Intel® Cyber Security Briefing:
Trends, Solutions, and Opportunities

Matthew Rosenquist, Cyber Security Strategist, Intel Corp

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.

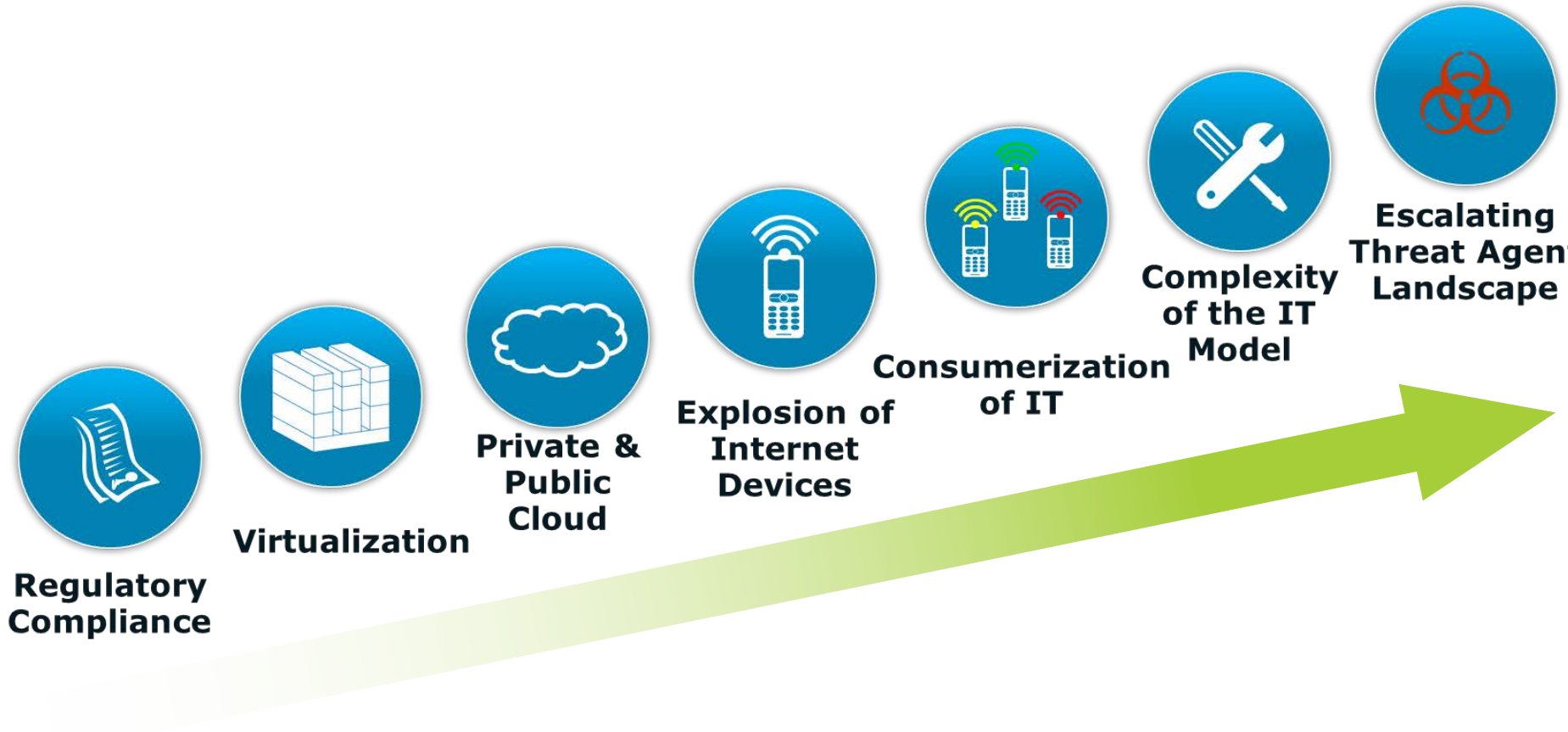
Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-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

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

Agenda

- Trends and Landscape
- Challenges of Cyber Security
- Defense in Depth Strategy
- Layered Security Technology
- Innovations for Endpoint Protection
- Summary, Questions, Discussion

