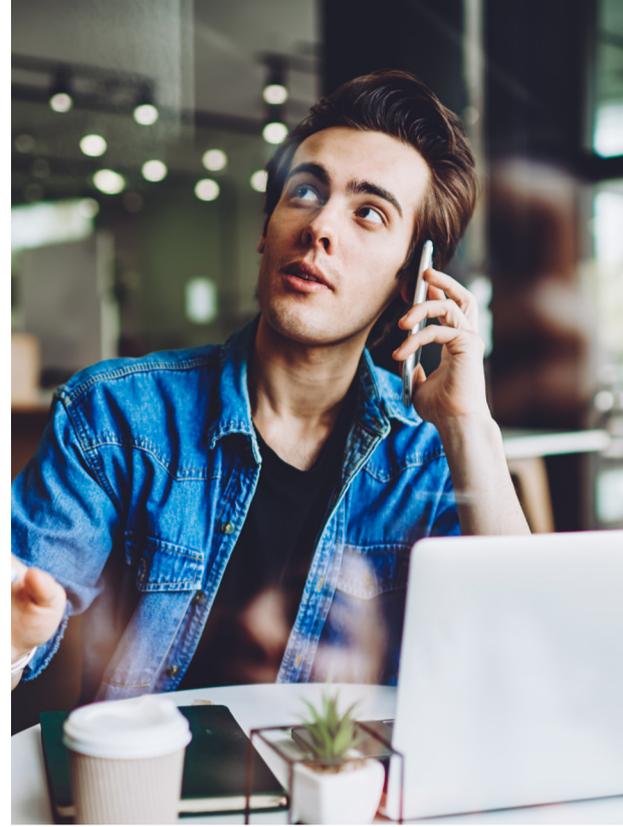


SAMSUNG

This is Protection. Samsung Knox



Samsung Knox Handbook



INTRO

**A new way of working demands
a new level of security.**

Are you sure your devices are protected?

This is protection.

Remember the good old days? The morning commute and the 9 to 5? Well those days are history.

Forget being tied to a desk and a schedule. Today's workplace has nothing to do with time or place and everything to do with productivity and mobility. Without compromise. Today's employees want the same access, speed and resources of the office, even if they're three time zones and two continents away.

While mobile, employees spend a significant amount of time outside of their protected corporate networks as they access the web from locations other than their offices. This can expose businesses to more attacks, errors, leaks and new dangers we haven't even encountered.

For IT leaders, supporting a mobile workforce while maintaining the same level of productivity they would have had in the office is extremely difficult. Doing it while maintaining top level security is nearly impossible. Nearly.

This entirely new way of working demands protection that works in real time, not sometimes. Protection that secures on every layer, not just one. Protection that understands that we're safer when we work together, instead of trying to go it alone. Most importantly, protection is security without compromise and protects without getting in the way of creativity, productivity or freedom.

Protection is what Samsung is all about and it's why we built Samsung Knox, a cutting-edge security platform for mobile experience embedded in your Samsung Galaxy device. We are talking real-time, end-to-end protection, with the best intelligence from leading partners and experts across the industry, including Google, Cisco and more. So if you want to stay a step ahead, you can trust Samsung Galaxy and Samsung Knox to fully protect your way of working.

This is protection. Samsung Knox.



SECURED FROM THE CHIP UP

Hardware-base Protection

The more the world turns to mobile, the more frequent and sophisticated the attacks become. Until recently, it might have been enough just to protect software using an anti-virus program - but not anymore. Hardware is increasingly a target, making protection from the component level an absolute necessity.

Maintaining security from the chip up provides users with the freedom to use devices as their professional and personal life demands. Defense-grade security built into your device with the Knox Security Platform's Knox Vault – a safe within a safe for your most sensitive data – and Samsung's complete supply chain control ensures devices cannot be tampered with.

Your wallet, passcodes and most critical biometrics are all protected by Knox Vault Processor, Knox Vault Storage and Knox Vault Protocol. They're also protected from various malware and viruses, all while letting users choose the tools and services to get the job done. Samsung Galaxy devices with Knox are the ideal combination to offer you and your employees the protection they need.

