ZECURION

*Protection as a Priority™*

# Securing Corporate Data on Mobile Devices

## Using Zecurion Mobile DLP to Ensure Data Protection

*Abstract*

Regulating the information flow between various devices has been a top priority for Information Technology (IT) managers. With the advent of bring-your-own-device (BYOD) to the workplace, their task has become even more challenging to secure data and ensure seamless data access between desktops, laptops and mobile devices. This situation is compounded by the fact that IT managers are often unaware of mobile devices being on the corporate network.

Mobile device management (MDM) solutions have come to the aid of some organizations. However, most MDM tools offer device-level security, leaving the data still vulnerable. In order to secure data, IT managers are considering mobile data leakage protection (DLP) solutions.

This paper explores the challenges of BYOD and how to ensure data security on mobile devices. It includes benefits of mobile DLP solutions and how **Zecurion Mobile DLP** can help ensure data traveling between mobile devices is not compromised.

## Bring Your Own Device (BYOD)

By 2018[1], nearly 93 percent of the devices in North America are expected to be smart devices. The growth of smartphones has been mainly fueled by an increase in mobile data services. For example, as of 31 March 2014, Facebook had over 1 billion[2] monthly active users accessing Facebook on mobile devices. From Facebook to mobile enterprise apps, smartphones touch every aspect of our lives.

The inconvenience of carrying two devices (work and personal) has pushed many organizations to ease the access restrictions imposed by corporate networks. Gartner predicts that by 2016, as many as 38 percent[3] of organizations will stop providing devices to their employees. In order to help their employees, companies are changing their device policy and gradually moving toward a BYOD strategy. With BYOD, one's personal device becomes his/her work device too. Gartner, in the same study, adds that, by 2015, the number of employees using smartphones will double.

BYOD offers a win-win situation for both employees and employers. Employees get the freedom to choose their device and applications, increase their mobility and harness the ability to combine work and personal lives. At the same time, employers gain employee satisfaction due to technology familiarity, increased productivity and lower costs.

Enterprise file sync and shared usage are the two most common work activities of employees on their mobile devices. BYOD allows greater flexibility to employees considering they can choose their devices and applications for improving productivity, and moreover, they can do all this on the go. At the same time, BYOD also opens new challenges for IT managers. From data security to employees mixing personal and business data in a single device, network breaches is becoming a real challenge for IT management.

## Challenges of BYOD

Connected laptops and desktops provide unlimited access to business-related information, including confidential and privileged information, to employees throughout the day. However, with the permission of personal devices for business purposes, this business information can flow out undetected, creating a clear and imminent danger.

The flow of data out of the network on personal devices poses various challenges:

**Security Issues**
The risk of data leakage from mobile devices is particularly acute and has become a bigger problem than malware. Mobile devices are designed to share data across applications, keeping user convenience in mind. They are not meant for file systems and controls, which increases the potential for data to be easily duplicated between applications and travel to various points over the cloud through those applications.

According to a Clearswift report, 58 percent[4] of data leakage incidents are attributed to insider threats mainly

[1] Cisco
[2] Facebook
[3] Gartner
[4] Info Security

from existing employees and ex-employees. The employees can further be categorized as negligent employees or disgruntled employees. Negligent employees are unaware their actions are unsafe and also lack respect for safeguarding any confidential information, whereas disgruntled employees seek to gain financially through illicit actions by not returning company devices or selling sensitive information for profit.

**Minimal Management and Inconsistent Security Policies**
IT managers are mostly unaware of data leakages and have limited awareness about the source of data leakages. According to a Cisco survey, 27 percent[5] of IT managers admitted they did not know the trends of data loss incidents over the past few years. Also, most companies implement BYOD on an as-needed basis for a few employees or departments, and in such cases policies are very generic. Over the course of time, the usage of BYOD increases, but often IT managers do not redefine the policies to safeguard the company's interest.

**Costs and Liabilities**
Employers can control initial costs by sharing them with employees for device purchases. However, legal and risk departments are concerned about the liabilities associated with data loss and theft that often occur on cloud-connected mobile devices.

