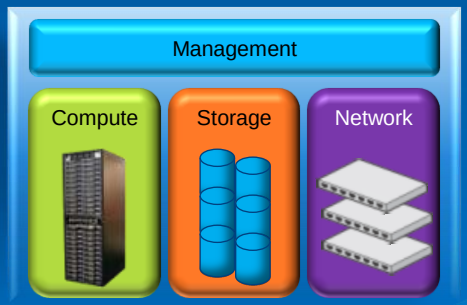
UWAGA!
Prezentacja przeznaczona jest tylko do użytku wewnętrznego firmy uczestnika VMware Cloud Day 2011.
Nie dopuszcza się dalszego prezentowania, wykorzystywania materiałów w części lub całości oraz dalszej dystrybucji/umieszczaniaw sieci.

Intel Hardware Security Technologies

Dariusz Wittek
EnterpriseTechnology Specialists
Intel

The Enterprise Datacenter is Evolving

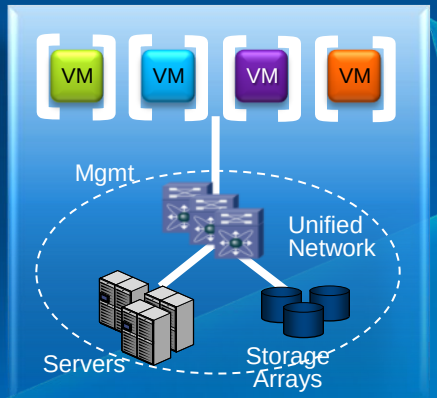
Discrete Datacenter



Consolidation

Discrete networks

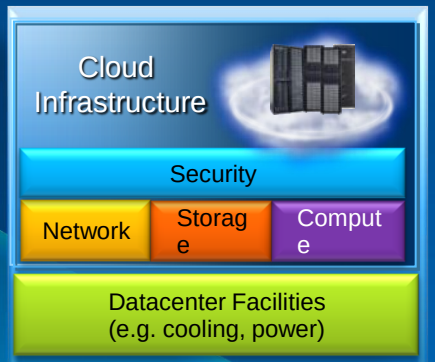
Virtualized Datacenter



Flexible Management

10G Unified Network

Cloud Datacenter



Efficient and **Secure**

Open Architecture

Simplified Network

Advanced Virtualization Requires…

…Advanced Capabilities

Security in the Cloud

Cloud and virtualization have inherent security requirements

- Abstraction of physical hardware
- Multi-tenancy movement implicitly require audit and security

"Twitter Embeds Encryption to Foil Firesheep hackers"
—PC World

"Webhost hack wipes out data for 100,000 sites
Vaserv suspects zero-day virtualization vuln"
—The Register

"IT ops, security pros at odds over virtualization risks
IT pros upbeat about virtualization, whereas security experts harbor doubts about the security role the hypervisor can play"
—IDG News Service

Cloud and Virtualization Break Many Traditional Perimeter-oriented Security Techniques

Security in the Enterprise: Layers

Traditional
Attack Targets/
Risk Area

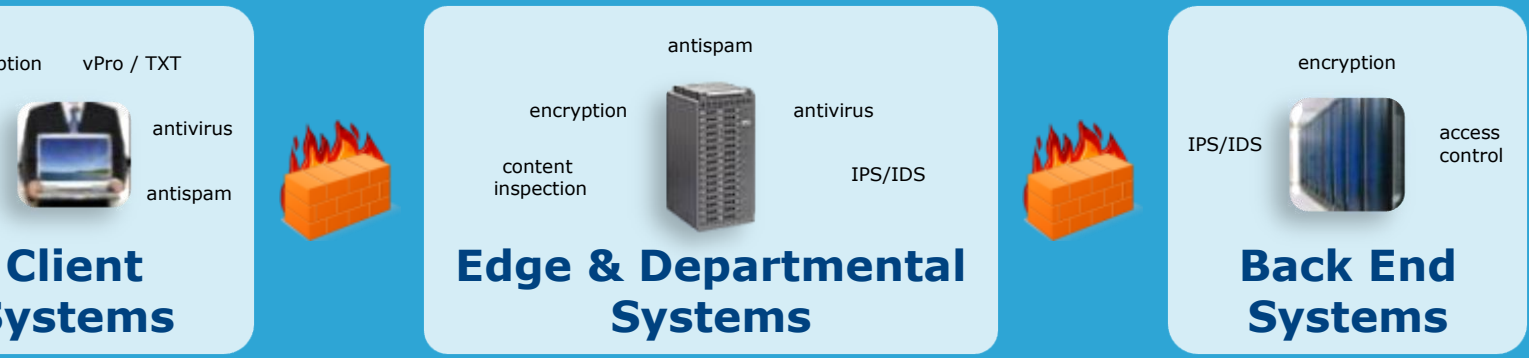
Limited physical protections and more human interaction

