SAMSUNG
Galaxy

Android

Modern mobile security mindset: Securing teams and mitigating risk

Table of Contents

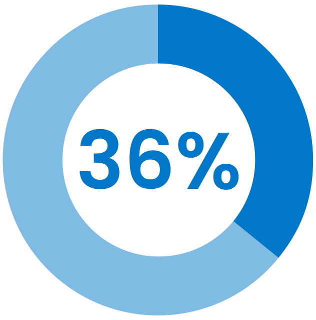
Introduction: The mobile threat landscape

Smartphones have been an ever-present element of our daily lives for almost 20 years and are now seen as an integral part of both our identity and our work.

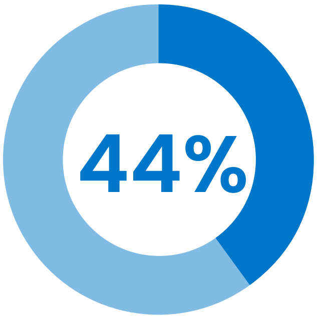
This dependence on smartphones, however, presents increased risk of device theft and malicious activity in a landscape of constant evolution. Businesses are now under constant attacks that stem from a combination of technological vulnerabilities, user behaviours, and highly innovative and malicious actors. It is a daily battle to thwart various types of phishing and detecting/avoiding malicious malware. These fights will only intensify with the emergence of generative AI.

In today's digital world, the scale of cyber threats is an immense burden on IT professionals. In the latest ISACA threat report, 66% of respondents suggested that their occupational stress was much higher now than it was five years ago while 81% attributed that stress to an increasingly complex threat environment.

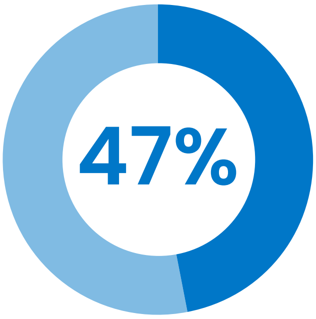
However, security professionals are still working to combat these emerging threats; they just have fewer resources. In ISACA's report, just 36% of respondents indicated that their budgets are appropriately funded – a 5% drop from the year before. What's more, 44% of respondents felt that their budgets were somewhat underfunded, which is an increase of 4% from the previous year. Respondents also gave a bleak impression of their future budgets, with only 47% believing that budgets will increase.



of respondents indicated that their budgets are appropriately funded



of respondents felt that their budgets were somewhat underfunded



of respondents believed that budgets will increase

1
2
3
4
5
6

The security challenges of distributed work and mobile devices

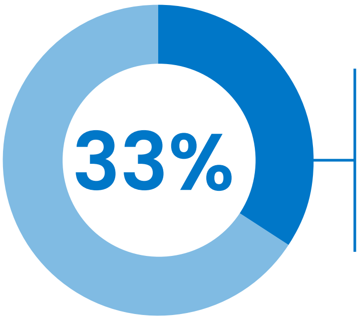
Human error still represents one of the biggest headaches for IT leaders, and its impact shouldn't be underestimated. Risky user behaviour, such as using weak passwords, shadow IT in the form of downloading apps from untrusted sources - or ones that are simply unauthorised by the organisation - and clicking on malicious links can all lead to serious breaches of security. Older devices with sideloaded apps and outdated operating systems also provide hackers with plenty of opportunities.

Making matters worse, the ubiquity of mobile devices and cloud applications has enabled many jobs to be done from almost anywhere, and we are now seemingly always available. This makes mobile devices a prime target for attackers, and phishing is the go-to method when exploiting lapses in human judgment.

In the UK alone, half of businesses and roughly one-third (32%) of charities told the government they had experienced some form of cyber security breach or attack in the last 12 months. The most common vector of a successful attack was phishing, with the report stating 84% of businesses and 83% of charities had been compromised this way.

Email phishing is arguably the most common strategy businesses will face, with smishing (SMS phishing) and vishing (voice phishing) more associated with the general public.

