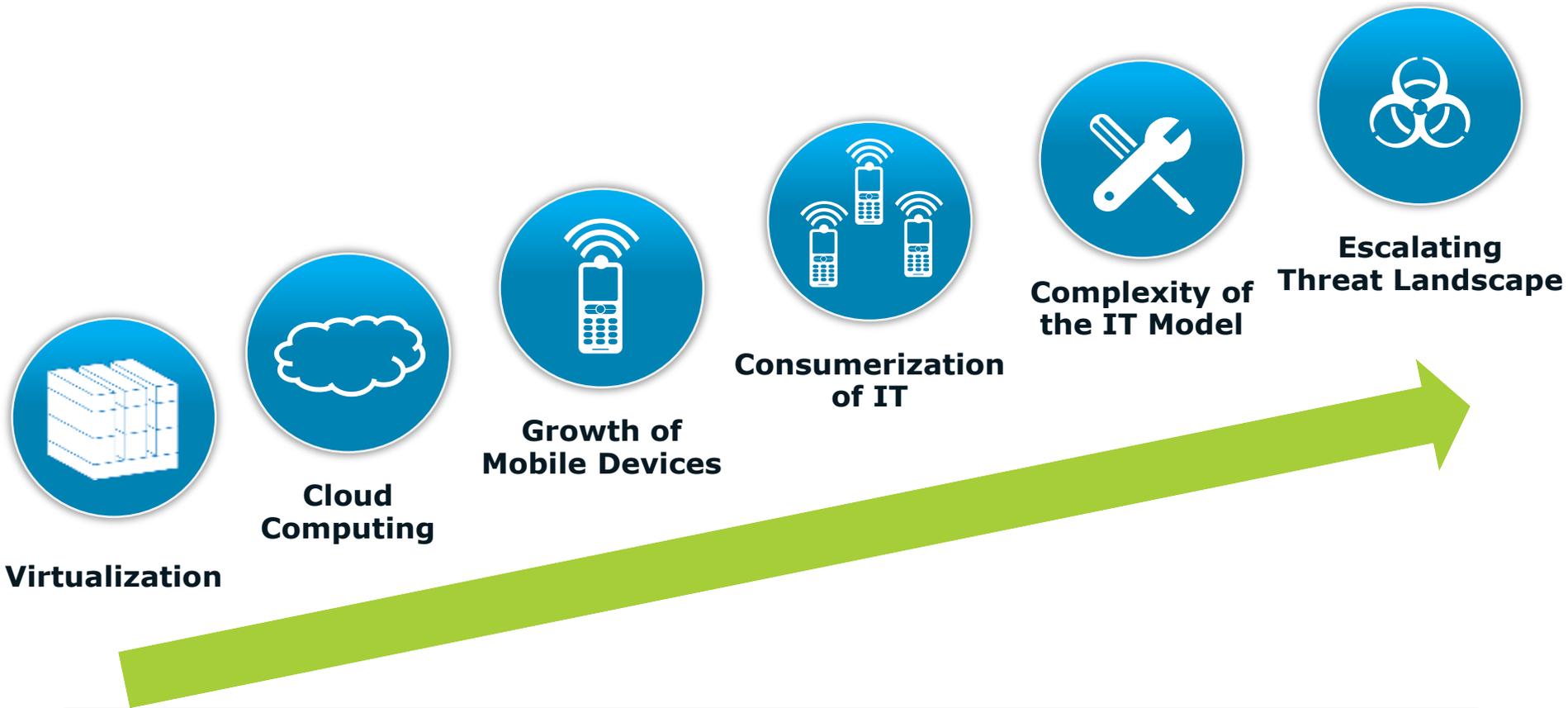
Stealth malware puts your business at risk being out of compliance with privacy regulations and policy



