Armed with their own mobile devices and faster wireless speeds, your employees are looking to access corporate data on the move. They are creating, consuming and storing mission-critical business information on laptops, smartphones and tablets. Sometimes those devices are corporate-issued, but often they are using their own personal devices.

As noted by Forrester Research[1], in order to avoid employees operating in an IT underground, you may be one of many organizations that are developing a Bring-Your-Own-Device (BYOD)[2] policy to address security concerns. Letting your employees use their own mobile devices may boost employee morale, but it also moves sensitive data outside the boundaries of an enterprise's data center onto devices that are out of your control.

Even if your organization has implemented policies to govern applications employees are permitted to use on mobile devices to access corporate data and configuring them so their memory can be wiped clean when required, you still run the risk of losing access to this data unless it is safely backed up to your authorized data center.

Imagine if an employee's laptop or tablet containing critical business data was lost or stolen: you could remotely wipe the device to prevent anyone else from having access to the information, but what if you've never backed up the data? You too would lose access to it. And how do you ensure your data and corporate intellectual property (IP) is protected in this scenario?

If you do not have a policy for backing up the data on these endpoint devices, there's a good chance your employees have been backing up data themselves. Some might backup data to USB devices, including external hard drives, and some to unsecure public cloud services such as iCloud. Others may use sync and share software. In all cases, you face the possibility of data being leaked outside your firewall. Your corporate IP may be residing unprotected on USBs which can be lost or stolen or might be getting shared indiscriminately across multiple devices with people who shouldn't have access to it.

Not having a policy for backing up endpoint devices puts your corporate data at risk. To protect yourself from threats to your competitive advantage, loss of reputation and regulatory non-compliance, you need a secure end-to-end data backup and recovery solution that protects all of your data, including the data residing on endpoint devices.

Introduction

Thanks to the rampant popularity of tablets and smartphones, the BYOD phenomenon is not going away. As employees bring their personal devices to the office your corporate IP now resides alongside family photos and personal text messages. Have you ever wondered what happens to your data when an employee leaves your organization? What if the device is lost and gets into the hands of someone who should not have access to this information?

To protect unauthorized access and loss of corporate data, you can obtain the consent of employees to wipe the device of all data in the event of device loss or theft. This is something your service provider can enable on any devices employees use to access corporate data. However, once you wipe the data, no one has access to it anymore – including you.

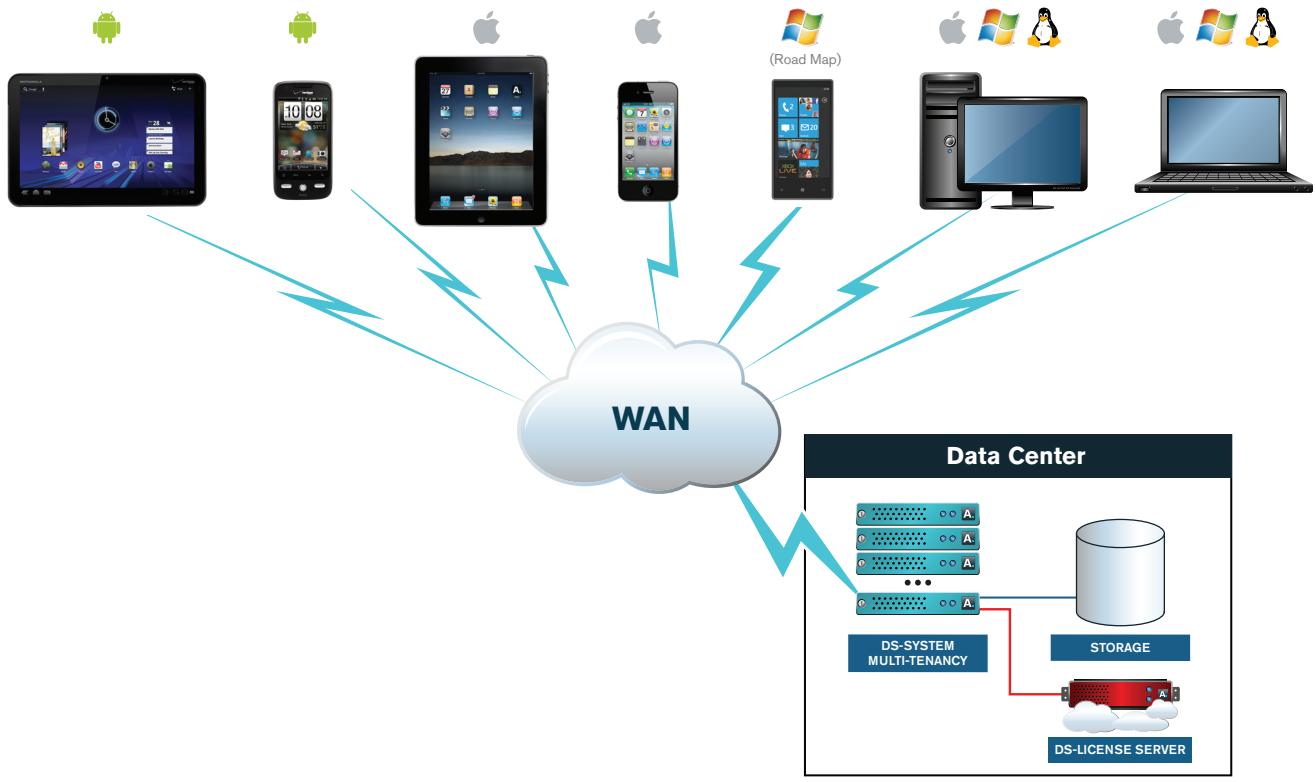
Most organizations do not have a policy for backing up data sitting on endpoint devices. So many employees have been using their own methods to makes copies of corporate data they consume and create, including USB devices and sync and share software, but these methods are not secure. They also move corporate data out of your control, potentially putting corporate IP into the hands of people who should not have access to this confidential data. Imagine if your competition gets its hands on sensitive information or if it reaches the media. Think of instances where highly sensitive corporate information in heavily regulated sectors such as healthcare and financial services is leaked. Your business may just come to an end and you may be left facing legal consequences.