A 2024 study of 3,000 combined UK office workers and business leaders (business owners and C-suite execs) commissioned by Vodafone found AI-driven phishing attacks were proving harder to spot. Only a third of the respondents were able to correctly distinguish a fake, AI-developed video or email from the real thing. Worryingly, more than half (55%) of the business leaders and 45% of the office workers revealed they had been targeted by a phishing attempt within the past two years. Here, email was the top method (82%), with vishing second (39%), and via social media third (22%).



of the respondents were able to correctly distinguish a fake, AI-developed video or email from the real thing

Generative AI is contributing to the problem by being used to create highly personalised and realistic emails and SMS messages. This is essentially social engineering enhanced by the power of generative AI, speeding up the process and making it easier for attackers to launch personalised campaigns against victims with the goal of accessing credentials or downloading malware. The latter, according to Netskope data, states that 9.8 out of every 1,000 users are tricked into downloading malware over phones and laptops every month.

The power of artificial intelligence is changing many facets of business, but in the realm of cyber security, increasingly it's less a "nice to have" and more of a necessity.

Challenges for industries with high-security needs

For IT security in financial service and government, the old security playbook is obsolete. The new frontline is mobile. Cybercriminals and state-sponsored groups aren't just probing networks anymore; they're targeting the phones in the employees' hands. They're aiming to intercept client calls, steal sensitive data, and hijack important transactions.

And the fallout from a mobile breach can be devastating. In finance, a single compromised device can threaten market stability, lead to huge financial losses, and bring about tough regulatory fines and lasting damage to the organisation's reputation.

For government agencies, the risk is just as real. A breach can leak state secrets, expose classified intelligence, and shatter public trust in an instant. In these high-stakes fields, strong mobile security isn't just a good idea—it's essential for keeping the organisation stable and secure.

That's why these organizations require fine-tuned control over the device and its apps. They need a way to enforce strict app policies, locking down devices to only a list of approved apps to stop data leaks and block malware–while still being able to audit communications.

Shifting to a zero trust mindset

Picture the scene: Peter, one of your employees, accessed a system from central London half an hour ago; now he's accessing that same system from 40km away in Slough. Another employee, Juan, logged in from Madrid 10 minutes ago, but now it looks like he's over 11,600km away in Manila.

One of these has a reasonable explanation – Peter travelled from London to Slough by train, which takes about 30 minutes. Juan's journey, on the other hand, should take about 20 hours by plane, so it is clearly suspicious. Without robust security in place, however, your fast-travelling employee's account may be allowed to carry on unimpeded.

Many of the ills that come our way through the internet, either human or AI-generated, can be prevented by simply being more sceptical. This is zero trust, which is as much a state of mind as it is a security protocol.

Instead of traditional network security, where those inside the network are assumed to be trustworthy, zero trust takes away that assumption and requires everything to be checked and approved in real time, every time, before any access is granted. The premise is that organisations should operate a "never trust, always verify" mentality to ensure as strong a security posture – particularly on mobile – as possible.

Applying a zero trust approach has benefits beyond simply security, however. Controls like single sign-on (SSO) actually make it smoother for users, adding a layer of efficiency into the workforce.

Why is zero trust so important now?
Since the dramatic shift to remote work in 2020, more workers access devices and systems from multiple locations. For the end user, it's just a laptop or a phone that they use to work from anywhere, but for the IT department, it's one of many access points and yet another area of potential risk.

Mobile devices must be fully considered when it comes to an overarching security framework. They are more easily lost or stolen than larger devices like a laptop, and are also more likely to be taken out regularly, particularly if they are considered personal devices. This is why the mobile factor is a critical component to wider organisational security and, thus, the zero trust approach is critical in keeping all endpoints – not just mobile – secure and operationally safe.

Applying a zero trust approach has benefits beyond simply security, however. Controls like single sign-on (SSO) actually make it smoother for users, adding a layer of efficiency into the workforce. Here, users only have to enter credentials once, rather than every time they want to use a different app or service, making it more efficient and more secure.

Finally, a zero trust approach is also a smart financial investment; the incentive can often be at the forefront in the minds of business leaders. As such, zero trust architectures should be seen as a form of insurance policy against stolen data. According to IBM, the average cost of a single data breach is thought to exceed $4 million, which is a hefty fee regardless of the size of your organisation. With that in mind, the implementation of a zero trust approach should be viewed as a shrewd investment.

Moving from theory to reality with mobile security

So now we know what is needed in theory, how do businesses go about putting it into action?