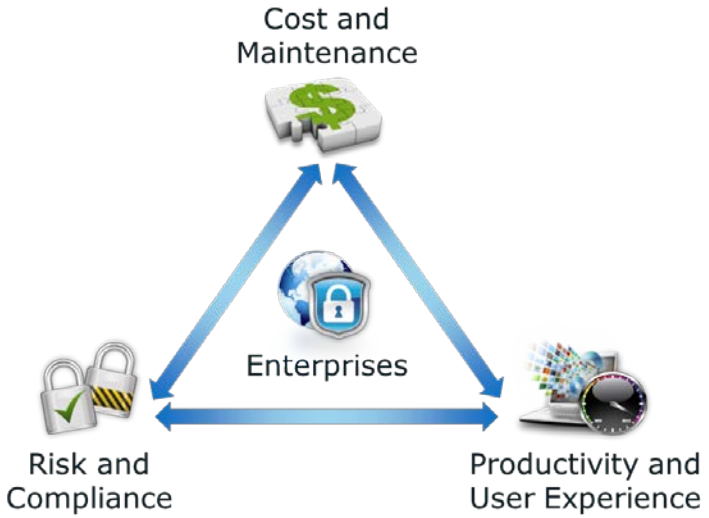
Industry Changes Drive Security



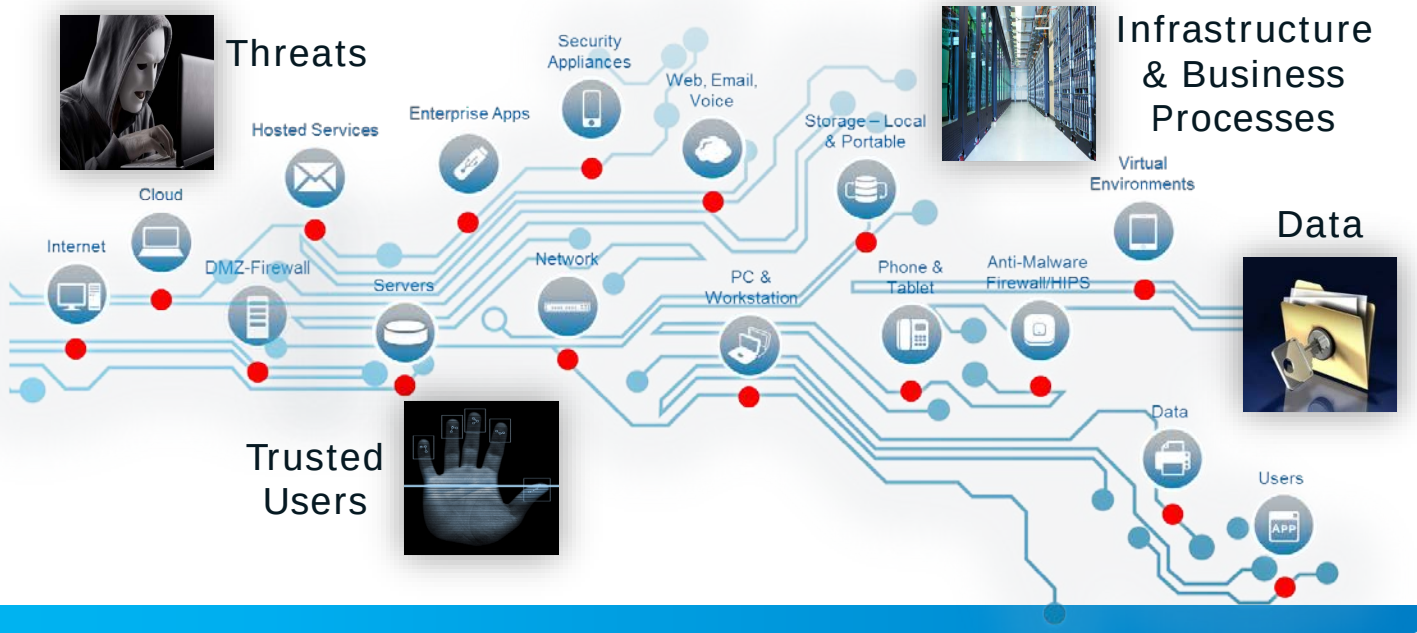
Challenges are increasing over time.
The risks-of-loss continues to rise as the cyber security industry grows in size, intensity, and complexity

