Samsung Mobile Security

offering enhanced core capabilities for enterprise mobility with Samsung GALAXY

Samsung GALAXY Enterprise Mobility

Enterprise-ready Mobility management for your business

BROCHURE

Prepare your enterprise for the growing BYOD trend

As mobile devices, including smartphones and tablets, are embraced by a larger segment of consumers, employees are more likely to want to use their own equipment for both work and personal purposes. In fact, estimates show that by the end of 2011, almost half the mobile devices used for work purposes were owned by employees, not employers. This presence of employee-owned mobile devices in the corporate environment is growing quickly. The phenomenon has been labeled “bring your own device,” or BYOD, and although it increases freedom for employees, it also creates security risks for organizations. BYOD introduces new risks that must be explored by each company’s IT management and mitigated with the appropriate technology.

Although BYOD increases freedom for employees, it also creates security risks for organizations.

Safeguard your organization against damaging security breaches

The BYOD trend presents several risks to enterprises, such as information theft, confidentiality leaks and virus infections:

- Personal and corporate data may become comingled.
- Small mobile devices are easily lost or stolen.
- Companies can become liable for accidental loss of users’ personal data.
- Compromised devices can be stolen and hacked, leaving on-device and network data vulnerable to theft and misuse.
- Data can be inadvertently shared by users.
- Third-party programs can result in data incompatibility and viruses that spread throughout the data network.
- Companies may not be able to meet compliance mandates.
- Insufficient security measures can lower device performance.

As more employees are dealing with both private and corporate information on their mobile devices, employers need better and safer mobile security infrastructures to keep up with the BYOD trend. Mobile security and manageability are the foremost concerns of CIOs. Yet, companies are still struggling to manage and monitor individual mobile devices, and many CIOs are less than confident that the security measures currently in place in their enterprise would satisfy an auditor. Gartner reports: “Only 27% to 28% believed their mobile security would satisfy an auditor, 41% to 42% believed it wouldn’t and the remainder were not sure.” [1]

Samsung Mobile Security helps companies customize and expand security technology.

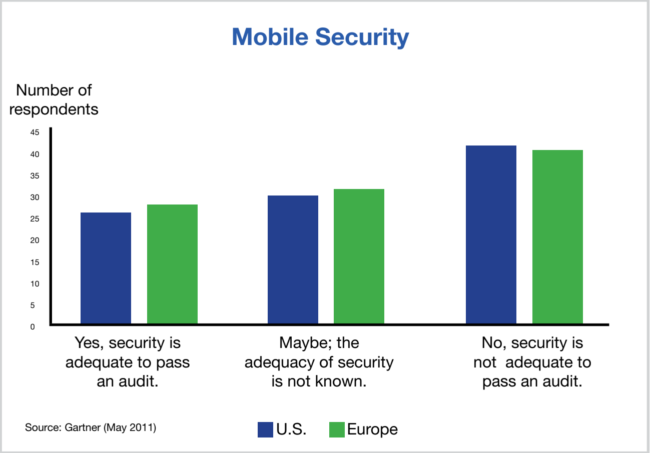

Figure 1. CIO confidence in current mobile security

To succeed with the BYOD trend, CIOs must ensure that their IT groups are armed with a relatively new genre of powerful tools that address several aspects of mobility management and security. Such tools make it possible for IT organizations to set and enforce corporate data policies across the mobile workforce without sacrificing usability.

Solutions to the BYOD problem are quickly maturing. To ensure robust mobility management, organizations require several critical security components:

- User authorization and authentication
- Virtual private network (VPN) and over-the-air (OTA) encryption
- Remote find, wipe or kill
- Hard-drive encryption
- URL, content and program download filtering
- Policy creation and enforcement

As an Android tablet and smartphone manufacturer, Samsung is committed to helping enterprise environments manage and secure their mobile deployments. Samsung products interoperate with leading suppliers of mobile device management (MDM), VPN security and other mobile security technologies, enabling enterprises to deliver an outstanding user experience while keeping corporate data assets secure.

