SAMSUNG

Modern security for the mobile mission

Introduction

Advances in mobile computing capabilities and connectivity are creating new opportunities to improve public safety, manage critical infrastructure and streamline delivery of public services. Whether it is maintaining situational awareness, investigating with AI-assisted evidence collection or documenting repair status across a utility network, mobile technology revolutionizes the way governments work.

As adoption of mobile technology continues to accelerate, it will significantly impact cybersecurity planning and operations. Though this may seem daunting given the early challenges of adapting consumer-driven technology for enterprise use, today's mobile security capabilities are far better aligned to enterprise needs than ever before. As government agencies expand mobile programs to support their missions, they have a fresh opportunity to adopt a more holistic, modern approach to enterprise mobile security — one that better supports the workforce and improves operational resilience.

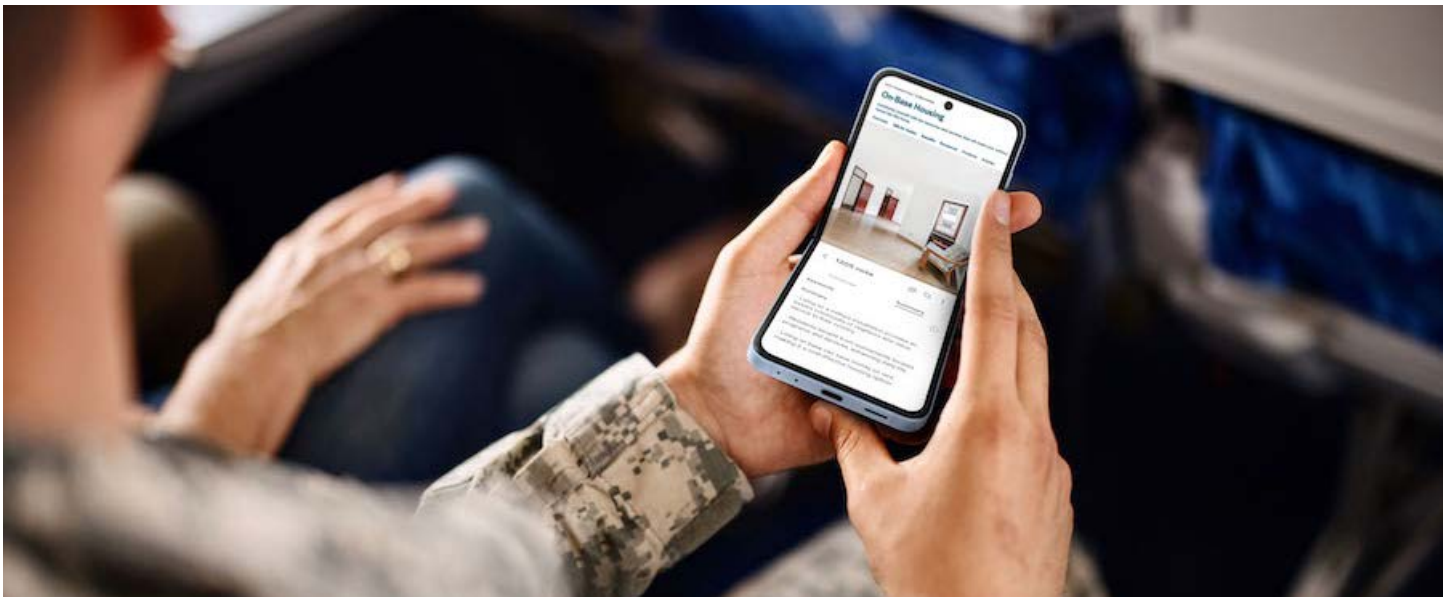
This paper provides a high-level overview of how Samsung's enterprise-ready mobile security capabilities drive trust in government mobility solutions, even in demanding operational environments. It highlights how Samsung helps agencies meet today's complex requirements for secure and trusted mobile technology through advanced hardware security protections, enhanced operational visibility and more precise control over security policies and enforcement. It also provides insight into how modern approaches to mobile security help government agencies better manage risk and create a mobile-friendly environment that enhances efficiency and mission outcomes.

The future is mobile

As agencies work toward digital transformation, they stand to benefit from rapid technological advancements driving the development of new, more powerful mobility solutions tailored to mission requirements. These include:

- increased processing power and advanced functionality of modern smartphones and tablets
- growing convergence of mobile device and PC capabilities
- broad availability of enhanced network connectivity, such as 5G
- emerging accessibility of situational awareness technologies for civilian use
- advancements in rugged mobile devices designed for tactical and field operations

As these developments come together, they are creating an enhanced mobile technology ecosystem that will positively impact mission areas across government, including defense, public safety, emergency response and critical infrastructure management.



The evolving mobile security landscape

Smartphones and tablets have become so integral to work and daily life that it's hard to imagine a time without them. Yet, in the early days of smartphones, government agencies were reluctant to adopt them in agency operations due to security concerns. Over time, that initial hesitance has shifted to a cautious — but increasingly proactive — adoption of mobile technology. However, some early perceptions of mobile security limitations persist.

