SAMSUNG

Samsung Knox Security

Built to Protect

Mission Statement

We empower people and organizations to utilize Samsung Galaxy devices without having to worry about security, letting them stay focused on what really matters.

Samsung Knox makes mobile security effortless – from secure hardware to real-time protection, and a comprehensive set of advanced security solutions. All you have to do is turn on your phone and go about your day.

Our philosophy on Security

Designed and built secure

Samsung hardware is built secure – from the design to manufacturing to the moment we put it in your hands, and for years of use beyond. We seek to deliver security throughout all steps with our own supply chain, built from the chip up.

Open to innovate

We strive to evolve our security solutions on a spirit of openness and partnership, starting with Android‘s proven multi-layered security and adding best-in-class technologies to address the constantly changing threat landscape.

Tools for your business

We also create a comprehensive suite of cloud-based solutions that extend the value of Knox security for businesses even farther. Fully optimized for Samsung Galaxy devices, they put IT admins in control and let people do their work securely and productively.

01 Mission

02 Pillars

03 Future

04 Accreditations

Safeguarding what matters most

1

Hardware backed

Trust begins with hardware

2

Data Protection

Secured from the inside and out

3

Continuous Protection

Knox never sleeps

4

Managed Security

Worry-free for work and play

Hardware-backed

1 Trust begins with hardware

Samsung security architecture has always been backed by advanced hardware solutions – and always will be.
We build security into each device from the ground up to safeguard your most precious data.

Knox Vault

Safeguarding your most important credentials

Trusted Boot

Secured from the boot up

Warranty Bit

Access only when trusted

Secure Supply Chain

Built by Samsung

Hardware-Backed

1 Trust begins with hardware

Knox Vault

Safeguarding your most important credentials

Protect your most precious information – passwords, biometrics, PINs, crypto keys – from tampering, probing, side-channel attacks and fault injection. *Knox Vault* architecture is CC EAL 4/5+* certified, with a dedicated security chip that only you can access.

Trusted Boot

Secured from the boot up

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

* Evaluation Assurance Lab certification from Common Criteria, an internationally recognized standard for security evaluation. Level of certification and specific architecture detail may vary by chipset specifications.

Hardware-Backed

1 Trust begins with hardware

Warranty Bit

Access only when trusted

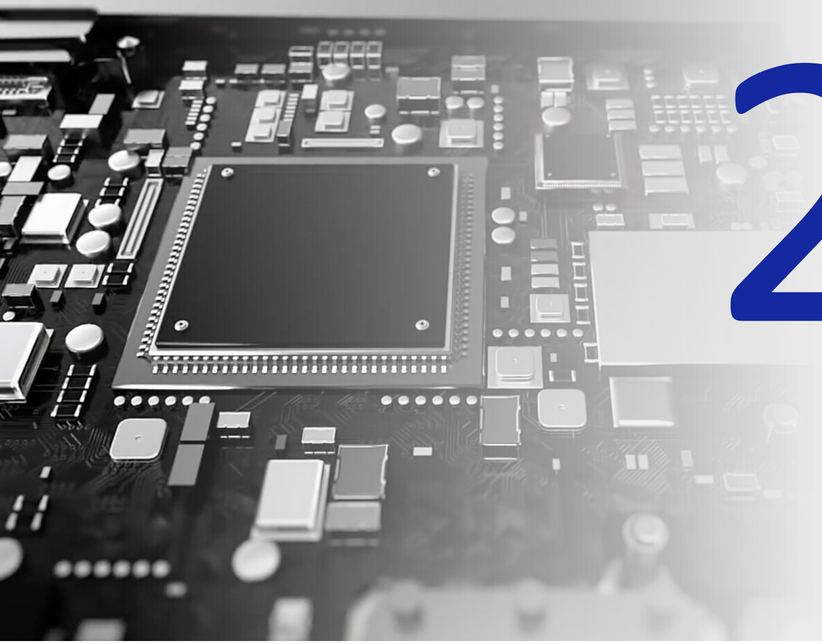
When Warranty Bit detects tampering, access to sensitive apps like Samsung Wallet (Samsung Pay), Samsung Pass, and your Android Work Profile will automatically be blocked to prevent misuse.
IT can check *Warranty Bit* remotely using *Knox Attestation*, and utilize with other management policies.

Secure Supply Chain

Built by Samsung

Samsung is one of the few companies with strong control over the design and manufacture of its own products.* This can ensure end-to-end security across the supply chain and throughout the product lifecycle.

*Manufacturing coverage may vary by model.