## Outcomes of BYOD

These challenges can mainly be attributed to various user actions in absence of proper data security solutions:

**Use of Consumer Applications**
Employees install multiple applications on their smart devices, which may or may not be accessible on the corporate network. When enterprise data is allowed on these devices, the risk of leakage increases for the enterprise, not just because of the rise of mobile malware but also because legitimate but unsupported apps may inadvertently create security risks for the organization. This aspect aggravates the problem further in the case of device loss.

**Loss of Productivity**
Productivity could be considered another problem for BYOD devices considering social media and consumer apps are accessible during work hours. Most of these apps push notifications, creating a constant stream of distractions.

**Creating Weak Passwords**
Since it is not possible for employees to enter strong passwords every time they wish to access their device to make phone calls, check messages, update Facebook statuses, etc., IT managers allow employees to use weak passwords, which pose a threat to data security.

**Syncing Data over the Cloud**
The increasing popularity and penetration of cloud storage like Dropbox, Google Drive, One Drive and others over HTTP and HTTPS domains create challenges of a different nature. There is no control over the files accessed and stored on the cloud under normal circumstances.

While productivity issues are internal and can be addressed by IT managers at the time of rolling out a BYOD

[5] Cisco

program, the remaining challenges can only be addressed through data security controls.

### Security Controls

There are many piecemeal data security solutions available in the marketplace. Some of these solutions include:

| Solution | Description |
|---|---|
| **Data encryption** | Uses cryptographic algorithms to protect the confidentiality and integrity of data |
| **Geofencing** | Defines a boundary and location to access specific apps |
| **Remote wiping** | Used to delete data when a mobile device is stolen or lost |
| **Reverse proxy** | Used to block sensitive data traffic flowing to and from mobile devices across networks |

However, in order to keep pace with the increased adoption of BYOD and its related challenges, it is critical for organizations to implement a proper mobile DLP solution along with clearly defined guidelines for employees. A mobile DLP solution will safeguard data from leakage during information flow between devices. A proper policy document will help employees understand the importance of data confidentiality in the event of corporate data being put under surveillance. The document must also include information about the apps that can pose a threat to the company along with what devices and operating systems are allowed, what should be done in case a device is lost and the consequences of noncompliance.

## Protecting Your Data with Mobile DLP

There are only a handful of organizations that have exerted effort and spent money to secure data. The bigger question IT managers are worried about is, "Do we have any single solution that is employee friendly and delivers strong security while preventing data loss on a real-time basis?" The answer is affirmative. The comprehensive approach of certain DLP solutions makes them ideal solutions because:

**DLP allows prevention of data leakage and safeguards unencrypted information.**
Users send and receive email from corporate and personal accounts, upload information to cloud services and send files to social networking sites. According to industry reports, the majority of data loss is generated by well-meaning insiders using standard information-sharing tools (email, Web upload, etc.) since the information is not sent in an encrypted format through mobile devices. A DLP solution acts as a gatekeeper to control confidential information from compromised and unauthorized access by routing the traffic through a corporate virtual private network (VPN) server.

**DLP allows access restriction for applications.**
Information access privileges are usually 100 percent for each mobile device user. A DLP solution can help enforce a restriction on usage of select applications by blacklisting them or exceptionally allowing some applications to users by whitelisting them based on user business requirements and approvals.

**DLP allows protection of Real-time data and FSS.**
A Gartner study reported that most data loss from mobile devices occurs through emails, multiple third-party

apps allowing data exchange and Internet tools for file sharing and synchronization (FSS)[6]. DLP solutions offer data routing and information scanning through corporate VPN to ensure no confidential information leaves the corporate network.

**DLP allows monitoring of chat (messages and voice).**
Mobile devices connected to the corporate network can be monitored for voice chat activities through control of HTTP/HTTPS and can also log all outgoing text as well as multimedia messages to prevent data leakage.

DLP solutions act like control centers for sensitive data, user profiles and device information. With careful definition of these three areas, they can offer lots of security and business flexibility—a perfect combination for mobile devices.

# Using Zecurion Mobile DLP Solution

The Zecurion Mobile DLP provides a unique security approach to prevent data leakage from a device in or outside a corporate network.

