IBM Power sistemler'de Güvenlik: PowerSC

Security and compliance for Power Systems

Kadri Aksoy, İş Geliştirme Yöneticisi CEE

Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

PowerSC™

20 Years of IBM RISC Technology Leadership

Commercial & Technical Workloads

Virtualization Technologies

Enhanced SMT Support

POWER7

POWER6

POWER5

POWER4

RS64
POWER3

PowerPC

RISC
POWER1

Performance Leadership

Reliability / Availability / Serviceability

1990

2010

Power Family supports all Power System servers...

Power 795

Power 780

Select from the broadest system portfolio in the industry

- The highest performance, most scalable UNIX system ever
- Modular footprints enable seamless growth
- The best selection of Entry servers and Blades for Linux

Power 770

POWER7™
BUILT ON
7
Power™

Power 750

Power 720/740

Power 775

Power 710/730

Power 7R2 Linux box

PS Blades

HMC & SDMC

PowerVM

IBM® Systems Director

redhat

suse

Linux

AIX

i for Business

Power 755

Where to find more information on Power Servers:

http://www.ibm.com/developerworks/wikis/display/LinuxP/Performance+FAQs#PerformanceFAQs-WheredoIfindreferenceinformationonthePOWER7systems

Power your planet.

Workload-Optimizing Systems

+

- Management
- Energy
- Security
- Availability
- Operating Systems
- Virtualization

IBM® Systems Software

AIX - The Future of UNIX

Total Integration with i

Scalable Linux ready for x86 Consolidation

PowerVM™

Virtualization without Limits
✓ **Drive over 90% utilization**
✓ **Dynamically scale per demand**

POWER7™ BUILT ON Power™

Dynamic Energy Optimization
✓ **70-90% energy cost reduction**
✓ **EnergyScale™ technologies**

PowerHA™

Resiliency without Downtime
✓ **Roadmap to continuous availability**
✓ **High availability systems & scaling**

IBM® Systems Director

Management with Automation
✓ **VMControl to manage virtualization**
✓ **Automation to reduce task time**

IBM's history of virtualization leadership

A 40-year tradition culminates with PowerVM

PowerVM™

| 1967	1973	1987	1999	2004	2007	2008
IBM develops **hypervisor** that would become VM on the mainframe	IBM announces first machines to do **physical partitioning**	IBM announces **LPAR on the mainframe**	IBM announces **LPAR** on POWER™	IBM intro's POWER Hypervisor ™ for System p and System i	IBM announces POWER6™, **the first UNIX servers with Live Partition Mobility**	**IBM announces PowerVM**

2011 Security Market - $50.7Billion

Figure 1. Enterprise Security Infrastructure Market by Segment, Worldwide, 2011 (Billions of U.S. Dollars)

- Security Software 13.9
- Security Services 28.2
- Network Security Equipment 8.6
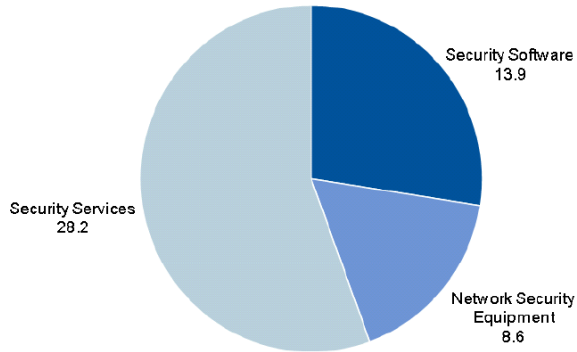
Source: Gartner (January 2011)

Annual Threat Assessment of the
US Intelligence Community
for the Senate Select Committee on Intelligence

Dennis C. Blair
Director of National Intelligence

February 2,

Compliance $29.9Billion

- AMR - North American Companies expected to spend $29.9B on regulatory compliance and will spend $8.8B on technology solutions to solve their compliance requirements.
- Forrester Research Approximately 6% to 11% of a company's overall IT spending will go to security.

Cyber Crime $100 Billion

- U.S. Department of Justice estimates financial losses from cyber crime at $100 Billion.

