verizon

Platform Guide for

SAMSUNG ANDROID

Making the Android platform business and government ready

CONTENTS

SAMSUNG AND VERIZON 4G LTE: REINVENTING SECURITY FOR ANDROID DEVICES

In the past year, the number of mobile devices deployed in the business world and throughout government agencies has grown dramatically—and so has the number of mobile security threats. In particular, attacks on Android™ devices have been increasing at an alarming rate.

*IN 2012, **ANDROID WAS BY FAR THE MOST COMMONLY TARGETED MOBILE PLATFORM**, WITH 103 OUT OF 108 UNIQUE THREATS.*

—SYMANTEC 2013 INTERNET THREAT REPORT

As a result, IT administrators are tasked with trying to minimize risk and protect data and network resources. Mobile security and manageability have become the top priorities for IT managers who are struggling to control a multitude of device platforms, applications and compliance policies.

While the openness of the Android platform contributed to its success in the marketplace, the resulting variants of its application and update distribution methods, as well as its dominating market share, have made Android the go-to platform for malware authors and hackers.

The fragmented Android ecosystem—the result of different versions, different device manufacturers and different carriers—makes it difficult for updates to be quickly deployed universally for all Android users. These inconsistencies between mobile devices can leave data vulnerable to attack. And these attacks are expected to become harder to prevent, more aggressive and more sophisticated in the near future.

However, with the abundance of Android applications and built-in access to Google Services, the Android platform is still the most popular choice for smartphone users and, as such, is quickly invading the workplace. Android devices give employees the powerful productivity features they want, so they can quickly and easily access business information, collaborate with colleagues and clients and even create content while traveling or working in the field.

Employee use of Android devices can help increase efficiency, which is good for business and the bottom line—but leaves IT managers asking themselves how they can support this demand while keeping the enterprise infrastructure safe and compliant.

FROM FRAGMENTED TO UNIFIED

As industry leaders, Samsung and Verizon understand the challenges of today's mobile business environment, and have joined forces to deliver new solutions that address the issues of Android fragmentation and satisfy the management and security needs of today's enterprise and government agencies.

Samsung has now systematically defragmented Android with a comprehensive and powerful platform variant called Samsung Approved for Enterprise (SAFE™), making all SAFE-certified devices consistent on the same platform version and with the same security features.

This innovative solution provides enterprise-level security that IT managers can feel confident about, while giving employees all the best productivity features that Android devices are known for.

With SAFE running on the secure Verizon 4G LTE network, enterprises can protect their network investments to deliver a secure, mobile productivity experience to their employees who want to work on Android enterprise-ready tablets and smartphones.

SAMSUNG SAFE:
SAFE DEVICES SUPPORT MOBILE DEVICE MANAGEMENT AND ENTERPRISE SECURITY.

SAFE represents the growing family of Samsung® Mobile Enterprise solutions that include the necessary security and feature enhancements suitable for business use.

Samsung SAFE devices exceed business requirements by:

+ Providing IT policies and certificate management along with comprehensive data security.
+ Limiting Android fragmentation by establishing a consistent level of IT compliance between all SAFE devices.
+ Simplifying mobile device management (MDM) by enabling remote, centralized support.
+ Maximizing return on investment (ROI) by increasing mobile productivity and boosting user satisfaction.

SAFE helps IT effeciently manage and secure the enterprise mobile enviroment with:

Corporate Email/Calendar/Contacts

SAFE goes well beyond native Android to cover 95% of Microsoft® Exchange ActiveSync® (EAS) IT policies and features.

This enables push synchronization of email, contacts and calendar items to SAFE devices, enhancing business-critical functions and maximizing efficiency.

Standard Android Features

+ Direct push
+ Email/Calendar/Contacts sync
+ Remote wipe
+ Multiple folder sync
+ Global address lookup
+ HTML email view
+ Auto-discover
+ Meeting request accept/reject

Additional Samsung Features

+ Out-of-office assistant
+ Follow-up flags
+ High-importance status
+ Partial download
+ Conversation view
+ SMS sync and voicemails in in-box
+ Task sync
+ Free/busy lookup
+ Invite response editing
+ Propose new meeting time
+ Access calendar from invite

With powerful on-device encryption and the support of leading third-party MDM providers, Samsung devices include all the necessary features to address the mobile challenges of employee and company-owned devices—they are enterprise-grade, IT compliant and secure for business use.