Scope

Businesses must find a balance through tradeoffs:



Security aspects are intertwined:



Defense in Depth

Process to drive cost efficiency and security effectiveness

Prediction

Predict the most likely attacks, targets, and methods

Prevention

Prevents or deters attacks so no loss is experienced

Detection

Identify attacks not prevented to allow for rapid and thorough response

Response

Rapidly address incidents to minimize losses and return to a normal state

Defense in Depth Cyber Security Strategy

Prediction: Proactive measures to identify attackers, their objectives and methods prior to materialization of viable attacks. Enables and maximizes Prevention activities.

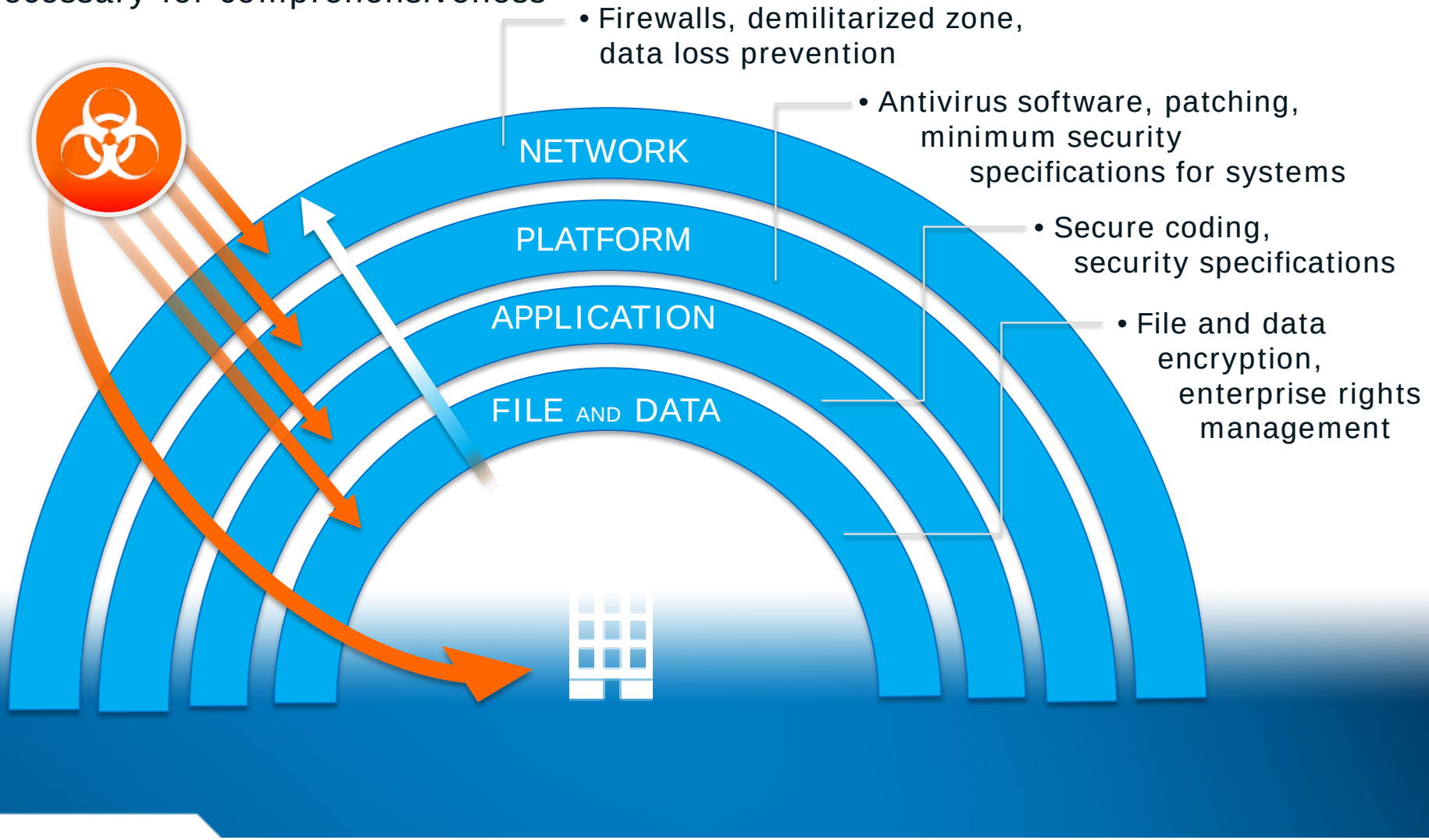
Prevention: Securing the computing environment with current tools, patches, updates, and best-known methods in a timely manner. Educating and reinforcing good user behaviors. Undermines most attacks.

