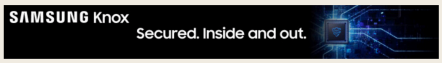
🚀 The new CIO.com hybrid search: 🔍 Explore CIO content smarter, faster and AI powered. ✨ **Try it!**

ADVERTISEMENT



MAKING MOBILE WORK: SECURITY AND CONTROL WITH SAMSUNG KNOX

See how Samsung Knox enhances mobile security, supports everyday workflows, and integrates with top EMMs—helping enterprises stay protected, productive, and in control.

Sponsored by Samsung

SAMSUNG

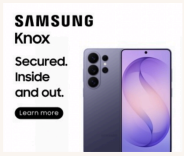
How Samsung completes your Zero Trust Architecture

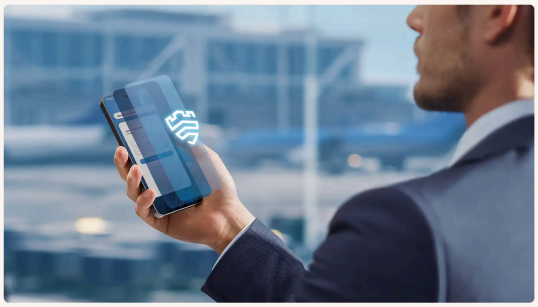
BrandPost • By Lee Radix

Aug 29, 2025 • 4 mins

To close gaps in Zero Trust, enterprises need mobile coverage. Samsung Galaxy and Knox Suite deliver stronger security and deeper visibility.

ADVERTISEMENT





Credit: Samsung

Let's cut to the chase: The average data breach now costs **$4.88 million**[1]—and even with a Zero Trust strategy in place, your risk *increases* if mobile isn't part of it. Every mobile device connected to your corporate network is a potential breach point. And with work happening everywhere, traditional perimeter security can't keep up. It's time to go beyond Mobile Device Management for Enterprise security and extend your Zero Trust strategy to mobile.

Zero Trust must include mobile devices

Zero Trust is becoming the standard for enterprise security—and for good reason. **The U.S. government is pushing agencies to adopt it.** Enterprises are following suit. And the philosophy is simple:

1. **Never trust, always verify.**
2. **Assume breach.**
3. **Give least privilege access.**

Every access request is checked in real time based on current risk signals. It's like checking someone's passport *and* scanning them for threats, not just assuming someone's safe because they were last week.

That works well for laptops and desktops... but what about mobile?

Security Operations Center (SOC) platforms—such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)—are evolving to incorporate Zero Trust Architectures (ZTA), particularly with AI-assisted security features.

However, a *significant* gap remains in the availability of high-quality data from mobile devices. This lack of data hinders accurate analysis of security posture and limits the ability to take necessary actions. This is where Samsung comes in.

Zero Trust-ready Samsung Galaxy devices give you deeper insight

As the maker of Samsung Galaxy devices and the cloud-based Knox Suite, Samsung offers a uniquely integrated approach to mobile security—capturing deep device telemetry to power SOC platforms **and support a true ZTA.**

Samsung Galaxy devices are secured from the chip up, with Samsung Knox built in at the manufacturing stage. This hardware-based foundation extends visibility and control across your security infrastructure, making these devices a trusted part of any Zero Trust strategy.

What's Knox Suite? It's Samsung's all-in-one solution for managing and securing Samsung Galaxy work devices. It also provides the controls and insights needed to support a Zero Trust approach—reducing risk and unlocking cost savings.

Even better, thanks to their exclusive partnerships, you can prevent, detect, and remediate threats faster, reducing potential risk:

- **With Microsoft Intune,** Samsung Galaxy devices, managed or unmanaged, verify their integrity before connecting to corporate resources.
- **With Cisco Secure Access,** enterprises can get high-speed Zero Trust Network Access natively from Samsung Galaxy devices.
- **With Knox Asset Intelligence** (a product of Knox Suite), real-time mobile signals flow into **SIEM tools like Microsoft Sentinel,** so your security team sees mobile threats just like any other alert.

With Samsung Galaxy and Knox Suite, mobile devices are no longer a security gap; they're part of your ZTA.

Why this matters now

CIOs and IT leaders are under pressure to prevent data loss, not just react to it. That means extending Zero Trust to mobile.

Samsung surveyed in 2024 and found that IT decision-makers and the workforce named data protection as their top concern when considering mobile security.

Samsung is the first OEM to deliver Zero Trust capabilities directly on mobile, with full device-level visibility, seamless integrations, and cloud-ready control.