Koobface threat used stealth techniques to secretly turn an endpoint into a BOT

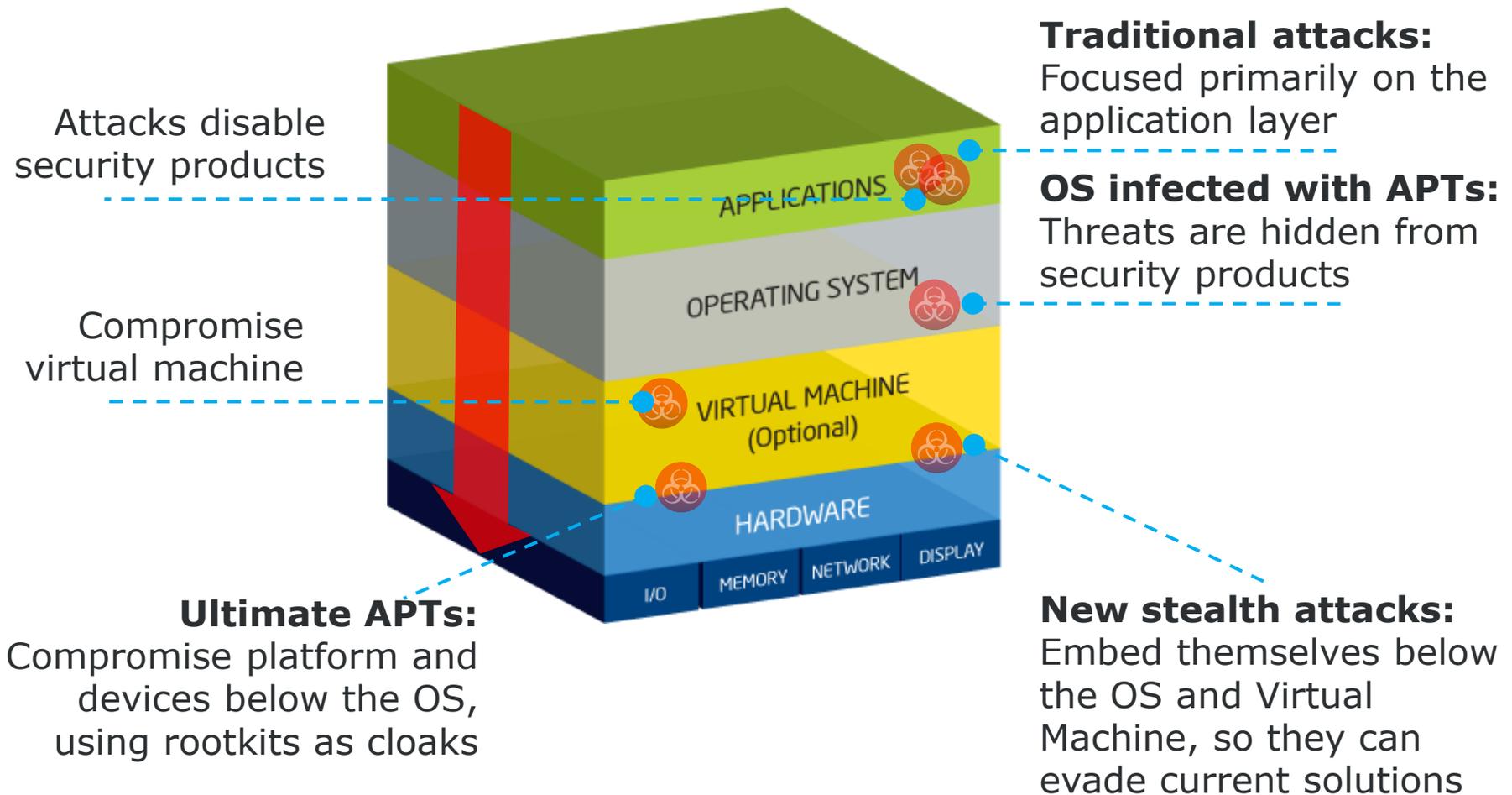
Hidden key loggers quietly steal confidential and personal information