AbsoluteSoftware

airwatch™ mobile device management

Centrify®

CITRIX®

Fixmo®

MobileIron

SOTI® WE MAKE MOBILITY WORK

SYBASE®

On-Device Encryption

SAFE features mobile encryption support which is easily implemented and does not sacrifice performance or functionality. This provides peace of mind for IT administrators through comprehensive encryption of all data, including app-specific internal data and internal/removable memory. Added performance comes from fast boot-up and conversion time during the initial device encryption process.

On-device encryption can be enabled:

+ Through Microsoft EAS IT policy.
+ Through third-party MDM IT policy.
+ Manually on the device.

Virtual Private Network

Samsung's support of virtual private network (VPN) connectivity provides mobile professionals with secure connections to corporate resources from almost anywhere. SAFE devices support protocols and authentication measures that enhance offsite productivity with better security and faster access to corporate resources from their device, such as:

+ Corporate intranet and email
+ Network resources
+ Software applications

Samsung works with a number of VPN providers to enable IP-based encryption for secure, persistent, behind-the-firewall access to critical enterprise assets via Wi-Fi and the Verizon network.

Mobile Device Management

Comprehensive MDM enables efficient and scaled mobile deployments while offering solutions that address even the most challenging management and security issues. Under the SAFE program, Samsung works directly with leading third-party MDM providers to offer over 338 IT policies.

SAFE MDM support provides a wide range of benefits for IT administrators to:

+ Support "desktop-like" central management.
+ Wirelessly configure and update settings.
+ Monitor and enforce compliance with corporate IT policies.
+ Remotely wipe or lock managed devices.
+ Control access to application stores and silently push/remove applications.
+ Remotely enable/disable capabilities, such as:
  - Camera
  - Wi-Fi
  - Bluetooth®
  - Microphone
  - Data roaming

SAMSUNG KNOX: A MORE COMPREHENSIVE LEVEL OF BUSINESS SECURITY AND PERSONAL PRIVACY

Samsung KNOX-capable devices enhance the SAFE platform's capabilities,* providing a deeper level of security with additional platform and application security features:

*Available on Knox-capable devices only.

For enterprise, government and regulated industries that need a high level of security and an employee-owned device solution, Samsung KNOX is the answer.

With its multi-tiered security model and industry-leading device management capabilities, Samsung KNOX fully addresses the shortcomings of the open-source Android platform for broad adoption to meet the needs of:

IT Administrators

Safeguard corporate data with KNOX's multi-layered security model and enhanced device management support. KNOX protects against data leakage, malware and malicious attacks, and offers more comprehensive management and enterprise integration capabilities.

Business Decision Makers (BDMs)

KNOX provides a secure dual-persona environment that separates personal and business data. Users remain productive, and confident about personal privacy on a device they want to use.

