RSA DATA LOSS PREVENTION FOR BYOD—iPADS, iPHONES, DROIDS AND MORE

A new approach to security for consumer devices used across enterprises

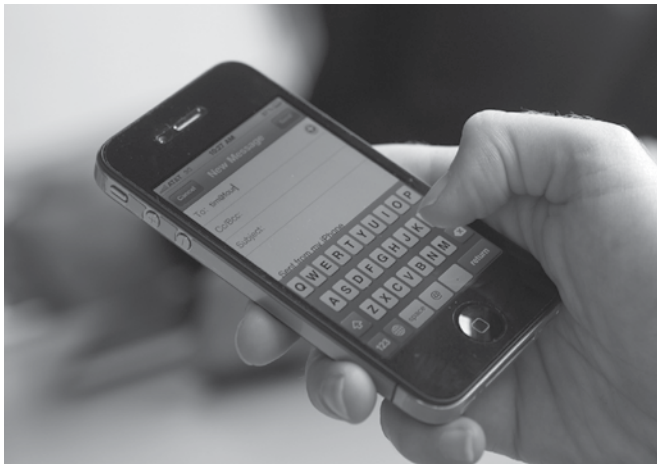
OVERVIEW

As consumer devices such as iPhones®, Droids®, and iPads® rapidly infiltrate enterprises, IT needs to rethink the way it approaches security and data loss prevention. Traditional enterprise-grade devices are no longer the only devices employees want to use. As employees become more mobile, they're opting for consumer devices because of ease of use and the convenience of combining personal and business use on one device. To support this growing trend, many organizations are developing a "bring your own device" (BYOD) strategy to provide employees the freedom and flexibility to choose from a wide range of laptops, tablets, and smartphones.

However, this freedom to BYOD introduces a huge blind spot for IT when it comes to protecting regulatory and corporate confidential data. How can organizations continue to pass audits to prove compliance, and reduce the risk of data breaches if they lose visibility into sensitive data on these devices?

As more consumer laptops, tablets, and smartphones are used across the enterprise for work purposes, it's critical to gain insight into the sensitive data accessed on, and sent from, these devices. RSA® Data Loss Prevention (DLP) provides the visibility and enforcement capabilities that are vital in the era of BYOD, so that regardless of the device used by employees, organizations can continue securing the use and flow of their most critical and confidential information.

Sensitive Data *accessed* via:
- email
- corporate web portals
- FTP sites
- VDI



And data *sent* via:
- email/webmail
- FTP/corporate portals
- cloud/apps/web
- VDI

Data Sheet

RSA EMC²

Key points

- Visibility into the risk of sensitive data on mobile devices
- Real-time monitoring and enforcement options
- Device-agnostic and agent-less approach

SENSITIVE DATA ACCESSED ON DEVICES

Whether it's sensitive data accessed from virtual desktops (VDI), virtual applications, or email containing customer credit card data being synched to mobile devices, organizations first need a way to understand what data is getting onto endpoint devices. RSA DLP provides unparalleled visibility into data accessed on smartphones, tablets, and virtual desktops and applications, so organizations can quickly identify areas of risk and even block highly sensitive data from being downloaded to devices. By taking an efficient infrastructure-based approach, RSA DLP helps organizations gain visibility and reduce risk without the need to install and manage agents on the mobile devices.

SENSITIVE DATA SENT FROM DEVICES

Once sensitive data is on the device, the concern then becomes about how the data leaves the device. For example, what is the risk to the organization if an email with details about a potential acquisition is sent to the wrong person either internally or externally? RSA DLP can monitor and enforce controls to protect sensitive data whether it's sent to someone inside or outside of the organization through corporate email.

Additionally, what if a file containing the roadmap or new product design details is uploaded to an open collaboration site such as Google® Docs, or if company financials are prematurely posted to social media sites? RSA DLP addresses these types of risks with a device-agnostic solution that leverages existing mobile device management (MDM) or VPN clients. RSA DLP works with all major MDM solutions and VPN clients to route traffic to the corporate network where it can be scanned, and any sensitive data identified can be properly protected. With this approach, RSA DLP provides real-time monitoring and active enforcement without the installation of additional agents.

Conclusion

With RSA DLP, organizations can easily identify and mitigate the risk of sensitive data on tablets, smartphones, VDI, and virtual applications to enable employees the freedom and flexibility to use a wide variety of devices while still maintaining compliance and protecting company confidential data.

Solution Benefits	Value
Real-time monitoring	Visibility into the risk of accessing or sending sensitive data from mobile devices
Active enforcement	Prevent the loss or misuse of sensitive data in real-time
Device agnostic	Broad coverage of devices with an infrastructure-based approach (iPads, iPhones, Macs®, Droids, etc.)
No DLP agent on end point	Reduce the costs and complexity involved with deploying and managing agents

h9714-dlpsp-ds-0412