The rapid consumer adoption of smartphones — and employee expectations for mobile-friendly workplaces — created significant challenges for enterprise IT departments. Teams worked to extend the protections and policies available in PC environments to mobile devices. Many of their early concerns stemmed from a lack of visibility and control over mobile devices, a common challenge anytime consumer technology finds its way into the enterprise.

As mobile devices have become essential in our personal and professional lives, mobile security has advanced to match their role as critical enterprise tools. This shift has driven a more proactive approach to mobile integration, enabling government agencies to mitigate today's mobile security risks with greater confidence.

Modern mobile security is now agile, enterprise-ready and integrated into every mobility solution prior to deployment. It follows a holistic approach that addresses three foundational areas critical to resilient operations:

Trust: Modern mobile security starts with trusted, hardened mobile devices. Every enterprise device should include built-in protections for sensitive information that can be relied upon even in an evolving and unpredictable threat landscape.

Visibility: IT and security teams must maintain real-time visibility into the security state and integrity of every device accessing their network to identify and mitigate risks at speed.

Control: IT and security teams should remove security responsibilities and decisions from end users. This means setting — and enforcing — security policies that automate protections and align with operational cybersecurity directives and regulations.

Can mobile devices replace PCs?

Government personnel frequently move between field assignments, vehicles and offices, yet many still operate in a PC-centric environment. Depending on their role, they often juggle multiple devices — smartphones, tablets, laptops, desktops, voice recorders, radios or rugged in-vehicle computers. This not only creates logistical challenges, requiring workers to carry and switch between devices while transferring data and logins between devices, but also increases the burden on IT departments to track, manage and secure a large and complex device fleet.

Shifting highly mobile workers from a PC-centric setup to a fully mobile environment enables agencies to improve workforce productivity, flexibility and engagement. It also simplifies security operations and provisioning by consolidating computing tasks onto secured mobile devices, eliminating the need to maintain additional laptops and PCs.

DeX delivers a PC-like experience by connecting a Galaxy smartphone or tablet to a monitor, keyboard and trackpad or mouse — eliminating the need for a separate PC.[1] Unlike simple screen mirroring, DeX optimizes mobile applications for desktop use, providing the functionality users expect from a traditional PC. DeX also supports USB CAC/PIV card readers, allowing secure access to enterprise applications within a FIPS-encrypted virtual desktop infrastructure (VDI) environment.

Common mobile security considerations

Mobile network attack surfaces: Mobile devices carry sensitive government data and applications, making them valuable targets for attackers. Their ability to connect to public infrastructure, including public Wi-Fi and cellular networks, adds new cyber-attack surfaces compared to a legacy workstation deployment. These new surfaces can be protected through new mobile hardware controls and visibility products.

Physical loss or theft: The portability of mobile devices enhances productivity but also increases the risk of loss or theft. Without proper safeguards, this could expose sensitive data or leak credentials, potentially enabling unauthorized access to agency network resources.

Surveillance risks: Mobile devices are prime targets for sophisticated attacks that track a user's location via GPS, Wi-Fi and cellular connections. Using the devices sensors against the user allows an attacker to monitor the user's activities, even turning the microphone into a remote listening device. While rare for the everyday smartphone user, mitigating surveillance risks can be a high priority for those agencies managing sensitive operations.

Personal use: Because mobile devices are always with us, the line between personal and work use is naturally blurred. This mixed use of our devices increases the risk of unintended security exposure. Seemingly benign personal apps for social media, fitness or entertainment introduce privacy risks, data collection and even covert surveillance. These risks extend beyond individual users to agency networks and operations.

Management control & visibility: The rapid evolution of mobile capabilities and their growing use in critical operations require agencies to implement security policies that address the unique needs and risks of mobile deployments. While enterprise mobility management (EMM) platforms provide centralized oversight, the stricter security architecture of modern mobile operating systems can limit deep visibility into device use and emerging threats. As a result, Zero Trust architectures have seen limited adoption in mobile deployments, until today...

Government agencies can successfully manage these risks by applying the right combination of security policy best practices and modern mobile security and endpoint management capabilities.

The government's evolving approach to cybersecurity

While mobile security is in focus here, it is part of a broader shift in government cybersecurity strategy, driven by an evolving threat landscape and ongoing digital transformation efforts. Federal agencies have made significant strides in modernizing cybersecurity practices and strengthening trust in digital systems. Notable federal initiatives include building a more resilient and defensible architecture through Zero Trust principles and collaborating with the private sector to enhance supply chain security. At an operational level, these changes require agencies to:

- manage supply chain risk
- implement Zero Trust principles
- improve operational visibility
- proactively address vulnerabilities
- detect and respond to incidents more quickly to minimize impact

For mobile solutions to reach their full potential in the field, their security and management must evolve alongside new mobile capabilities, while aligning with broader operational security priorities.