Federal Government and Regulated Industries

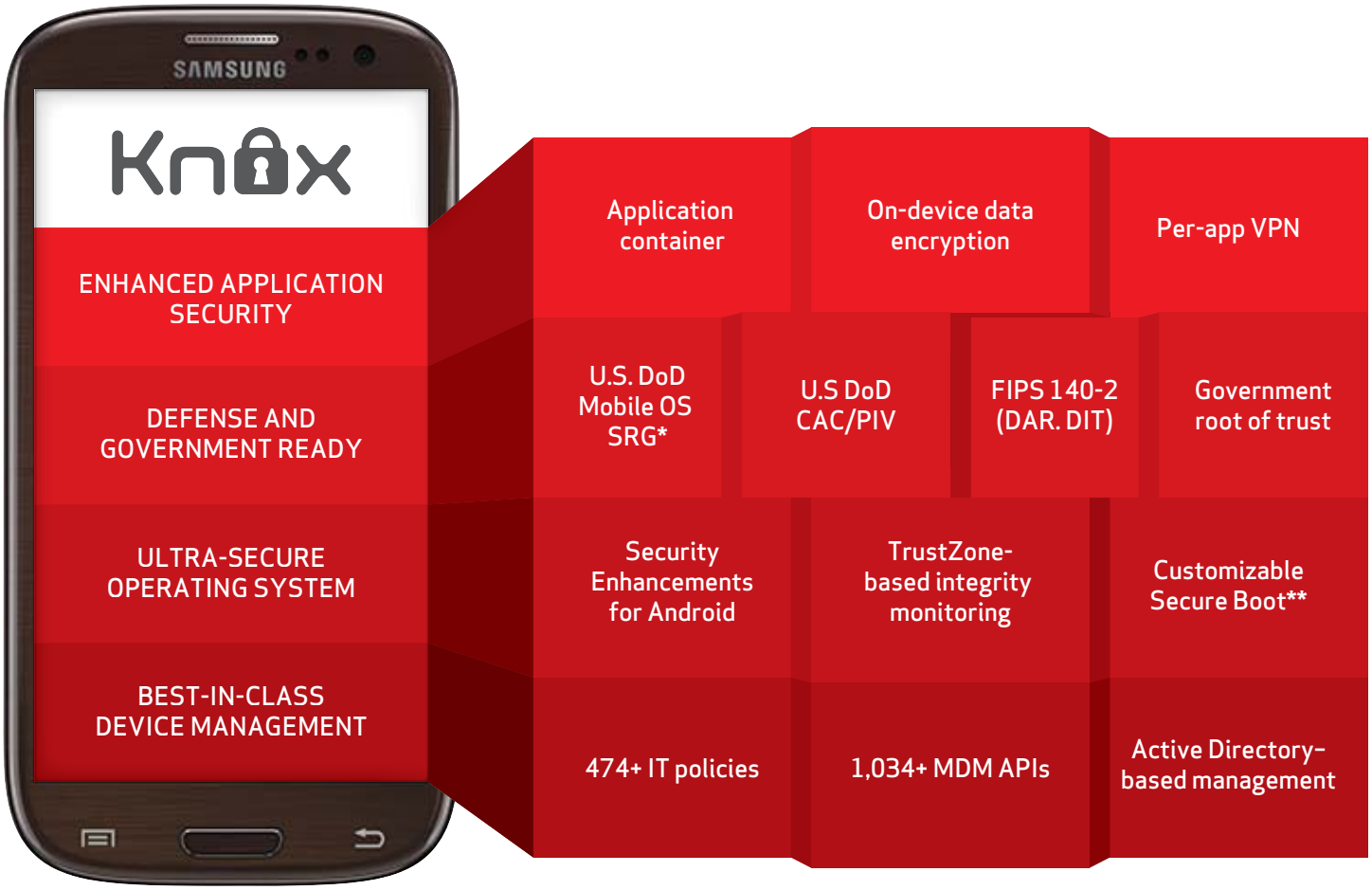
With its unique application container technology and high-level security features such as Boot Attestation, Common Access Card (CAC) support and National Institute of Standards and Technology (NIST) certifications, KNOX meets stringent government security requirements for mobile devices and puts security control in the hands of government agencies and regulated businesses.

Designed from the Ground Up with Security at the Forefront

Samsung KNOX incorporates key technologies patented by the National Security Agency (NSA) and leverages hardware-level features to provide enhanced security to protect the operating system (OS) and applications.

In addition, Samsung KNOX has been submitted to the U.S. government, including the Department of Defense (DoD), to test compliance with initiatives, requirements and standards for mobile device security, which enables its use in government and other highly regulated environments.

Samsung KNOX, combined with its unique application container technology, supports both employee-owned and corporate-liable devices without compromising corporate security or employee privacy. KNOX retains full compatibility with Android and the Google® ecosystem, while integrating fundamental security and management enhancements.



SAMSUNG KNOX DELIVERS: PLATFORM SECURITY + APPLICATION SECURITY + MDM

Platform Security

KNOX addresses security at the operating-system level, with a comprehensive, three-pronged strategy that includes:

Security Enhancements for Android (SE for Android)

Security Enhanced Linux (SE Linux) is a technology invented by the NSA in 2000. SE for Android provides an enhanced mechanism to enforce the separation of information which is based on confidentiality and integrity requirements. It incorporates a strong, flexile Mandatory Access Control (MAC) architecture into the device kernel that isolates applications and data into different domains on the device.

KNOX is provisioned with a set of security-policy configuration files designed to strengthen the core Android platform. This architecture prevents a compromise in one domain from affecting others.

Customizable Secure Boot

Secure Boot is the first line of defense against malicious attacks on KNOX-enabled mobile devices. It is a procedure that prevents "unauthorized" operating systems and software from loading during the startup process. It requires the device boot-loader, kernel and system software to be verified by the device hardware. The secure boot loader will only continue if the authorized secure binaries signed by the hardware are present. Next, Secure Boot verifies the cryptographic signature of the kernel and system image before handing control to the OS.

TrustZone-based Integrity Measurement Architecture (TIMA)

KNOX utilizes SE for Android to enforce MAC policies to isolate applications and data within the platform. TIMA was developed to close vulnerabilities by continuously monitoring the device kernel. If TIMA detects that the integrity of the kernel is violated, it notifies the IT administrator via the MDM console, which can then take policy-driven action.

In a survey of 500 leading British CIOs, conducted by Virgin Media Business, ***51% indicated their secure IT network was breached due to employees using personal services.***

Application Security

Data leakage is common when a user sends sensitive information outside of the corporate network via a personal email account, social network site or public cloud storage system.