Growing
Attack Targets/
Risk Area

Changing perimeters and increased access

Emerging
Attack Area

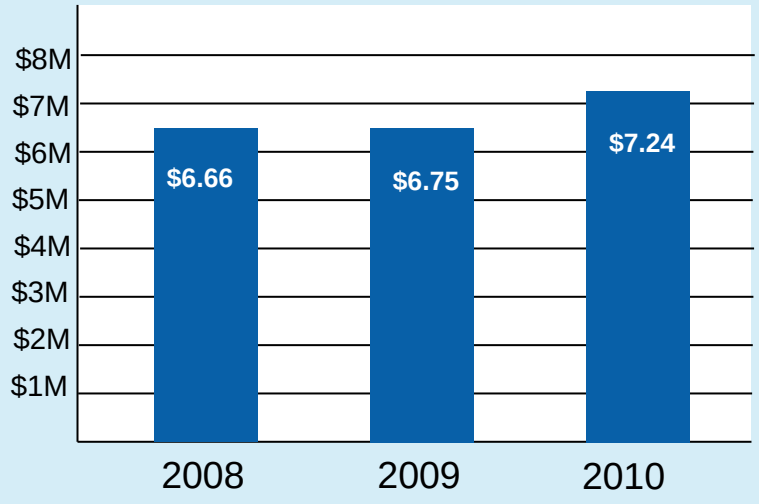
Strongest physical isolation and lowest accessibility



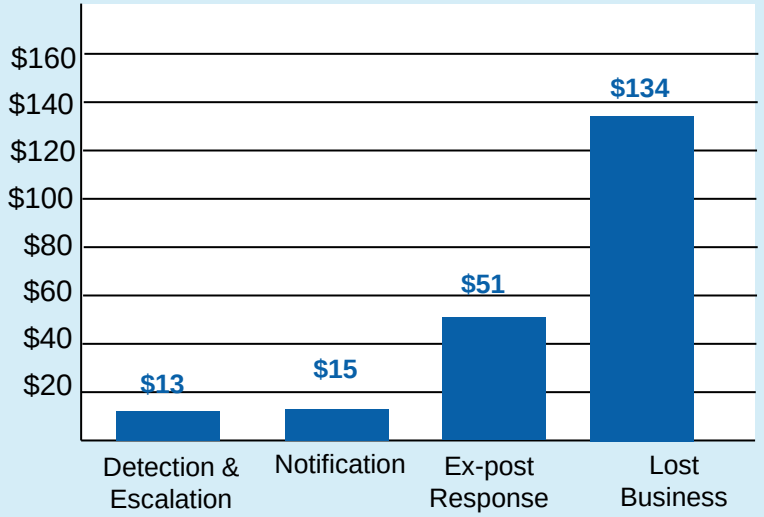
Enabling Protections Deeper into the Datacenter

Breaches Cost the Enterprise

Average Organizational Costs of a Data Breach, 2008-2010 (in $ Million)



Average Costs of a Data Breach by Cost Activity on a Per Record Basis (2010)



Source: Ponemon Institute - 2010 Annual Study: Cost of a Data Breach . March 2011

Risks and Costs Growing, Prevention the Best Solution

Risks and Costs Growing, Prevention the Best Solution

Security Preventing Adoption of The Cloud

51%

Security is the greatest concern surrounding cloud computing adoption.

- Gain visibility
- Maintain control
- Prove compliance

Source: CIO Magazine 2010 State of the CIO Study

Validated by Intel's End User Discussions (EBOA, ODCA, etc)

Open Data Center Alliance

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

From Vision to Action

IT & Service Providers

Define and Prioritize IT Requirements

Products & Technologies

Take Advantage of New Capabilities in Intel Platforms

Intel® Cloud Builders

Utilize Proven Reference Solutions to Ease your Deployments

Pain Point #1: Data Protection

- Increasing demand to protect data
- Encryption is becoming a core standard for this

– Specific legislation as well as industry standards

- Encryption provides "last line of defense" and legal safe harbor
- Also protects confidentiality in uses where physical isolation is impossible

Nevada Enacts *Encryption* Law for Data Transmission

Nevada put into effect Wednesday the nation's first data encryption law, which prohibits businesses from electronically transferring customers' personal data outside their organization unless it's encrypted.[1]

Encrypt Now to Meet New Massachusetts Data Protection Law[2]

Louisiana Personal Information Data Privacy Notification and Encryption Laws: SB 205 Act 499[3]

Louisiana passed a data breach notification law which went into effect on January 1, 2008. The law is called the "Database Security Breach Notification Law" (Senate Bill 205 Act 499), and requires any people or companies that lose sensitive, personal data to notify those that are affected. If the information was protected using encryption software, the breach notification is not necessary.[3]

1 http://www.crn.com/security/210605176;jsessionid=3BR5SYATQOCOHQE1GHPCKHWATMY32JVN

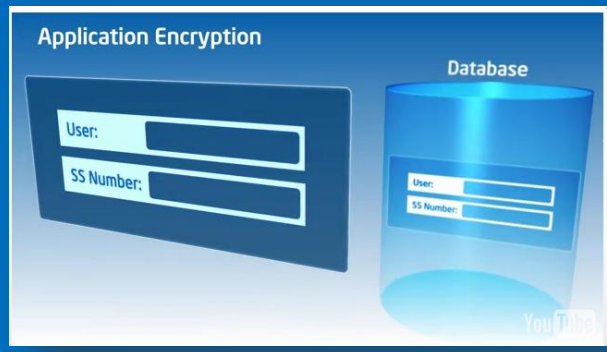
2 http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1346761,00.html

3 http://www.alertboot.com/blog/blogs/endpoint_security/archive/2009/10/16/louisiana-personal-information-data-privacy-notification-and-encryption-laws-sb-205-act-499.aspx

Intel® AES-NI: What is it?