# Computing Trends and Security Implications



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

# Attacks Are Moving “Down the Stack”, to Gain Greater Stealth and System Control

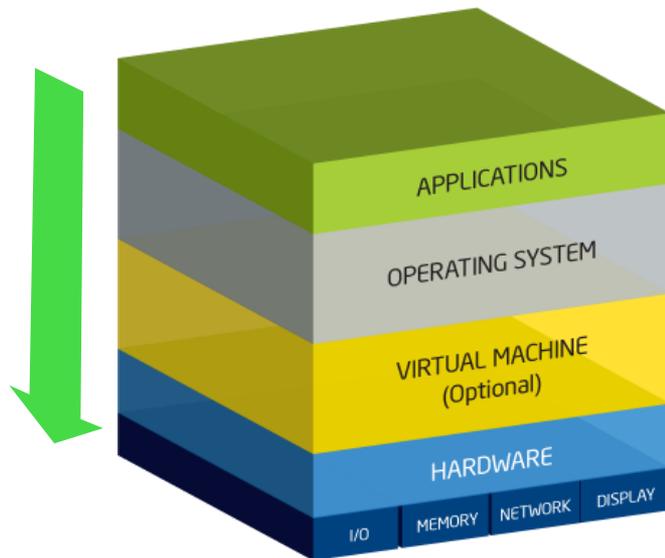


# A New Approach Is Required:

# “Hardware-assisted Security”



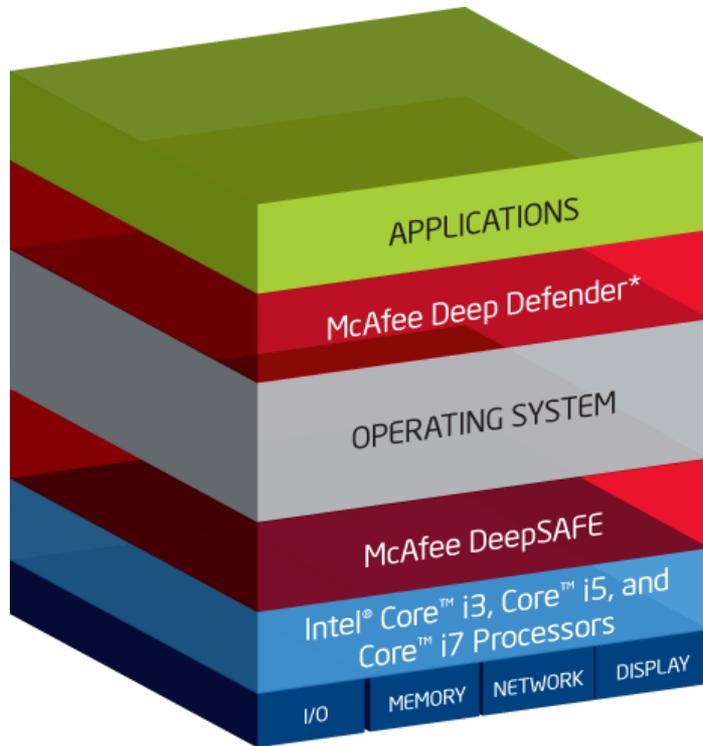
- **Move critical security processes *down into the hardware***
  - Encryption, Authentication, Manageability, and Platform Cleansing
  - Hardware is inherently less vulnerable to modification or corruption
- Establish a **security perimeter from the hardware layer up**
- **Isolate** the security services 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**

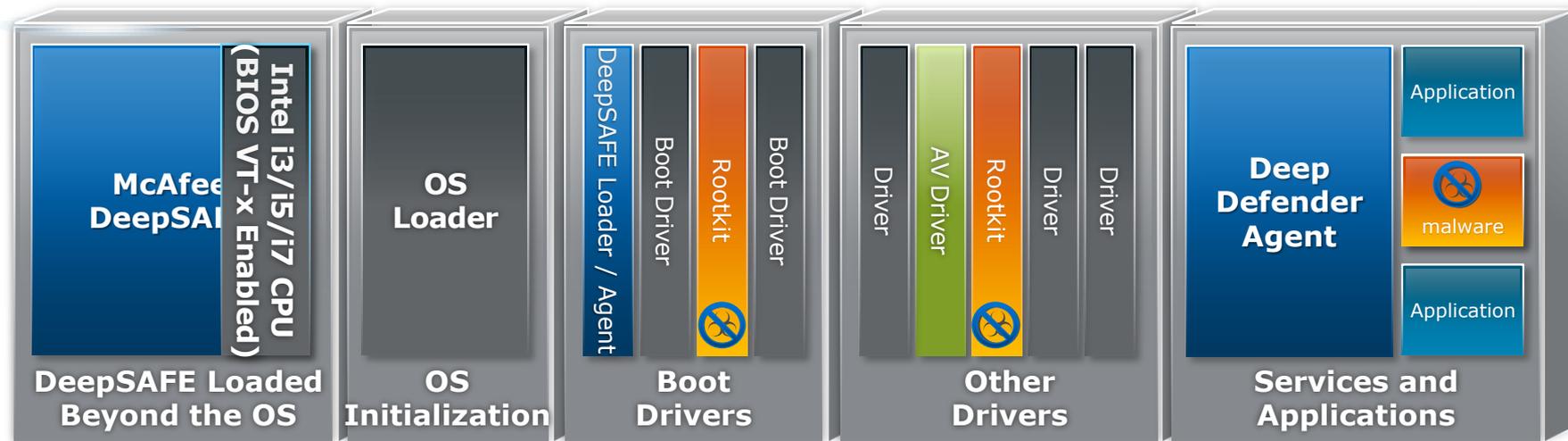
# Example of Hardware-assisted Security: McAfee DeepSAFE Security Platform



- **DeepSAFE is the first hardware-assisted security platform from Intel and McAfee, utilizing Intel Virtualization Technology. 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