In addition to securing the platform, Samsung KNOX provides solutions to address the security needs of individual applications, including:

Application Containers

The Samsung KNOX container provides a separate Android environment within the mobile device, complete with its own home screen, launcher, applications and widgets. It empowers enterprises to embrace the employee-owned device (EOD) trend by creating a secure zone in the employee's device for corporate applications. Access to corporate data and network resources can then be restricted to applications within the container, providing a secure, virtual Android environment for business use, separate from personal apps and content. This isolation of applications and data within the container enables a powerful solution for data leakage associated with the EOD model.

Samsung KNOX ensures that any data downloaded from the enterprise, such as email attachments and files, cannot be accessed by applications outside the container. All the data stored by applications inside the container are encrypted via strong encryption algorithms (AES-256). A password is required to gain access to applications inside the container.

KNOX Advanced On-Device Data Encryption

The use of NIST-compliant algorithms for on-device encryption (ODE) in Samsung KNOX devices satisfies federal data-at-rest (DAR) requirements. The ODE feature allows users and IT administrators to encrypt the entire device including the SD card, as well as any configured Samsung KNOX container.

The ODE feature on Samsung devices uses a Federal Information Processing Standards (FIPS) 140-2–certified kernel encryption (AES-256), and offers the levels of security required by government and regulated industries. Encryption can be activated directly by the user via the Settings user interface, or remotely by the IT administrator as a policy setting, using Exchange ActiveSync or an MDM system.

KNOX High-Level VPN Support

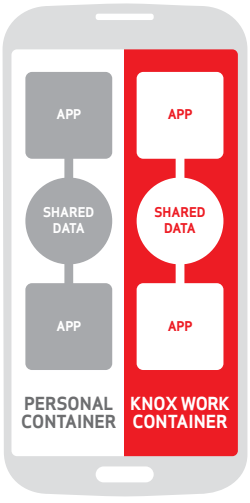
Samsung KNOX offers a high level of comprehensive support for VPNs. This enables an optimized, secure path to the enterprise intranet from their EOD or corporate-issued devices. Samsung KNOX VPN is FIPS 140-2 certified, enabling its use in regulated environments like government, healthcare, finance, etc. Its implementation offers broad support for the IPsec protocol suite:

+ Internet Key Exchange (IKE and IKEv2)
+ Triple DES (56/168-bit), AES (128/256-bit) encryption
+ Split tunneling mode
+ NSA Suite B Cryptography

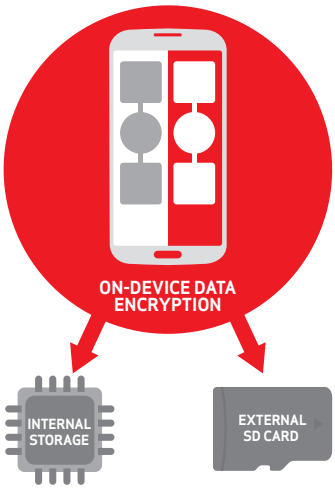
Another distinguishing feature of Samsung KNOX VPN is the ability to configure, provision and manage the use of VPN on a per-application basis. This capability allows the administrator to automatically enforce the use of VPN only on a specific set of corporate applications. This ensures that data is communicated on a secure connection, while keeping the user's personal data from overloading the company's Internet connection. In addition, the per-app VPN feature allows personal-use applications to bypass the VPN and connect directly to the Internet, preserving user privacy.

Other features of Samsung KNOX VPN implementation include:

+ Up to five simultaneous VPN connections
+ RSA SecurID® support for Cisco® VPN gateways
+ CAC support for government use



Application Containers



KNOX Advanced On-Device Data Encryption

KNOX High-Level VPN Support

KNOX Mobile Device Management (MDM)

KNOX builds upon Samsung's industry-leading SAFE MDM capabilities by providing additional policies for security, integration and applications, such as asset tracking, remote control and more. With KNOX, IT can monitor, control and administer all deployed mobile devices across multiple mobile service providers.

The rich set of MDM policies enables IT administrators to better manage employee- and corporate-liable devices and offer improved support by being able to remotely configure various features, including Wi-Fi, VPN and email.

