



By Annette Cormier
Mark Christenson
John McDonald

PROTECTING CRITICAL INFRASTRUCTURE AND MOBILE DATA: AN INFORMATION-CENTRIC SECURITY STRATEGY

Sharing data among internal IT environments, mobile users, and applications or remote monitoring systems outside the firewall can expose organizations to multiple points of vulnerability. Dell, EMC, and RSA have teamed up to provide an efficient and flexible information-centric security strategy spanning the enterprise infrastructure from client laptops through applications and storage systems.

The ability to integrate and share data across multiple systems and networks is a necessity in today's data centers. Global IT command centers rely on merged networks, shared data, and rapid communications for IT operations, business intelligence, and emergency response. Web 2.0 technologies such as Twitter and blogs, combined with citizen journalists and mobile phones, are making it possible to enhance disaster response with rapid information sharing and levels of detail not previously available. Additionally, IT operations staff may need to connect their enterprise networks to separate networks, including plant-based process control networks (PCNs) and outsourced supplier networks for supply chain management and hosted e-business applications.

Efficient business intelligence and emergency operations often depend on hybrid networks that include a variety of technologies and protocols. These hybrids may bring together IP-based enterprise networks; satellite, voice, and video communication networks; PCNs used in utilities and chemical manufacturing for linking systems based on supervisory control and data acquisition (SCADA), human-machine interface (HMI) systems, and programmable logic controller (PLC) technologies; and wireless networking for remote mobile workers such as utility operators, field engineers, or military ground troops.

For example, many gas and electrical utility companies connect plant PCNs to business networks to enable efficient integrated management and accelerate the coordination of communications to restore plant shutdowns caused by natural disasters or turbine failures. Equipment manufacturers may connect business networks to supply chain automation solutions outside the firewall to share a common dashboard, to make rapid updates in pricing and inventory availability, or to facilitate commodity trading. Closed-circuit television is often transmitted wirelessly and utilized for monitoring traffic flows on highways, allowing visitors in zoos to observe newborn animals without disturbing them, and enhancing safety at public transportation facilities.

This connectivity enables increasingly efficient operations but can open up multiple points of vulnerability in the infrastructure, creating a complex set of security requirements. PCNs and legacy networks, in particular, are inherently insecure because of specialized infrastructures that cannot be patched or are too costly to replace. PCN vulnerability to cyberattacks could have devastating consequences—for example, endangering public health and safety if there is interruption in chemical processing or electric grid transmission. Many recognized security threats affect a variety of industries and individuals, including

organized e-fraud gangs, man-in-the-middle and zero-day attacks, and a host of other threats. And, of course, simply losing a laptop with confidential information can be highly detrimental.

DISCOVERING THE VULNERABILITIES OF THE CLOUD

New security challenges are now appearing in the computing cloud, such as hyper-jacking, virtual machine jumping, and guest hopping. Malware projects such as SubVirt, virtual machine rootkits, and Blue Pill capitalize on virtualization technology to create an ultra-thin hypervisor that takes control of the underlying OS.

Adding to the security complexity of today's environments, organizations must also meet a growing number of standards to help protect confidential data. These standards include requirements from the Payment Card Industry Data Security Standard (PCI DSS), the U.S. National Institute of Standards and Technology (NIST), the U.S. Federal Energy Regulatory Commission/North American Electric Reliability Corporation (FERC/NERC), the Sarbanes-Oxley Act (SOX), and others.

At the same time, traditional perimeter security measures have reduced effectiveness, can be ineffective when zero-day attacks occur, and have become increasingly difficult to scale with the constantly evolving security attack vectors and universal expansion of information sharing across the enterprise and beyond the firewall.

