Acronis

# EMBRACING SECURE BYOD

# what **you need** TO **KNOW**

# Introduction

The Bring Your Own Device (BYOD) movement has evolved from a buzzword and a trend to a full-fledged corporate phenomenon. Tablets and smartphones have become virtually ubiquitous with enterprise employees and many of these devices are employee-owned. In fact, many people are rarely seen without their smartphones or tablets.

For many organizations, the spread of consumer devices has led to many employees using their personal devices for work-related phone calls, calendars and emails. These are the basics that we are all familiar with. But as mobile devices have become more powerful, and more engrained in our workflow, there is an increasing need to move beyond the basic uses and really harness the power of these devices. For many IT organizations this has started with Mobile Device Management (MDM) to secure and manage the devices.

However, these tools fail to deliver the comprehensive functionality required to put end-users on the path toward major productivity and efficiency leaps – the ability to access and interact with content!

Content, defined as the files, documents, presentations, spreadsheets, images, and reports that we interact with every day, is the lifeblood of any organization. Whether mobile devices are corporate-owned or part of a BYOD plan, enterprises need to figure out how to give safe and secure access to content on mobile devices in order to fully realize the productivity and efficiency gains of these devices.

# THE CHALLENGE OF BYOD AND CONTENT

While BYOD has a lot of advantages it also presents its own share of security and management challenges. Mobile workers want access to their content on their devices, and in many cases to do so, they have employed methods that put enterprise content at risk. To ensure that they do not resort to these methods, IT must understand what users want to do with content and meet their needs. There are three general use cases for how mobile users want to use their content:

**Access Corporate Content**

Securely access, edit and create content on their mobile devices

**Sync Content across All Devices**

Anytime, anywhere access to their individual content regardless of the device – phone, tablet, desktop/laptop - they choose to use.

**Share Content**

Securely share business content with others colleagues, customers, partners and other external constituents.

These three cases could create significant risks for many organizations that do not put together an appropriate strategy for access, sync and share solutions. IT organizations are left grappling with data leakage, arising from the following:

- Many employees resort to mailing files to themselves to attain access on their mobile devices. And then use unauthorized third-party apps to edit documents, spreadsheets, presentations and other files.
- Others use consumer-grade solutions, such as Dropbox, to sync files across their devices and to share with others. IT has no visibility into what files are moving in and out of the organization, where they have been, if they have changed, if there are copies, if the files ever come back, who is sharing with whom, etc. A complete lack of enterprise visibility.
- Lost or stolen devices could also compromise corporate content.
- Employees leaving the organization may retain sensitive corporate content on their personal devices.

By using the proper mobile content management solutions, IT can securely and safely manage the security risks posed by BYOD to empower employees so they can get the job done anywhere, anytime, and from any device.

# MANAGING BYOD AND CONTENT

The BYOD trend shows no signs of slowing down. Instead of hiding or fighting it, how can your organization embrace this shift in the way business is done, all while minimizing potential security threats? Almost 60% of organizations do not have a BYOD policy yet. Proper procedures established by the IT department can safeguard and secure content, and help to foster happy employees, increased productivity, and streamlined, managed workflows. Furthermore, enterprises need to evaluate access, sync and share solutions that allow them to derive the greatest amount of benefits and advantages for the company.

Comprehensive access, sync and share solutions should balance the need for consumer-grade simplicity for the end-user with enterprise-grade control, security and management for the enterprise. Organizations evaluating these solutions should consider the following:

1. **On-premise deployment –** 100% on-premise solutions give the enterprise the greatest amount of control and security without sacrificing any end-user flexibility.

2. **Active Directory integration -** this ensures seamless authentication, provisioning and user management.

3. **Policy Setting –** allows IT to create security policies for content, users and devices.

4. **Encryption –** protects data in-transit and on the device.

5. **Remote wipe –** ensures sensitive corporate material is protected if a device is lost or stolen.

6. **Document editing -** “in-app” Office document creation, editing and PDF annotation within the secure sandbox eliminates data leakage and improves end-user productivity.

7. **Audit logs -** Gives IT the visibility to see what users are doing, what documents they access, who they share them with.

# THE FUTURE OF BYOD

The advent of smartphones and tablets—and a wide variety of corresponding productivity applications— present substantial benefits to the enterprise. And many of these devices are employee owned. This trend will only increase. IT organizations need to take proactive steps to address and utilize this phenomenon.

Strategies need to be developed that balance the needs of the end-users with the needs of the enterprise to stay in control and address security, management, compliance and visibility. Organizations should evaluate solutions that support the integration of diverse computing platforms and devices into the existing, complex enterprise environment.

By taking advantage of the emerging access, sync and share solutions, IT can gain peace of mind and employees attain the confidence that they are not causing any security breaches.

Acronis

## About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2002, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com**.
Follow Acronis on Twitter: **http://twitter.com/acronis**.