- Processor assistance for performing AES encryption -7 new instructions
- Makes enabled encryption software faster, stronger and better data protection
- Forms building blocks for AES as well as other crypto algorithms

- Provides better security and performance
- Support -Native/Guest OS
- Microsoft Windows Server* 2008 R2 &Microsoft BitLocker *WS2008R2
- McAfee Endpoint Encryption for PC 6.0 with McAfee ePolicy Orchestrator 4.5
- OpenSSL patch, Red Hat Enterprise Linux* 6
- Fedora Linux* 13
- VMware* ESX 4.0 U1 (supports AES-NI usage in the guest OS)
- Oracle Berkeley* DB 11.2.5.0.26
- Oracle Database* 11.2.0.2

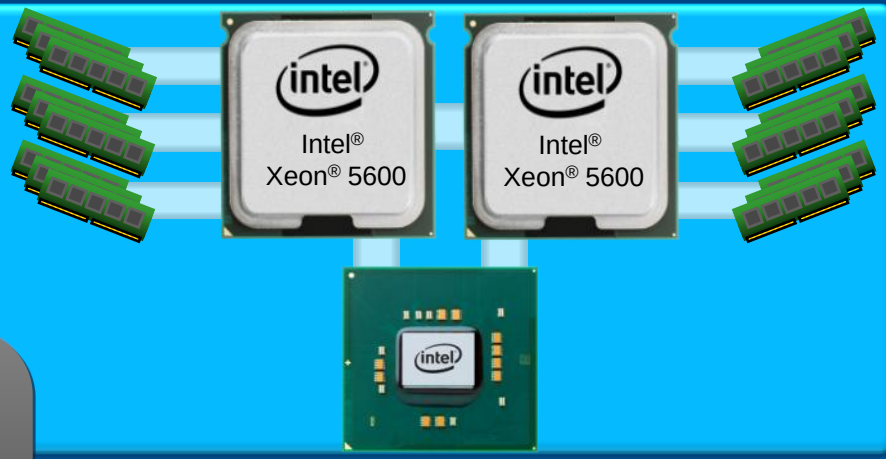


Intel® AES-NI support - Intel® Xeon® 5600 & Intel® Xeon® E7

Energy Efficient Performance
Intel® Xeon® 5600/E7-4800

Westmere (32nm) architecture
up to 6-cores with up to 12MB L3 cache

18 DIMM slots support up to 288 GB of memory



Intel® Turbo Boost Technology (Turbo Mode) Intel® Hyper-Threading Technology

Intel Virtualization Technologies

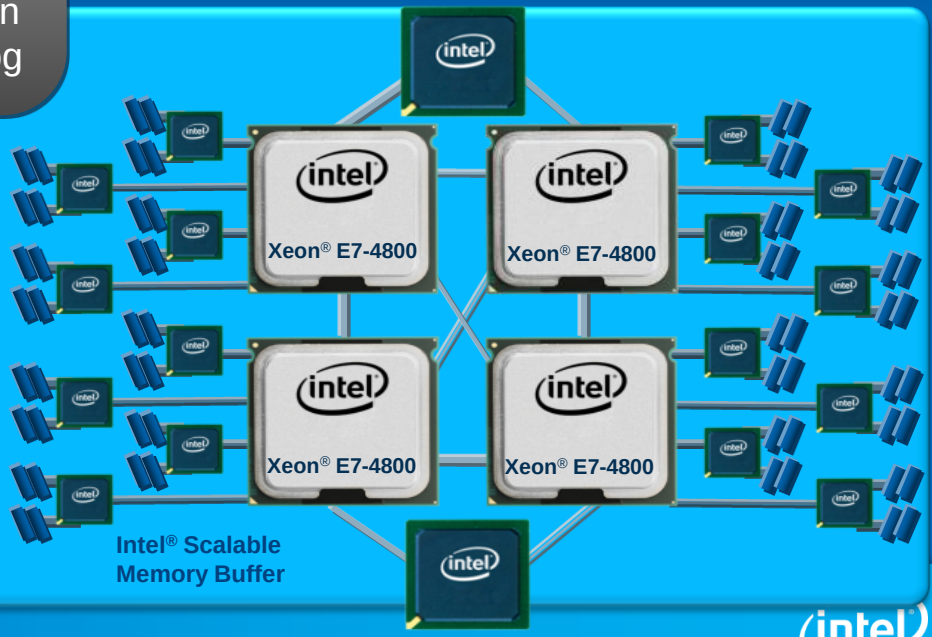
AES-NI and Intel® Trusted Execution Technology

Westmere (32nm) architecture
up to 10-cores with up to 30MB L3 cache

64 DIMM slots support up to 2 TB of memory
(4 sockets)

Scaling from 2-256 sockets

Mission Critical Class Reliability features



Intel® Xeon® 5600 the Best Overall Solution[1]