Zero Trust in brief

Zero Trust is a cybersecurity model based on one simple principle – no user or device can be trusted by default. It recognizes a need to scrutinize every access access request, even those that come from users, devices and apps that are inside the network. Zero Trust requires a system that is designed to:

- verify every identity and device connecting to the network explicitly;
- always assume the possibility of breach;
- enforce least privilege access; and,
- continuously monitor for and take action against abnormal or malicious activity

Learn More ›

A modern approach to mobile security

From the first hardware-backed mobile key store to kernel-enforced separation of personal apps from work apps, Samsung has led the way in mobile security advancements that matter to enterprise. As a longstanding partner to government agencies, classified smartphone deployments began with Samsung technology, an area that we still lead in today. Samsung government solutions leverage commercial off-the-shelf-technology (COTS) to allow agencies to deploy ready-to-use solutions or configure them to specific needs, including mission-defined security requirements, and meet the demands for secure, modern technology capabilities at a lower cost. Samsung prioritizes security at every stage of an enterprise deployment to ensure our solutions are mission ready, whether supporting field operations, enhancing public safety or improving workforce productivity. The cornerstone of these security efforts is Samsung Knox — a defense-grade security platform built into Samsung devices from the chip up. Knox combines hardware-based protections with a comprehensive suite of cloud-based solutions, enabling IT administrators to secure, deploy and manage devices to meet their cybersecurity requirements. Since its introduction in 2013, Knox has secured over 2 billion Samsung devices and has been used to manage over 150 million devices.[2] It has successfully met rigorous security requirements set by governments and major enterprises worldwide, including Common Criteria and FIPS 140-2 (and soon FIPS 140-3).[3]

Samsung Knox extends beyond core Android Enterprise capabilities, providing granular security controls and advanced management features exclusive to Galaxy devices. This unique mix of advanced security, enhanced visibility and precision control enables government agencies to tailor their mobile deployments to align with their operational security priorities.

Advanced security protection starts with a foundation of trust

In today's rapidly evolving threat landscape, government agencies must trust the hardware and software they rely on to carry out their mission. Delivering such trust requires a holistic approach that prioritizes **supply chain integrity** and delivers hardened, **secure-by-design technology** from the ground up.

Built for trust

Samsung devices are engineered with security at their core, ensuring protection from concept to deployment and throughout years of operational use. With end-to-end control of its supply chain, Samsung prioritizes security at every stage of the product lifecycle, ensuring product integrity and promoting trust.[4]

Hardened for secure use

Samsung Galaxy devices come protected out of the box through the advanced, hardware-backed security of Samsung Knox. Built-in and multilayered, Knox extends security from the chipset level to the operating system and higher application layers. This proactive protection mitigates common attack pathways without relying on user intervention.

Hardware-backed device integrity

Knox isolates critical security processes and data — such as passwords and cryptographic keys — from the Android operating system (OS) and apps. It does this by leveraging TrustZone, a hardware capability that creates a trusted environment outside of Android to run security-critical code and handle password, pins and keys. This isolation provides robust protection against attacks originating from apps or even the OS itself. Knox also continuously monitors the integrity of the software running in this trusted environment, detecting and blocking attempts to alter its state. For even stronger hardware-based protection, Samsung flagship devices include Knox Vault — a dedicated, tamper-resistant processor and memory to safeguard a device's most sensitive data.

Key Knox features for trusted devices

Secure Boot
Ensures device security with on-device, OS-independent integrity checks. If the firmware was rooted or there were changes to system components, they can be found when the device boots up.

Real-time Kernel Protection
Continuously checks core layers in real-time, keeping unauthorized attempts from accessing or changing the kernel. It also blocks malicious code from accessing system-level permissions.

Warranty Bit
Denies access to sensitive apps like Android Work Profile if tampering is detected. IT can check Warranty Bit remotely using Knox Attestation in line with other management policies.

Defeat Exploit (DEFEX)
Monitors for abnormal app behaviors and takes action, automatically shutting them down to block attacks when needed.

Knox Vault
Isolates and protects highly sensitive information, such as passwords, biometrics, PINs and crypto keys, from tampering, probing and other OS-based attacks.

Knox Vault builds on the TrustZone security model by introducing a physically separate hardware environment for processing secrets, adding resistance to speculative execution attacks targeting the device's main CPU. This ensures that Knox Vault remains isolated from all OS- and app-based attacks.

Knox hardware-backed protections make it extremely difficult for attackers to tamper with the device and require little to no action from users. This offers a significant security advantage, especially for agencies working to integrate Zero Trust principles into their operations. Zero Trust mandates explicit verification of device health and identity before granting network access. Knox supports this by providing trusted boot and device attestation to verify that only Samsung-authorized platform software components are running on the device and to confirm device integrity.

Additionally, through its partnership with Microsoft, Samsung offers an on-device, mobile hardware-backed attestation solution that works equally well on enterprise-managed and consumer devices, an essential capability for agencies with Choose Your Own Device (CYOD) policies.