Detection: Monitoring of key areas and activities for attacks which evade prevention. Identifies issues, breaches, and attacks. Supports rapid interdiction by Response capabilities

Response: Efficient management of efforts to contain, repair, and recover as needed to return the environment to normal operations. Reduces losses by rapidly addressing issues and feeds intelligence into Prediction and Prevention areas

Layered Defense

Necessary for comprehensiveness



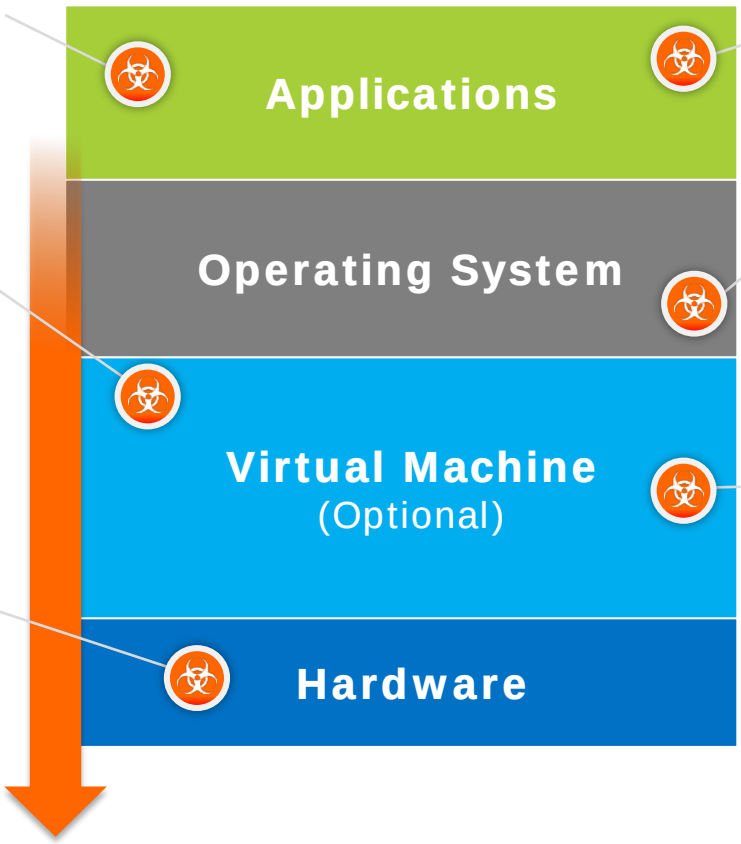
Innovation on the End-Point

Attacks are Moving Down the Stack:

Attacks disable security products, steal and control applications

Compromise virtual machine

Attacks against hardware and firmware affect the root-of-trust



Traditional attacks:
Focused primarily on the application layer

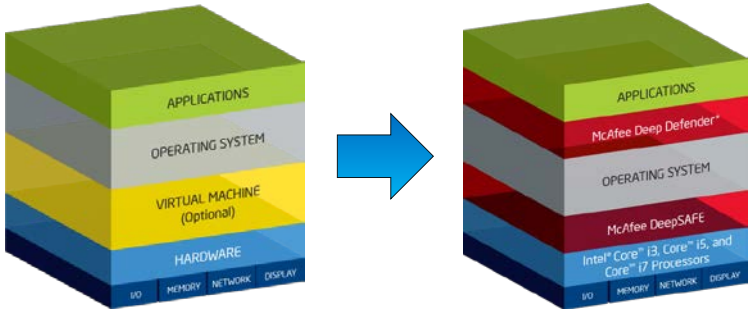
OS infected:
Threats are hidden from security products