## Unique Security Approach

Zecurion Mobile DLP helps protect your organization from accidental and deliberate data leakage. It acts like a traffic controller and routes all data flow to the network DLP (i.e., Zgate) for analysis and action. This includes analysis and protection of sensitive data sent from email clients, Web browsers and applications such as Facebook, Twitter, Dropbox, etc. In the event of an incident, the user is notified of the violation of security policies.

## Mobile DLP Security Model

Zecurion Mobile DLP offers an end-to-end solution to ensure data traveling between smart devices is fully protected from the start to end points. The Zecurion security model has two key elements:

1. **Data Protection**—It segregates personal data from corporate data and ensures personal data is protected from monitoring and corporate data is protected from leakage or loss.

2. **Securing Network Access**—It ensures data that travels in the network is secure, based on analysis of the content of the messages and file sharing on Google Talk, Yahoo Mail, etc. It also keeps tab on the information uploaded to cloud services, covering all information flow on HTTP/HTTPS.

## Mobile DLP Benefits

By providing security and management at the application layer, IT managers can establish policies to prevent mobile data loss without interfering with personal use. The solution offers multiple benefits:

1. **Securing Devices Running Android OS**—Most of the existing solutions focus on Windows OS or iOS environments, but Zecurion Mobile DLP caters to securing Android devices, which has been a challenge for a long time.
2. **Respecting Employee Privacy**—IT staff can manage corporate data on personal devices while respecting employee privacy. By applying policies at an application level, IT can implement and enforce

[6] Gartner

strong enterprise-grade policies for passwords, timeouts and other security controls without impacting an employee's overall personal experience.

3. **Ease of Use**—The Zecurion solution is user friendly and can be easily installed either manually or through Google Play. IT staff need only manage corporate data, e.g., in case of device loss, rather than remote wiping the entire device and/or wiping only the corporate data, leaving personal data and applications intact. Employees can use their own mobile devices without compromising their personal user experience, which increases employee satisfaction and productivity.

## Key Features

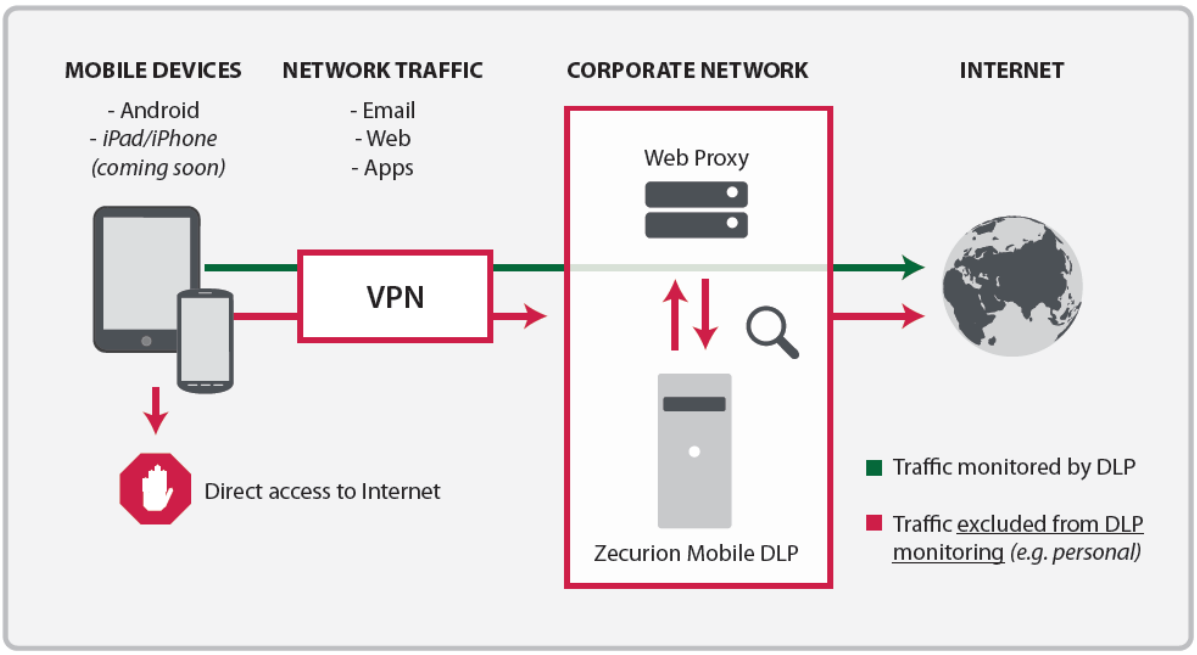
- File scan (analyze type and content on schedule as well as in real time—"discovery" feature); Files are scanned on the device and on the plugged memory card.
- Application control (whitelist/blacklist of applications allowed/not allowed to run on the device)
- Direct HTTP/HTTPS traffic to corporate VPN server where it can be inspected by Zgate; logging of calls, SMS and MMS
- Monitoring mobile devices connected to computers and other devices

