An Overview of Mobile Security

THE SITUATION | THE CHALLENGES | THE SOLUTION | THE BENEFITS
As organizations move into the future, they’re moving toward mobility. In fact, 34.9 percent of the global workforce — more than 1.19 billion workers — will be using mobile technology by 2013.¹ It’s a competitive necessity. But while it enables workers, it complicates things for IT. Beneath the flashy mobile devices and revolutionary flexibility lie serious security challenges.

76.9 billion mobile apps are expected to be downloaded in 2014.²

THE SITUATION

Security threats are already exploding in both number and sophistication. Throw the complexity of mobility into the mix, and you’ve got a recipe for data security disaster:

- Smartphones
- Notebooks
- Tablets
- Bring Your Own Device (BYOD)
- Applications
- Operating systems
- Outside networks
- Cloud computing

By 2015, there will be an estimated 15 billion mobile devices.³
THE CHALLENGES

When mobile workers hit the road, they bring your organization’s digital assets with them. Without the proper security technologies in place, your data and resources could get lost along the way. Here are just some of the ways in which outward-bound data can take a wrong turn:

**Device loss** — If left unlocked and unencrypted, lost devices can result in lost data. This includes intellectual property and other confidential information.

**Jailbreaking or rooting** — Users may jailbreak or root their devices in an effort to bypass certain built-in controls. This allows side-loading of unapproved applications, which could be malicious.

**Autosaving passwords** — Some users may autosave their email and Virtual Private Network (VPN) passwords directly on their device — granting access to whomever may pick it up.

**Unsanctioned applications** — Third-party apps may contain threats that compromise your data. A whopping 69 percent of users admit to installing these applications on their work devices.⁴

**Outside access points** — In the absence of encryption, unsecure public access points such as Wi-Fi hotspots and cellular networks can put your data at risk.

**BYOD** — Today’s users are accessing organizational data from personal devices. Left unregulated by robust policies, these devices can create significant security challenges for IT.

![45% of mobile devices at large organizations are not secure.⁵](image)
"Anytime, anywhere" connectivity demands "anytime, anywhere" protection.

Mobile security goes beyond mobile devices. It includes data, applications and networks, too. With a comprehensive mobile security solution, we can prepare you on all levels with the technologies, tools and policies you need to open your workers to the world without opening your network to a world of risk.

**MOBILE DEVICE MANAGEMENT (MDM) SOFTWARE**
From organization-issued devices to your workers' personal ones, MDM software helps keep IT in control wherever users go with capabilities like:

**Remote Locking and Wiping**
IT staff can remotely lock a given device on demand, thereby blocking user access to key credentials. Staff can even wipe a device in case of loss.

**Mobile Application Management (MAM)**
Application sandboxing “wraps” an application so that when it executes, inside information cannot go out, and outside information cannot come in.

**MULTIFACTOR AUTHENTICATION**
In this type of access control, users gain access using a passcode generated by a token, which only an authorized user can possess. This helps ensure that users are who they say they are, so that only authorized users can gain access.

**DATA LOSS PREVENTION**
Also known as data leakage protection, this kind of security software helps protect sensitive data outside the network perimeter from exfiltration. It can monitor three types of information:

- Stored information
- Transmitted information
- Information manipulated by actions on each device
**Encryption**

Encryption uses an algorithm to convert your organizational data into code. This makes your information undecipherable to anyone without an encryption key.

- **Application-Level Encryption**
  This can be used instead of a Virtual Private Network (VPN) when the incoming traffic to be protected involves particular applications.

- **Storage Encryption**
  This approach protects data at rest on the user's device in one of three ways. Disk encryption protects all data on a piece of media. File encryption protects individual files on a device. And virtual disk encryption creates an encrypted virtual container to hold all sensitive files.

- **Network-Level Traffic Encryption**
  Typically implemented as a VPN, it encrypts data traveling to your organization’s network, thereby protecting it against unsecure Wi-Fi hotspots and cellular networks.

- **Cryptographic Keys**
  Unlike many encryption technologies, this approach uses the public key to encrypt data and the private key to decrypt it.

**Wireless Network Security**

- **Secure Wireless Architectures**
  By creating a separate, dedicated network for BYOD access only, organizations can isolate BYOD traffic from all other traffic. This segregated network can be more easily monitored and secured than a mixed network.

- **Wireless Access Point Security**
  To protect wireless networks from eavesdropping, organizations should consider using strong wireless networking encryption protocols, such as Wi-Fi protected access 2 (WPA2), and avoid using weak ones, such as the original Wi-Fi protected access.