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

Innovation

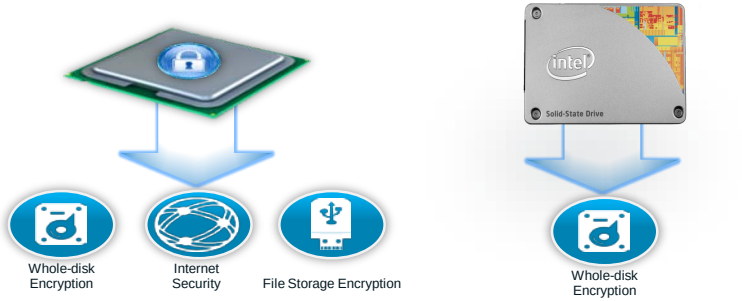
Security below the OS

- Sensors under the OS to detect stealth malware
- Passes data to Anti-Malware software to block, and remove



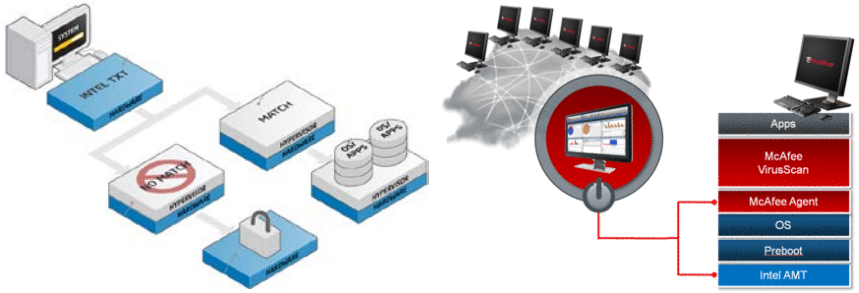
Faster Encryption

- Hardware acceleration of encryption algorithms (up to 4x faster) improves user experience and productivity, while protecting data



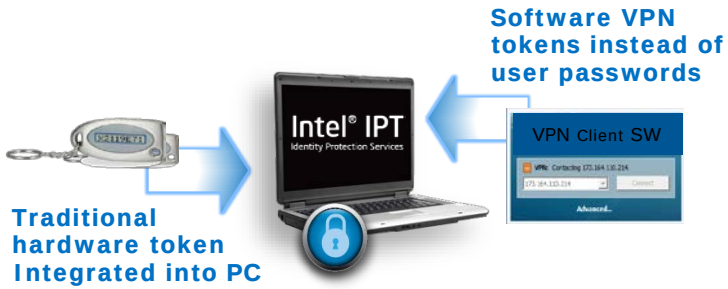
Strengthening Data-Center Security and Control

- Attestation of VM and cloud security
- Out-of-Band security monitoring, management, and recovery



Hardware Enhanced Authentication

- Eliminating the need for separate hardware tokens
- Faster software VPN login, for improved user experience and productivity

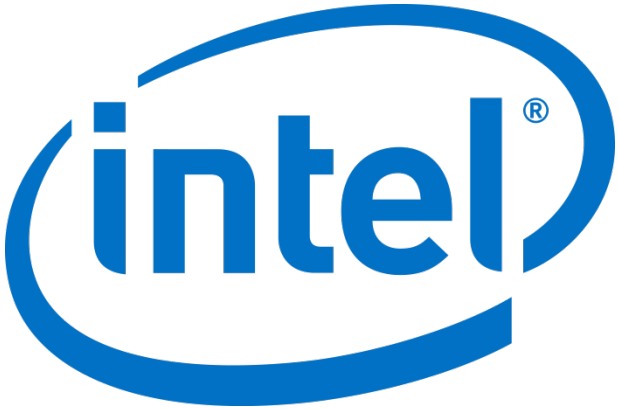


Summary

- ✓ A well thought out cyber strategy is necessary to secure assets, operations, reputation, and competiveness
- ✓ Strive for achieving and maintaining the optimal balance of security for your organization
- ✓ Executive commitment and support is a prerequisite to success

Two types of victims exist: those with something of value and those who are easy targets.

Therefore: *Don't be an easy target, and protect your valuables*


intel