SAFEGUARDING INFORMATION WHEREVER IT IS LOCATED

Taken together, these factors are driving many organizations to adopt an information-centric security approach designed to protect data at rest, data in motion, and data in use (see Figure 1). Solutions for security include verified launch and secure root of trust technologies, segmentation techniques, hardening of infrastructure and data, encryption, software patching, and solutions for monitoring and management. In addition, a backup of data is a minimum

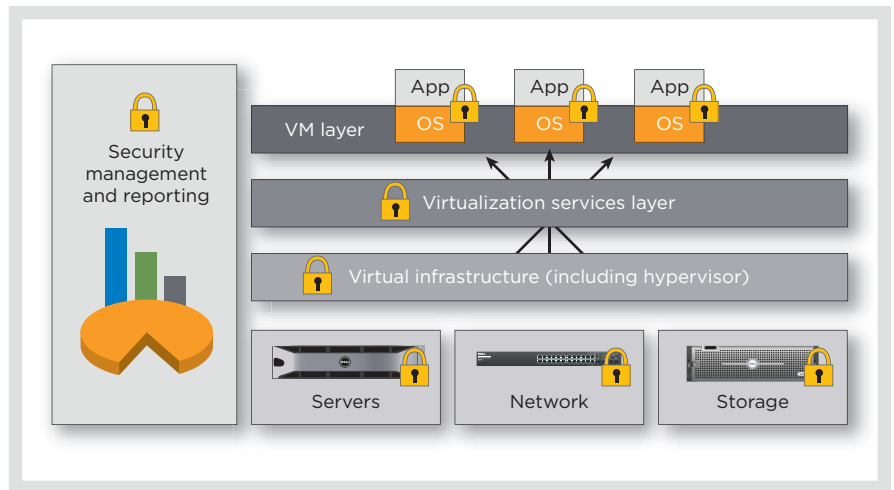


Figure 1. Driving information security enforcement throughout the infrastructure

requirement to enable rapid recovery from downtime caused by a security breach.

Dell, EMC, and RSA have teamed up to deliver an information-centric security strategy that spans the infrastructure from client laptops, through network applications, to the storage systems where data ultimately resides at rest. In this multilayered model, Dell/EMC CX4 Series storage area network (SAN) arrays, Dell™ NX4 network attached storage (NAS) devices, and EMC® Celerra® unified storage systems provide storage-based security with extensive security certifications. EMC RecoverPoint™ data protection software offers automated backup and rapid recovery of data. EMC PowerPath® Encryption with RSA software and RSA security appliances provide host and application security and encryption. And client security features are provided by the Dell ControlVault™ utility, which is embedded in Dell Latitude™ laptops.

ESTABLISHING A FOUNDATION WITH STORAGE-BASED SECURITY

The information-centric security strategy begins with a secure storage management network topology, leveraging the security features in Dell/EMC CX4 Series SAN arrays, Dell NX4 NAS devices, and EMC Celerra NS-120 NAS systems (see Figure 2). EMC storage is designed to

meet Common Criteria for Information Technology Security Evaluation (ISO 15408) global security standards. Also, internal EMC policy mandates 80 distinct security-focused requirements for EMC hardware and software, including support for advanced security functions such as IP version 6 (IPv6) and IP Security (IPsec). These requirements ease integration into existing security infrastructures and provide a common security implementation across Dell and EMC storage systems that implement EMC security technologies (see Figure 3).

Security capabilities of Dell/EMC CX4 Series SAN arrays

Organizations using Dell/EMC CX4 Series SAN arrays can benefit from a variety of built-in security features. Standard authentication mechanisms are provided for both the EMC Navisphere® Manager software's graphical user interface and Navisphere Command-Line Interface (CLI) through encrypted, authenticated communications. Administrators must provide valid Navisphere Manager credentials, including username and password, to conduct storage system management operations. Authorized users can be authenticated using Lightweight Directory Access Protocol (LDAP) or the Microsoft® Active Directory® directory service, the Microsoft implementation of LDAP.