This starts with changing the organisation's outlook on IT and security. After all, zero trust is more of a mindset than a protocol. There are zero trust processes and settings to put in place, such as multifactor authentication and biometric logins, but ultimately, it's a way of approaching IT access that requires different thinking across the organisation.

Education is key; having open discussions with the people in your business, reminding them to be vigilant, and repeating that message will make it second nature.

Businesses can also implement training and offer support to staff so that they are knowledgeable about the best practices of zero trust.

Making security a fundamental ingredient of any technology in use is both less of a headache later down the road and also a way to reduce unforeseen costs.
When it comes to truly successful mobile device security, you need the right combination of hardware, software, and operating system, with tight security controls for all three. Which is why Samsung and Android Enterprise have partnered to help organisations tackle some of these biggest challenges.

Innovation in action: secure solutions from Samsung and Android

Samsung and Android's partnership boasts numerous business benefits, such as a secure and manageable mobile experience that protects an organisation's data and its employees.

Samsung devices use Google's Android OS, the most widely used operating system in the world. Built on a hardened Linux kernel, Android is an open source operating system, rather than a walled garden like other operating systems. This brings the benefit of a "many eyes" approach to security at the base level; as it's open source, anyone can examine the code, try it out, and discover bugs or flaws. This means they can potentially be identified and fixed more quickly than if only a handful of developers and security experts had their eyes on it.

The integration of Samsung Knox and Android Enterprise simplifies device management for IT administrators.

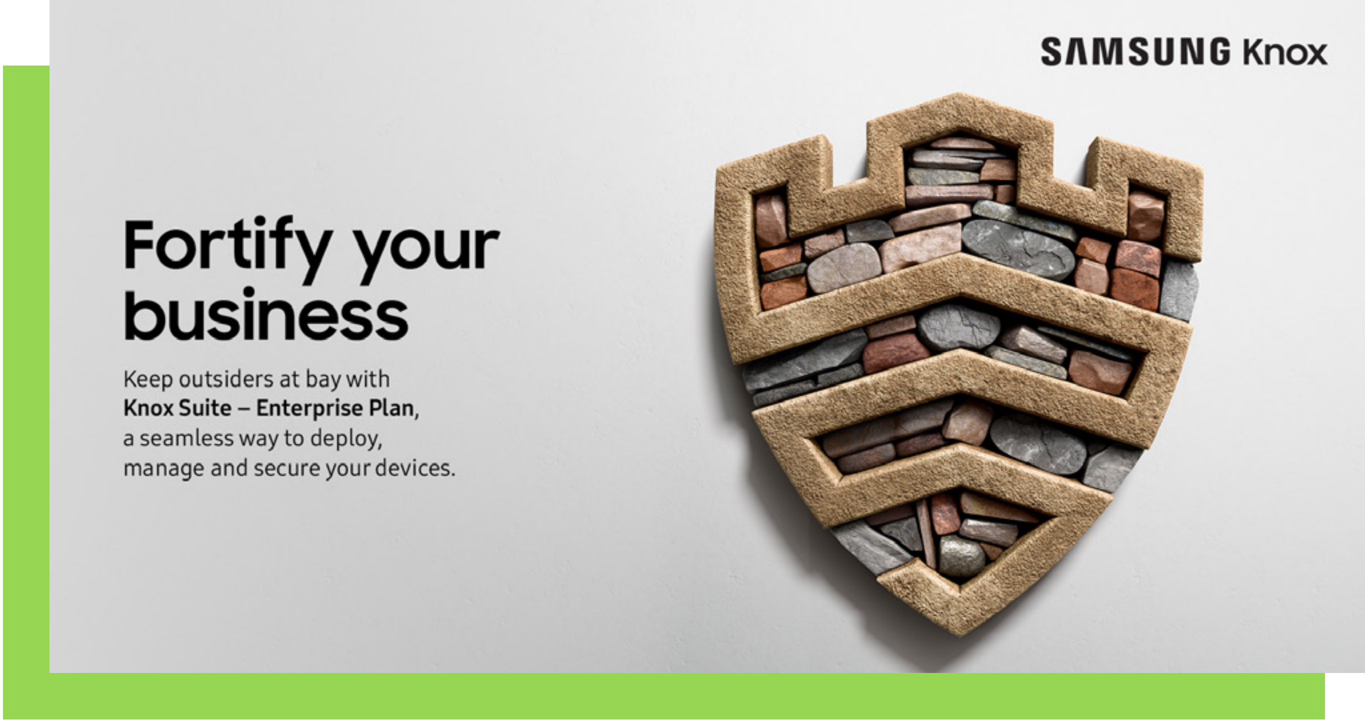
To give context to how this partnership is benefiting organisations around the world, let's take a closer look at some of the specific challenges referenced above, and how Samsung and Android are working together to address them.