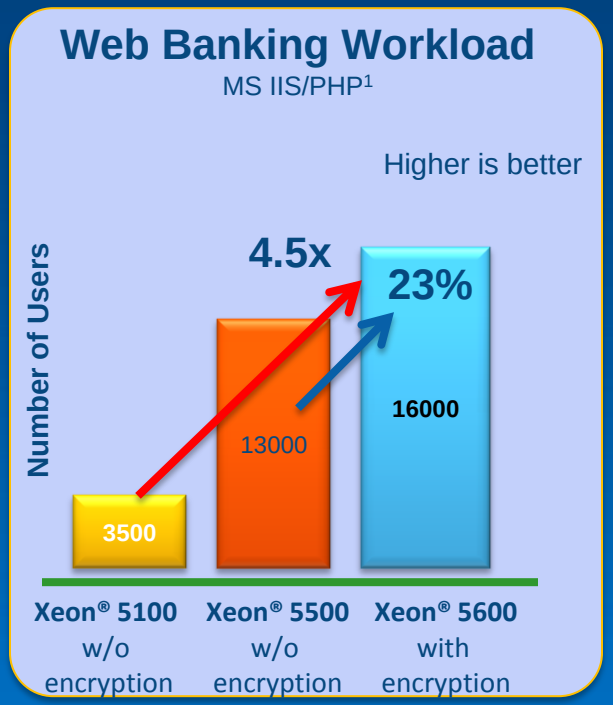
Intel® Xeon® Processors

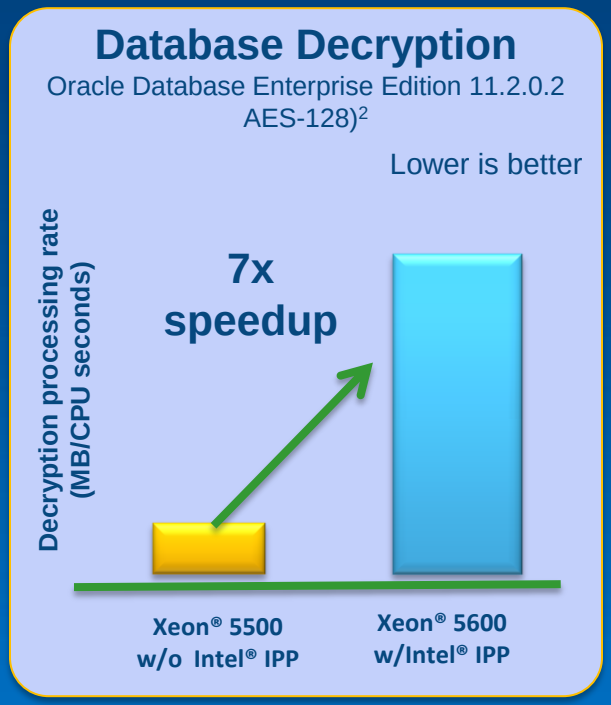
	5600 Series	E7 8800/4800/ 2800 Product Families	E3 1200 Product Family
Performance[2]	Low — High	Low — High	Low — High
Energy Efficiency • Processor—perf/watt • System—total power			
Scalability • Compute • Memory • I/O			
Security RAS[3]	✓	✓	✓
Targeted Workloads	**Mainstream Enterprise** Enterprise Server Cloud Computing HPC & Workstations[2]	**Scalable Enterprise** Mission Critical Cloud Computing HPC	**Small Business** Low-end multi-purpose Entry Workstations[4]
	Best Balance of Performance, Power Efficiency & Cost	**Top of the Line Performance, Scalability and Reliability**	**Economical and More Dependable vs. Desktop**

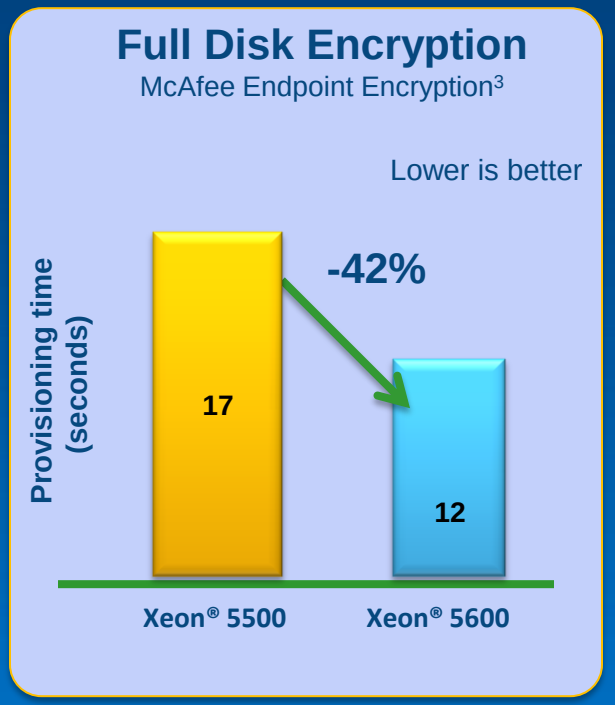
1. As demonstrated by its #1 position in the market with XX% market segment share
2. Xeon E7 targets transaction type performance. Xeon 5600 aims for a balance of transaction and frequency sensitive performance needs
3. RAS= reliability, availability and serviceability
4. Available with integrated graphics

