globalscape™
securely connected

Whitepaper

Enterprise Mobility Management 101

Enabling security and productivity

"87 percent of IT managers believe that the biggest threat came from mobile devices in the hands of careless employees."

ZDNet

The greatest thing about enterprise mobility is that it empowers employees to be more productive – from anywhere and at any time. Mobility offers that freedom and flexibility so that an employee will no longer need to be tethered to an office to access the files they need to work.

At the same time, true mobility means that employees are enabled to easily access or transfer files to their colleagues, clients or business partners. Enterprise mobility changes the way we work, and it changes the way we do business.

So, how can you embrace enterprise mobility and safeguard your network?

Minimize security risks by implementing a BYOD policy

With BYOD, the line between business and personal resources becomes increasingly blurred. Implementing a BYOD policy is the first step in creating a productive and secure environment.

BYOD doesn't have to be a free for all. Organizations can restrict which types of devices, operating systems, and other tools are permissible for use at work and on the corporate network.

Businesses must prevent employees from introducing vulnerabilities and threats into their secure environments. Develop requirements for employees to use antivirus programs and secure passwords. Require encryption for sensitive data and institute continuing education programs for employees regarding when it is acceptable to use cloud applications - or why they cannot.

"By 2016, 65 percent of employees will use a mobile device to access company data."

Gartner

Setting rules and the policy is only part of the process. You must also establish plans and protocols to enforce BYOD policy requirements. The measures must be clear and communicated well to workers. Information privacy is also an important consideration here.

Employees can be uncomfortable with the idea that their IT team can monitor their device accounts, which also can be used for personal reasons. Organizations should also be aware that a number of states have introduced legislation limiting employers' abilities to access specific information or data on their workers, like their social media accounts.

After consulting with legal teams, organizations should balance protecting corporate resources with respecting workers' privacy regarding the personal information on their devices. Decision-makers must establish how they'll control and manage user access to company accounts and applications, which can help create clearer distinctions between corporate and personal resources.

Lastly, establish an employee exit plan. When workers leave the organization, especially if leaving on unpleasant terms, it could pose significant risks and open your organization up to a potential data breach. Establish processes and procedures for removing access to apps and resources previously accessible or stored on BYOD devices. This should include the ability to wipe corporate data from devices. Such protocols should be clearly explained to workers before they begin taking part in a BYOD initiative.

It's clear that there are many security risks involved with enterprise mobility and BYOD. Implementing a strong BYOD policy is a very effective preventative measure and it's key to successfully managing enterprise mobility and BYOD. As you continue to research and plan, be sure to review the Enterprise Mobility Management Checklist below.

Enterprise Mobility Checklist

- ✓ Does your organization have a BYOD policy in place? If so, does it need to be updated?
- ✓ Have you designated who will own and manage mobility?
- ✓ Can your employees securely access files from your organization's network?
- ✓ Do you have control over your information assets?
- ✓ Do you have visibility into who accesses your information assets?
- ✓ Is your network compliant?

Tools that support Enterprise Mobility

Not all technologies are created equal when it comes to EMM. Managed file transfer platforms and enterprise file sync and share tools should meet specific requirements to provide you with the visibility, security, and control necessary for your BYOD-friendly environment.

Enhanced File Transfer™ (EFT™) by Globalscape is a managed file transfer solution that offers simplicity, security and stability. If you're looking for enhanced mobile controls with your managed file transfer solution, EFT has two specific clients that help provide the EMM controls you're looking for.

- The Web Transfer Client (WTC) allows access to the EFT file system from any modern browser. This highly mobile tool means ease of connectivity for its users. For administrators, the WTC means more flexibility for partners, lower cost, reduced setup and implementation times, zero maintenance, and connection from any computer connected to the Internet.

- The Mobile Transfer Client (MTC) mobile app, developed for use with EFT, allows your employees to use their mobile devices to access corporate data, while keeping your network secure. MTC is a BYOD and enterprise mobile friendly tool that keeps files safe in transit and while at rest. With MTC, your organization has the right balance of employee productivity, efficiency, and corporate data security, allowing employees to be on the move with secure access to EFT.

Deploying an enterprise file sharing tool is an easy way to enable a secure EMM environment. Globalscape recently released its file synchronization and sharing solution, scConnect. If your employees are begging you to allow them to share files and data with people outside your network, scConnect is a secure alternative from widely-used consumer cloud products.

- scConnect™ is an on-premises file synchronization and share solution that gives enterprise users secure content mobility, providing the ability to share and access corporate data anytime on any device, while giving IT the administrative oversight, control, and security necessary to keep users and corporate assets safe. scConnect offers secure content mobility, which means that you can access and share content without the same security risks you would face using a cloud-based solution.

Conclusion

If you want to keep your network secure and protect your corporate assets, then a BYOD policy is paramount. Secure mobility in an enterprise environment is achievable, just folllow the steps in this whitepaper. First, be sure to restrict the types of mobile devices or applications that are permitted on your network. You can also keep sensitive data safe through encryption. Mobile devices are often an insecure point of entry for hackers or theives, so be sure to require the use of an antivirus program and password protection for mobile devices.

Additionally, there are often legal implications to consider when drawing out your BYOD policy. Since individuals may be using a personal mobile device to view work assets, there will be privacy issues to consider. Consult with your legal team on how to balance workers' privacy, while protecting corporate assets. And last, always have an employee exit plan. Regardless of the situation, anytime an employee leaves there is a greater risk for a data breach.

Enterprise mobility and BYOD is here to stay. Minimizing the many security risks through a strong BYOD policy is the best way to navigate through this modern dilemma. Ultimately, you want to empower your technology managers to own the process. Soon you will find that your organization's network will be more secure and your employees will be more productive and happy.

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features Enhanced File Transfer, the industry leading enterprise file transfer platform that delivers military-grade security and a customizable solution for achieving best in-class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments, and small businesses.