Samsung Mobile Security includes four technologies that provide comprehensive data protection for mobile devices:

1. **MDM**. Provides broad compatibility for a wide variety of partner solutions. It enables companies to control certain functions on employee-owned mobile phones to comply with company security policies.
2. **VPN connectivity**. Provides mobile professionals with secure connections to corporate resources from almost anywhere.
3. **Samsung On Device Encryption (ODE)**. Provides a high level of encryption for internal and external memory. It protects data in the event of loss or theft. Samsung ODE provides the best device encryption technology and is Federal Information Processing Standard (FIPS) 140-2 certified.
4. **Samsung Enterprise Software Development Kit (SDK)**. Helps companies expand mobile security technology and functionality and develop additional IT policies.

These enhanced core capabilities for enterprise mobility are available only on Samsung Android devices. These qualifications clearly distinguish Samsung GALAXY smartphones and tablets from other Android mobile devices.

Many CIOs are less than confident that the security measures currently in place in their enterprise would satisfy an auditor.

MDM maximizes ROI, increases employee productivity and decreases IT support.

Optimize mobile security with MDM

MDM enables your IT department to watch, control and administer all deployed mobile devices, across multiple mobile service providers. MDM functionality consists of remote deployment of applications, data and settings. With enhanced MDM, most mobile security failures can be prevented. Samsung Mobile Security offers comprehensive MDM capabilities to enable efficient, scaled mobile deployments.

Samsung Mobile Security provides broad compatibility for most prominent MDM partner solutions and offers technology that addresses critical management and security issues. Samsung is dedicated to satisfying customer needs and offering exceptional value. Samsung works closely with MDM solution partners to provide to customers IT security policies that competitors cannot offer. These exclusive security policies are developed through collaboration with MDM partners and have been made available only by Samsung.

With 338 IT policies through 727 application programming interfaces (APIs), Samsung Mobile Security enables companies to enhance software and hardware component control and prevent mobile security failures.

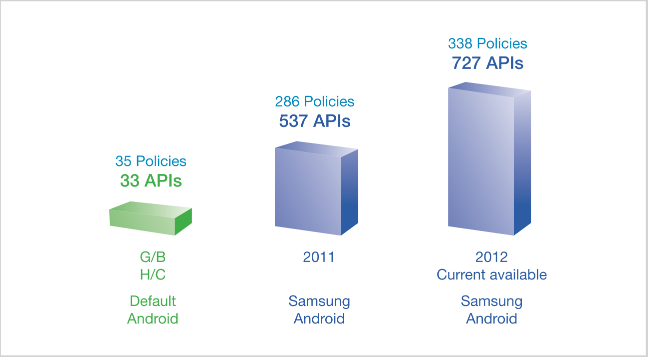

Figure 2. Samsung Mobile Security APIs

Samsung GALAXY mobile devices provide ultimate flexibility for IT administrators by allowing them to remotely manage mobile applications and overall device functionality. With Samsung GALAXY mobile devices, IT administrators can:

- Remotely control devices using help desk-like functionality
- Configure and update settings over the air
- Monitor and enforce compliance with corporate IT policies
- Remotely wipe or lock managed devices
- Enable or disable specific capabilities, such as camera, Wi-Fi, Bluetooth, microphone and data roaming

Enhanced MDM provides companies several benefits. It:

- Maximizes ROI on mobility by increasing employee productivity and decreasing IT support
- Provides strong security, including IT policy management, certificate authority and theft protection
- Reduces business risks and downtime
- Supports BYOD without compromising security or user experience, and balances security and privacy for employee-owned devices

MDM solution partners include SAP, SOTI, MobileIron, AirWatch and many more, with the number of partners continuing to increase.