- US Intelligence Annual Threat Assessment - 2010
- Number 1: *"Far-Reaching Impact of the Cyber Threat"*

Bloomberg

- Carbon Thieves Force European Union to Improve Security, Close Spot Market

Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba
Grand Hyatt İstanbul

What are the Key Customer Pains?

1. Control cost, increase operational efficiency and innovate

- Organizations are keen to take advantage of cost savings opportunities, including new computing architectures such as the cloud, virtualization, etc However, these new models can increase risk substantially without the proper controls and visibility in place. With years of proven innovation, IBM allows you to enable new business initiatives and opportunities where trust risk converge.

2. Keep IT infrastructure and information safe from threats

- At the most basic level, IT teams need to "keep the lights on" and a key aspect of this is maintaining the security, privacy, and availability of business assets. The more easily organizations can "operationalize" security throughout the entire lifecycle of their data, applications, systems, networks, processes and personnel, the better their overall security posture will be. IBM allows you to increase the resiliency of the data, systems, applications, networks, and devices that enable your business to operate.

Stay Ahead of the Threat

X FORCE

And, don't forget...

What are the Key Customer Pains?

3. Maintain and demonstrate compliance

- Managing varied and dynamic regulatory requirements requires accurate, reliable visibility and comprehensive reporting – in order to stay ahead of both the threat and the auditor. In addition to enabling new innovation and maintaining the security, privacy and availability of critical business assets, IT organizations still need to prove it. IBM allows you to put security processes in place (people, technology) to meet and report on compliance guidelines outlined by legal and industry requirements.

Security Standards Help Target Customers

To Whom Does Payment Card Industry(PCI) Data Security Standard Apply?

> **All merchants & service providers that store, process, use, or transmit *cardholder data***

- **Retail** (e commerce & brick & mortar)
- **Hospitality** (restaurants, hotel chains, etc.)
- **Convenience Stores** (gas stations, fast food)
- **Transportation** (i.e. airlines, car rental, etc.)
- **Financial Services** (credit processors, banks, insurance)
- **Healthcare/Education** (hospitals, universities)
- **Government** (where payment cards are accepted)

To Whom Does the following standards apply to?

- DOD STIG – US Department of Defense

- Sarbanes Oxley (usually implemented using COBIT best practices) – All public companies that have registered securities with US Securities and Exchange