A safe within a safe for extra peace of mind

Threats to device and data security are getting more sophisticated every day. Some of the most insidious threats come from attacks targeting device hardware because attackers know these are the least likely to be secured. That's why Samsung Knox prioritizes protecting the deepest inner-workings of its Samsung Galaxy devices.

At the heart of Samsung Knox is Knox Vault. It's a safe within a safe to protect your most valuable data including PINs, passwords, biometrics and more from the most hardened attacks. Attackers targeting device hardware attempt to cause the device to malfunction by introducing lasers, heat or a power glitch. If they succeed, they can manipulate user data to bypass other security measures. Alternatively, if they manage to detach the chipset, they can access sensitive data with microprobing.

But not with Samsung Knox Vault. EAL-5+ level, tamper-resistant technology means hackers are less likely to get past the Vault's sensors which shut down the device, locking the data inside. In the event of a hijacked device, Knox Vault will even self-destruct, leaving no way for hackers to access sensitive information.¹



1. Currently available on Samsung Galaxy S21. For more information, please visit www.samsungknox.com

Complete ownership of the supply chain

Security only counts when you can be confident every part of your device has been tested and scrutinized to the max. Samsung is one of the few companies in the world that designs and develops its own products, software and services, giving it total control over every single component, from threat identification at the design stage to risk assessments in the supply chain.

Owning the whole product development lifecycle ensures total control over the process, making Samsung devices less open to attack. While other phones stick to protecting your data through software, Samsung Knox is anchored from the chip up, including a unique failsafe security key that gives users the high level of protection against hardware-based attacks as certified by the CCTL.



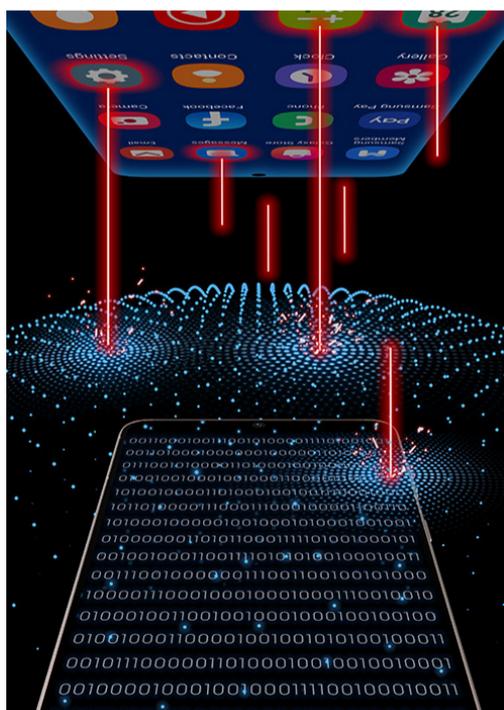
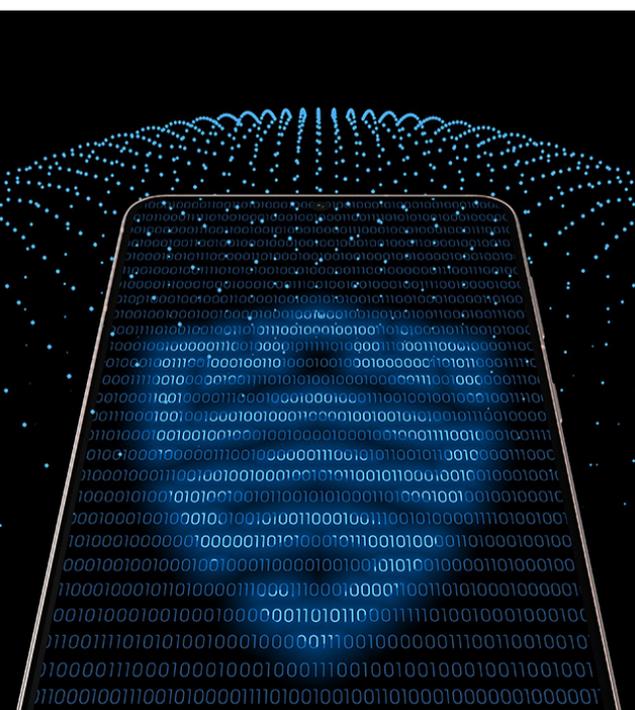


PROTECTION THAT IS ALWAYS ON, IN REAL TIME

Real-Time Protection

In today's flexible working environment, employees are always on and so are their devices. When devices are on almost 24/7, it opens a wide array of opportunities for attacks, hacks, viruses, malware, leaks - and just good old-fashioned human error. With no opportunity to turn off and gain the protection of the device's automatic secure boot at restart, real-time protection is a necessity.