- **Data protection and compliance**
  The protection of data is a key part of mobile security. As is compliance with conflicting global data regulations. For example, Samsung and Android devices have several features that aid with compliance, particularly for enterprise customers, such as audit logging required by the National Information Assurance Partnership (NIAP).

  For greater control over the apps on a device, managed Google Play allows enterprises to curate the apps available to employees on fully managed devices and within an Android Work Profile. Separating work and personal data on the device with a Work Profile offers organisations a more secure way to protect devices enabled for personal use, while still retaining full control over the content in the Work Profile.

  With Samsung Knox Manage[1], businesses can also centrally manage device policies such as blocking a device if it leaves the defined geo-fenced location and enters one that has vastly different data laws – avoiding any compliance issues altogether.

1
2
3
4
5
6


SAMSUNG Knox
Fortify your business
Keep outsiders at bay with
Knox Suite – Enterprise Plan,
a seamless way to deploy,
manage and secure your devices.

[1] Please note some Samsung Knox Suite solutions incur an additional fee. Knox Suite – Base Plan incorporating Knox Mobile Enrolment (KME) and Knox Platform for Enterprise (KPE) is included with Samsung Galaxy device purchases at no additional fee.

Knox is embedded in Samsung devices, which helps customers with data protection and compliance through a multi-layered security approach that integrates hardware and software safeguards. The Samsung Knox Secure Boot and Hardware Root of Trust ensures only verified software loads during boot, preventing tampering and supporting compliance with security standards. Real-Time Kernel protection, constantly monitors the OS kernel to detect and block unauthorized changes or exploits.

From a development perspective, Android's built-in security features, like sandboxing, permissions management, and encryption, also help developers build secure apps and mitigate risks, which contribute to overall compliance. There is also 'User Notifications and Actions', where, if a device is non-compliant, Android can display notifications to the user, giving instructions on how to resolve the issue and regain access to work resources.

The Samsung Knox Secure Boot and Hardware Root of Trust ensures only verified software loads during boot.

- **Phishing protection in the age of AI**
  AI is helping to increase the volume of phishing attacks by enabling scammers to create more believable emails. It is also automating their creation so that more can be written all at once, reducing the time it takes to make a targeted email, and making it far easier to spam potential victims. This also isn't just text; AI has also become increasingly good at developing convincing voice messages that are used for voice phishing.

  Samsung devices benefit from Google's AI-powered Scam Detection[2], to help protect against phishing attempts. The device sends an alert when a caller or text message is phishing for information, flagging scams on the phone in real time using AI.

  In addition, Samsung's Auto Blocker can prevent the side-loading of apps from unknown sources, ultimately preventing malware from infecting a device. This also includes blocking USB updates to prevent the installation of malicious software.

  Android also uses AI and Machine Learning to detect threats, with Google Play Protect scanning 200 billion apps daily to help combat malware, phishing, and ransomware.

[2] Accuracy may vary. Availability varies.

- **Implementing a zero trust approach**
  All Samsung devices have zero trust security principles embedded into their architecture, making them a secure and reliable entry point for any network. As such, when a Samsung device is used as an endpoint, it can continuously monitor how devices are being used and flag potential vulnerabilities through Knox Asset Intelligence.

  Network requests can also be routed through the Knox Zero Trust Network Access framework, where user and device metadata can help decide to allow or deny access. This is both an example of zero trust in action and how secure-by-design policies can work in business settings.

  At the same time, Device Trust from Android Enterprise[3] allows organizations a new way to verify the trust status of any Android device used for work. As long as the device is managed by an EMM or approved third-party security app installed on the device, organizations can harness the trust signals on the device to enforce zero trust access policies.

- **Managing mobile device theft**
  Mobile device theft is a global problem and a significant headache for businesses, both from a cost and data security point of view. Samsung's devices, however, have Android theft protection – a multiple security feature designed to prevent theft. So, if a thief snatches the device while it's in use, for example, it will detect the motion associated with theft and automatically lock the screen to prevent the perpetrators from accessing any data.