Specific MDM enhancements include:

+ Policies to comply with the U.S. DoD Mobile OS Security Requirements Guide (MOS SRG)
+ Support for Samsung KNOX containers
+ Support for management via ActiveDirectory/Group Policy Manager
+ VPN and Wi-Fi provisioning
+ Idle-screen and lock-screen configuration

ENTERPRISE NEED	KNOX MDM POLICY GROUPS*	
Remote Management	+ Wi-Fi	+ Security
	+ Bluetooth	+ Password
	+ Email accounts	+ Browser
Limited Features and Functions	+ Kiosk mode	+ Application permissions
	+ Firewall	
Secure Access to Enterprise Resources	+ VPN	+ Exchange account
	+ Application	
Geofencing	+ Location	
Real-Time Access to Enterprise Resources	+ Device inventory	
Manage Voice and Data Usage	+ Roaming	+ Phone restrictions
	+ VPN settings	
Real-Time Mobile User Support	+ Remote control	
Prevent Data Leakage	+ Email forwarding	+ Container management
	+ Inegrity management	
Enterprise Integration	+ Single sign-on	+ Active directory

*Availability of Samsung KNOX features may vary by MDM partners.

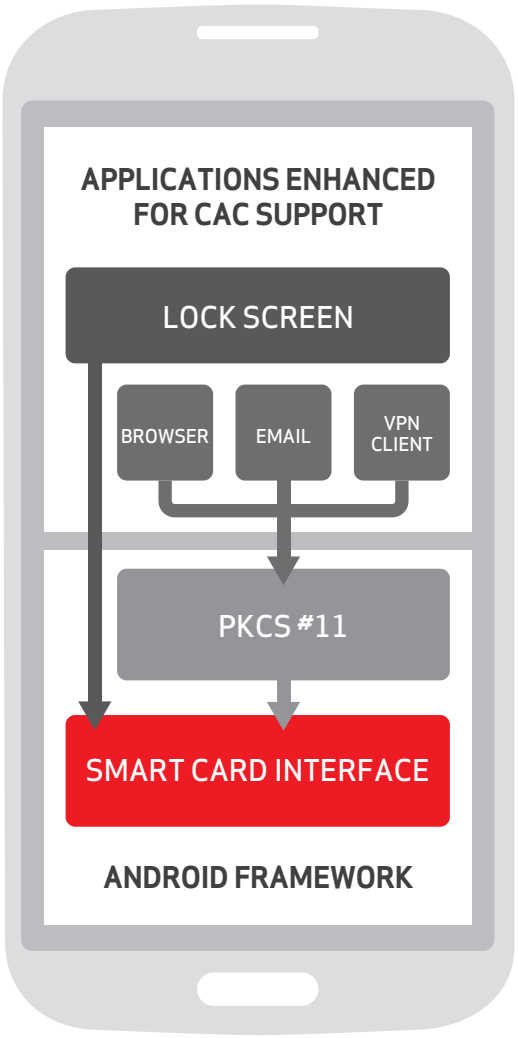
KNOX FOR GOVERNMENT AND HIGH-SECURITY USE: HEIGHTENED SECURITY FOR SENSITIVE INFORMATION

Smart-Card/CAC Support

The U.S. DoD has mandated the use of Public Key Infrastructure (PKI) certificates, enabling employees to "sign" documents digitally, encrypt and decrypt email messages and establish secure online network connections.

In compliance with DoD regulations, Samsung KNOX allows the PKI certificates to be stored securely on the mobile device (software certificates) or be retrieved from a CAC (hardware certificates).

Samsung KNOX provides applications with access to the hardware certificates on the CAC via Public-Key Cryptography Standards (PKCS) application programming interfaces (APIs). This enables the use of the CAC by the browser, email application and VPN client, as well as other custom government applications. In addition, Samsung KNOX allows the lock screen to be secured by the CAC, providing an additional level of device security.



Certification and Validations

Issued by the NIST, the FIPS are a U.S. security standard that helps companies that collect, store, transfer, share and disseminate sensitive-but-unclassified (SBU) information and controlled unclassified information (CUI).

FIPS 140-2 Level 1 certification

Samsung KNOX meets the requirements for FIPS 140-2 Level 1 certification for both DAR and data in transit (DIT). The Samsung KNOX support for DIT covers the following:

+ Web browser (HTTPS)
+ Email (S/MIME)
+ IPsec VPN

Defence Information Systems Agency (DISA) MOS SRG Compliance

The Defense Information Systems Agency (DISA) is an agency within the U.S. DoD that publishes Security Requirements Guides (SRGs) to improve the security of DoD information systems. SRGs guide the development of Security Technical Implementation Guides (STIGs), which document specific product policies and requirements, as well as best practices for configuration.

In 2012, the DISA published the Mobile Operating System (MOS) SRG to specify the security requirements that commercially available mobile devices should meet in order to be deployed within the DoD. On May 2, 2013, DISA approved the STIG for Samsung KNOX drafted for the MOS SRG.