Samsung Mobile Security MDM partner solutions

- SAP
- SOTI
- MobileIron
- AirWatch
- Juniper Networks
- Over 35 others, including Zenprise, SDS and Fiberlink

Samsung GALAXY maintains the industry's highest standards for VPN security.

Ensure safe accessibility to corporate networks with VPN security

Samsung's support of VPN connectivity provides mobile professionals with behind-the-firewall access for a secure connection from anywhere. Samsung is the first company to provide Secure Sockets Layer (SSL) VPN with Juniper Networks for the Android platform and is the leader in mobile security for Android-enabled mobile devices.

Samsung GALAXY mobile devices maintain the industry's highest standards for VPN security. GALAXY devices support protocols and authentication measures that provide security and faster access for enhanced off-site productivity. Enterprise users are provided an optimized, secure path to corporate resources from their device:

- Corporate intranet and email
- Network resources
- Software applications

The devices provide broad VPN compatibility for most partner VPN solutions and cover all levels of VPN security, including IPsec, PPTP and L2TP.

Samsung works with several VPN providers, such as Cisco, F5 and Juniper Networks, to enable IP-based encryption for secure, persistent, behind-the-firewall access to critical enterprise assets through Wi-Fi and cellular network connections.

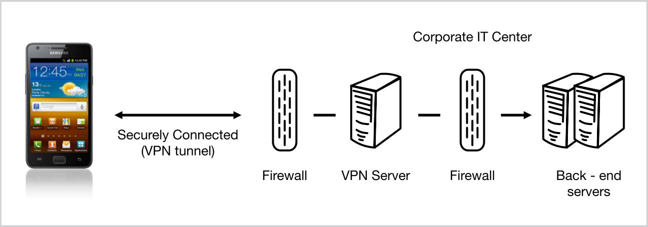

Figure 3. SSL VPN solution architecture

Samsung Mobile Security VPN partner solutions

- Cisco
- Juniper Networks
- F5
- Others

Samsung Mobile Security provides a high level of encryption and an enhanced security platform.

Rely on high-level device encryption to safeguard data with Samsung ODE

Samsung ODE-embedded Android devices help companies achieve higher levels of mobile device encryption for internal and external memory to prevent data loss or theft. Samsung ODE prevents unauthorized access by converting data to an unreadable format reversible only by security key or password, and uses AES-256 bit encryption to mitigate the risk of virtual or physical attack. Samsung ODE provides internal (device and internal secure digital, or SD card) and external (SD card) storage encryption. The internal storage encryption protects corporate or customer information, preferences and databases. The external storage encryption protects the separate SD card. SD card encryption is a Samsung exclusive function not supported on the native Android platform.

Samsung's ODE solution provides a high level of device encryption. Samsung GALAXY mobile devices that use Samsung ODE have been granted FIPS 140-2 Security Certification from the US government, making Samsung ODE the first FIPS 140-2-certified solution for Android-enabled devices. Issued by the National Institute of Standards and Technology, FIPS is a US security standard that helps ensure companies that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information can make informed purchasing decisions when choosing devices to use in their workplace.

Using advanced device encryption technology, Samsung ODE helps companies prevent the loss or exposure of confidential corporate data if a mobile device is misplaced or stolen. The Samsung ODE hardware acceleration feature enables mobile users to safeguard corporate data (such as email, documents and customer information) and private data (such as photos). Mobile users can also experience exceptional performance when using Samsung mobile devices.

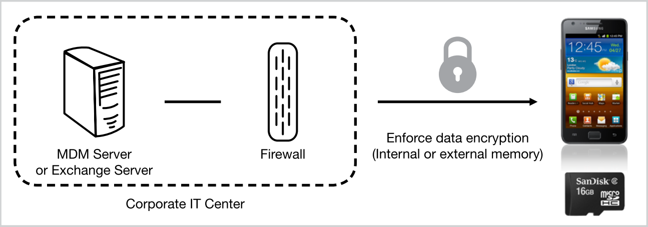

Figure 4. Samsung ODE architecture

Update mobile security technology with Samsung Enterprise SDK

To achieve greater mobile security, enterprises need a mobile security platform that supports IT policies for different security issues. Samsung Enterprise SDK enables companies to enhance their mobile security platform to embrace third-party mobile security solutions on Samsung Android-enabled devices.