Internal Intel Measurements

Intel® Xeon® 5600 Encryption Performance







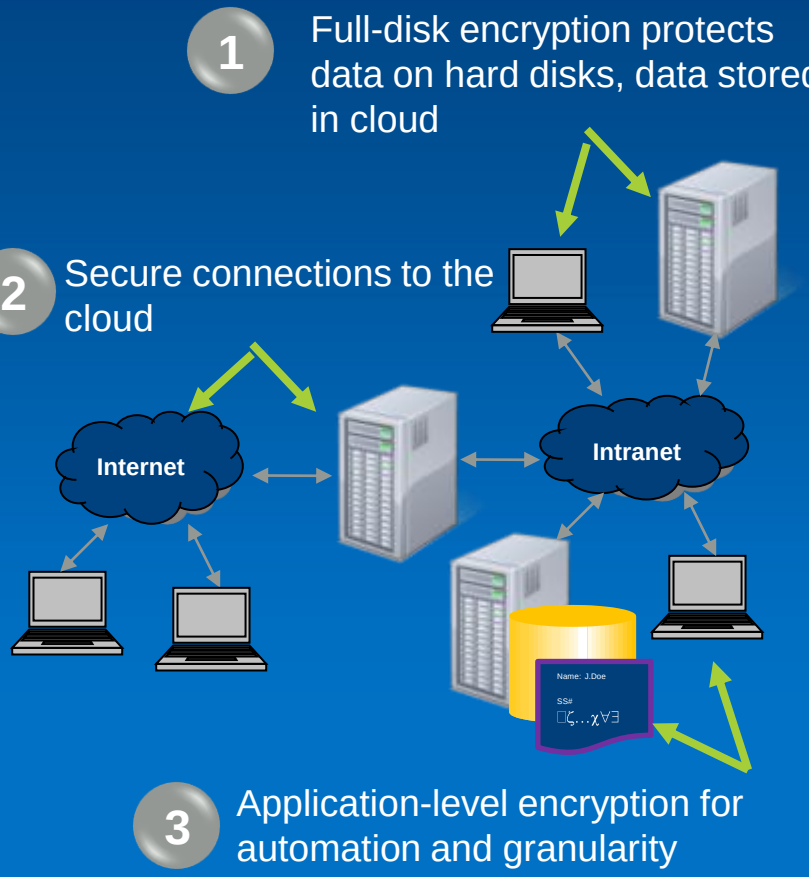
1 System configuration: Windows 2008 R2 x64 Ent. Server. PHP banking sessions /users measured with Intel® Xeon® X5680 (3.33 GHz) vs Intel Xeon® 5160 (3.00 GHz) and Intel Xeon® X5570 (2.93 GHz), 24 SSD RAID 0 arrays, TLS_RSA_with_AES_128_CBC_SHA cipher suite.

2 System configuration: Oracle 11g with TDE, time takes to decrypt a 5.1 million row encrypted table with AES-256 CBC mode on WSM 3.33 GHz optimized with Intel® Performance Primitives crypto library (IPP) vs NHM 2.8 GHz without IPP. Timing measured is per 4K of data.

3 System configuration: McAfee Endpoint Encryption for PCs (EEPC) 6.0 package with McAfee ePolicy Orchestrator (ePO) 4.5 encrypting a 32GB X25E SSD with WSM 3.33 GHz vs. NHM 2.93 GHz. 24GB of memory.

Data Protection with Intel® AES-NI

1. Full disk encryption software protects data automatically during saving to disk
2. Secure transactions used pervasively in ecommerce, banking, etc.
3. Most enterprise and many cloud applications offer options to use encryption to secure information and protect confidentiality



More Ways to Use of Encryption for Protection of Business Information Assets

Pain Point #2: Platform Protection

- New threats are emerging that are focused on attacking the pre-runtime environment
- Low-level attacks are hard to detect and can be difficult to recover from
- Emerging need for hardware-based trust

Mebromi: The First BIOS Rootkit in the Wild

"In the past few weeks a Chinese security company called Qihoo 360 blogged about a new BIOS rootkit hitting Chinese computers. This turned to be a very interesting discovery as it appears to be the first real malware targeting system BIOS since a well-known proof of concept called IceLord in 2007."[1]

NIST Guidelines Seek to Minimize Risk of BIOS attacks[2]

US Dept of Homeland Security Cyber Security Research & Development Broad Agency Announcement (BAA): BAA 11-02