The tables and information in the above section were provided by the Samsung KNOX white paper which can be found at:
https://www.samsung.com/global/business/business-images/resource/white-paper/2013/06/Samsung_KNOX_whitepaper_June-0.pdf

STAYING A STEP AHEAD: MAXIMIZING PRODUCTIVITY WITHOUT SACRIFICING SECURITY

Samsung devices running over the secure Verizon network provide all the functionality and coverage employees need for peak performance on the go. Productivity features include:

S Beam

Using Near Field Communication (NFC) and Wi-Fi Direct™ protocols, S Beam lets users share multimedia files in real time by simply tapping phones together.* S Beam supports the transfer of files up to 1 GB in size. They can also quickly send contacts, calendar events and links, as well as actual files like photos, videos and documents to remote coworkers.

S Beam in Action:

Steve, a field engineer, needs to send a 40 MB tutorial to another engineer that he's working with in the field, but the file is too large to send as an email attachment. Using S Beam, Steve can send simply tap his phone with his coworker's phone and send the video tutorial and technical specification documents in less than 10 seconds.

Samsung Link

Samsung Link connects multiple devices so you can access presentation, documents, product videos and more from multiple locations. View, play and send content from one device to another or access saved content on storage services such as Dropbox and SugarSync. With a simple touch, you can send files from your mobile device to a smart TV, computer, smartphone or tablet for enhanced viewing.

Samsung Link in Action:

While conducting a presentation at a client's office, an account exec's notebook suddenly dies. She simply uses Samsung Link on her smartphone to quickly access the file from her cloud-based email. Once she locates the file, she just connects her phone to the monitor to continue the presentation. It's that easy.

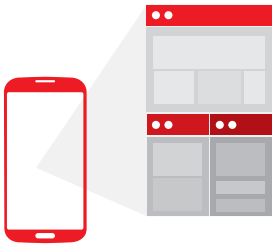
Smart Pause

Smart Pause* senses when you look away and automatically pauses the video you're watching. When you look back at the screen, it resumes playing the video where you left off—so you don't miss anything.

Smart Pause in Action:

A financial advisor is sharing a product portfolio video during a client consultation. When the client interrupts the video with a question and the advisor looks away from the device screen, the video pauses automatically. As soon as he turns his head to resume watching, the video resumes play right where it paused.

*Available on Android Beam- and S Beam-capable devices.

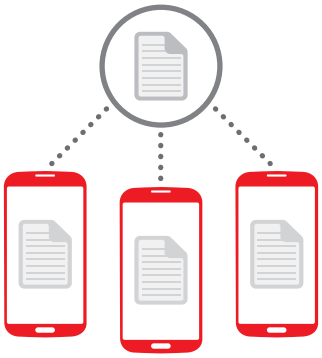


Multi-Window Support

See and use multiple applications at once with Dual View and Cascade View—resulting in shorter response times, faster interaction and greater visibility into all business activity.

Multi-Window Support in Action:

As a busy retail executive, Michelle spends about 75% of her time on the road visiting store locations in her region and attending industry events. Multi-Window Support on her Samsung device lets her easily complete multiple tasks on one screen. The feature helps her increase productivity and save time as she takes notes while watching a training video.



Group Play

Group Play lets multiple people view and interact with content at the same time, with each person on their own mobile device. During a presentation, you can mark up content in real time using the touch screen, and all attendees can see the changes as you make them.

Group Play in Action:

Peter, CEO of a top marketing firm, and his dispersed PR and marketing team need to collaborate in real time to meet a deadline for finalizing his keynote speech at an important industry event. With Group Play, the writer can make updates and the creative director can adjust the presentation layout, and the rest of the team can see the adjustments as they happen.

Additional Features

S Voice. A personal voice-activated assistant that can launch apps and turn-by-turn navigation; voice dial; compose a memo; search contacts; schedule tasks; and unlock the phone.

Air View and S Pen. Preview emails, videos, calendar and more, without having to open them. Simply hover over email and messages to preview what's inside.

ChatOn. A global communication service available in more than 120 countries and supporting up to 62 languages, ChatOn lets you collaborate instantly with remote coworkers and clients through chats, screen and calendar sharing. ChatOn works seamlessly across your smartphone, tablet and PC. All you have to do is sign into your Samsung account.

S Translator. A handy companion while traveling abroad, S Translator allows you to easily communicate with locals and colleagues. You can explore your surroundings by quickly translating typed or spoken phrases into nine languages, as well as hear the translations aloud to ensure accuracy.