If Zero Trust is your goal, mobile *must* be part of the strategy, and Samsung makes that possible. Ready to learn more about Samsung Knox security? **Learn more here!**

🚀 The new CIO.com hybrid search: 🔍 Explore CIO content smarter, faster and AI powered. ✨ Try it!

ADVERTISEMENT



MAKING MOBILE WORK: SECURITY AND CONTROL WITH SAMSUNG KNOX

See how Samsung Knox enhances mobile security, supports everyday workflows, and integrates with top EMMs—helping enterprises stay protected, productive, and in control.

Sponsored by Samsung

SAMSUNG

Why CIOs are pairing Samsung Knox Suite with their EMM

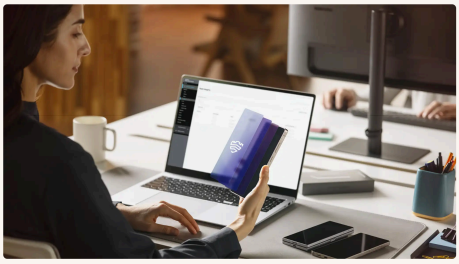
BrandPost • By Lee Radix

Sep 25, 2025 • 4 mins

See how Samsung Knox enhances mobile security, supports everyday workflows, and integrates with top EMMs—helping enterprises stay protected, productive, and in control.

ADVERTISEMENT





Credit: Samsung

Your EMM is doing its job. But it can do more with Samsung Knox.

Most enterprises use a unified endpoint management (UEM) or enterprise mobility management (EMM) platform to manage device fleets. But for Samsung Galaxy devices, Knox Suite goes beyond the standard EMM feature set, unlocking deeper security, tighter control, and smarter device insights—extending the value of your EMM solution *without* disrupting your existing workflows.

Read on to learn how pairing Know Suite with your current EMM can greatly improve your mobile strategy.

Built to enhance the EMM you already use

Samsung builds Knox Suite for Samsung Galaxy devices, so the integration goes far deeper than any third-party solution can offer. Designed to enhance the IT admin experience on your existing EMM system, Knox Suite provides more advanced capabilities and granular control over your Samsung fleet, *without the need to migrate platforms.*

Whether you're using Microsoft Intune, Omnissa Workspace ONE, SOTI MobiControl, Ivanti Neurons for MDM, or other mainstream EMMs, Knox Suite complements your setup.

Put simply, Knox Suite extends your existing EMM's reach.

Go beyond standard security

Traditional endpoint tools provide basic policy enforcement, but Knox Suite brings device-level assurance that most other tools can't access. For example:

- **Knox On-Device Attestation** confirms device integrity *before* access is granted—using hardware-backed verification to spot signs of tampering or rooting. This is now a **default setting** for all new Android App Protection Policies in Microsoft Intune MAM!
- **The Security Center dashboard** surfaces operating system (OS) vulnerabilities and patch levels specific to unique chipsets across your Samsung fleet, giving IT a centralized view of where to take action.

Together, these features help you stay ahead of evolving threats, without adding operational overhead.

Simplify and secure device enrollment

Enrollment is often the first source of friction for IT and end users (sound familiar?). Knox Suite simplifies the process while improving control and flexibility—*and* accelerates time to productivity for employees. Here's how:

- **Knox Mobile Enrollment** locks devices to your organization—even after a factory reset—until released by an admin, ensuring unmatched control and security.
- **Knox Mobile Enrollment – Advanced Settings** allows you to pre-load local apps, prevent unauthorized removal, and trigger security responses like auto-lock if tampering is detected.

These tools ensure your devices are ready for work from the moment they're powered on—now that's a flex.

Support your frontline

Knox Suite includes powerful tools to support productivity and operational continuity—especially across shared or task-based devices in frontline, retail, healthcare, and logistics environments:

- **Knox Capture** turns Samsung devices into high-performance barcode scanners.
- **Knox Authentication Manager** streamlines shared device access—even for non-SSO apps—saving time and keeping devices secure between shifts.
- **Knox E-FOTA** ensures critical Line-of-Business apps keep running smoothly by letting IT control OS versioning—preventing unexpected updates that might break functionality or drain battery.
- **Knox Asset Intelligence** can extend your device fleet's daily battery life by up to 20% with battery auto optimization.[1]

These tools are built to reduce friction and keep work moving—no matter where or how it happens.

Make smarter decisions with better data

Knox Suite unlocks **rich telemetry data** from Samsung devices—data your EMM alone can't access.