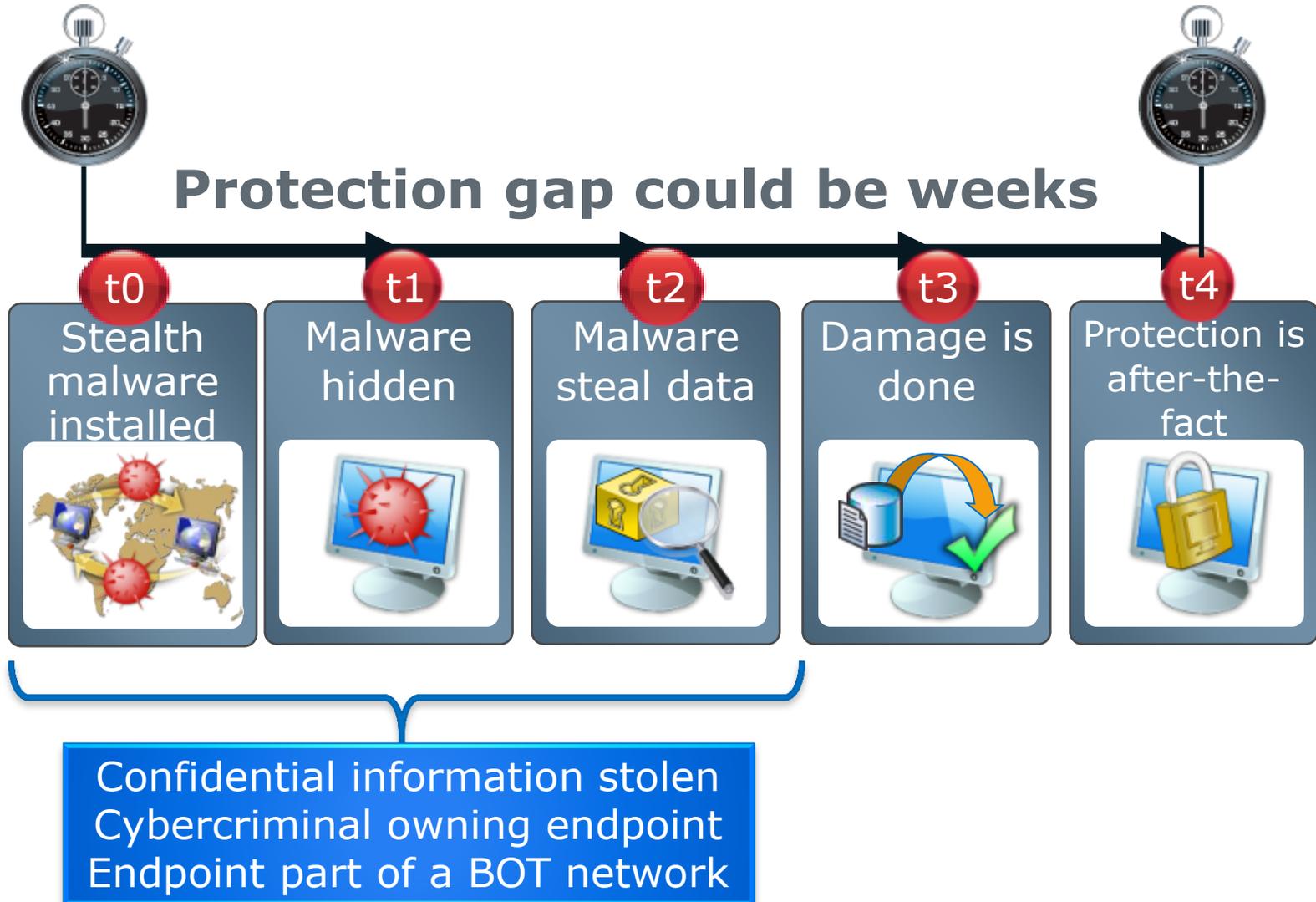
**Next-generation “beyond the OS” security enabled by Intel® processor technology**