"TTA #11: Hardware-Enabled Trust

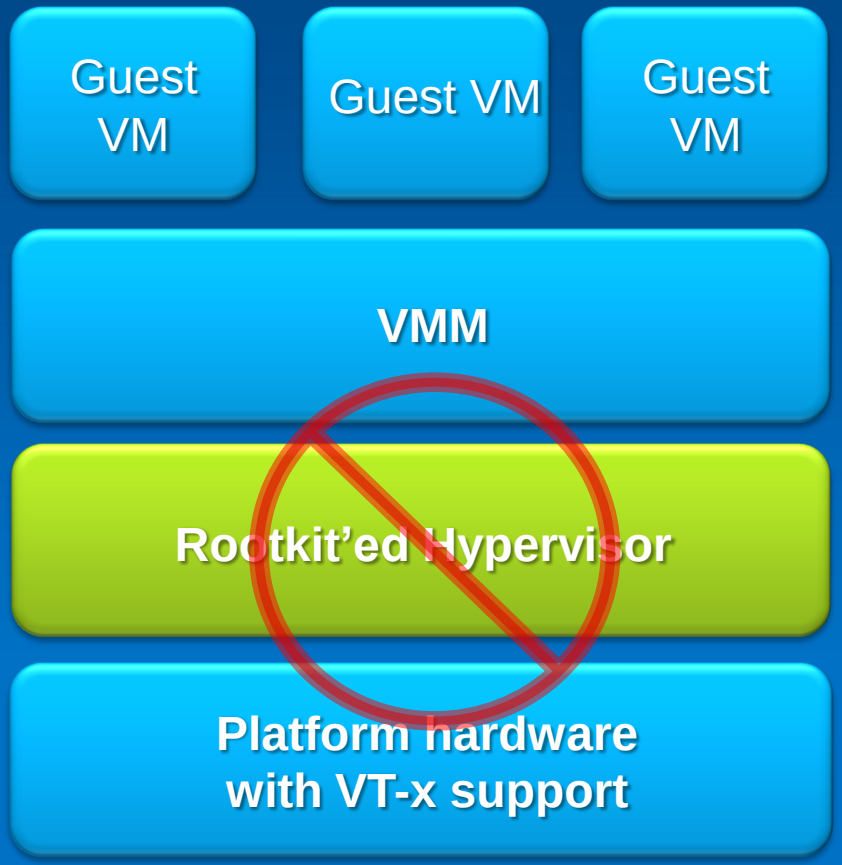
a. Hardware can be the final sanctuary and foundation of trust in the computing environment, based on the technologies that can be developed in the area of hardware-enabled trust and security. With cyber threats steadily increasing in sophistication, hardware can provide a game-changing foundation upon which to build tomorrow's cyber infrastructure."[3]

[1] http://blog.webroot.com/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/
[2] http://searchsecurity.techtarget.com/news/1280089766/NIST-guidelines-seek-to-minimize-risk-of-BIOS-attacks?asrc=EM_NLN_14955025&track=NL-102&ad=848433&
[3] https://www.fbo.gov/download/560/560a331a2f0105f32ca8c1e4f068c5e6/Cyber_Security_BAA_11-02_Amend_00014.pdf

New Controls to Protect Infrastructure by Pre-empting Emerging Classes of Attacks

Intel® Trusted Execution Technology (TXT) Protects Against Software-Based Attacks

- **TXT operates at Launch time**
- **Enforces control through launch enviroment measurement, memory locking and sealing secrets**
- **TXT works on white list model versus black list mode, measures and confirms integrity up to the VMM**
- **Allows greater control of launch stack and enables isolation in boot process**
- **Helps prevent highjacking by rootkit**



Intel® TXT: How it Works

With Intel TXT: The Positive Case
Software can be measured and verified as known good

Power on platform

System firmware verified by TXT prior to boot

Firmware / BIOS match? Yes

TXT Platform

Hypervisor code measured by TXT and compared to known good value prior to allowing launch

Hypervisor measure match? Yes

Hypervisor

TXT Platform

Launch VMs, OS, etc

Hypervisor

TXT Platform

With Intel TXT: The Negative Case
Unknown software is measured, detected and can be blocked

Power on platform

System firmware verified by TXT prior to boot

Firmware / BIOS match? Yes

TXT Platform

Hypervisor code measured by TXT and compared to known good value prior to allowing launch

Hypervisor measure match? **No**

???

TXT Platform

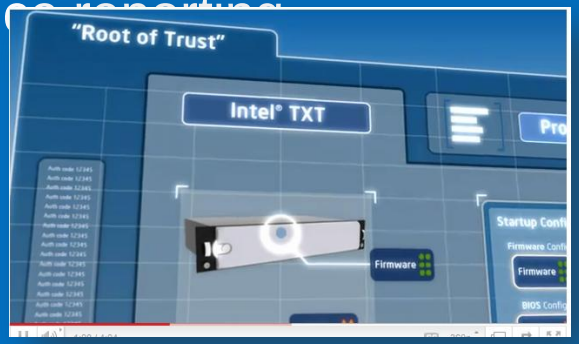
TXT blocks launch of Rootkit Hypervisor

TXT Platform

Intel® TXT Use Models

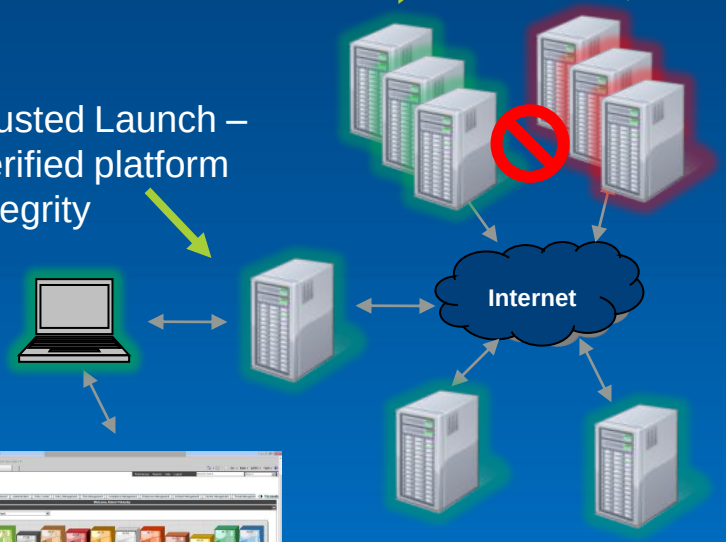
- Addresses critical needs in virtualized & cloud use models

1. Hardware enforced detection of launch components —reduce malware threat
2. Control VMs based on platform trust (and more) to better protect data
3. Hardware support for compliance reporting



