RSA DATA LOSS PREVENTION ENDPOINT

Complete data loss prevention for sensitive data on laptops and desktops

AT-A-GLANCE

- Reduce risk by discovering and protecting sensitive data on laptops and desktops
- Minimize the time, costs and staff required to comply with regulations
- Monitor and control how end users interact with sensitive information in real-time as defined by policy
- Involve end users in remediation to build awareness of data security policies and reduce administrative costs

DATA SHEET

Overview

Every day employees work with sensitive data on their laptops and desktops, whether it's creating reports with unreleased company financial results, handling customer credit card information, and much more. Not only can that sensitive data be saved locally to their devices, but it can also be transferred to removable media, copied to network drives, printed, etc. How do you ensure your organization's most sensitive information is secured while it's in use on endpoints?

RSA® Data Loss Prevention (DLP) Endpoint addresses this very problem by helping you protect sensitive data on laptops and desktops, whether they are connected or disconnected from the corporate network, and even virtual desktop and applications. RSA DLP Endpoint comes in two modules: Discover and Enforce. The Discover module identifies sensitive information at rest by analyzing content of files on the local hard drive. The Enforce module monitors actions such as print or copy on endpoints, and offers a variety of remediation actions if a security policy is violated. With this type of visibility and protection, RSA DLP Endpoint can help protect brand value by ensuring your organization's most sensitive data is secure.

Major Use Cases

- Identify which laptops present the greatest risk due to the amount of sensitive data found, and ensure they are properly secured
- Prevent confidential company documents from being copied to a USB or burned to a CD/DVD
- Prove that a lost laptop did not contain customer personally identifiable information based on the last discovery scan
- Educate end users about policy violations and enable them to make more educated decisions when handling sensitive data
- Prevent users from copying credit card data from their virtual desktops to the connecting physical devices

Benefits

- Protect sensitive data on and off the network with a completely self-sufficient agent that maintains full functionality and content analysis capabilities without constant connectivity to a management server
- Save time and streamline the incident handling process through a broad range of remediation options based on user, action and content type
- Increase visibility into endpoint policy violations by senders, recipients and content type

"RSA DLP Endpoint showed potential at the onset. Our main requirements during the initial testing were that the solution needed to be extremely accurate, scalable and offer the highest performance. In particular, precision was critical because it has one of the biggest impacts on the ongoing total cost of ownership of the solution."

Scott Mackelprang, Vice President of Security and Compliance, Digital Insight

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa..

www.EMC.com/rsa

- Educate end users through an optional self-remediation option that provides real-time feedback on policy violations
- Ease deployment with a distributed architecture that enables hundreds of thousands of endpoint agents to be managed at remote locations with minimal latency and network congestion
- Increase security by applying file encryption, usage and permission controls to documents at rest on laptops and desktops with flexible Extendable Controls
- Leverage existing third party digital rights management and file encryption solutions to protect sensitive data copied to network shares and removable media.

Features

- **24/7 Protection:** Prevent sensitive data from leaking via the Internet, webmail, or instant messaging – even when employees are disconnected from the network.
- **Permanent and Temporary Agents:** Temporary agents scan data, collect policy violations and self-uninstall to allow organizations to survey their risk landscape with minimal footprint. Permanent agents can be deployed based on the organization's needs to provide maximum flexibility.
- **Comprehensive Actions:** Monitor and/or prevent transfer of sensitive data to a broad range of targets such as local and network printers, USB devices and CD/DVDs.
- **Whitelist Devices:** Authorize the use of specific devices for transfer of sensitive data. For example, permit copying only to a corporate-approved encrypted USB drive.
- **Audit Trail and Incident Management:** Retain logs of end user actions, helping administrators to simplify the compliance process. Integration with the RSA Security Analytics platform allows organizations to prioritize incidents based upon their level of severity and streamline auditing and reporting for compliance.
- **Support for Virtual Desktops and Applications:** Allow employees to bring their own devices and prevent data from being transferred from the virtual environment to the connecting physical device.
- **Sync to Mobile Support:** Monitor and prevent users from copying, moving, and saving sensitive data to iOS, Blackberry and Nokia devices via iTunes and Media Transfer Protocol

Supported Systems

RSA Data Loss Prevention Endpoint supports laptops or desktops with Windows 2000 SP4 or higher, including Windows 7. It also supports virtual desktop infrastructure, including VMware® View, Citrix® XenDesktop, and Microsoft HyperV, as well as Citrix XenApp virtual applications.

Published in the USA. 08/13 Data Sheet H12220

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.