2

Data Protection

Secured from the inside and out

Securing your device and data is a round-the-clock commitment.
So we built a range of encryption options to guard your data at rest, and more ways to protect your data in transit. In use on the phone, surfing the web, or even when your phone is misplaced, your data can be in safe hands.

Data Encryption

Multi-layered encryption

Secure Wi-Fi

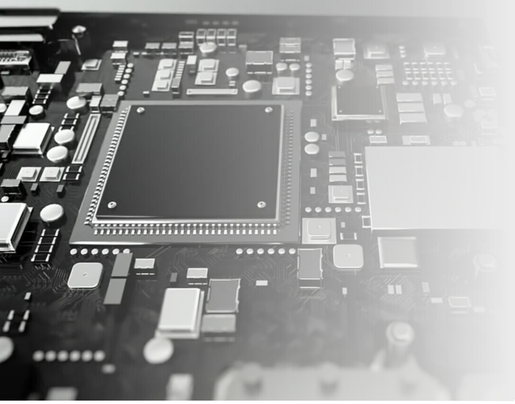
Safety on public networks

Permission Manager

Protecting personal data privacy

SmartThings Find

Remote lock for lost devices



Data Protection

2 Secured from the inside and out

Data Encryption

Multi-layered encryption

When it comes to encryption, you have plenty of options. File-Based Encryption offers separate encryption keys by default. Or you can store materials in our *Secure Folder* using independent credentials. Businesses can even secure Android Work Profile data using their specified cryptographic module with *DualDAR*.*

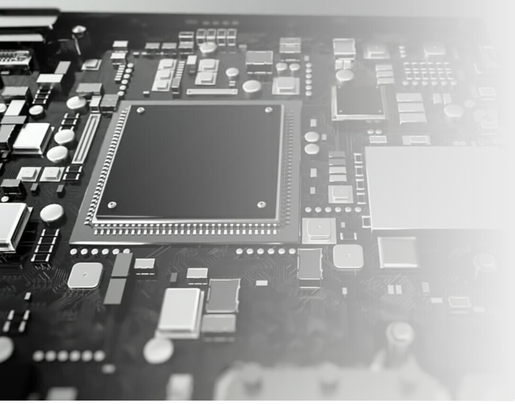
Secure Wi-Fi

Safety on public networks

Secure Wi-Fi feature is designed to let you browse the internet safely, even when you're using unsecured, public Wi-Fi networks.**
It offers protection by encrypting internet traffic and blocking tracking apps, so you can feel safer connecting.

Have visibility on your protection history in charts and lists, based on Wi-Fi names.

*DualDAR requires a separate license purchase.
** Secure Wi-Fi availability may very depending on the country, carrier, or network environment. Subscription required for usage exceeding default protection plan.



Data Protection

2 Secured from the inside and out

Permission Manager

Protecting personal data privacy

Permission Manager gives you control over your data like your photos or key functions where data can be leaked, such as the microphone, camera, and GPS. *Live Indicator* notifies users when apps access the camera or microphone.

SmartThings Find

Remote lock for lost devices

SmartThings Find doesn't just help you locate your lost device. It can remotely lock, erase, or display customized messages at lock screen to secure your data and asset.*

*Supported on Galaxy smartphones and tablets with at least Android 8, Galaxy Watch3 or higher, Galaxy Buds Live, Galaxy Buds Pro or higher, Galaxy Buds2 or higher. Support services may vary by country/region/carrier.

3

Continuous Protection

Knox never sleeps

Security threats lurk around every corner, and mobile devices are increasingly targeted with sophisticated attacks. Knox counters these with threat management solutions that run throughout usage cycle – keeping your digital journey worry-free.

App Security

Keeping malware at bay

Message Guard

Protecting against attacks through SMS/MMS

Security Patch

Regular security updates for the long term

Real-time Kernel Protection

Real-time protection

DEFEX

App behaviors under control

3

Continuous Protection

Knox never sleeps

App Security

Keeping malware at bay

Samsung Auto Blocker can stop the side-loading of apps from unknown sources, even if a user accidentally approves it. It can also block USB updates to prevent malicious software from being installed. Google Play Protect regularly scans downloaded apps to detect malware and spyware.

Message Guard

Protecting against attacks through SMS/MMS/RCS

Samsung Message Guard neutralizes potential threats before they have a chance to do you any harm. It automatically isolates and decodes images in a sandbox so your device is unaffected.*

*Samsung Message Guard supports protection against the following image formats: PNG, JPG/JPEG, GIF, ICO, WEBP, BMP, WBMP.
Default messaging app varies by market. One UI 5.1 or higher.