---

1 Your workforce is already using their personal computers to boost efficiency. Instead of forcing them to operate in an IT underground, it's time to develop a bring-your-own-device (BYOD) program that addresses security concerns while building a solid base for future innovation. – Forrester Research

2 Bring-your-own-device (BYOD) is an alternative strategy allowing employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data. – Gartner Research

Figure 1: Asigra supports the backup and restore on a wide range of endpoint devices and operating systems



The Risk of Leaving Endpoint Data Unprotected

Business decision makers understand the need for safeguarding data on these devices in the same way they protect all on-premise data that resides on your LAN, but you may be holding off enabling this much needed protection because of resistance from your employees.

For example, mobile workers who connect infrequently to your enterprise network may oppose the installation of any backup software on their laptops because they worry that time-consuming backup jobs will impact the performance of their machines. When it comes to personal devices, including smartphones, end users are wary of installing any applications provided by corporate IT. After all, they contend, it is their device and so they have the right to refuse to install any software that may harm their smartphone.

IT managers may be tempted to look the other way when it comes to backing up endpoint devices because it might increase bandwidth use and lead to clogged networks when mobile devices hop back on to corporate networks after a long time and time-consuming backup jobs kick in. They may also be concerned that managing the backup of these devices will need special tools and strategies to support the wide array of devices employees are bringing into the corporate environment, leading to additional costs and the need for completely new service providers and investments in new infrastructure.

Whatever your reasons, not implementing a policy for backing up the data on these devices can leave you exposed to the threat of losing confidential information and the consequences of data loss.

Complete Endpoint Device Backup Powered by Asigra

Our cloud backup solution powered by Asigra provides organizations with a single solution to protect all data in the enterprise, no matter where it resides, including mobile endpoints. We can backup data and applications from any device that holds your organization's confidential information. From enterprise servers to physical and virtual machines to desktops, laptops, tablets, smartphones and cloud-based applications, our cloud backup service can backup all data seamlessly to your own authorized, secure offsite data center.

According to Gartner, by 2015 more than 60% of enterprises will have suffered material loss of sensitive corporate data via mobile devices.

Comprehensive OS support

The BYOD world is full of aficionados who swear by particular operating systems and device brands, so we understand that any solution to protect data on these endpoints must be broad-based and include support for multiple operating systems and platforms. Our cloud backup service is hardware and software independent and supports all major operating systems. Whether your desktop or laptop users run Windows, Linux, or Mac OS, our solution can protect the data on their PCs. It can also protect Apple iOS and Android devices, thereby supporting the majority of tablets and smartphones found in corporate environments today, whether they are personal devices brought into the organization by employees or issued by the company.

Bandwidth and storage optimized backups

Our cloud backup service uses incremental forever functionality to make sure only changed files are sent over the network to the backup repository. In addition, all data is deduplicated and compressed before it is transmitted, thereby ensuring efficient use of your bandwidth. Our cloud backup solution also performs deduplication at the target to efficiently store your data in our secure offsite data center.

Secure backups

Our cloud backup service powered by Asigra encrypts your data at the source and during transmission to the backup repository using secure AES encryption to encode the information to prevent unauthorized access during the backup and restore processes and when it is stored in backup repositories.

Intuitive and easy to use

We can configure your backups to run according to your preferences to ensure your data is backed up at regular intervals and that it is always protected. Our cloud backup application lets employees run backup and restore jobs on their devices if necessary, using a simple and user-friendly interface.

Certified Endpoint Backup Apps available for download

The Asigra Cloud Backup™ application for tablets and smartphones that powers our cloud backup service is available for download from the Apple App Store and from Google Play, so your employees can download it for free. This helps you overcome their objections about not wanting to install a suspect custom application on their personal devices.

For more information on our cloud backup services for endpoint devices or to schedule a complimentary Recoverability Assessment contact us today.

About ITC Infotech

ITC Infotech is a specialized global scale - full service provider of Domain, Data and Digital technology solutions, backed by a strong business and technology consulting focus. The company caters to enterprises in Supply Chain based industries (CPG, Retail, Manufacturing, Hi-Tech) and Services (Banking, Financial Services and Insurance, Airline, Hospitality) through a combination of traditional and newer business models, as a long term sustainable partner. ITC Infotech is a fully owned subsidiary of USD 7bn ITC Ltd – one of India's most admired companies.

For more information, please visit www.itcinfotech.com | or write to: contact.us@itcinfotech.com

---

ITC INFOTECH
Business-friendly Solutions

POWERED BY Asigra