Data protection

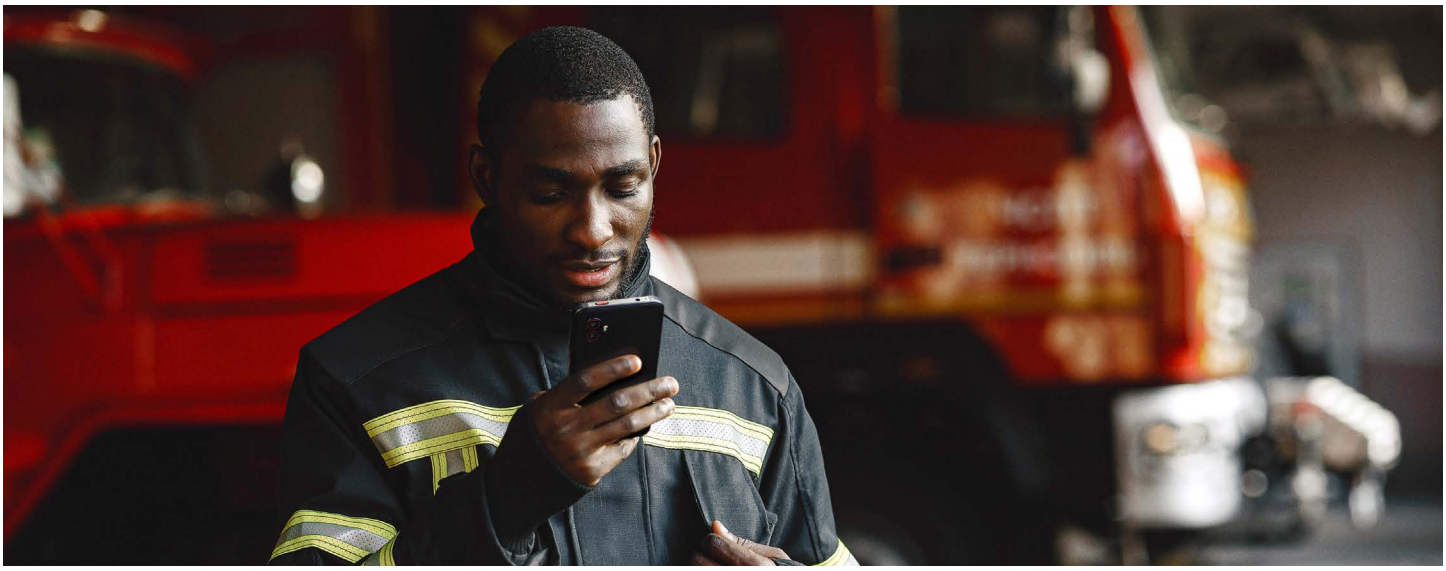
Safeguarding critical data is a core concern for government agencies, particularly those handling sensitive information. Concerns over data security — especially the risks of lost or stolen devices and unsecure network connections — is a commonly cited reason for hesitance in adopting fully-featured mobility solutions for certain mission sets.

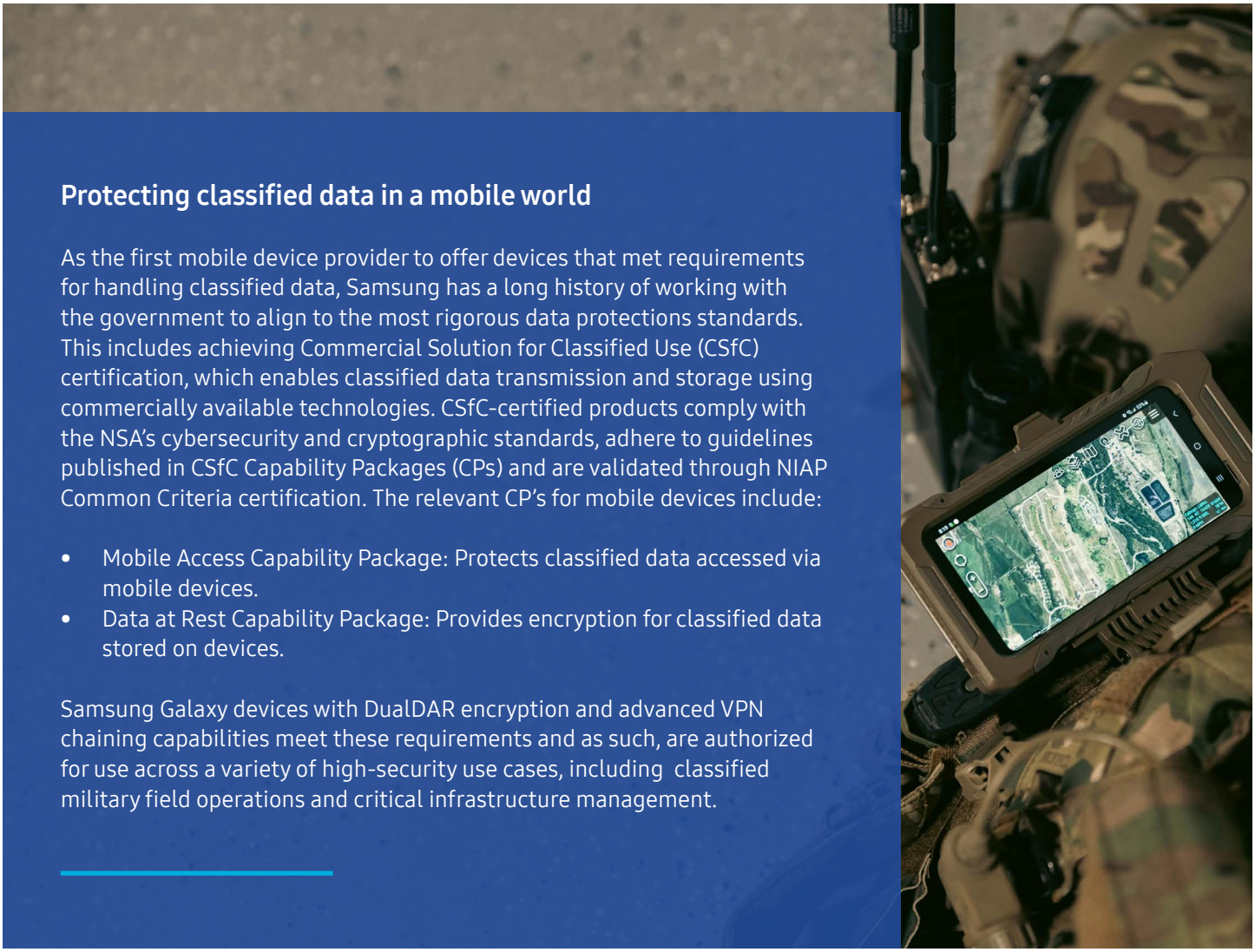
To address these challenges, Samsung Knox delivers authentication and encryption technologies that enable secure use of its mobile devices even in high-security environments. This includes highly advanced encryption capabilities that align with National Security Agency (NSA) and Defense Information Systems Agency (DISA) requirements for handling classified information.