2 Trusted Pools

1 Trusted Launch – Verified platform integrity



3 Compliance Support – enhancing auditability of cloud environment

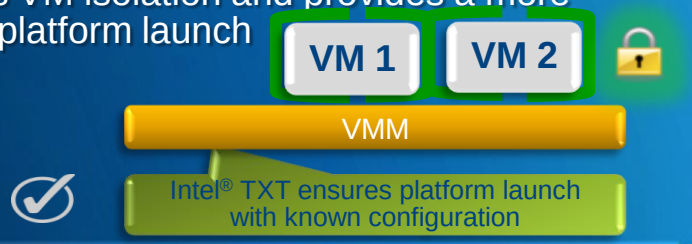
Leadership Use Models: Trust Provides a Powerful Control Point on Client and Server

Intel® Technologies: Cloud Security

Isolate

Intel® VT & Intel® TXT

protects VM isolation and provides a more secure platform launch



Encrypt

Intel® AES-NI

delivers built-in encryption acceleration for better data protection

Enforce

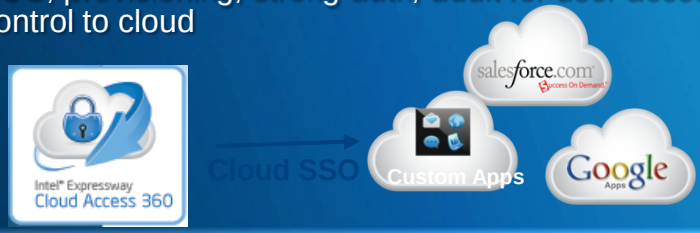
Intel® TXT

establishes “trusted” status to enable migration based on security policy

Connect

Intel® Expressway Cloud Access 360

SSO, provisioning, strong auth, audit for user access control to cloud



Establishing the Foundation for More Secure Clouds

Intel® TXT and Intel® AES-NI Enable More Secure IT Solutions †

Support and/or Reference Architectures Featuring:

- VMware
- Dell
- Enomaly
- EMC
- HyTrust
- Parallels
- OpenStack

Trusted Infrastructure

Intel® TXT

Data Protection

Intel® AES-NI

Support and/or Implementation White Papers Featuring:

- Microsoft
- Oracle
- McAfee
- Red Hat
- OpenSSL
- CheckPoint
- VMware

† Not all features and capabilities will be supported by all listed providers

Growing Ecosystem Support
More Expected for Security Features in 2011-12

Reference Architecture Guide – *Enhanced Cloud Security*

*Other brands and names are the property of their respective owners.

From Usage Model to Proven Solution

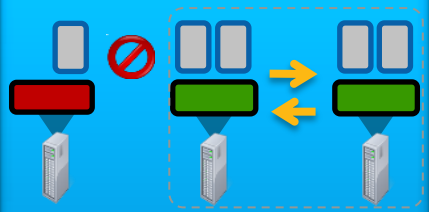
A Need for Security

Define → **Enable** → **Prove** → **Scale**

Pain Points

Enterprise Vulnerabilities

Usage Model



- Trusted Pools
- Compliance Reporting

Solution Stacks

HyTrust

vmware

- Applications
- Management
- OS
- Policy Engine
- VMM
- Chipset
- CPU

Prove out in lab

Intel® Cloud Builders

Execute End User IT POCs

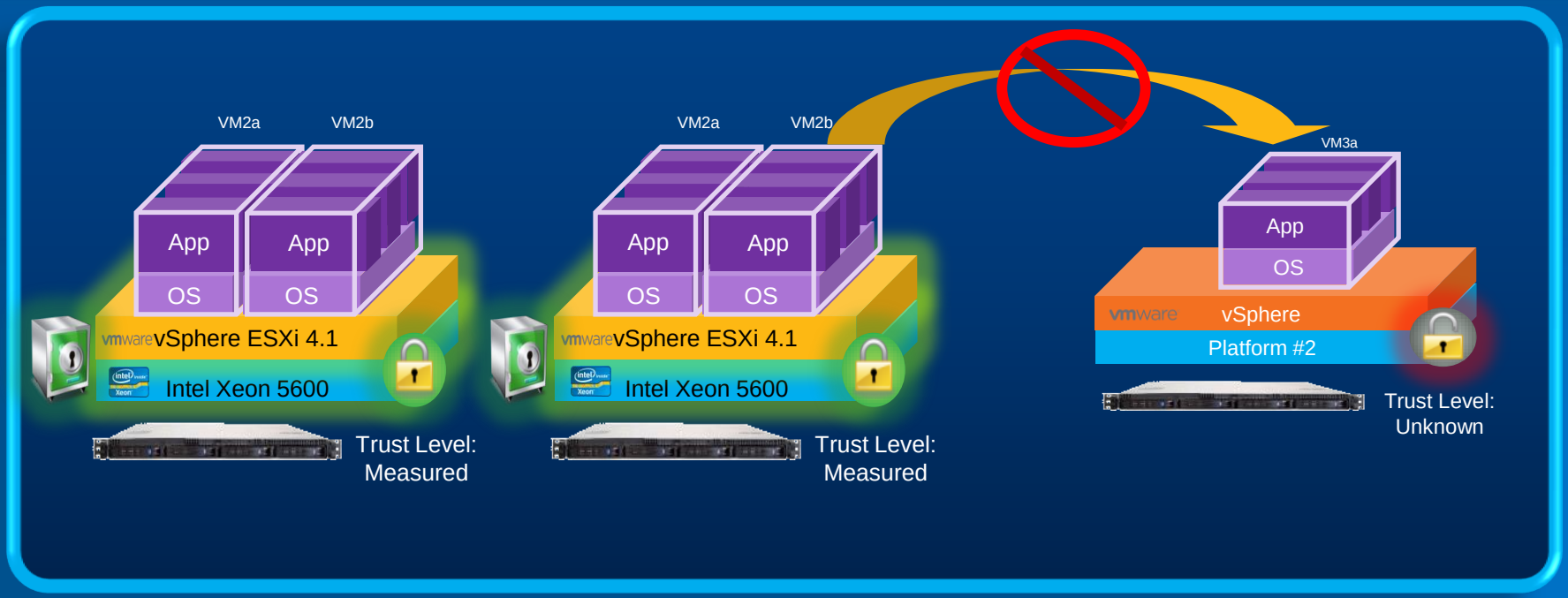
Intel® Cloud Builders Reference architecture

