

Customer Profile

EMC Corporation

EMC benefits from holistic, risk-based approach to IT security

Acceleration

“At EMC, information security is viewed as a business accelerator rather than an inhibitor. An Information Risk Management Strategy from our own Security Division – RSA, enables us to innovate, introducing business initiatives that balance risk and reward, helping us to maintain our leading position in the market.”

Roland Cloutier, VP and CSO, EMC

AT A GLANCE

Business Challenge

- Keep information secure across the enterprise, while implementing new initiatives that support business growth and aid competitive advantage
- Introduce an end-to-end security policy that is both proactive and holistic

Solution

- An Information Risk Management strategy from RSA based on a global risk framework
- Components include: information classification and discovery, controls on data, controls on access, and reporting audit and compliance
- RSA Access Manager®, RSA SecurID®, RSA Authentication Manager®, RSA Entitlements Policy Manager®, RSA Federated Identity Manager®, RSA Data Loss Prevention Suite®, RSA Encryption and Key Management Suite®, RSA FraudActionSM® and RSA enVision®

Results

- Strong governance, risk management and compliance, and greater protection against security threats
- Simplified management and deployment and a lower total cost of ownership
- Information security is a business enabler, rather than a business inhibitor

EMC is one of the world's leading providers of infrastructure information systems, software and services, employing approximately 40,000 people around the world. Its clients range from Fortune Global 500 enterprises to start ups, across all industry sectors, including financial services, manufacturing, transportation, public services, telecommunications, healthcare and life sciences. To learn more, please visit: www.emc.com

BUSINESS CHALLENGE



Information is an organization's most valuable asset, yet traditional security practices have either not provided adequate protection of information or have been so restrictive that they have prevented organizations from making maximum use of information to innovate, collaborate and achieve competitive advantage. This is primarily down to the reactive approach to security many organizations have been forced to take in the past. Rather than viewing information security as a business enabler, they have tended to view it as a business inhibitor – a defensive strategy, designed to prevent bad things from happening.

What's more, security policy has tended to be fragmented, especially for large global corporate organizations whose IT infrastructure spans many countries and business units. Taking this approach has been likened to a game of Whack-a-Mole – the problem is that good efforts in one area can be quickly nullified by failures in another. For example, a bank may protect its online banking portal from fraud only to have a privileged user copy confidential customer data to an unsecured laptop, which they then leave in a restaurant. These days, however, forward-thinking organizations like EMC recognize the benefits of moving away from reactive



The Security Division of EMC

EMC²
where information lives[®]



'silo security' to take a more proactive and holistic approach to information security and compliance, based on the established discipline of risk management.

SOLUTION

To help with its security transformation, EMC called upon the expertise of RSA – its own Security Division. RSA's Information Risk Management strategy brings together, within a global framework, all components an organization needs to plan and implement an end-to-end and holistic approach for protecting a business's most critical information assets.

Tracking data across the enterprise

The first step in this approach is to understand what information is critical to key business initiatives. EMC, for example, relies on a number of enterprise portals to share information and business processes across its global, organizational boundaries. By enabling collaboration between employees, partners, customers and suppliers through the sharing of critical business information, online resources such as EMC Powerlink, give EMC a competitive advantage in the market. However, they also create additional risk.

EMC Powerlink is the front-end for over 30 applications and has over 300,000 registered users. Some people are allowed access to more information than others, and this must be provided through a secure online transaction. It is also important to note that these online transactions hit all parts of the IT infrastructure: from the end point, through to the network and the data center. However, rather than letting this risk hinder its business initiatives, EMC works with it to minimize its impact.

Following RSA's Information Risk Management approach, EMC 'follows the data' involved to gain a more holistic view of all the places it exists across the organization, where the points of vulnerability are, and what events could put the business at risk. This kind of exercise is very complex, since data resides in many places, is mobile, and is constantly being transformed.

Prioritizing investments

The second core concept behind RSA's Information Risk Management strategy is the idea that security investments should be prioritized, based on the amount of risk a given activity entails relative to the potential business reward, and

in keeping with the organization's appetite for risk. In this context, risk is defined as the likelihood that an event will occur and the consequences if it does.

EMC works together with RSA to enable its highest priority business initiatives by protecting the information that is most valuable at the points where it is most vulnerable. Once this enterprise information has been located and the risk assessment performed, EMC then implements controls, including policies, technologies and tools, to mitigate that risk. Here, repeatability and reuse of security controls is central to RSA's strategy.

Ideally, this control framework should be established on best practices or standards like ISO 27001, ensuring that it is broadly applicable and effective in addressing most security

"We have a huge global network and the RSA Data Loss Prevention Suite allows us to locate and secure our critical information assets throughout our organization. It detects policy violations in real time and blocks or flags risky action, and has now become central to the acceleration of our global corporate security system."

V.Jay LaRosa, Supervisor, EMC Critical Incident Response Team, Office of Information Security

challenges an organization may face and building necessary controls. The range of controls will be very wide, but RSA places significant importance on two groups of information-centric controls, data controls and access controls.

Implementing security controls

Using RSA Access Manager to secure information at the end point, EMC is able to manage large numbers of external users to EMC Powerlink, whilst enforcing a centralized security policy that protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs – rather than having to remember multiple usernames and passwords they are able to enter single sign-on (SSO) to multiple resources.