For information stored locally on the device, Samsung Knox provides both full device and file-based encryption, which binds to the hardware-backed protections of Knox and user authentication. This encryption ensures data is decrypted only on the device and only by its owner.

For government users handling sensitive or classified information, Samsung's Dual Data-at-Rest Encryption (DualDAR)[5] offers a second layer of customizable encryption for the most sensitive work profile information on the device. DualDAR was designed to meet the NSA two-layer encryption requirement for Commercial Solution for Classified Use (CSfC) certification. It provides highly reliable, validated and continuous data protection without being cumbersome to the user.

To protect data in transit, Samsung Knox offers a wide selection of virtual private network (VPN) features that enable IT to configure and enforce data protection policies that meet their specific needs. This includes an advanced VPN-chaining architecture that allows for the configuration of a second VPN to isolate and safeguard sensitive data. DualDAR and VPN chaining exemplify technologies providing security resilience, preventing the failure of any single encryption layer from compromising data security.





Protecting classified data in a mobile world

As the first mobile device provider to offer devices that met requirements for handling classified data, Samsung has a long history of working with the government to align to the most rigorous data protections standards. This includes achieving Commercial Solution for Classified Use (CSfC) certification, which enables classified data transmission and storage using commercially available technologies. CSfC-certified products comply with the NSA's cybersecurity and cryptographic standards, adhere to guidelines published in CSfC Capability Packages (CPs) and are validated through NIAP Common Criteria certification. The relevant CP's for mobile devices include:

- Mobile Access Capability Package: Protects classified data accessed via mobile devices.
- Data at Rest Capability Package: Provides encryption for classified data stored on devices.

Samsung Galaxy devices with DualDAR encryption and advanced VPN chaining capabilities meet these requirements and as such, are authorized for use across a variety of high-security use cases, including classified military field operations and critical infrastructure management.

Certified for government

Samsung Knox has earned more global government security and third-party analyst certifications than any other mobile device, platform or operating system[6] — demonstrating its leadership in securing mission-critical environments.

Samsung devices were the first commercial smartphones to achieve certification for handling classified information.[7] Today, select Samsung Galaxy devices are certified for Commercial Solution for Classified (CSfC) use and NIAP Common Criteria requirements. The cryptographic modules used in Knox have also achieved FIPS 140-2 certification, ensuring compliance with stringent encryption standards.

Samsung has also led the development of Security Technical Implementation Guides (STIGs) for mobile devices, working closely with DISA to ensure Samsung Galaxy devices meet the Department of Defense's strict security requirements. Over the years, Samsung has refined its STIG creation process and developed tools that simplify compliance for IT administrators, making it easier to configure devices according to STIG checklists and achieve a compliant security posture for DoD deployments.

Beyond federal certifications, Samsung Galaxy devices are Android Enterprise Recommended, meaning they are validated by Google to meet specific requirements around performance, consistency, and security transparency and support.[8]

To help agencies streamline deployment and promote assurance, Knox Common Criteria Mode will automatically configure select Samsung Galaxy devices into a secure state aligned with Common Criteria guidelines. This is especially beneficial for smaller federal, state and local agencies with limited IT resources.

Supported to last

Samsung offers one of the industry's longest security support commitments for mobile devices, providing continuous firmware updates for seven years.[9] This means agencies can trust that Samsung Galaxy devices will be safe and secure for long-term use.

Enhanced operational visibility drives stronger security

Visibility over the fleet of devices, their health and security posture is foundational to cybersecurity planning. Monitoring assets and eliminating blind spots, especially in highly distributed environments, is a critical priority for IT security teams seeking to align with federal cybersecurity priorities.