  Android theft protection features include:

  Theft Detection Lock: When machine learning detects an unlocked device getting snatched, the device automatically locks itself to protect sensitive information.
  Offline Device Lock: If a device disconnects from the network for a set period of time, the device screen automatically locks.
  Remote Lock: In the case of theft or a missing device, users can remotely lock their device screen by going to android.com/lock and entering their own phone number.[4]

  To protect sensitive data from being accessed, Samsung also has a range of solutions, such as the Samsung Warranty Bit, which if it detects tampering, access to sensitive apps like Samsung Pay, Samsung Pass, or Android Work Profile will be automatically blocked to prevent misuse. IT teams can check Warranty Bit remotely using Knox Attestation, and utilise with other management policies.

- **Day to day secure operations and deployments**
  Samsung Knox Suite - Enterprise Plan covers everything from device enrolment, deployment, management and analysis offering a holistic security portfolio that wraps around work devices and apps to protect them. Within Knox Suite – Enterprise plan, there are distinct capabilities that handle different aspects of security or general management, such as the Knox Platform for Enterprise, which is government-grade security for hardware and device management.

  Exclusive to this whitepaper, we interviewed senior security leaders at Samsung and Android to get their perspective on the current security landscape and to dive deeper into how they are supporting businesses. You can find these insightful interviews at the end of the paper.

[3] Device Trust from Android Enterprise solutions are built and offered by third-party providers integrating into the Android Management API. Exact features may vary depending on third-party integrations.
[4] Theft Detection Lock, Offline Device Lock, and Remote Lock requires Android 10+ and an internet connection. Android Go devices are not supported. Support may vary based on your device model. The user must be using the phone while it is unlocked.

Conclusion: Where next for mobile security?

No matter how good your security posture or how secure you feel your IT network is, the mobile threat landscape is always evolving. As such, organisations must do the same. The key to success here is working out where it will change and what will drive it.

One thing that will undoubtedly continue to drive innovation in mobile device security is hybrid work. Devices will get faster and more intuitive, generating a greater need for even more access controls and verification, not just on our devices, but for our business apps and services as well.

Regulations will also undoubtedly change and evolve, which will present both opportunities and challenges for businesses. New governments will seek to put their own policies into action, advancing technologies will require tweaks and updates to existing laws, and evolving threats will force us to rethink laws that become either outdated or too weak to match the threats we face.

Undoubtedly, AI is changing the status quo today and may never stop evolving as it becomes more intuitive and adaptable to us and our ways of working.

Zero trust will also become the default for both businesses and their mobile devices. This means continuous verification for not just devices but also the apps and tools that businesses deploy. What's more, this will also require ongoing verification for not just devices but also the apps and tools that businesses deploy, to protect and respond quickly to threats. With a remote workforce, there is a greater need to verify and protect.

"Super-smart" phones

Undoubtedly, AI is changing the status quo today and may never stop evolving as it becomes more intuitive and adaptable to us and our ways of working. In the future, we could be using 'super-smart' phones, according to Haseeb Awan, the CEO of Efani Secure Mobile. With AI, Awan predicts that smartphones will be able to monitor for suspicious activity even more, mixing edge technology with security and taking the burden away from both the user and the business.

He suggests AI and machine learning could identify potential threats in real time, such as malware, and block them before they cause any harm, like a self-learning security system.

"Your phone's security might become more like that of a learning organism, adapting and improving over time," he said.

"Imagine your phone learning from your past experiences – what websites you visit, what apps you download – and using that knowledge to identify potential risks more effectively."

AI will also become an accelerator of more common threats, making them far more dangerous and more ubiquitous. Malware and phishing, for example, will be more sophisticated, with machine learning enabling them to learn user behaviours for more targeted attacks. This may even include the ability to evade detection, adapt in ways that allow it to bypass security measures, and also become more personalised – and more effective as a result.

Thankfully, AI and machine learning will help those working to defend systems with AI-powered threat detection. Much of this is already being harnessed in Samsung Knox and the Android operating system.