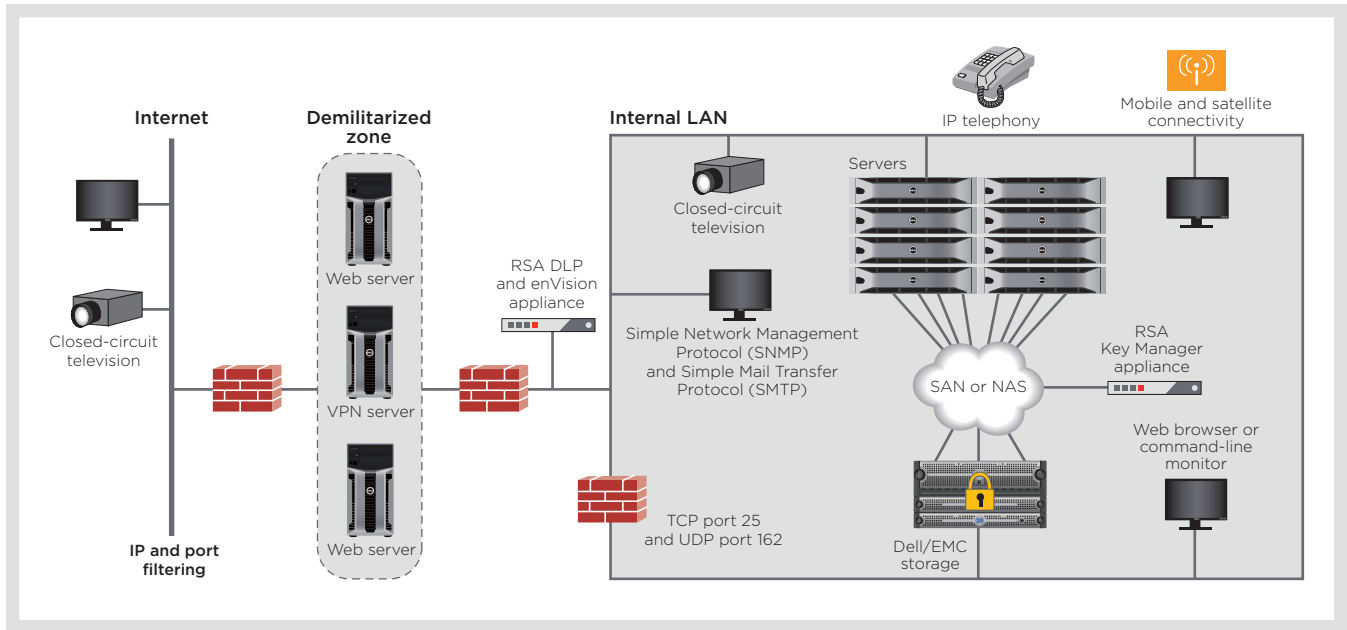


Figure 2. Deploying a highly secure storage management network topology

Navisphere Manager is designed to authorize user actions based on the role associated with the authenticated user. Each role has different access privileges for data and functions, providing account administrators with a tool to help simplify assigning access rights. Roles include administrator, security administrator, manager, monitoring, recovery, replication, and local replication only. Navisphere Manager also provides 256-bit symmetric data encryption using the RSA algorithm, which helps deliver the same level of cryptographic strength as is employed in e-commerce.

When a client connects to a server over the network, it is important that the client can verify the identity of the server—otherwise, any node on the network can potentially impersonate the server and extract information from the client, which is also known as a man-in-the-middle attack. Navisphere Manager uses Public Key Infrastructure (PKI) cryptography to help verify the identity of the Dell/EMC CX4 Series array when a client connects. Each Dell/EMC CX4 Series array processor contains a PKI certificate with a corresponding public key that is presented to the client.

Audit information for Dell/EMC CX4 Series arrays is contained within an event log for each storage processor. Navisphere Manager creates a detailed event log each time a user logs in, enters a request, or executes a command. Using this record, checks for suspicious activity can be performed periodically and the scope of activity can be determined, enabling the organization to take appropriate action.