EMC has also issued RSA SecurID tokens to all employees to add an additional layer of security for access to enterprise portals like EMC Powerlink. This offers authentication based on two factors: something the user knows – a personally selected PIN; and something the user has – an RSA SecurID hardware or software token – which generates a new password every 60 seconds. RSA Authentication Manager



is used to verify authentication requests and centrally administer authentication policies for enterprise networks. EMC is also looking to implement RSA Entitlements Policy Manager, which extends access management and SSO beyond Web URLs to the most granular applications, and is evaluating the benefits of RSA Federated Identity Manager, which extends SSO beyond the enterprise. It is also testing various RSA SecurID software tokens, including the RSA SecurID Toolbar Token, RSA SecurID Token for BlackBerry and RSA SecurID Token for Windows® Mobile. Embedded

“Many people think risk management is about risk minimization, and it’s not. It’s about risk optimization. There are some risks you want to take because the payoff is so great; the challenge is to mitigate your risk to a tolerable level. A good risk management program allows you to take risks that your competitors can’t.”

Bob Blakley, Analyst, Burton Group

into a wireless device or laptop, they eliminate the need for users to carry a second device to perform two-factor authentication.

But it’s not just the end point that needs to be secured. When someone requests information via EMC Powerlink it draws data down from applications and across the corporate network. EMC must also ensure end-to-end data security, not just at the end-point.

To do this, EMC uses RSA Data Loss Prevention (DLP) Suite across its entire enterprise to discover, classify and take policy-based action on all of its structured and unstructured data, whether it is in use, in motion, or at rest on endpoints, networks and servers. It makes it possible for the Information Security Division to locate critical assets, detect likely policy violations in real time, advise users when they are attempting a prohibited action and block actions that appear to be risky, or flag them up for further scrutiny.

Beyond this, RSA DLP Suite enables EMC to monitor activity in different business units and develop campaigns targeted at specific user groups. For example, it can help it understand which particular departments display high bandwidth usage, meaning they are using the Internet quite often. It can then monitor these business units more closely, since the chances of a security breach, such as a Trojan embedded in a web page, will be higher for them than in other departments that use the Internet much less.

RSA FraudAction offers EMC additional real-time, end-to-end protection against external online threats such as phishing, pharming and Trojan attacks, including 24x7 monitoring

and detection, real-time alerts and reporting, forensics and countermeasures, and site blocking and shutdown.

It monitors both EMC, RSA and RSA Hosted Operations domains for new domain name registration by unauthorized parties. In Q4 2008, for example, the RSA Anti-Fraud Command Center (AFCC) identified that an unauthorized company was trying to register the domain “rsasecurity.in” and was able to intercept the registration in order to prevent abuse of the EMC brand.

Reporting, auditing and compliance

Finally, the RSA enVision platform provides EMC with the means to audit its controls and document their effectiveness with regard to compliance and security regulations. This security information and event management (SIEM) solution collects and analyzes huge amounts of data regarding access in real-time.

RSA enVision provides EMC with a centralized view of the log information from thousands of security devices, including data generated by RSA DLP Suite, RSA SecurID and its Intrusion Detection System (IDS). Identifying correlations between logs from all these sources can help it in the early identification of potential security threats via EMC Powerlink,

Centered around three core principles, RSA’s Information Risk Management approach follows information as it is created, distributed, stored, copied, transformed and interacted with throughout the lifecycle.

Information-centric approach: Assesses what information is critical to key business initiatives, such as growth through acquisitions or expanding partnerships. Then diligently ‘follows the data’ to gain a more holistic view of all the places where it exists across the organization, where the points of vulnerability are, and what events could put the business at risk.

Risk/ reward analysis: Prioritizes security investments based on the amount of risk a given activity entails relative to the potential business reward, and in keeping with the organization’s appetite for risk.

Ensuring repeatability: Once enterprise information has been located and a risk assessment performed, implements controls, including policies, technologies and tools, to mitigate that risk. Here, organizations often turn to frameworks like ISO 27001.



for example. It is also helping the company to identify important cost efficiencies, ensuring it can continue to lead the market in infrastructure information systems provision. For instance, EMC's Information Security Division can see what percentage of a business unit, region or site is causing

“With RSA enVision we can look from the highest level into the health of the network, track down anomalies and create comprehensive remediation plans. And we now have enough aggregated information to make a real difference in the way security is applied to the business.”

David Martin, Senior Director of Information Security, EMC

the most impact to network performance or causing risk to EMC, its partners and customers and use it to drive remediation discussions. This and other insights into IT usage have the potential to save hundreds of thousands of dollars.

RESULTS

Thanks to Information Risk Management from RSA, EMC is benefiting from a less fragmented risk-based approach to IT security. This integrated holistic system is enabling stronger governance, risk management and compliance, whilst balancing risk, cost and convenience.

A centralized model eases management and deployment and is less costly and time consuming to the business. Employee productivity is improved and the IT department is able to concentrate on more strategic projects. Additionally, the ability to better map business metrics to IT usage across separate divisions has huge cost-saving potential.

Most importantly, however, Information Risk Management enables EMC to treat information security as an enabler of business growth. It is able to rollout new business initiatives like online resources to aid collaboration with the confidence that its business critical information is secure.



“Centralized access management, web single sign-on and two-factor authentication improve productivity, as well as user experience, helping us accelerate innovation and increase competitiveness.”

Howard Hantman, Strategic Architect, EMC Global Security Organization



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

EMC²
where information lives®

RSA, the RSA logo, and SecurID are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the property of their respective owners. ©2003-2009 RSA Security Inc. All rights reserved.
EMC_CP_10/09