

Service Management Storage Encryption

“Must Have” Security for Service Organizations

Gartner projects that 85 percent of large enterprises will initiate data-at-rest encryption projects by mid-2006.

Service Organizations Held to a Higher Standard

Outsourced service providers keep the global economy turning by providing critical technological underpinnings – hosting, transacting, aggregating, and storing everything from market trades and credit card payments to healthcare records and federal tax returns. Given that many service organizations provide cross-industry solutions, they are bound by a dizzying array of mandated data privacy regulations.

Think of a security directive (i.e., GLBA, HIPAA, Sarbanes-Oxley, NIST/FISMA, PCI, DPEC, and Basel II) and service organizations must be prepared to meet it and all others with a pragmatic and comprehensive security strategy. Usually, they are also required to meet security service-level agreements and SAS 70 Type II, SysTrust, and ISO 17799 auditing standards that hold them to an even higher standard than the customers they represent. Now, with the latest round of privacy legislation (i.e., CA SB 1386, NY ISBNA), service organizations – and their customers – must publicly disclose security risks and subsequent actions taken, even if they so much as *suspect* a security breach. The new legislation ups the ante that much more, significantly increasing the demand for security.

Security Becomes a Business Differentiator

All of these factors have made security an important business differentiator for service organizations. Take Payformance

Corporation, a provider of electronic payment processing services to the banking, health-care, insurance, and retail industries. “Confidentiality is a big priority for our customers...and data privacy regulations are only going to become stricter over time,” noted George Betancourt, information security officer at Payformance. “We need a secure technology infrastructure that will support today’s regulations as well as tomorrow’s.” Service organizations must consider not only regulations and customer trust but also liability issues. Brent Luckman, CEO of Transend Business Services, an organization that provides Web-based managed business transaction services, explains, “Our customers, who are liable for the security of their own customers’ information, pass that liability on to us.”

Storage Encryption: The New Line of Defense

These days, everyone is lining up to implement encryption because it not only meets mandated requirements for both backup media and networked storage but also significantly minimizes the risks and liabilities associated with both internal and external security breaches. In fact, Gartner has increased its forecast to project that “by the second quarter of 2006, 85 percent of large enterprises will initiate data-at-rest encryption projects in response to regulatory compliance or industry initiatives.”¹



¹ Use the Three Laws of Encryption to Properly Protect Data, Rich Mogull, Gartner, August 2005.

The NeoScale CryptoStor® storage security appliances for tape, virtual tape, disk, and Fibre Channel link encryption offer:

True Wire-Speed Encryption

The custom hardware data path used by purpose-built NeoScale CryptoStor storage security appliances ensures true wire-speed performance – providing virtually no latency delays and minimal response time impact.

Certified FIPS 140-2 Level 3 Security

NeoScale delivers the only storage security appliances with top-to-bottom, appliance-level FIPS 140-2 Level 3 certification. FIPS security extends from hardware components to the operating system and reaches out to system-level user-access control and key management features for both primary storage and SAN extension applications.

Global Key Management

NeoScale appliances automate and simplify encryption key security for global data storage. Comprehensive key management tools and centralized key archival make distributed information recovery simple and easy. Automation avoids inappropriate use of encryption technologies.

Local and Remote Clustering

NeoScale clustering supports highly available access to secure information via redundant network paths. In the event of a failure, data remains accessible – without any manual re-configuration – and can be recovered anywhere, via any clustered appliance.

Certified Multi-Vendor Interoperability

NeoScale certifies industry-leading solution partners, including EMC, SUN/STK, IBM, and HP, to ensure integrated products and solutions.

Lowest Cost; Lowest Operating Impact

NeoScale innovations reduce deployment risks, minimize ongoing operational complexities, and are available at the lowest possible price point.

“Every time I read in the news about identity thefts or lost backup tapes, it makes me wonder why any company entrusted to protect sensitive data would neglect to encrypt that data,” Payformance’s Betencourt observed. Service organizations like Payformance and Transend demand a security strategy that fully encompasses data encryption best practices, like centralized encryption key management, access control, and authentication. These companies turn to NeoScale Systems, Inc., the industry leader in enterprise storage security, for security solutions that meet the higher standards they face.

NeoScale Solutions — Seamless. Reliable. Secure.

NeoScale delivers a range of storage security appliances that automate encryption of data headed to storage and decryption of data headed to applications, making stored data unreadable to unauthorized users. Using NeoScale’s centralized management features, service organizations can ensure that encryption keys, access controls, and authentication are customized to each customer’s needs.

NeoScale’s CryptoStor® storage security appliances make it possible to consolidate the storage infrastructure while at the same time isolating each customer’s information, thereby ensuring that only the right information is available to the right people in the right way.

Protection Without Crippling Complexities

IT professionals are justifiably concerned about the complexities that encryption can impose on transaction processing performance and the storage infrastruc-

ture. However, CryptoStor storage security appliances are purpose-built, providing ubiquitous, immediate, and transparent protection of storage data regardless of application, transport, media type, or location – with virtually no latency delays and minimal impact on response time. They securely automate the transfer and recovery of information from primary and secondary storage, while minimizing operational complexity at the lowest possible cost. Easy to deploy, NeoScale CryptoStor enterprise-class solutions offer high-speed security that can selectively compress, encrypt, and authenticate data.

NeoScale Customers Save Costs Across the Board

With NeoScale solutions, service organizations like Payformance and Transend save by decreasing both risk and liability. Transend’s Luckman succinctly illustrates the point: “By implementing NeoScale storage security appliances, we cut our product and services liability with a major Canadian bank from \$1 million down to \$100,000.”

Find Out More

Find out more about how NeoScale solutions can provide a complete encryption solution, with the lowest operational impact and at the lowest total cost. Visit us on the Web at www.neoscale.com or contact us at 1-408-473-1303.



Copyright © 2006 by NeoScale Systems, Inc. All rights reserved. NeoScale, the NeoScale logo, and CryptoStor are registered trademarks of NeoScale Systems, Inc. All other names and/or trademarks herein are the property of their respective owners.

Seamless. Reliable. Secure.