Security features of Dell NX4 and EMC Celerra NS-120 NAS systems

EMC Celerra Manager provides security available in Dell NX4 and EMC Celerra NS-120 NAS systems, starting with industry-standard authentication. Protection for Microsoft Windows® files includes Microsoft NT LAN Manager (NTLM and NTLMv2), NTLM Security Support Provider (NTLMSSP), and Server Message Block (SMB) signing. Protection for Linux® and UNIX® OS files includes Kerberos, Network File System version 4 (NFSv4), and secure NFS protocols.

Like Navisphere Manager, Celerra Manager provides granular, role-based authorization. Administrative roles defined in Celerra Manager are system administrator, security administrator, and operator,

and custom roles can also be defined. Flexible password management includes features such as minimum required length and complexity, and password expiration.

A separate management processor also helps limit access to data stored on Dell NX4 and EMC Celerra NS-120 systems. Administrators communicate only with the Control Station software available in these systems, and independent data movers then respond to Control Station management requests. Actions can be controlled by a defined set of management functions.

Multilevel privacy is built into Dell NX4 and EMC Celerra NS-120 systems. The proprietary Data Access in Real Time (DART) OS is designed to be immune to Windows and UNIX vulnerabilities. Celerra Manager is network protected with Secure HTTP (S-HTTP) for secure remote management; it checks for a valid session token and then tears down the token after a session is ended. Celerra CLI is network protected with Secure Shell (SSH) for secure remote management; it provides an encrypted session, and access is restricted to authorized clients or systems.

For auditing purposes, an event log is created each time a user logs in, enters

a request, or executes a command. Celerra Manager also supports virtual LANs (VLANs) to help secure data networks. VLANs provide a limited broadcast domain, helping reduce potential eavesdropping. Administrators can restrict traffic to specific ports and restrict access based on user ID.

BUILDING OUT THE SOLUTION WITH HOST AND APPLICATION SECURITY

To provide the next layer of protection in the information-centric model, Dell/EMC CX4 Series SAN arrays, Dell NX4 NAS devices, and EMC Celerra NS-120 NAS systems can leverage the capabilities of EMC PowerPath Encryption with RSA software, EMC RecoverPoint appliances, the RSA Key Manager (RKM) Suite, RSA enVision appliances, and the RSA Data Loss Prevention (DLP) Suite.

EMC PowerPath Encryption for data protection

EMC PowerPath Encryption provides host-based encryption for data at rest on disks, helping protect data against unauthorized access if a disk drive or array is removed from the system. It encrypts and decrypts data at the host, as the data moves to and from the array. The solution helps protect against unauthorized access or inadvertent loss of unprotected information through malicious attacks and spoofing of Fibre Channel hosts, and is designed to make information inaccessible in the event of physical theft of drives from the data center.

Data recovery and backup solutions are a key part of an effective security strategy to enable rapid recovery from downtime caused by security breaches such as zero-day attacks and hard drive theft. EMC RecoverPoint offers a unified

solution to help protect and/or replicate data on storage systems by providing synchronous and asynchronous local and remote replication and continuous data protection for point-in-time recovery. Using PowerPath Encryption in conjunction with backup software, encrypted data can be copied synchronously or asynchronously to a disaster recovery site and remain protected regardless of where it resides.

RSA Key Manager to help simplify the key life cycle

RKM for the Datacenter provides a module that supports PowerPath Encryption. This module enables centralized enterprise key management for a consistent encryption methodology in mixed environments and helps simplify key management scalability as the organization grows.