- **Network Access Control (NAC)**
  An NAC solution evaluates the security characteristics of a device attempting to connect to the wireless network. If they’re up to organization standards, the device is granted access. If not, the device is either denied access or directed to a separate ‘remediation’ network for corrective action.

**Mobile Use Policies**

This critical step helps define mobile device limitations, establishing a code of conduct for their use, selection and deployment. From a BYOD perspective, organizations should consider the following:

- Which mobile devices are allowed on the network?
- What resources or types of resources can they access?
- What software and services can be used to provision, deploy and manage them?
THE BENEFITS

Whether you take a high-enablement approach to mobile security or a more restrictive one, organizations of all types can enjoy a range of benefits.

PRODUCTIVITY AND PEACE OF MIND

With the right policies, tools and technologies in place, remote users are able to work free, worry-free. This heightened security gives workers the freedom to be more productive while giving IT greater peace of mind.

IMPROVED I.T. MANAGEABILITY AND ROI

MDM tools allow you to wrangle your widespread cross-platform mobile devices — including their security settings, applications and use — through automated, centralized administration. This enables you to optimize the functionality and security of a mobile communication network while minimizing cost and downtime, so you can support BYOD initiatives with confidence.

A BETTER OVERALL USER EXPERIENCE

When mobile devices are preconfigured with the right MDM security settings, remote workers don’t have to worry about them. This makes for a smooth, hassle-free user experience, which can result in greater worker productivity.

Top drivers for investing in mobility in 2012:

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaining productivity advantages</td>
<td>86%</td>
</tr>
<tr>
<td>Need for real-time information</td>
<td>81%</td>
</tr>
<tr>
<td>Lowering operating costs</td>
<td>67%</td>
</tr>
</tbody>
</table>

THE PROOF IS IN THE PRODUCTIVITY

According to CDW IT Monitor, nearly 75 percent of IT decision-makers surveyed thought the use of tablets and smartphones has led to an increase in productivity within their organization, with 25 percent saying it has improved productivity “significantly.”
As more and more users are taking their work to-go, a comprehensive mobile security plan can help keep IT in the driver’s seat. CDW can get you off to the right start. We’ve got the people, the products and the plan to help your initiatives take flight.
We partner with some of the most trusted names in mobile security. From VPN and BYOD to MDM, their innovative mobility solutions offer interoperability and cross-platform support.

**AirWatch's Mobile Device Management (MDM) solution**

Enables you to manage deployments of mobile devices. The solution provides the ability to quickly enroll devices in your environment, configure and update device settings over the air, enforce security policies and compliance, secure mobile access to corporate resources, and remotely lock and wipe managed devices.

**Cisco AnyConnect Secure Mobility Client**

Makes the VPN experience easier and more secure. Cisco Identity Services Engine (ISE) helps secure BYOD with automated user onboarding for consistent access, control and compliance. It gives access to user-, device- and application-based policy controls in a single pane — simplifying IT staff’s tasks and improving their productivity.

**Symantec Mobile Security**

Offers comprehensive protection for Android™ and Windows® mobile devices against malicious threats while ensuring compliance with regulatory requirements. Mobile Security provides antivirus technology, advanced firewall and SMS antispam features to ensure mobile assets and maintenance of compliance policies.

**Certifications**

- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification (GIAC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Security Essentials Certification (GSEC)
- PCI Approved Scanning Vendor (ASV)
- Cisco Certified Security Professional (CCSP)
- Cisco Certified Internetwork Expert (CCIE): Security
- Cisco Master Security Specialization
- Symantec Master Specialized Data Loss Prevention

**Awards**

- Cisco Americas Partner of the Year — 2011
- Cisco Americas Commercial Partner of the Year — 2011
- Cisco Americas Public Sector Partner of the Year — 2011
- Cisco Nationals Collaboration Partner of the Year — 2011
- Cisco West Area Borderless Networks Partner of the Year — 2011
- Cisco East Area Commercial Partner of the Year — 2011
- Cisco Central Area Partner of the Year — 2011
- Cisco Central Area Cisco Capital Partner of the Year — 2011
- Symantec Public Sector Partner of the Year — 2011
- Symantec SMB/Commercial Partner of the Year — 2011

Get tips for securing BYOD in our Reference Guide.

CDW.com/BYODguide

---

2 IDC, “The Application of Everything,” 2010
3 Cisco, “Visual Networking Index Forecast,” June 2012
4 Kaneshige, T. “CIO Challenge with BYOD: Don’t Fall Down the Rabbit Hole,” CIO.com, May 17, 2012
5 IDG, “Enterprise Mobility Survey,” June 2012

CDW®, CDW • G®, and PEOPLE WHO GET IT™ are trademarks of CDW LLC; all other trademarks and registered trademarks are the sole property of their respective owners.