Polaris Office. Polaris Office is a pre-installed productivity app you can use to view, edit and create documents, spreadsheets and presentations in Microsoft Office formats. Easily send files to yourself and others by email or an online file-sharing service such as Dropbox. You can also convert the files to Adobe® Portable Document Format (PDF), as well as open and read PDF files directly.

THE ULTIMATE IN BUSINESS PORTABILITY

As the top smartphone manufacturer worldwide, Samsung offers innovative, in-demand tablets and smartphones that employees want.

Smartphones

Today's advanced smartphones are essentially computers, capable of accessing key corporate resources that mobile workers need.

Employees are most likely to use smartphones to stay:

+ Informed by easily checking and responding quickly to email.
+ Productive during downtime like waiting in the security line at the airport or during a taxi ride to meet a client.

For employees on the go, smartphones provide freedom by placing the work environment at their fingertips, providing real-time access to valuable business information sent across the Verizon network. This highly portable device is helping make mobile employees more responsive, more flexible and better on-the-fly decision makers. Smartphones are always-on devices that allow employees to be available anywhere and anytime by voice, email or text.

Tablets

Tablets help employees get things done quickly, so business can operate more efficiently.

The tablet landscape is evolving rapidly, making tablets one of the most transformative tools in a mobile engagement and the fastest-adopted devices in history.

Tablets offer businesses a high return on mobility by making remote workers more productive, so:

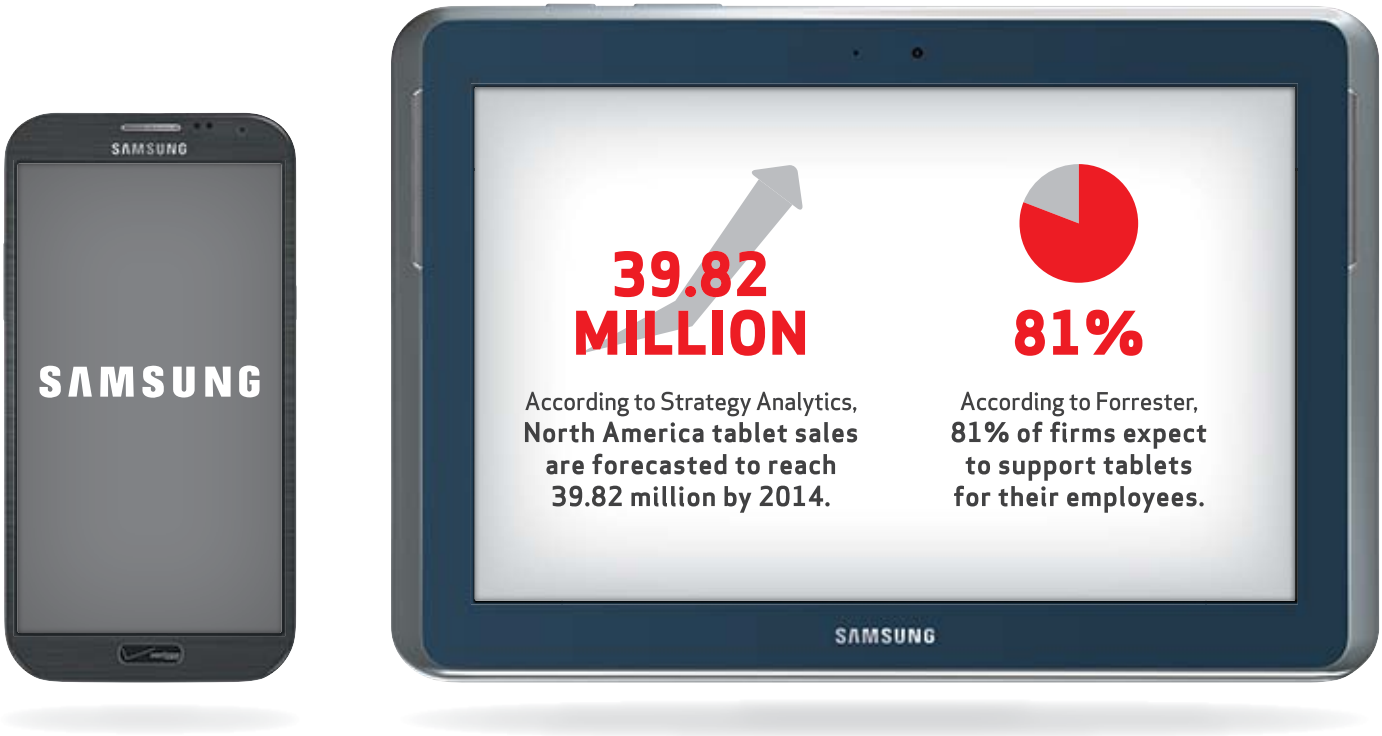
Employees Spend More Time Working.