Intel-VMware*-HyTrust* Enables Trusted Compute Pools

Request from console to migrate VM 2b to Platform 2

Policy check: VM2b requires trusted platform

Fail Policy Stop Move Report error



Visit Intel® Cloud Builders
www.intel.com/cloudbuilders

Easing Cloud Deployments via Proven, Interoperable Solutions for IT

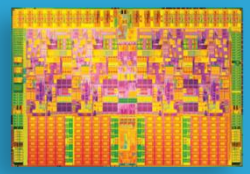
Evolution of Data Center Security

Intel Role: Become the foundation of data center security

Data Center Security
- Trustable tenants mobile perimeter
- Security policies move with mobile VMs

Trustable Infrastructure
- E2E protection with encryption
- Trustable VMs with verification

Platform Hardening & Acceleration
- Trustable launch
- Flexible encryption (storage, net)
- Mitigate attacks



2010-2011 | Future

Intel Has the Vision and Ability to Enable These Capabilities

Intel® Advanced Technologies

Security

Data Protection
Advanced Encryption Standard—New Instructions

Intel® AES-NI

Platform Security
Trusted Execution Technology

Intel® TXT

Resilience

High Availability
Mission Critical Class Reliability, Availability, and Serviceability

Advanced RAS

Service Delivery

Virtualization
Near-Native VM Perf. & Seamless VM Migration

Intel® VT
(CPU, Chipset, and I/O)

Intel® VT-x, Intel® VT-d and Intel® VT-c

Performance

Automatically Adapt to the Workload

Intel® Hyper-Threading

Intel® Turbo Boost

Power

Processor Power

Integrated Power Gates *and* **Automated Low Power States**

System Power

Intel® Intelligent Power Node Manager

Data Center Power

Intel® Data Center Manager

Different Technologies Optimized for Different Needs

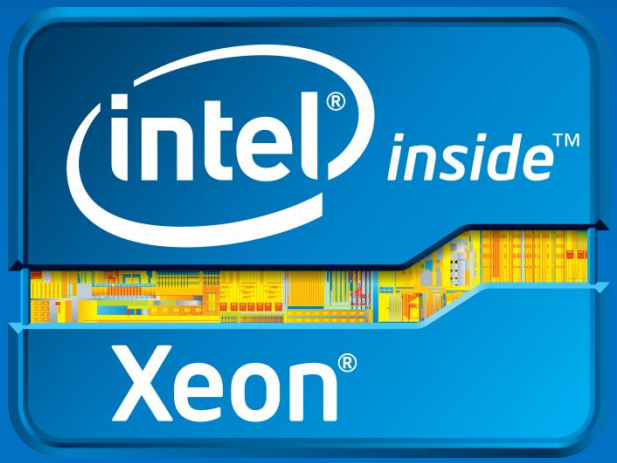

intel®

Intel® Xeon® Processor Family

An Intelligent Choice for Virtualization

Intel® Xeon® processor 5600:
Mainstream 2S platform for cloud computing

- Excellent Energy Efficient Performance
  - Up to 60% faster than previous generation[2]
  - Up to 30% lower power[1]
- Great for web apps, core IT infrastructure, virtualization, small/mid scale DBs, and more
- Intel® Virtualization Technology (Intel® VT) & Security features to enhance data protection



1Source: Fujitsu Performance measurements comparing Xeon L5650 vs X5570 SKUs using SPECint_rate_base2006. See http://docs.ts.fujitsu.com/dl.aspx?id=0140b19d-56e3-4b24-a01e-26b8a80cfe53and http://docs.ts.fujitsu.com/dl.aspx?id=4af74e10-24b1-4cf8-bb3b-9c4f5f177389
2Source: Internal Intel measurements for Xeon® X5680 vs. Xeon® X5570 on BlackScholes*.

Intel® Xeon® Processor Family

An Intelligent Choice for Virtualization

Intel® Xeon™ Processor E7 Family:
For the Most Demanding Workloads

- 2 - 8S+ platforms with leadership performance
- Scalable Performance, Advanced Reliability, Large Memory
- Large Scale, Mission Critical Virtualization
- Great for large databases, ERP, BI, among others
- Intel® VT and Security features to enhance data protection