Your phones don't sleep and neither do attackers. Their inventiveness knows no bounds and they can come up with endless ways to get hold of your data. Reaching the core of your operating system – the kernel, which is essentially your device's 'brain' – is their ultimate goal. Success means a potentially catastrophic data leak, remote monitoring and even complete control of affected devices. Samsung Knox pulls out all the stops to keep it safe.



Samsung's patented Real-time Kernel Protection (RKP) prevents any changes to the kernel – including modification of kernel code or data structures. With RKP in place, users are safe knowing that nothing will threaten the integrity of their data or device.

Without the protection of secure boot technology, your apps are also at risk. They need an extra layer of defense against unauthorized changes to app privileges. That's where Samsung Knox's "DEFEX" (short for Defeat Exploit) comes into play. DEFEX prevents potential critical and illegal operations on your device by detecting and anticipating attacks, while the device is operational.



SECURED TOGETHER

Collective Protection

As the amount of time spent on devices and the number of ways they are used have grown, so too, has the range of threats. Once easier to track, now they're coming from all angles – chipset, operating system, applications, network, and all points in between.

At Samsung we are proud of our security capabilities and innovations like Samsung Knox Vault but we also believe no single company can or should try to tackle these numerous current and future threats alone. Trying to do so is both arrogant and irresponsible as it puts the businesses and people who rely on our devices at risk.

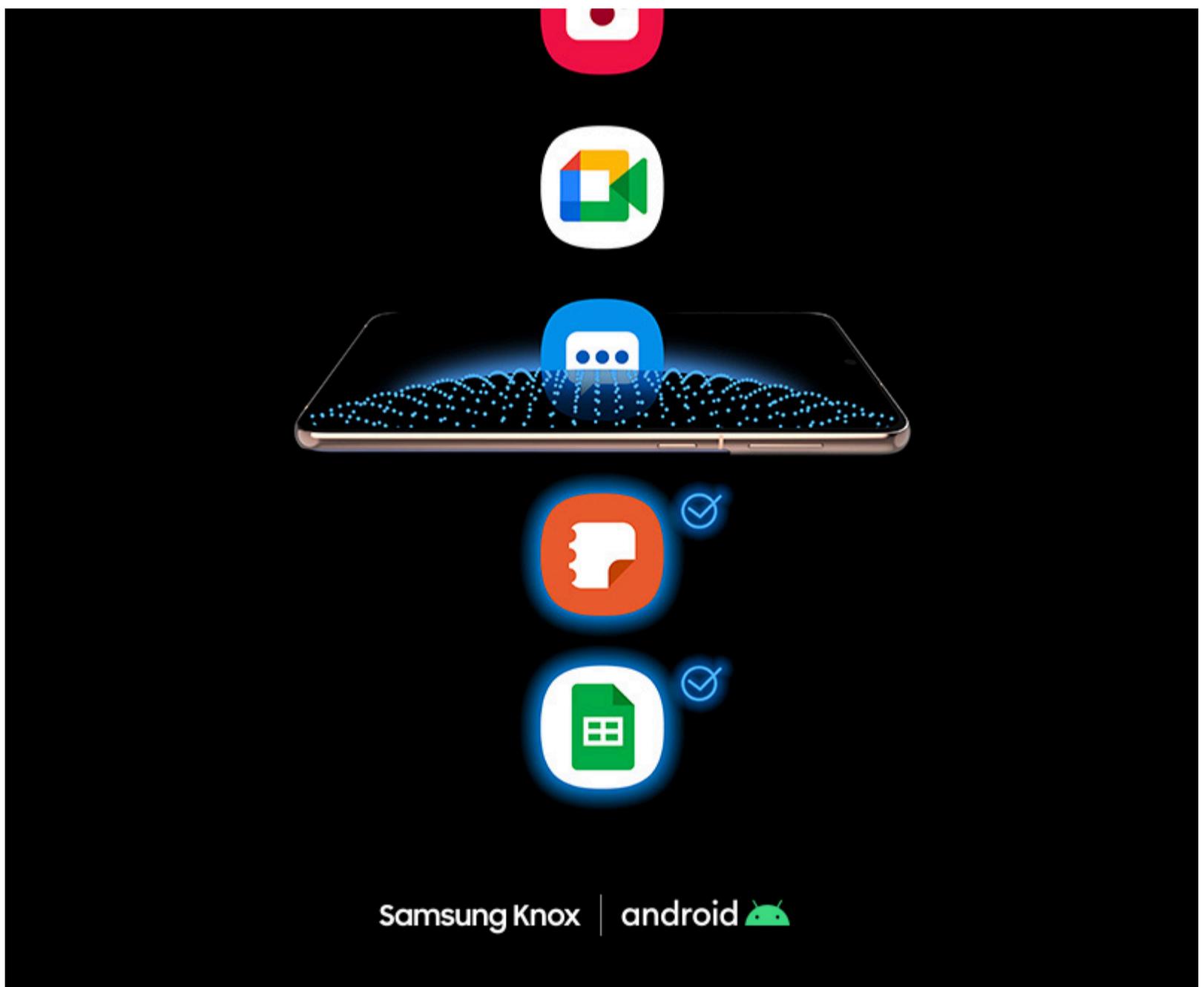
Some companies would have you think that 'closed' is safe and 'open' is dangerous, but the truth is exactly the opposite. With the unprecedented rise in quantity and quality of mobile security threats, barricading the gates is the most dangerous route you can take. Collaborating with allies to create an unmatched protection force is the smartest way to go.