3

Continuous Protection

Knox never sleeps

Security Patch

Regular security updates for the long term

Samsung Galaxy devices, regardless of carrier, receive up to 7 years* of security and OS updates. Application updates can also be automated from Google Play or Galaxy Store.

Real-time Kernel Protection

Real-time protection

Knox constantly checks your core layers in real-time, keeping unauthorized attempts from accessing or changing the kernel. It also blocks malicious code from accessing system-level permissions.

DEFEX

App behaviors under control

Defeat Exploit(DEFEX) monitors abnormal app behaviors and takes action. If an app tries to make potentially dangerous requests such as privilege escalation on your device, *DEFEX* can automatically shut it down.

*Applicable for Galaxy S24 and select later models, starting from the year of respective device model's market release. Specific details may vary by region and model.

Managed Security

4 Worry-free for work and play

Samsung Knox offers intuitive, yet granular controls to setup and manage devices to suit your organization’s need. We empower IT admins to manage with confidence and help team members streamline workflows and boost productivity.

Management and Configuration

Powerful mobile device management

Knox Suite

Secure, deploy manage, and analyze

Security Center

Check security status on device fleet

Android Work Profile

Keep work and play separated

Galaxy AI

Business-friendly AI with data sovereignty

Managed Security

4 Worry-free for work and play

Management and Configuration

Powerful mobile device management

Knox Platform for Enterprise is built into Galaxy devices, offering robust and flexible MDM/EMM controls for IT. These are accessible through Knox Suite or a wide range of EMMs using the *Knox Service Plugin*.*

For industries with more stringent requirements, in-depth configuration may be explored for extra protection.

e.g.) DualDAR, HDM (Hypervisor-based Device Manager: Peripheral device access control)**, and more.

Knox Suite

Secure, deploy manage, and analyze

Knox Suite is a comprehensive set of solutions made by Samsung and optimized for Galaxy devices.

- ✓ Ensure compliance with company policies while maximizing worker productivity.
- ✓ Designed for flexible use: As a standalone end-to-end EMM, or on top of your MDM/EMM for added controls on Galaxy.

* Knox Service Plugin support and compatibility may vary by EMM/MDM service provider.
** Knox DualDAR and Knox HDM requires a separate license purchase.

Managed Security

4 Worry-free for work and play

Security Center

Check security status on device fleet

Security Center offers detailed insights and visibility on your fleet's security status. IT admins can maintain device health with early detection of vulnerabilities(CVEs), based on security patch levels and routine attestations.

Android Work Profile

Keep work and play separated

Android Work Profile separates work and personal data on a single device, with dedicated work and personal profiles. Have security and control over company data while respecting employee privacy.

Galaxy AI

Business-friendly AI with data sovereignty

With *Knox Platform for Enterprise**, IT admins can set *Galaxy AI** features to run safely on-device only, without cloud processing or storage. Empower users with *Galaxy AI* productivity tools while protecting work data against leaks or misuse.

* Knox Platform for Enterprise license is required. (Free). Allow process data only on device policy will limit some Galaxy AI features.
**Galaxy AI features by Samsung will be provided for free until the end of 2025 on supported Samsung Galaxy devices. Availability of Galaxy AI features may vary by model or environment.

Future:
Zero Trust-ready devices and solutions by Samsung Knox

Threat actors never stop, and neither do we. Businesses around the world face a growing range of threats, from zero-day exploits to state-sponsored hacks, targeting critical operations.

We continue to innovate and evolve to meet the changings needs of our dynamic and increasingly networked environment. Samsung fully embraces Zero Trust security and we are already working closely with market-leading UEM, network, and security orchestrations players to deliver comprehensive Zero Trust solutions.

Microsoft Intune

Protect access to your data with Knox Attestation

With mobile hardware-backed attestation, enterprises can verify a Galaxy device’s integrity before allowing access to corporate resources using Intune MAM.

Cisco Secure Access

Zero Trust Network Access supported on Galaxy devices

Cisco Secure Access ZTNA on Galaxy devices provides users with role-based, least-privileged access to apps and resources. This protects corporate resources with minimized public exposure, while also granting quick access.

Expect more
in 2024 and beyond.

01 Mission

02 Pillars

03 Future

04 Accreditations

Samsung Galaxy devices have been verified by government agencies and partners globally

Common Criteria

DISA (USA)

ANSSI (France)

CCN (Spain)

Traficom (Finland)

ISCCC (China)

FIPS 140-2
(USA, Canada)

NCSC (UK)

BSI (Germany)

AIVD (Netherlands)

ASD (Australia)

STRK (Kazakhstan)

Samsung Knox + Android

Highest security rating

Gartner

Strong

27 out of 30*

android enterprise recommended

70+

Devices
as of Feb 2024

Providing a wide range of Android Enterprise Recommended Galaxy devices -
including smartphones, tablets, and ruggedized models.