PowerSC

- PowerSC provides a **security** and **compliance** solution designed to protect data centers virtualized with PowerVM **enabling** Higher Quality Services.
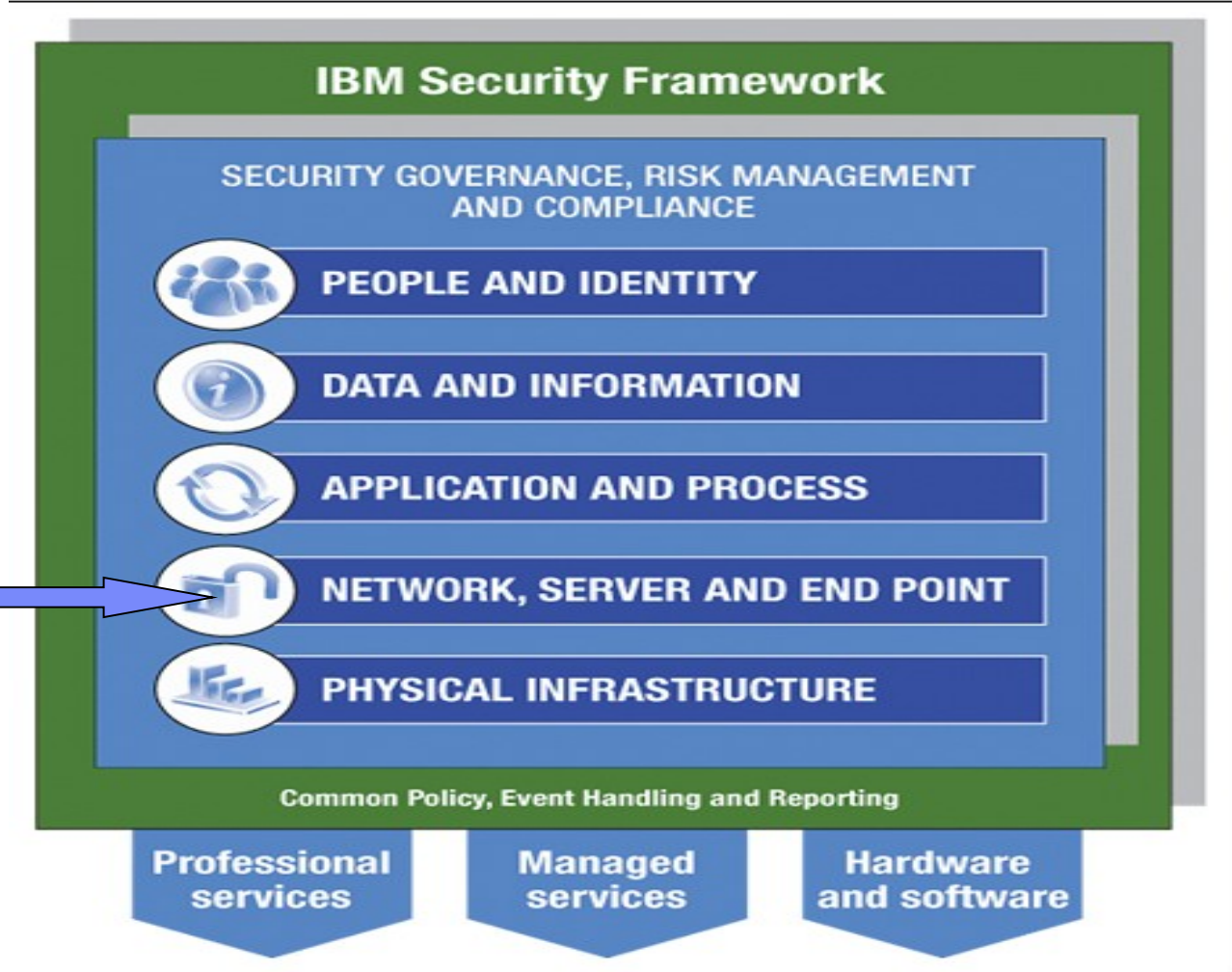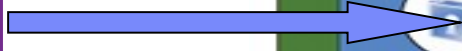
Client Benefits

- *Simplifies management and measurement of security & compliance*

- *Reduces cost of security & compliance*

- *Improves detection and reporting of security exposures*

- *Improves the audit capability to satisfy reporting requirements*

- *Provides "virtualization aware" security extensions*

Where Does PowerSC Fit within the IBM Security Framework?

PowerSC provides

• Additional Security and Compliance Specifically for Power Systems

• Focused on the AIX Operating System and Hypervisor

PowerSC™

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

PowerSC Features

PowerSC provides a security and compliance solution to protect datacenters virtualized with PowerVM enabling higher quality services

Business Requirements

- Compliance and Audit

- Guarantee that the OS has not been hacked or compromised in any way

- Ensure that every Virtual System has appropriate security patches

- Compliance and Audit to External Standards

Trusted Logging
The SVM/VIOS capture all LPAR audit log information in real time.

Trusted Boot
Boot images and OS are cryptographically signed and validated using a virtual Trusted Platform Module (vTPM)

Trusted Network Connect and Patch Management
With the Trusted Network Connection protocol imbedded in the VIOS, we can detect any system attempting to access the network and determine if it is at the correct security patch and update level.

Security Compliance Automation
Pre-built compliance profiles that match various industry standards such as Payment Card Industry, DOD and Sox/Cobit. Activated and Reported on centrally using AIX Profile Manager

Capabilities

- ✓ Tamper-proof logs

- ✓ Defense against tampering

- ✓ Notification of unpatched systems

- ✓ Compliance automation and reporting

Entegre Servis Yönetimi ve Güvenlik Çözümleri

PowerSC Moves to "Known Good Model"
Only Allow Known Trusted Software to Run

- Security Vulnerability Detection tends to work on a "**Known Bad Model**" This is the way intrusions have been blocked based on historical break-ins

- With features like PowerSC Trusted Boot, this model is being switched to a "**Known Good Model**" which only allows trusted systems to run. This can only be done with a **tight interlock** between the hardware, virtualization and software.