With Samsung Knox Suite,[10] agencies maintain granular visibility over their Samsung device fleet's health and security state. Knox provides clear and actionable asset intelligence that goes beyond traditional mobile device management platforms and enables agency IT to quickly identify and troubleshoot device performance and security issues. This is done through Knox Asset Intelligence (KAI), which offers real-time insights into device health, battery life, app stability, connectivity and location. It also provides a comprehensive, device-level view of the current security status of the entire Samsung fleet via the KAI Security Center dashboard. This includes the total number of devices with outdated security patches, the total count of Common Vulnerabilities and Exposures (CVE), and the number of devices that failed Knox Attestation integrity checks.

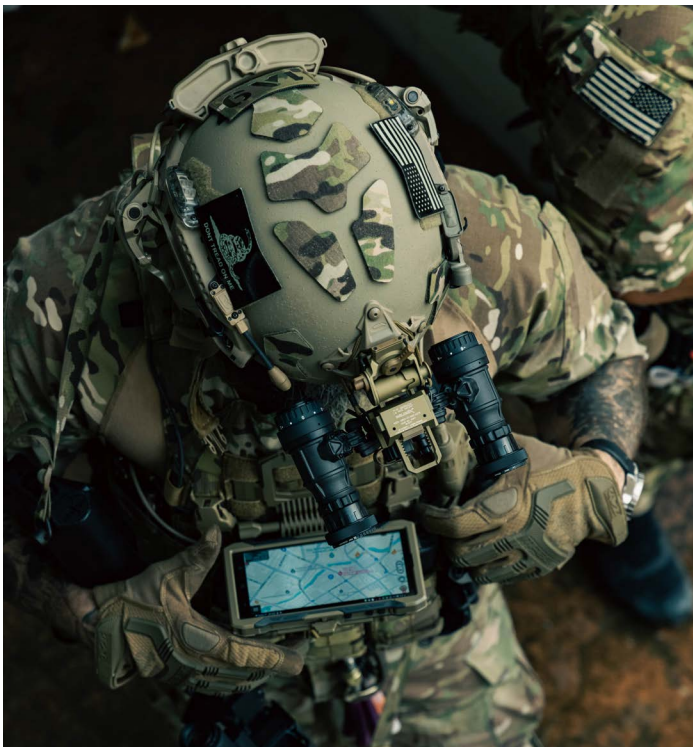
Precision control enables confident operation

Knox Suite and the open Android platform provide unmatched control over the entire Samsung device fleet at all times. Government agencies can precisely tailor their device security to meet their operational needs — from timing and verification of system updates to strict separation of work and personal data to stringent enforcement of app and feature usage policies. The ability to intuitively and centrally define, monitor and enforce granular device usage, health and security policies is a key reason why agencies select Galaxy devices, especially those working with specialized or high-security mission sets. Below are a few examples of areas where Samsung Knox offers precise policy setting and enforcement that agencies can tailor to their mission needs.

Advanced software update control

Knox E-FOTA (firmware over the air) provides IT with complete control over the delivery of software updates and the Android OS version running on every Samsung Galaxy device in its fleet. This allows them to test updates to ensure compatibility with in-house apps before pushing them out and centrally enforce which OS version runs on their fleet of devices, even if it is not the latest release. This is a critical capability that minimizes disruption from unforeseen compatibility issues.

When ready to update, they can deploy the latest verified firmware and security patches to all enrolled devices without requiring user interaction or risking user rejection or delay. However, Knox E-FOTA also allows for more granular control of update timing for agencies with specialized user needs. For example, most office workers are accustomed to firmware updates being deployed outside of business hours to limit any impact on productivity. Yet, this one-size-fits-all timing is not always suitable for government work. Many government agencies can have personnel in the field at any hour — often working on critical operations like managing disaster response or maintaining public safety. They cannot afford to have the devices they rely upon slowed down by firmware updates, even for a few minutes. These agencies significantly benefit from Knox E-FOTA's ability to more precisely control update timing and allow optional postponement for end users in the midst of critical tasks.



In summary, Knox E-FOTA offers a number of unique and significant advantages and addresses a pressing enterprise need for more control over the firmware update process. With Knox E-FOTA, enterprise IT teams can:

- Target any firmware version, not just the latest
- Time updates based on usage or local time windows
- Specify which network types to use to save on mobile data or prevent swamping local networks with update traffic
- Manage test groups to assess firmware updates before rolling out broadly
- Prevent users from manually updating firmware prior to completion of IT-led internal app testing and update approval
- Update firmware without any user intervention or action

Enforced separation of work and play

Smartphone users typically want their personal and work apps on the same device, but many agencies choose to deploy in a "corporate-owned" device model, devoid of any user data and apps. This model allows enterprises the ability to track and control device use without employee privacy conflicts, but prevents use of essential apps like airline or ride-sharing apps that employees rely on when traveling for work.

The available options have historically been imperfect trade-offs:

- Allow **personal apps as corporate apps,** increasing security exposure
- **Prohibit personal apps entirely,** forcing employees to care a second device
- Shift to a **personally-enabled device model,** losing that guarantees of full device control and tracking

While the Android Work Profile provides basic separation models, is not designed to address such strict corporate controls while still allowing some personal use.