Tablets give workers anywhere, anytime access to corporate infrastructure. Because tablets offer a faster boot time, fewer hassles when updating device software and a more portable form factor, users spend more time working in places they wouldn't typically consider with a laptop.

Employees Stay Connected to What Matters Most.

From the warehouse to the sales floor, companies are creatively using tablets to connect employees with customer relationship management (CRM) systems, email, intranet portals, sales force automation, instant messaging systems, order management systems and more— to enhance productivity, accessibility and drive bottom line growth.

With automatic connectivity to the secure Verizon 4G LTE network, users spend more time working and less time searching for an Internet connection for their device.



KNOX is not currently available on tablets. SAFE is available on SAFE-enabled tablets

FOR BEST RESULTS, PAIR SAMSUNG SAFE AND KNOX WITH THE RIGHT WIRELESS PROVIDER.

Choosing the right mobile device operating system is one step in creating a solid mobility strategy, but finding the right provider is equally important. The advanced Verizon Wireless network, products and services can help enterprises leverage mobile communications to securely and cost-effectively power productivity and boost communication and collaboration.

Verizon was the number-one-ranked telecom company in Fortune® magazine's 2012 list of the world's most admired companies, including first-place rankings for innovation and quality of products and services.

Together with Microsoft and other partners, Verizon is committed to enabling and empowering a range of devices, services and applications that capitalize on the powerful 4G LTE network. At Verizon, we've made substantial and deliberate investments to bring together the asset that will help you reap the benefits of technology convergence.

No matter where your business falls in the mobility spectrum, we can help, whether it's driving a new mobility initiative or making the most of your existing program and assets. We have the devices, plans, coverage, services and partners to help you accomplish your goals.

Explore Mobility Offerings from Verizon.

Mobility Solutions

Verizon can assist with planning, design, implementation and operation and management of mobility solutions.

Mobility Management

This service helps you understand and manage your mobile inventory, spend, logistics and apps, and protect company data with secure managed connections for remote workers.

Wireless Devices

Verizon makes it easy to find the right devices, whether you need tablets, smartphones, basic phones, mobile hotspots/ Verizon Jetpack® devices or USB modems.

Voice and Messaging

Voice and messaging services from Verizon give your team the quality and functionality they need to respond faster and keep your business moving. With services like messaging, Group Communications and Push to Talk, your entire team can communicate simultaneously.

Mobile Application

Whether you need to organize your sales force, monitor vehicle usage or convert to a mobile office, Verizon can get you there with applications that help you close more deals, control costs and increase productivity.

Mobile Broadband

With Verizon Mobile Broadband, you can securely log on via VPN from more places—for instance, from inside a taxi, in an airport terminal or even at a job site at the end of a dusty road.

Global Communications

Verizon's global solutions—supported by our global partners—give you the power to support your workforce virtually anywhere business takes them.

Private Network

Verizon Private Network offers your organization its very own reliable and secure wireless extension to your IP network.

The Right Technology to Set You Apart

The intersection of cloud, mobility and security is driving a massive revolution in business and government IT. Our strategic acquisitions and investments have allowed us to build out our core competencies. We've expanded our global IP network and 4G LTE networks in the U.S., and our security practices, with Cybertrust. Most recently we've expanded in the critical areas of cloud, IT and machine to machine with Terremark, Cloudswitch and nPhase.

To deliver that value, Verizon has created an innovative portfolio of platform technologies, the foundation to building solutions that help overcome today's challenges to your industry, your business and your customers.

Our broad portfolio of device vendors allows us to objectively recommend the equipment that best fits the needs of your business. Our Verizon Partner Program includes over 150 companies that help us tailor industry solutions to meet the unique needs of your business and customers. Working with world-class technology and application vendors enables us to create and deliver end-to-end business, communications and industry solutions.

Verizon leverages its investments, partners and highly experienced workforce to create complete turnkey, configurable solutions that span the globe; together, we're solving industry-specific challenges and inspiring the big ideas of tomorrow.

With the Samsung SAFE and KNOX platforms connected over America's largest 4G LTE network, you can be sure you are providing the best enterprise-ready productivity platform for your employees, and IT administrators can feel confident supporting an Android ecosystem that is no longer fragmented. The result: Your employees stay connected and productive with optimal coverage.

To learn more about Samsung Mobile Solutions for Enterprise, contact your Verizon Wireless business specialist, or visit us at **verizonwireless.com/contactrep**

HS20950813