	Secure access	Secure data	Secure audit
Dell/EMC CX4 Series SAN arrays	<ul style="list-style-type: none"> Secure remote support gateway LDAP and Microsoft Active Directory authentication Internet SCSI (iSCSI) Challenge Handshake Authentication Protocol (CHAP) Logical unit (LUN) masking Role-based accounts Management domains Secure administrator IP address filtering 	<ul style="list-style-type: none"> EMC Certified Data Erasure Service Secure Sockets Layer (SSL) in EMC Navisphere Manager Secure CLI Secure remote support Encryption with PowerPath 	<ul style="list-style-type: none"> Secure audit log RSA enVision integration
Dell NX4 NAS devices and EMC Celerra NS-120 NAS systems	<ul style="list-style-type: none"> Secure remote support gateway LDAP and Microsoft Active Directory authentication iSCSI CHAP LUN masking Kerberos Secure management access NAS access control lists (ACLs) and locking Password management 	<ul style="list-style-type: none"> EMC Certified Data Erasure Service File retention write once, read many (WORM) File extension filtering Secure NFS Antivirus integration 	
EMC Symmetrix DMX™ arrays	<ul style="list-style-type: none"> Secure remote support gateway LDAP and Microsoft Active Directory authentication iSCSI CHAP LUN masking Role-based accounts Kerberos (SymCLI) System identifier (SID) lockdown EMC Symmetrix® access control Service credential 	<ul style="list-style-type: none"> EMC Certified Data Erasure Service Integrated data erasure (EMC Enginuity™ 5772 OS) SSL in console and CLI Encryption with EMC PowerPath 	
EMC Centera® storage	<ul style="list-style-type: none"> Secure remote support gateway Access profiles Role-based access (management profiles) Cluster locking 	<ul style="list-style-type: none"> EMC Certified Data Erasure Service Data shredding WORM File retention 	
EMC ControlCenter® storage management software	<ul style="list-style-type: none"> LDAP and Microsoft Active Directory authentication Role-based management Fine-grained access control 	<ul style="list-style-type: none"> SSL encryption 	<ul style="list-style-type: none"> Comprehensive auditing Secure audit log

Figure 3. Implementing security features across Dell and EMC storage

“The information-centric security strategy begins with a secure storage management network topology, leveraging the security features in Dell/EMC CX4 Series SAN arrays, Dell NX4 NAS devices, and EMC Celerra NS-120 NAS systems.”

The importance of controlling security keys becomes clear when disaster strikes. For example, if an organization's primary site burns down, the fire may destroy the DVD holding the organization's keys. When the IT team subsequently seeks to recover data at its disaster recovery site, the team would not be able to access data stored on encrypted backup tapes because the encryption keys are not available to decrypt the tapes. Another use case for enhanced key management includes simplifying support and maintenance of heterogeneous and legacy infrastructures. In legacy and new technologies, each application and OS may create its own keys, which can get lost because of staff turnover or aging systems.

The RKM appliance is designed to simplify the implementation, management, and availability of encryption keys throughout the life cycles of disparate applications, operating systems, and infrastructure. RKM provides functionality such as remote replication of keys to a disaster recovery site, application-level authentication and authorization, secure key storage, audit logging of key management operations, and reporting of key use across applications.

RSA enVision appliances for threat monitoring and forensic analysis

Dell/EMC CX4 Series arrays, Dell NX4 NAS devices, and EMC Celerra NS-120 NAS systems can provide log file audit trails through integration with RSA

enVision to help simplify log management and forensic analysis and alerting. RSA enVision can collect log data from over 130 event sources from firewalls to databases, including syslog and custom or proprietary sources using standard transport protocols. The appliance compresses and encrypts log data so that it can be stored for later forensics analysis, while helping maintain data confidentiality and integrity.

RSA enVision is designed to analyze data in real time to check for anomalous behavior that requires an immediate response, and then optimizes logs for later reporting and forensic analysis. Built-in reports and alerts provide quick access to data that is easy to understand, and both standard and custom reports are available for compliance security including PCI DSS, SOX, and other compliance regulation modules.

RSA Data Loss Prevention for compliance and policy enforcement

The RSA DLP Suite is designed to give IT staff insight into the risk status and use trends of sensitive data across the enterprise based on policies, regardless of whether the data resides in a data center, on a network, or out at the endpoints. The suite helps safeguard data at rest by scanning across desktops, laptops, and file servers to locate and automatically monitor usage to provide protection of sensitive content. It also helps protect data in motion by tracking sensitive content

movement across networks, creating an audit trail, and automatically blocking or remediating policy violations. The suite also monitors the use of sensitive data, exclusive of the application and destination, and can block prohibited actions.

