Bring your own device (BYOD)
Cirius white paper

Introduction

Over the past few years, personal mobile and tablet devices have infiltrated nearly every enterprise. Employees are opting to use their personal Smartphone, tablet, laptop and other mobile devices over traditional enterprise-grade mobile hardware. To provide employees the convenience and flexibility of using their personal devices to access corporate resources, namely email, forward-thinking organizations are adopting a policy of Bring Your Own Device (BYOD).

As a result of this trend, businesses are struggling to secure mobile communications against data loss. BYOD increases the risk of data leaks as employees transmit data via unsecured email accounts, and mobile devices get lost or stolen - exposing business data, IP and other sensitive information to unauthorized access or theft. To secure and monitor corporate data now accessible via a host of various mobile devices, organizations are turning to mobile device management (MDM) solutions and enterprise-grade email encryption. These solutions often make mobile email applications difficult to use, undermining the very convenience and flexibility BYOD was intended to provide. In many instances, BYOD users simply disengage or circumvent such protocols. Information Technology administrators often install enterprise-level software across a fleet of mobile devices and then face the challenging task of enforcing different policies across varying devices with different operating systems.

cirius

secure corporate messaging

Why does it matter to you?

BYOD applies to all organizations that directly maintain and transmit personally identifiable information, protected information such as PHI, credit card information (PCI), financial information (SOX), in all electronic forms. It also applies to third party vendors and business partners that exchange data with organizations that directly maintain and confidential customer information.
It's no secret that non-compliance can be costly, or even crippling to your business. For example, under HIPAA regulatory compliance, healthcare organizations that fail to secure PHI against loss or unauthorized disclosure face fines of up to $250,000 per incident while individuals responsible can face up to 10 years in prison for noncompliance. Without question, the ensuing legal entanglements, reputation damage and financial cost of violations threaten your business's bottom line and may critically your organization's ability to do future business.

What does BYOD require for compliance?

All organizations must implement appropriate policies, technical and physical safeguards for information systems that maintain confidential information, including email, to ensure the security and confidentiality against loss or unauthorized disclosure. Considering the prevalence of accessing, sending and receiving confidential information via email, and the vulnerabilities of doing so, **it is obvious that BYOD policies call for an enterprise grade email encryption product.**

How can my organization meet these requirements?

In the maze of email encryption offerings, fortunately there are a few that stand out as clear solutions leaders to BYOD requirements. You should ensure that the product meets the following criteria:

- **Support for all Smartphone and tablet device operating systems.** Native Apps for iOS, Android, BlackBerry and Windows Phone. Other devices should be supported through a universal mobile-enabled secure thin client Portal without the need for encryption keys.
- **Support for all email addresses including Microsoft Outlook and Gmail.** The product should not only cater to your organization's internal needs, but those outside the organization, without forcing external users to change their behavior.
- **Ensure data is stored in cloud, not on the device.** As a cloud-based solution, emails and file attachments are stored securely in the cloud and are safe even if a device is lost or compromised.
- **Mobile access can be remotely disabled after a handheld device has been lost or stolen.** This feature adds an additional layer of protection by preventing unauthorized access.
- **Should not require any enterprise software or hardware installation** for external users.
- **Support for Global, Mobile Device Management (MDM).** The product should deployable via MDM, DLP and policy should be manageable globally from any device.
- **Support for API integration** capability with existing DLP rules engine to provides consistent policies with your existing engines.
- **Ensure there are no cumbersome encryption keys to manage,** simplifying management complexity.