## Capabilities

- SMS/MMS logging
- Allow/disable certain Wi-Fi networks
- Remote blocking/cleaning of the device
- Logging of the geo location
- Installation from Google Play or Zecurion Configuration Server

## How It Works

Zecurion DLP Mobile works in conjunction with mobile solutions to configure and manage VPN. It also relies on a DLP server deployed in the corporate network and, in conjunction with a Web proxy, analyzes all outgoing network traffic, including SSL-encrypted content.




All traffic passes through a VPN and arrives at the server for content analysis. Emails sent through Web mail, messages in social networks, publications on forums and blogs are all analyzed in accordance with established policies installed on the Zecurion DLP Server. After analyzing the content, communication can be either blocked or saved to archive, offering the possibility for future forensics and investigation. More than 10 various content analysis algorithms allow detection of virtually any type of confidential information, from credit card numbers to software source code.

## Summary

BYOD offers numerous advantages to employees and employers, but those advantages also prove to be risky for some employers in cases where data is compromised through mobile devices. Zecurion Mobile DLP monitors data on a real-time basis and controls apps on mobile devices, empowering organizations to ensure round-the-clock data security and confidentiality.

# About Zecurion

Zecurion is a global technology innovator in security solutions that reduce risk of data loss by addressing internal threats. Started in 2001, Zecurion has successfully developed and implemented data loss prevention solutions providing proven and reliable protection against leaks for more than 10,000 companies around the world. The company's solutions provide comprehensive protection against leakage of information throughout the course of its lifecycle – from creation, to recording and archiving, and deletion.

Zecurion's advantages lie in reliable and transparent backup encryption, server storage security, mobile data and email security as well as control of peripheral devices incorporated in networks with clear, easy-to-use administrative interfaces and tools. The company's unique forensic capabilities are unmatched, providing an additional layer of risk management through the shadowing and storage of communications transactions for future auditing. As organizations realize the operational and financial benefits of cloud computing and transition data storage from internal resources to cloud-based data storage services, Zecurion provides an effective, intuitive and cost-effective solution for encrypting and protecting sensitive data no matter where it resides.

Zecurion is led by an executive team experienced in developing security software and deployment across the enterprise. With over a decade of experience in developing encryption-based security solutions, Zecurion allows IT departments to efficiently protect corporate information from internal threats, as well as from loss or theft of backup storage media.

# References


- Cisco Whitepaper on *"Data Leakage Worldwide: The High Cost of Insider Threats"*
- ESG Whitepaper on *"DLP for Tablets: An Intelligent Security Decision"*
- Gartner Report on *"Best Practices for Data Loss Prevention: A Process, Not a Technology"*
- Gartner Report on *"Survey Analysis: What IT Leaders Need to Know About Employee BYOD Attitudes in the U.S."*
- Zecurion Mobile DLP Product Brochure
- Gartner Report on *"Employee Attitudes Toward Bring Your Own Devices"*
- Gartner Report on *"Three Crucial Security Hurdles to Overcome When Shifting From Enterprise-Owned Devices to BYOD"*
- Gartner Presentation on *"User Survey Analysis: U.S. Consumers Show Little Security Concern With BYOD"*
- Gartner Report on *"Bring Your Own Device: The Results and the Future"*