That's why Samsung Knox openly partners with the big names in tech like Google and Cisco. We constantly work with teams of experts to explore every scenario and solve potential vulnerabilities - before they become a problem. Because effective protection means staying open to every possibility.

Secure at the core with Android

For over a decade, our partnership with Google has allowed Samsung Galaxy users to leverage Android's hardened security platform and intelligent security services like Google Play Protect to prevent software compromises and stay one step ahead of malware and other threats. In addition to monthly device updates from Android, Samsung Galaxy devices are supported with five years of regular Samsung security updates, so your data is protected with the latest patches from our network of research partners.

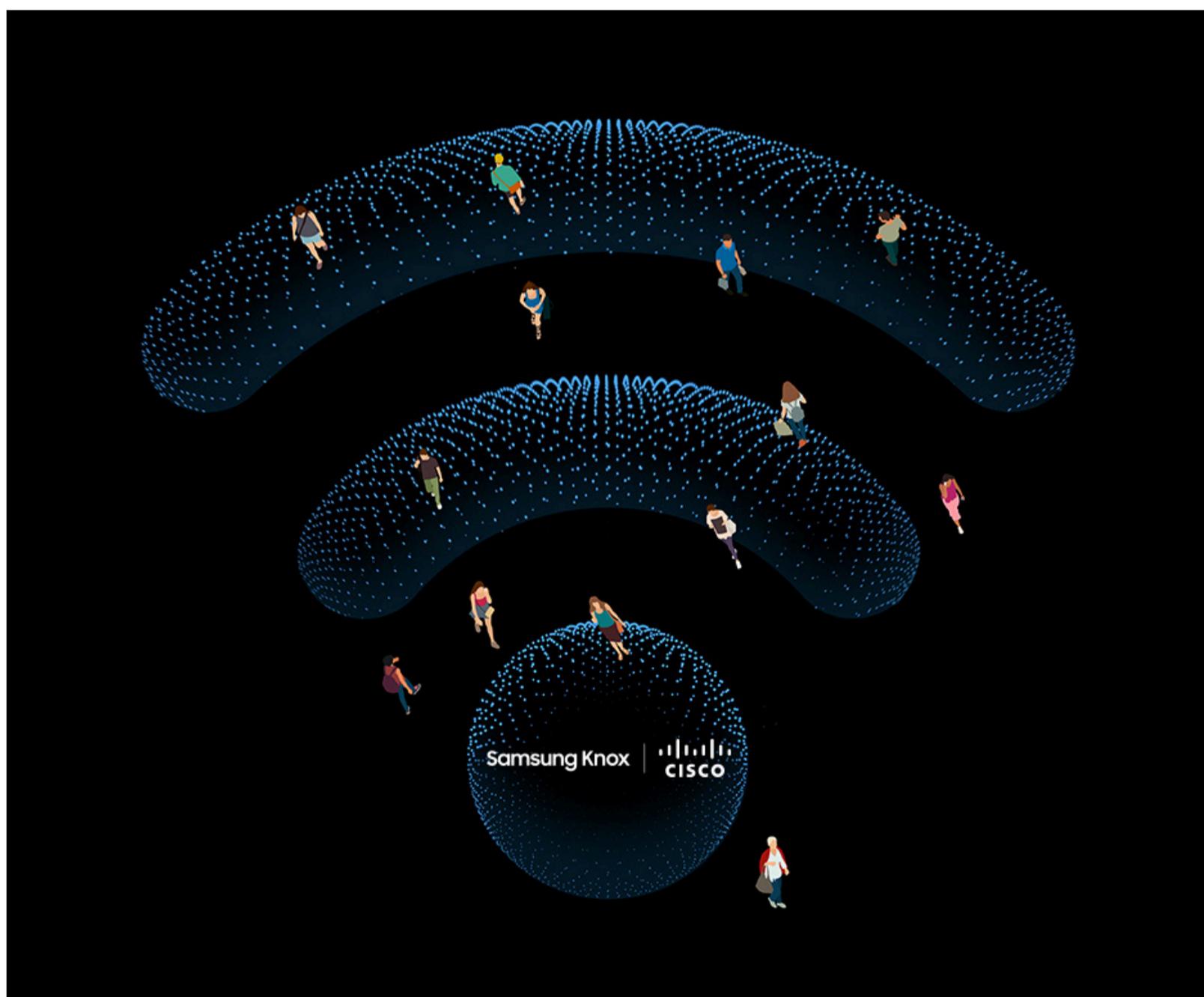
By delivering additional defense-grade hardware protections and critical controls that exceed the hardware and software requirements set out by Google for enterprise, Samsung Knox is able to address even the most demanding security challenges. Together with Android, you can be sure that Samsung Galaxy devices offer a powerful security experience, harnessing open collaboration and collective expertise, and giving customers comprehensive and complete protection.



Safely connected with Cisco

Public Wi-Fi can be great news for an employee working from a coffee shop, but it's also a risk. That's why we have joined forces with Cisco to provide users with seamless, secure Wi-Fi onboarding through OpenRoaming. All Samsung Galaxy devices automatically and securely connect to OpenRoaming networks when available. And through unique encryption, users are protected from session hijacking or web snooping without the need for extra passwords or other credentials.

Our longstanding, open collaboration with Cisco gives Samsung Galaxy users the power to turn compromised public Wi-Fi into a secure and reliable connection in a single swipe. That's how Samsung delivers seamless protection: one partnership at a time.