In summary, Samsung and Android have a strong, trusted relationship that delivers enhanced device security through the Samsung Knox platform and its integration with the Android operating system. It's a partnership that has developed over decades and one that ensures Samsung devices are secure from the hardware level up to the operating system and beyond.

Q&A Mike Burr, Senior Security Consultant, Android Enterprise, Google

Can you provide an overview of your role and key responsibilities?
As the Android Enterprise security go-to-market (GTM) lead, I collaborate cross-functionally with various Android Enterprise teams, including marketing, product, partnerships, enablement, customer success, and partner product adoption. My role involves evangelizing and promoting Android Enterprise security to partners and customers, tailoring the message to their level for enhanced understanding.

I am responsible for developing the annual Security Technical Implementation Guide (STIG) for US Federal Android use, writing articles for the customer community, and I recently started hosting "The Secure Element" podcast.

What are some of the biggest misconceptions (either currently, historically, or both) around mobile security, particularly on Android devices?
The most common misconceptions we hear are based on the idea that Android is less secure than other operating systems. For example, some people believe the Google Play store is full of malware, Android and Google cannot be trusted to secure privacy, AI will leak my data, etc. There's also the misconception that Android is less secure due to being an open platform, and that Android devices have more vulnerabilities and zero-day issues.

What is driving this misinformation, and how can organisations ensure they don't fall foul of it (and instead benefit from the value mobility and mobile security bring?
A lot of these misconceptions stem from misleading online articles and a general lack of understanding regarding the best-in-class implementations of Android security, which, contrary to popular belief, often surpass those of other operating systems. Numerous studies and industry accolades consistently affirm Android's robust security, such as Omdia and Leviathan reports from 2025, so it's crucial to stay informed with the latest details and exercise discernment when reading online articles to avoid succumbing to alarmist narratives.

There's a clear need for increased public awareness about Android's security advantages and how an open platform can actually be more secure than a closed ecosystem. Closed ecosystems can be full of undetected vulnerabilities due to researchers' inability to access source code.

This openness has been instrumental for Android innovating in mobile security. Operating within a closed system is like not being able to see the sharks swimming below you until it's too late. Why not embrace a transparent environment, where a diverse group of researchers, industry experts, security vendors, and academics collectively work to identify and mitigate threats?

Android 16 became available in June 2025 – are there any security-specific updates you would like to highlight in this release? Why do they exist and, importantly, why do they matter?
One of the key advancements in Android 16 is the introduction of Android Advanced Protection. This feature consolidates several security-related features into a single setting, making it easier for users at higher risk to activate all available security measures. Additionally, we've integrated Memory Tagging Extensions (MTE) and Device Trust from Android Enterprise.

MTE is a significant step forward in reducing memory-related vulnerabilities like buffer overflows, helping to reduce such issues. This is especially valuable for applications that may not be optimally coded or those built on "memory unsafe" development platforms. For administrators, MTE can be easily enabled across their fleet of A16 devices using an EMM API.

Why is the continued evolution of Android (through a security-focused lens) important to Google?
Android is the most popular operating system in the world, with over 3.5 billion users. We have a responsibility to ensure safety, security, and privacy for all of these users, and we take that incredibly seriously.

How do you balance security with other features, or is it the case that security underpins everything by default?
We believe in a multi-layered security approach that addresses diverse attack vectors, from device-level vulnerabilities to phishing and scam attacks. We've enhanced Google Messages and Google Phone with AI-powered phishing and scam protections, recognizing that many attacks exploit user trust rather than penetrating system vulnerabilities. Android's inherent device and OS hardening helps significantly reduce the success rate of attacks seeking to exploit real vulnerabilities for data access. We also have additional security layers from services like Google Play Protect to scan the device for malicious apps and malware.

> *A good mobile security posture for enterprise administrators, in simple terms, means having a set of rules and tools that protect the company data accessed.*

For consumers, these security features are available without them having to think about it, while Enterprise users benefit from administrator controls that allow customization of security features based on specific use cases. Furthermore, to mitigate privacy concerns related to AI and data leakage, EMM administrators can also control user access to AI features. For instance, Gemini Nano-powered apps like the voice recorder process speech-to-text and summarize recordings entirely on-device. The enterprise version of Gemini also provides robust controls for administrators to manage AI usage within Google products.