# Deep Defender— Stopping a Stealthy Rootkit

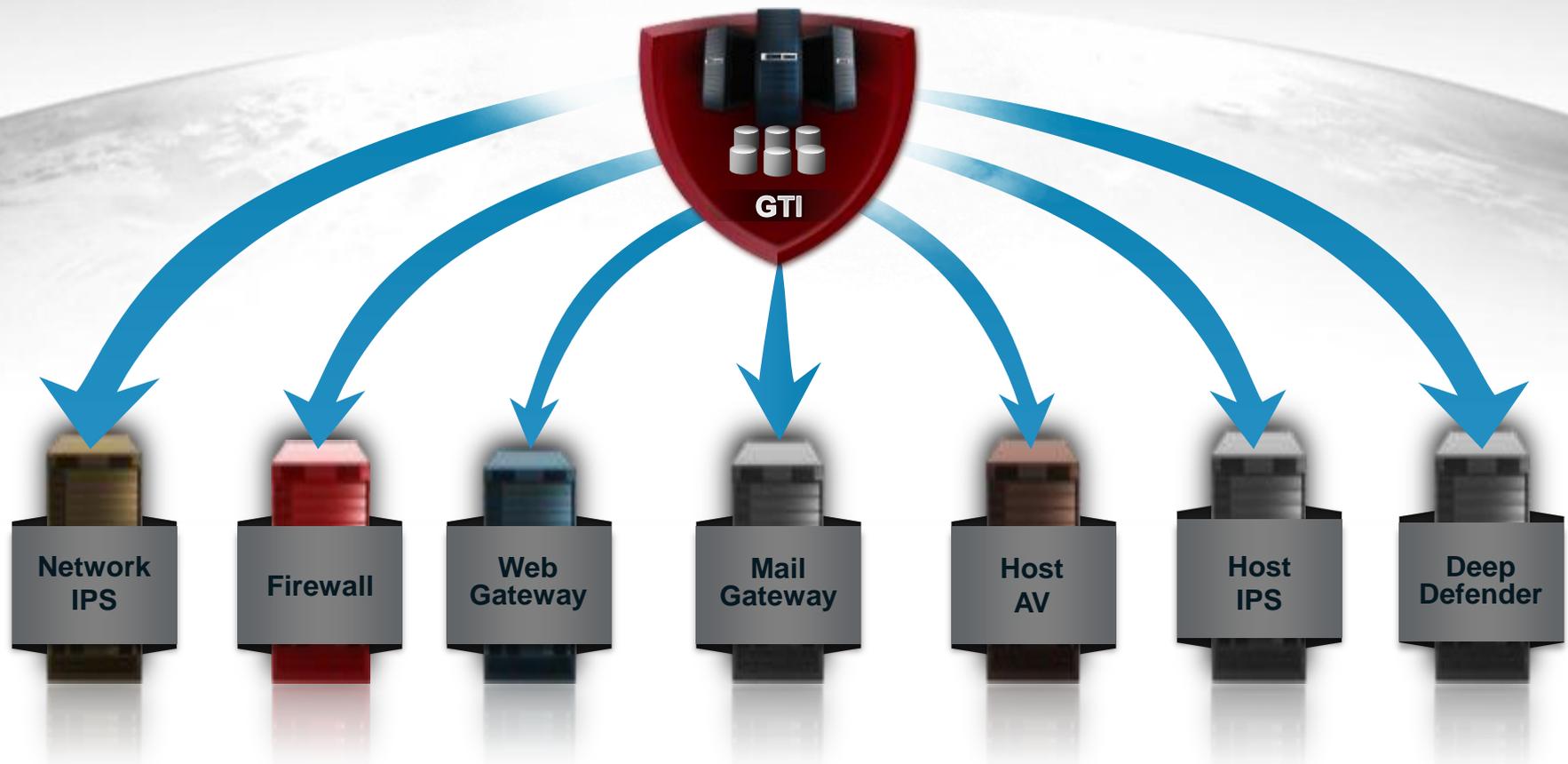


- Real-time kernel-level monitor of memory
- Identifies kernel-mode rootkits in real-time
  - Prevents the drivers from loading
  - DeepSAFE technology loads before the OS
- DeepSAFE technology informs Deep Defender of suspicious behavior

# Stealth Rootkits – After the Fact is Too Late!



# Deep Defender Enabling Global Threat Intelligence



# Deep Defender Deployment Details

- Supported Intel chipsets
  - Intel® Core™ i3, i5, i7 processors
- Supports Windows 7; 32 & 64 bit
- Integrates with McAfee's GTI cloud
- Utilizes Intel VT in the Core iSeries processors



# Talk to an Expert: Question & Answer



Today's experts:

*John Skinner, Director of Secure Enterprise and Cloud, Intel*

*Ed Metcalf, Director of Product Marketing for Intel solutions, McAfee*

Submit your questions:

- Ask questions at anytime by pressing the Question tab at the top of the player.

More information:

- Download content at the top of the player
- Visit [www.intel.com/pcsecurity](http://www.intel.com/pcsecurity)
- Check out the Intel IT Center, a valuable source of unbiased, relevant information to help you meet your most challenging IT demands:  
[www.intel.com/itcenter](http://www.intel.com/itcenter)

# 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.

Copyright © 2011 Intel Corporation, All Rights Reserved