To solve this, Samsung Knox Suite provides Separated Apps from the Knox Service Plugin, a capability that provides IT teams with a better fit for corporate needs and personal use. This Samsung-unique feature allows employees to use a limited number of third-party apps in a separated, sandboxed folder. This prevents the personal apps from interacting with agency apps or data, while still allowing their use on the device. This enables secure access to essential services like airline or ride-sharing apps, without compromising security or requiring employees to carry a second device.

With Knox Suite, IT admins also maintain stronger control over users' ability to transfer data between work and personal files. This covers things as simple as a contact or calendar event to more robust files or clipboard data.

AI usage control

Commercial smartphones are rapidly introducing new AI-powered capabilities to support a wide range of everyday tasks. While agencies benefit from COTS devices, they must also ensure that new features comply with their security requirements. Recognizing this, Samsung provides a number of granular controls over AI feature usage, allowing agencies to govern AI deployment with confidence.

Samsung provides government agencies with controlled and confident operation of its suite of Galaxy AI-assisted intelligence tools through two key approaches:

1. On-Device AI processing: Select Galaxy AI features, such as Live Translate with Galaxy AI,[11] are designed to run entirely on the device, ensuring that data never leaves the device or is shared for training purposes.

2. Enterprise AI governance: Knox Suite provides centralized IT control, allowing agencies to determine which AI features, if any, can be used on their devices.

Samsung Knox is a business platform for configuring and managing mobile devices – offering efficient and customized use in various industries. Keep your mobile infrastructure connected, protected and productive.

Knox Platform for Enterprise
Government-grade security for businesses

Knox Mobile Enrollment
Bulk device setup and deployment

Knox E-FOTA
Control OS Updates

Knox Authentication Manager
Unlock devices and autofill credentials with facial authentication

Knox Asset Intellegence
In-depth usage analytics

Knox Capture
Transtorm devices into barcode scanners

Knox Manage
Powerful mobile managemnet

Knox Remote Support
Make troubleshooting easier by controlling devices from a PC

Additional Knox solutions:

Knox Configure
Remotely tailor Samsung devices

Knox Guard
Restrict use of fraudulent devices

Tailored security for specialized uses

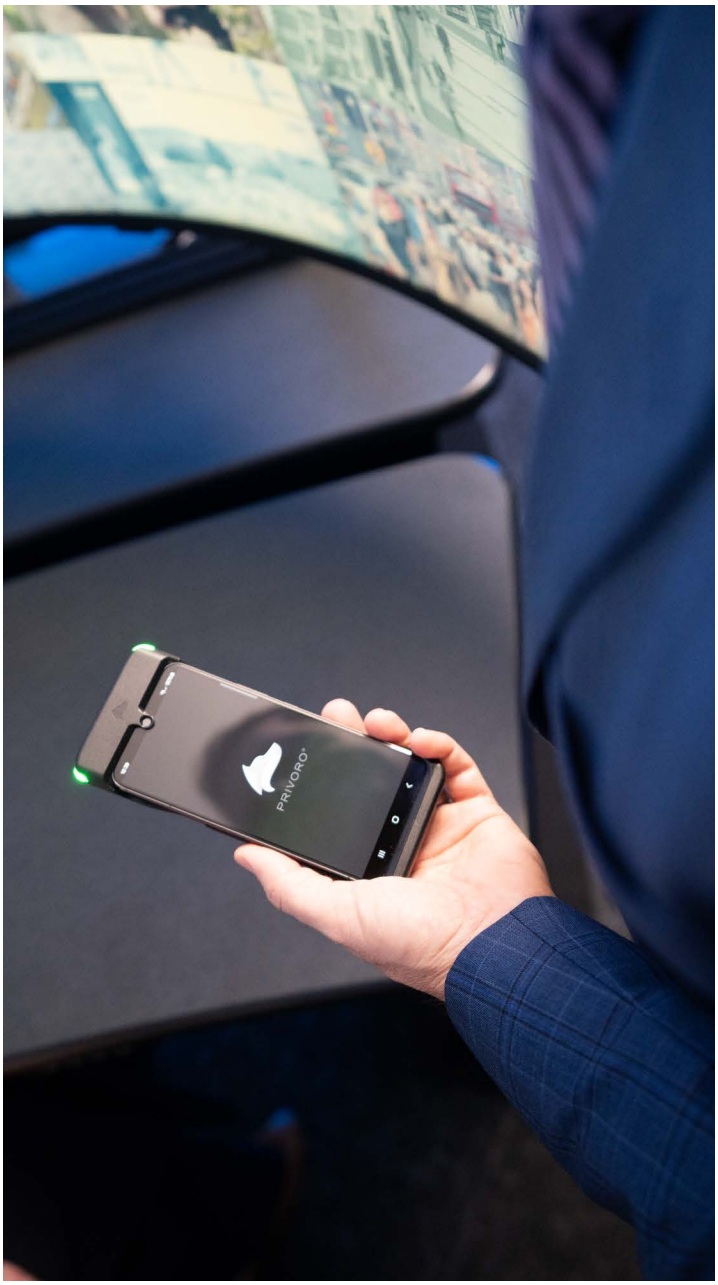
Samsung's ability to build mission-ready custom security solutions enables it to meet an agency's specialized needs. Examples include:

- Samsung Tactical Edition devices feature a custom operating system developed to support precision military operations with enhanced security, connectivity and tactical functionality
- Secure Spaces, developed in partnership with Privoro, provides advanced mobile security and surveillance protection through Samsung new hardware sensor and radio controls.