The world of remote and hybrid working is here to stay – what advice would you give companies that may still be sceptical about the benefits and fearful about the security implications?
Mobile use is here to stay, whether using phones or tablets. Beyond this, there is a rise in companies that are beginning to offer a mobile-only approach with desktop mode, such as Samsung DeX. The main reason we are given is that the mobile OS (Android) is more secure than desktop systems. The total

cost of ownership (TCO) is also lower in many cases. Additionally, the network requirements to protect data in transit are much more robust and secure in many cases than traditional desktop platforms.

With remote work, it's also very important to implement a zero trust model for mobile devices. We solved this problem with Device Trust from Android Enterprise this year. We provided access to many device signals for EMMs, IDPs, and MTDs that will enable a very robust model. For example, we can provide access to the status of Google Play Protect, password requirements, and whether devices are rooted for these partners before allowing a user to access company apps and data. These are just a few of the signals we provide.

What does a good mobile security posture look like from your perspective?
A good mobile security posture for enterprise administrators, in simple terms, means having a set of rules and tools that protect the company data accessed. It starts with control over devices. Admins need to know what devices are accessing company data and have the ability to enforce security policies on them. This is done through Enterprise Mobility Management (EMM) solutions.

Next, company data should be kept separate from personal data on the employee's device. This way, if an employee leaves a company or loses their device, the company can wipe only the corporate data without affecting their personal apps and data. This can be achieved using an Android Work Profile. For app security, only approved, secure applications should be allowed to access company data by using managed Google Play. Admins should be able to block risky apps and ensure that all apps are up-to-date, and disallow the sideloading of applications. Additionally, all company data, both on the device and in transit, should be encrypted. This makes it unreadable to anyone who shouldn't have access. Ensure backend systems require SSL for connections.

Android Enterprise lays down the foundation for security and controls. Samsung enhances the already built-in capabilities by extending security and controls with Samsung Knox.

Employees should also have to use passwords, biometrics, multi-factor authentication, and Device Trust from Android Enterprise to secure access to company resources. This prevents unauthorized access even if a device is stolen. In general, the system should be able to detect and respond to threats like malware, phishing attacks, or devices that have been tampered with, or "rooted". Google Play Protect is a great example of this.

Finally, employee education is critical as people are often the weakest link and need to be trained on security best practices, such as recognizing phishing and scam attempts.

How important are partnerships like Android/Google and Samsung when it comes to helping organisations tackle the mobile security challenges of today and tomorrow?
Android Enterprise lays down the foundation for security and controls. Samsung enhances the already built-in capabilities by extending security and controls with Samsung Knox, especially for security-conscious markets and verticals such as government and financial industries.

Is there anything else you would like to add?
Some users may have concerns about the privacy of their personal information when it comes to using an Android Work Profile. It's important to highlight the fact that with Work Profile, company data is kept separate from personal data on the employee's device.

Companies cannot see what users are doing outside of a work profile on a BYOD deployment model. Admins cannot see what apps, pictures, or websites an employee is using.

1
2
3
4
5
6

Q&A James Pak, Corporate Vice President, Global Mobile B2B Product Management (Knox and Devices), Samsung Electronics

Can you provide an overview of your role and key responsibilities?
I oversee Samsung's Global mobile B2B hardware and software product management roadmap under the Knox brand name, responsible for delivering a B2B mobile lifecycle experience for enterprises and SMBs alike.

What are the biggest challenges facing organisations when it comes to mobile security?
Since mobile devices are now more ubiquitous than ever, especially for the company-issued devices, just the sheer number of corporate-connected end-point devices (now including wearables and AR/VR) out there that could be targeted for exploitation/penetration is a major concern for recognizing relevant threats and maintaining robust security.

Also, AI-assisted attacks are becoming more prevalent with heightened speed, cleverness, and accuracy, and AI-enabled platform/device expansion also brings additional pressure on corporate and personal data protection and privacy challenges.

Thus, finding a balance between productivity/usability and strengthened security has become of the utmost importance to many enterprises and government entities.

Why are these threats so prevalent now – is it natural evolution, or are there other factors at play?
The velocity of technology adoption in mobile technology has certainly exacerbated the issue. It's only natural for attackers to be attracted to end-point devices where people are spending more time using them to access sensitive data, and could make more mistakes thanks to their ever-present nature.