RSA Data Loss Prevention and enVision for combined deployment

Combining RSA DLP and enVision appliances helps fine-tune security and compliance policies based on actual use and needs from within an organization. To detect and audit sensitive data, IT organizations can first configure policies and content detection modules in DLP, and run an infrastructure security scan to identify risks. As events are generated, DLP forwards events and alerts to the enVision appliance. RSA enVision then correlates this information with existing forensics data. Feedback from that analysis can be used to fine-tune DLP policies to help ensure sensitive data is stored and used appropriately.

COMPLETING THE STRATEGY WITH CLIENT-BASED SECURITY

Many organizations need a mobile workforce with access to enterprise networks and sensitive data, and must be certain that only users with the proper credentials are logging on to the network. Remote users often cannot remember passwords and other security credentials, and should not carry them around in written form, but they still need the credentials to access data and do their jobs. Organizations can implement the required security using Dell Latitude laptops with Dell ControlVault software based on RSA SecureID. RSA and Dell have worked together to provide users of Latitude laptops with embedded technology for two-factor authentication to virtual private networks (VPNs), Microsoft Office Outlook® Web Access, Citrix® applications, and other network resources.

This solution offers the hardware-level security with the cost-effectiveness and convenience of a software token;

administrators no longer need to replace lost tokens, and end users benefit from a consolidated device. ControlVault is designed to keep passwords, biometric templates, and security codes within firmware and locked away from malicious attacks.

TYING THE SOLUTION TOGETHER WITH SECURITY ASSESSMENT SERVICES

Customized security assessment services can bring together the elements of an information-centric security strategy by establishing a common framework. Dell ProConsult and EMC services are available to help organizations define security policies, discover and classify sources of sensitive information across the infrastructure, and implement appropriate controls. Auditing services are available to help ensure and document compliance with security policies. Organizations can also have Dell ProSupport proactively support Dell/EMC CX4 Series, Dell NX4, and EMC Celerra NS-120 storage systems—including monitoring, notification, diagnosis, and repair.

UNIFYING SECURITY MANAGEMENT ACROSS THE INFRASTRUCTURE

The adoption of Web 2.0 and the integration of hybrid networks, combined with the need to enable an IT infrastructure that supports rapid disaster response, makes an effective, enterprise-wide

security strategy more important than ever. To help meet these needs, organizations are adopting an efficient, information-centric approach to data protection and security that authenticates, authorizes, and audits critical information assets and identities—helping to simplify the scalability of a secure architecture and streamline compliance.

Organizations looking to implement an information-centric security strategy may consider the multilayered protection provided by combined Dell, EMC, and RSA security capabilities designed to address today's increasingly complex security requirements. The ultimate goal of an information-centric security strategy is to help simplify deployment of security standards throughout the infrastructure stack—enabling efficient security management, forensic analysis, compliance, and data protection. 

Annette Cormier is a solutions marketing manager for Dell/EMC storage solutions. She has 20 years of experience in developing and bringing to market enterprise storage, network management, and security products for Dell, Hewlett-Packard, and SGI, and has previously been a SAS database programmer at Pacific Power and Light. Annette has a B.S. in Computer Science, Artificial Intelligence, from Colorado State University.

Mark Christenson is an EMC services partner manager for Dell/EMC solutions. He has

25 years of experience, including managing technical solution teams for enterprise infrastructure, security, and cloud services. As a tenure manager at EMC, and previously with EDS and Chase, he holds numerous industry certifications. Mark has a bachelor's degree from Ferris State University and a master's degree from Central Michigan University.

John McDonald is a security evangelist for RSA, where he is responsible for working with customers to design and deliver the EMC/RSA message and strategy. A Certified Information Systems Security Professional (CISSP), John has over 25 years of experience in the security industry, and has been actively involved with security at EMC and RSA for more than 9 years. Before joining EMC, he worked with several consulting companies performing security audits and security infrastructure design.



MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

Dell/EMC alliance:
DELL.COM/EMC

RSA, the Security Division of EMC:
www.rsa.com