* Gartner: A Comparison of Security Controls for Mobile Device, 2019

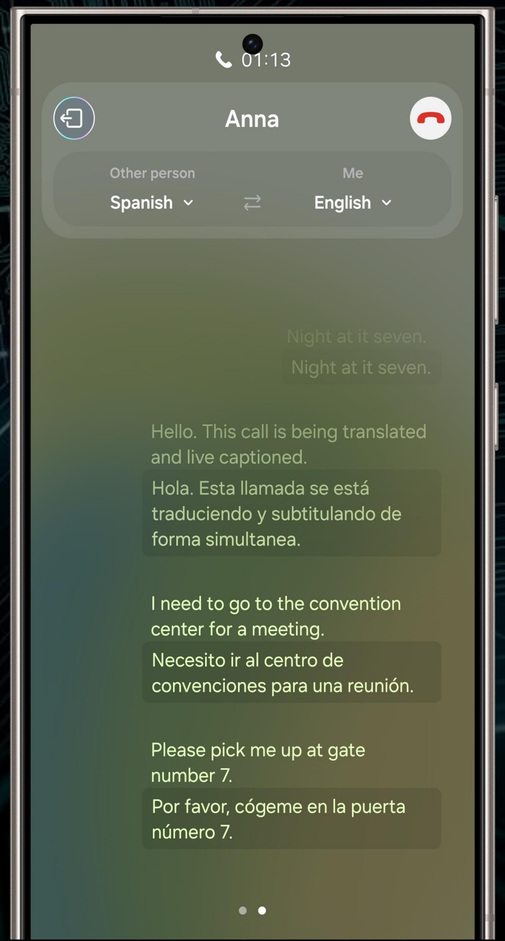
Appendix

Secure AI

Galaxy AI is safe to use. There’s no need to worry about what you share with it

Peace-of-mind with the usage of on-device Galaxy AI features

On-device Galaxy AI
-Does not store data on the device
-Does not upload data to the cloud
-Performs tasks locally on device without relying on cloud server
-Does not educate AI engine with user inputs



Galaxy AI in the workplace

Out of the box, your AI device is secure. Galaxy AI processes user functions without storing user data and protecting user privacy. Use Galaxy AI to securely streamline translations and increase efficiency.

Image simulated for illustrative purposes. Actual UI may be different.
Galaxy AI features by Samsung will be provided for free until the end of 2025 on supported Samsung Galaxy devices.

AI under control

Take control over cloud-based AI features to remove security risks

Disable cloud processing for added security with Galaxy AI

Some Galaxy AI features are processed in the cloud. This can be easily disabled and the user can still utilize on-device AI features.

※ Individual cloud-based AI features cannot be turned off separately.

Knox Service Plug-in at work

IT admins can use Knox Service Plug-in to disable the cloud-based AI features of the device fleet.

Knox Service Plug-in is available on major EMMs including Microsoft Intune, VMware, Knox Manage and more.

Image simulated for illustrative purposes. Actual UI may be different.
Galaxy AI features by Samsung will be provided for free until the end of 2025 on supported Samsung Galaxy devices.

On-Device and Cloud based AI

Galaxy AI is powered by on-device and cloud based AI capabilities

Feature Name	Experience	On Device	Cloud
Note Assist	Auto format text, Generate cover, Correct spelling, Summarize		o
	Translate	o	
Transcript Assist	Summarize		o
	Translate	o	
	Transcribe	o	
Browser Assist	Summarize		o
	Translate	o	
Call Assist	Live translate	o	
Chat Assist	Tone change, Correct spelling	o (English and Korean only)	o
	Chat app live translate	o	
Interpreter	Quick panel live translate	o	
Generative Wallpaper	Prompt wallpaper, Layered wallpaper		o
Photo Assist	Generative edit		o
	AI edit	o	
Instant Slow-mo	Instant Slow-mo	o	

*Tone change and Correct spelling supports both on-device and cloud for switching between Korean and English, but on-device will turn off when cloud is turned off.

CONFIDENTIAL
By accessing information on this slide, the viewer agrees and acknowledges that all contents and information are confidential and proprietary information of Samsung, shall be subject to the non-disclosure agreement, and shall not be disclosed by the viewer to any third party.
Samsung Proprietary and Confidential