How can Samsung help organisations address these challenges?
Samsung has industry know-how and unique best practices on delivering and up-levelling mobile security management. For example, customers can address mobile OS update and security patching headaches by utilizing Samsung Knox E-FOTA, a service that's designed to provide granular yet powerful update/patch deployment so that admins can deliver time-sensitive security updates to target devices without end user intervention for successful applications, adhering to the organisation's security compliance policies. Samsung can address security challenges in the following three general areas;

- **Secure end-point protection via security-chain**: From low-level hardware chip to app run-time level, Samsung provides security checks at each major layer for integrity and tampering verification, and sensitive data is also protected at rest and in transit by encryption.
- **Security signal against continued threats:** Device attestation combined with device layer-level threat signals provides the foundation for a zero-trust-ready secured device experience.
- **Granular on-device AI control:** Sensitive data is not to be processed in the cloud; Instead, provide settings to enable on-device processing to ensure personal data protection.

What are the key reasons organisations should primarily consider Samsung when it comes to mobile security?
Samsung has been putting efforts into providing both personal and corporate use of Samsung Galaxy devices with its underlying security technology.

Corporate/gov use: With a number of incredible advancements made with Knox Platform for Enterprise and Android Enterprise, plus many years of domain expert knowledge, Samsung has been delivering industry-leading robust security controls for managed mobile devices, accepted by many top enterprises and government entities.

Samsung exemplifies this by producing the industry with top government-grade global security certifications, including the US DoD's STIG and NSA's CSfC." (Knox security certifications and guidance)

Personal use: SMS based malware is automatically blocked by Message Guard, and app side-loading is also disabled by default thanks to Samsung Auto Blocker. Newer models starting with the Galaxy S24 series are benefiting from up to seven years of system update service.

(Samsung Auto Blocker | Fundamentals | Samsung Knox Documentation, Software Lifecycle and Updates | Fundamentals | Samsung Knox Documentation)

Are you able to highlight any key features or innovations that Samsung brings to the table that really showcase mobile security in action?
Samsung leads the industry early on with how the end-point devices should be zero-trust-ready. Samsung devices can be challenged remotely with an attestation function to validate their integrity on an ongoing basis. We have also been working with industry leaders such as Microsoft and Cisco to interface our security event signals so that they can implement SIEM (MS Sentinel) and zero trust-based conditional network access control. You can learn more here:

https://www.samsungknox.com/en/blog/knox-asset-intelligence-for-microsoft-sentinel

https://www.samsungknox.com/en/blog/the-role-of-the-endpoint-in-zero-trust

Are there any use cases or case studies you can share that will inspire others looking to turn mobile security from a burden to a business enabler?
Mobile security shouldn't be seen as a burden but rather as an opportunity to gain a better understanding of how devices are being used and can be optimized for better productivity with an improved security posture.

A prime example of this would be a global leading retailer - Walmart. Samsung has modernized store associates' daily work experience through its introduction of Android-based semi-ruggedized devices whose continuous security updates are

achieved seamlessly by elaborate firmware controls thanks to the Knox E-FOTA solution. (How Samsung Is Helping Walmart Transform the Retail Associate Experience – Samsung Global Newsroom)

There are many other examples of customers adapting Samsung solutions, and they can be found at our samsungknox.com website.

What is Samsung's attitude to partnerships across mobile security?
Samsung thrives in openness, as evidenced by collaboration with Google/Android and other key partners, such as aforementioned Microsoft, Cisco, and more. We understand that by working together, our customers can benefit from synergy that not only improves overall security across multi-tier but also honours customers' technology investment by getting more out of it.

Also, when it comes to addressing security vulnerabilities, again, openness plays an important role in active monitoring and detecting unknown security threats and proactive responses at the collaborative community level.

> *Mobile security shouldn't be seen as a burden but rather as an opportunity to gain a better understanding of how devices are being used and can be optimized for better productivity with an improved security posture.*

What do you think the future holds for mobile security?
I think the unprecedented nature of AI advancement will further proliferate the increase in system vulnerability attacks. This will undoubtedly put pressure on enterprises to spend more money on security, which leads to further growth of the security solutions market.

A year from now, what sort of things would you like to be talking about, and conversely, what do you not want to be talking about?
AI is both an enabler but also seen by some, as a risk to many establishments. I would like to see more embracing of device security policy automations thanks to AI integrations.