Secure Spaces: defending against mobile surveillance risks

In classified environments and covert operations, espionage risks — such as spyware-enabled phone surveillance — have forced agencies to either ban mobile devices or accept serious risks to maintain device access. While necessary for security, these restrictions impede productivity, limit information flow and frustrate personnel. To address this specialized need, Samsung has partnered with Privoro to mitigate the surveillance threat traditionally associated with smartphone usage. Our joint solution provides:

- physical camera protections and audio masking to prevent spyware-based eavesdropping
- chip-level radio frequency (RF) signal control (cellular, GPS, WiFi, Bluetooth, NFC) to block unauthorized tracking and connectivity



Secure tactical mobility

Trusted and proven by operators

The success of Samsung Galaxy Tactical Edition smartphones for military operations exemplifies the potential of commercial technologies to drive successful outcomes across a number of mission sets, even in highly secure, demanding environments. Combining a COTS Samsung smartphone with a custom-developed ROM, Samsung's Tactical Edition has been tested and proven to provide the durability, functionality, processing power and security required for precision military operations. Samsung developed its first custom, tactical OS while working closely with DoD and commercially launched the Galaxy S9 Tactical Edition in 2018. The Galaxy S9 Tactical Edition proved itself with special operations personnel, and their input was subsequently incorporated into the Galaxy S20 and S23 Tactical Editions, which have been reliably supporting thousands of military personnel across all branches of the military.

This control is enabled through Privoro's hardware integration with Samsung's unique Hardware Device Manager (HDM) capability. HDM allows partner solutions to enforce hardware-level disablement of radios, sensors and peripheral in hardware — while cryptographically proving they are disabled. Because this occurs outside the OS, it provides stronger isolation from common mobile attacks. By strictly disabling a device's cellular, NFC, Bluetooth and Wi-Fi radios at the hardware level, HDM prevents local and remote attacks, including mobile tracking, call and message interception, and GPS data logging. This signature management capability prevents adversaries from tracking user movements in the field using common electronic warfare (EW) tactics, including signals intelligence (SIGINT) collection and RF-based geolocation. As part of an emission control (EMCON) strategy, it provides critical protection for agencies conducting highly sensitive missions.

Notably, the Secure Spaces solution utilizes two separate, isolated hardware systems and enforces device policy at a level below the OS. As a result, there is no single point of failure, ensuring that app and OS kernel vulnerabilities cannot bypass security policy enforcement. This provides the high-assurance security and control needed for mobile device use in classified and/or covert deployments.

A secure mobile future will be built on trust

Mobility solutions are at the heart of the government's ongoing digital transformation, enabling advances in public safety, critical infrastructure management and the delivery of citizen services. As capabilities and connectivity expand, so do the opportunities to drive mission success. However, secure and confident adoption of mobility solutions must be built on a foundation of trust — one that keeps pace with increasingly sophisticated adversaries and attack techniques. Samsung remains committed to earning that trust. Every Samsung government mobility solution is built to deliver the advanced security, enhanced visibility and precision control agencies need to ensure mission readiness — no matter the operational requirements.

For more information on Samsung's advanced government mobility solutions and Samsung Knox security, please visit our **government solutions page.**

About the author

David Thomson

David Thomson is a security expert who started his career working on Department of Defense contracts. His projects focused on protected classified data on Linux-based workstations and network appliances. He came to Samsung Research America in 2013 as a security engineer and helped bring Security Enhanced Linux (SELinux) protections to the Android OS. He has since worked as Product Manager for the core Knox security platform and now leads mobile B2B security at Samsung Electronics America.

Footnotes

1 Samsung DeX supported on selected Galaxy, Note, and Tab devices. (More details on the FAQ Page).
2 https://www.samsungknox.com/en/about-knox
3 For a full list of Knox certifications, visit: https://www.samsungknox.com/en/knox-platform/knox-certifications
4 Manufacturing coverage may vary by model.
5 Requires separate license.
6 For a full list of Knox certifications, visit: https://www.samsungknox.com/en/knox-platform/knox-certifications
7 https://news.samsung.com/global/samsung-galaxy-devices-based-on-knox-platform-are-the-first-consumer-mobile-devices-niap-validated-and-approved-for-u-s-government-classified-use
8 Visit Samsung Knox to see the current list of Android Enterprise Recommended devices.
9 Up to 7 years, monthly update for 4 years and quarterly for 3 years. Applicable for Galaxy S24 and select later models, starting from the year of respective device model's release. Specific details may vary by region and model.
10 Requires separate license.
11 Live Translate feature for Call Assist does not need a network connection. Calls need a network connection to activate Live Translate. Samsung Account login required. Live Translate is only available on pre-installed Samsung Phone apps and some third-party apps. Service availability may vary by language or region. Certain languages may require language pack download. Accuracy of results is not guaranteed.