

Project	4027_B IBM STG PowerEnterpriseSystems SatyaSharma
Document Title	4027_B_IBM_STG_PowerEnterpriseSystems_SatyaSharma_ AsProduced_Transcript_120312
Date	12/03/2012
Client	IBM
Centerline Leads	Lauren Childs, Senior Project Manager

## **4027\_B Power Enterprise Systems - Satya Sharma – As Produced Transcript**

Our clients are very focused around three major issues in IT: Cloud, Data and Security. And while all of these topics are crucial for success in this new information era, I would like to spend a little time focusing on Security and how IBM Power Systems are addressing the need to protect the huge growth in customer data and to streamline compliance for increased regulation.

As organizations offer more and more digital services to customers – online and over mobile and social channels – they're also creating new vulnerabilities. Meanwhile, attacks are becoming more sophisticated, average corporate IT infrastructure is attacked nearly 60,000 times a day and the average total cost of a single data breach to an organization is over \$5 million dollars – with some breaches costing organizations in the hundreds of millions of dollars.

And of course, there's the damage to a business's reputation which can affect customer loyalty--and the company's share price--for years. We've even seen cases where companies have gone bankrupt within two months of being breached. So security really is a make or break for your organization.

IBM Power systems are designed to the highest level of security standards. They address security at all levels: from high performance encryption in the systems to management that ensures that applications are trusted as well as the network, and into the database to ensure that data is secured.

Let me start by highlighting the built-in PowerVM virtualization fault/security isolation. I call it the Coke/Pepsi standard. What do I mean by that? What I mean by that is that our isolation is so good that two different fierce competitors can run on the same system, as if they are running on two separate systems. This capability is vital for cloud and multi-tenant IT environments, as well enterprise customers, as they deploy a mix of test and production or mix multiple workloads on a shared infrastructure.



Power Systems have an excellent track record when it comes to security vulnerabilities.

The security issues result in greater labor cost to constantly apply security fixes as well as disruption to the operations. In the highly virtualized world, these costs can really multiply because of the explosion in the number of operating system images.

In our newest Power System offerings, we are enhancing security even further with our crypto hardware accelerator in the Power7+ systems. In the past, organizations had to choose which data to encrypt because there was a performance impact from encryption.

Our new Crypto accelerator is designed to reduce the performance overhead with encryption and decryption operations so you can encrypt more of your data, meet service levels, and reduce impact on application performance.

We have built-in exploitation of the crypto accelerator in AIX Encrypted File System and IPSec capabilities. This accelerator is also available to ISVs, software providers, and customers. Our objective behind developing the crypto accelerator is to increase adoption of encryption in the market place.

Organizations are also dealing with the complexity and the costs of complying with increased industry and government regulations. PowerSC, which stands for Power Security and Compliance, has capabilities to cost-effectively assure compliance.

- The first capability is Security Compliance Automation. Regulatory compliance requires setting security on systems in a uniform manner so they comply to various industry standards. This process can be tedious, time consuming and error prone. Security Compliance Automation provides pre-built profiles that are certified to comply with industry standards like the Payment Card Industry. Benefits of this are labor cost reduction associated with ensuring compliance as well as centralized reporting on an ongoing basis to demonstrate compliance to standards for auditing purposes. This enables customers to go through audit processes with great ease.
- Next, our Trusted Firewall capability provides network isolation and firewall services between Virtual Machines as traffic flows from VM to VM. This capability eliminates the need for sending traffic externally to enforce firewall rules.
- And third, our Trusted Boot capability provides a Virtual Trusted Platform Module for Virtual Machines. It ensures that system images have not been altered either accidentally or maliciously.



Our new Power Systems offerings bring substantial enhancements to PowerSC to bolster compliance even further:

- First, Trusted Surveyor Product provides an independent audit of virtualized network landscapes against defined network segregation and isolation compliance policies. This gives clients the ability to monitor configuration drift automatically.
- Second, we have added a healthcare industry HIPAA compliance profile to simplify configuration and reduce cost of compliance for systems that must adhere to HIPAA standards.
- And third, real time compliance monitoring sends alerts to administrators when systems are out of compliance. These alerts can take the form of email, SMS messages, or any other forms of communication including integration with IBM QRadar product.

Beyond PowerSC, the AIX operating system has role-based access control capabilities which enable custom roles such as “DBA”, so root access isn't required for many of the tasks.

In summary, CIOs have identified Enterprise Risk Management as a key issue for their companies. Power and AIX security capabilities are designed to alleviate this risk. They also reduce the labor cost component associated with ensuring security compliance.

Finally, in this age of cloud computing, security capabilities take on added importance.

Power offers highly differentiated security capabilities, which customers will not find in other industry platforms. It is our intent and commitment to lead in the market place with future security innovations, ensuring Power Systems' position as a compelling security platform, including making use of advanced security analytics like IBM QRadar.