



The Security Division of EMC

# EMC Critical Incident Response Center

A State-of-the-Art Converged Security Hub





The CIRC utilizes EMC and RSA technologies to centrally monitor and protect EMC’s globally dispersed operations – including 500 corporate and sales offices, 40,000 employees and scores of partners in more than 60 countries.

---

### Protecting a Global Organization

---

EMC is the world’s leading information infrastructure company. Its clients range from Fortune Global 500 enterprises to start-ups across all industry sectors, including financial services, manufacturing, transportation, public services, telecommunications and life sciences. The company employs 40,000 people worldwide, more than 40 percent of whom work outside the U.S., and it works closely with a global network of technology, outsourcing, systems integration, service and distribution partners.

As with most large enterprises, EMC faces the constantly evolving challenge of protecting its employees, customers, facilities and information assets – from maintaining physical building security and preparing for natural disasters, to safeguarding the confidentiality and integrity of digital information assets from a growing range of cyber threats.

---

### Converged Security Organization

---

To address these changing needs and priorities, EMC practices continuous improvement of its security strategy as well as the organization that supports it. The company no longer depends on independent security devices and security teams working in siloed environments to protect its operations. Today, EMC requires a holistic view of the enterprise – both physical and digital – to gain a better understanding of incidents and trends throughout the company.

To achieve this, EMC has built a converged security organization that includes its Information Security, Risk Management, Corporate Protection and Investigation, and Customer Security Management groups. By combining these organizations under a single umbrella, EMC is able to identify metrics and

trends from all areas to achieve a correlated view of risk throughout the whole organization. For instance, if the Corporate Protection and Investigation team identifies a significant number of intellectual property theft issues, the Information Security group can use that information to create controls to prevent future IP loss from occurring.

---

### State-of-the-Art Converged Security Hub

---

To support this converged strategy, EMC built the Critical Incident Response Center, a next-generation security facility that combines workflow and correlated data from multiple areas of the organization, security devices and technologies to create a single vision of monitoring and enforcement for EMC’s global operations. This state-of-the-art converged security center provides business-critical security services that integrate the assurance of the enterprise, the integrity of the company’s data and the safety of its work force. Established using technologies and best practices developed by RSA, the CIRC supports global log aggregation of more than 1,400 security devices and 250,000 end nodes from more than 500 sites globally.

Within the CIRC, a team of highly skilled analysts continuously monitor the IT and global security environments, responding to immediate threats and vulnerabilities, malware and data leakage. The team also monitors for physical security-related incidents, such as diversion and loss management, threats of violence, and assists in event protection from afar by integrating alerts from EMC’s Physical Security Solution. With this single integrated view of the global enterprise, analysts can provide advice and guidance to EMC management – feeding critical information into the continuous improvement cycle of its security strategy.



---

## Technology and Services

---

The technology and services supporting the Critical Incident Response Center include some of the market-leading products and services offered by EMC and RSA.

**RSA enVision® Platform.** The RSA enVision platform is a single, integrated 3-in-1 log management solution for simplifying compliance, enhancing security and mitigating risk, and optimizing IT and network operations through the automated collection, analysis, alerting, auditing, reporting and storage of all logs. The RSA enVision platform collects all the event logs generated by IP devices within EMC's network, permanently archives copies of the data, processes the logs in real-time and generates alerts when it observes suspicious patterns of behavior. CIRC analysts can interrogate the full volume of stored data through an intuitive dashboard, and advanced analytical software turns the complex, unstructured mass of raw data into structured and actionable information.

**RSA® Data Loss Prevention Suite.** The RSA Data Loss Prevention Suite, which is integrated with the enVision platform, helps EMC to uncover business risk associated with the loss of data and dynamically lower that risk through policy-based remediation and enforcement of controls. The suite of DLP products – RSA Data Loss Prevention Datacenter, Network and Endpoint – allows EMC to mitigate this risk regardless of whether the data is at rest in a data center, moving as network traffic or driven by an end user out at an end point.

**EMC Physical Security Solution.** The EMC CIRC monitors the physical security of the enterprise through the EMC Physical Security Solution, which integrates a wide range of physical security devices and systems, such as video surveillance cameras, access control devices, and sensors and alarms, with powerful analytical software.

- Supports a converged security strategy that protects both digital and physical corporate assets
- Increases efficiency and lowers total cost of ownership by building workflows and correlations from multiple technologies into a single integrated system
- Prevents security gaps by interweaving physical and cyber security technologies to provide a holistic and integrated approach to security incident response
- Greatly accelerates EMC's ability to predict and respond to threats by providing continual trends and correlating disparate security data identifying complex security issues
- Regularly audits EMC's IT security policies ensuring compliance
- Provides senior management with critical information to continually improve security policies and procedures throughout its worldwide operations

**RSA® FraudAction™ Service.** The EMC CIRC has integrated the RSA FraudAction service into its operations. At the core of this service is the RSA Anti-Fraud Command Center, a 24x7 war room that is set up to detect, block, monitor, track and shut down phishing, pharming and Trojan attacks, which occur across more than 140 countries, for organizations throughout the world. Analysts within the CIRC benefit from an ongoing feed of information from the Anti-Fraud Command Center that provides knowledge and visibility into the world's cyber threat landscape.

Monitoring more than 1,400 security devices and over 250,000 end nodes worldwide – tracking and logging more than 18 million events per hour.



Incident Response Team

## RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

RSA, RSA Security and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC. Windows is a registered trademark of Microsoft Corporation in the U.S. and/or other countries. All other products or services mentioned are trademarks of their respective companies.

CIRC SB 0909



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

**EMC<sup>2</sup>**  
where information lives<sup>®</sup>