A vigilant community at your side

Protection means keeping every eye out for potential threats. Without active monitoring, even some of the biggest and best-resourced global organizations have seen cyberattacks go undetected as long as 200 days – sometimes longer. During that time, malware and other threats don't just affect the target company, they can also spread throughout its partner network. Protection means tackling threats quickly.

Samsung Knox proactively protects users' devices by engaging with a wide range of experienced researchers and vendors in

cyberthreat communities. We worked with SoC providers like Qualcomm to design the hardware processing unit. We engage with the Linux wider security research communities, as well as academic institutions and mobile operators to gain the very latest intel. From the Samsung Mobile Security Rewards Program to the Incident Response and Management team, there are observers engaged and active worldwide, protecting Samsung devices from attack. Our defense-grade Samsung Knox protection is proof that we all work better when we all work together.





OUTRO

**This is protection.
Samsung Knox.**

Flexible, mobile ways of working are becoming the norm. Advances in technology naturally open up a new world of possibilities. But this new world is not without risk. Your employees take more than your reputation out into the world, they also take your vitally sensitive information. You want solutions that allow your employees to achieve their goals with maximum freedom and security, without interruption.

Samsung Knox is the trusted real time, end-to-end security platform that is working across the industry to deliver best-in-class security for your business, your employees and your partners.

This is protection. Samsung Knox.

For more information, please visit www.samsungknox.com/security