Samsung Enterprise SDK also enables enterprises to design and develop more advanced applications to meet higher security standards. With this ability, companies can reduce security threats and risks, such as theft of sensitive corporate data from lost or stolen devices.

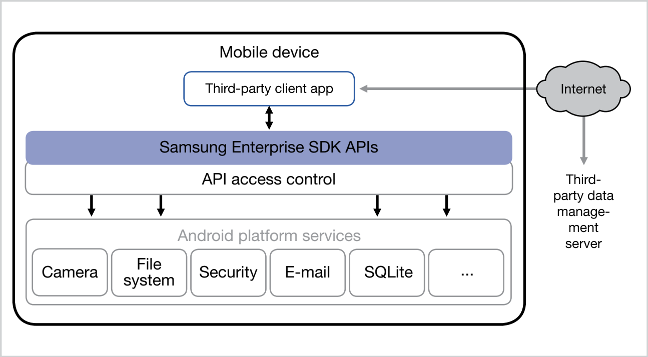

Figure 5. Samsung Enterprise SDK framework

Samsung offers solutions for the growing BYOD trend.

Keep your data safe with enterprise-ready Samsung Mobile Security

BYOD enables workers to consolidate personal and business functions in one mobile device. However, BYOD presents challenges to companies, which must be confident that employees' devices meet enterprise security standards. Though BYOD is a growing phenomenon, many CIOs doubt the effectiveness of current security measures. Samsung now offers robust mobile security options for Android-enabled mobile devices.

Samsung is leading the mobile security market by offering a high level of partnership with MDM- and VPN-related vendors, and developing more advanced technology with Samsung ODE and Samsung Enterprise SDK. Using MDM, VPN, Samsung ODE and Samsung Enterprise SDK, enterprises can safely access all their corporate information and keep their personal data private, without compromising functionality or security as a result of mobile device loss or theft.

Samsung GALAXY devices are designed to maximize the efficiency and productivity of large enterprise users. With incorporated Samsung Mobile Security solutions, Samsung GALAXY devices are ideal for widespread corporate deployment. Enterprise-ready Samsung GALAXY devices meet rigorous security criteria and are configured specifically for business use. The deployment of GALAXY devices helps ensure that your organization's mobile workforce is protected to the greatest possible degree.

For more information

For more information about Samsung Mobile Security, visit www.samsung.com/enterprise

1. Nick Jones, "CIO Attitudes Toward Consumerization of Mobile Devices and Applications," Gartner, Inc., May 25, 2011.

Samsung Electronics Co., Ltd.
416, Maetan 3-dong,
Yeongtong-gu
Suwon-si, Gyeonggi-do 443-772,
Korea

www.samsung.com

SAMSUNG

TO CIOs,

WE APPRECIATE THE CHALLENGES YOU FACE.

When you want to	We can support
Prevent breaches in mobile security,	Top-tier MDM solutions with 338 IT policies.
Keep business communications safe without limit,	Enhanced Exchange ActiveSync.
Ensure high-level of safe accessibility to corporate networks,	Expanded VPN Protocols : SSL, IPsec, L2TP, PPTP.
Guarantee proven device encryption to secure corporate data,	Samsung On Device Encryption, the first to receive FIPS 140-2 Security Certification for Android devices.
Use one device for both personal and work,	Personal and enterprise separation using Virtualization.

We are prepared. Samsung GALAXY

The aim of every Samsung GALAXY device is to maximize efficiency and productivity of enterprise users.
To learn more, visit www.samsung.com/enterprise or contact enterprise@samsung.com.