- Monitor app usage, performance, and crash patterns.
- Detect battery drain issues or poor Wi-Fi connectivity.
- Diagnose bugs quickly with on-device logging and debug tools.
- Connect to your Security Operations Center to surface device-level security threats.

With these insights, you can proactively support users, extend device lifecycles, **and cut support costs.**

One investment, many returns

Knox Suite isn't here to replace your existing systems—it's built to extend them. By pairing it with your current EMM, you gain:

- Better device-level security
- Enhanced frontline operations
- Improved user productivity
- Lower TCO across your Samsung Galaxy fleet

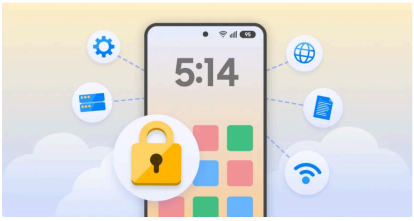
Explore Knox Suite or **talk to a Samsung Knox expert** to see how it fits into your mobility strategy.



How Samsung Knox Helps Stop Your Network Security Breach

The Hacker News
Feb 06, 2026

Mobile Security / Threat Detection



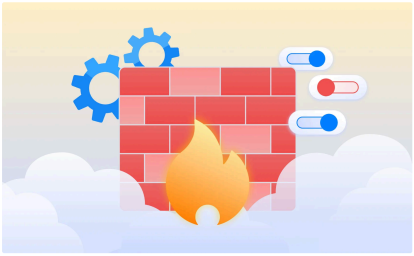
As you know, enterprise network security has undergone significant evolution over the past decade. Firewalls have become more intelligent, threat detection methods have advanced, and access controls are now more detailed. However (and it's a big "however"), the increasing use of mobile devices in business operations **necessitates network security measures that are specifically tailored to their unique operating patterns.**

Yes, enterprises have invested heavily in robust network security such as firewalls, intrusion detection, and threat intelligence platforms. And yes, these controls work exceptionally well for traditional endpoints—but mobile devices operate differently! They connect to corporate Wi-Fi and public networks interchangeably. They run dozens of apps with varying trust levels. They process sensitive data in coffee shops, airports, and home offices.

The challenge isn't that organizations lack security—it's that **mobile devices need security controls that adapt to their unique usage patterns.**

Samsung Knox is specifically designed to address this reality. Let's find out how.

Samsung Knox Firewall offers granular control



Change my mind: Most mobile firewalls are blunt instruments. Traffic is either allowed or blocked, with little visibility into what's happening—or why. That makes it hard to enforce meaningful policies or investigate issues when something goes wrong.

Knox Firewall takes a more *precise* approach. It gives IT admins granular, per-app network controls and the transparency security teams expect.

Instead of defaulting to "allow all" or "block everything," rules are tailored to individual applications. A confidential document viewer can be restricted to specific IP addresses. Collaboration tools can be limited to approved domains. Each app gets network access based on its risk profile—not lumped in

Knox Firewall also supports IPv4 and IPv6 filtering, domain and sub-domain controls, and both per-app and device-wide modes. Because it's built into the device architecture, it avoids the performance overhead and deployment complexity common with third-party firewalls.

Key takeaway: Knox Firewall gives IT teams granular control and complete visibility, turning a "block or allow" firewall into a proactive, investigative tool.

Zero Trust Network Access that works alongside your VPN



Perimeter security isn't enough anymore. Access decisions need to consider device health, user identity, and context—and they need to do it continuously, not just at login.

That's where the Samsung Knox Zero Trust Network Access (ZTNA) framework comes in. It supports Zero Trust principles while working alongside your existing VPN investments, **not replacing them.**

By using host-based micro-segmentation, the Samsung Knox ZTNA framework isolates network traffic by app and domain. The result? A smaller attack surface and far less room for lateral movement if a device or app is compromised.

Key features include:

- split DNS tunneling to balance security and performance
- context-rich metadata (such as app package name, signature, version) to enable precise access policies
- dynamic policy evaluation at access time based on device and application context
- privacy-aware traffic handling that respects enterprise and user boundaries

Most importantly, the Samsung Knox ZTNA framework is built for real-world environments. It works alongside the VPN and mobile threat defense tools organizations already use—no rip-and-replace required!

For organizations with existing VPN infrastructure, the Samsung Knox ZTNA framework enables a gradual migration path. That's Zero Trust in practice—precise access control, reduced attack surface, and the flexibility to evolve security architecture at your own pace.

Key takeaway: The Samsung Knox ZTNA framework brings practical Zero Trust to life, working with the tools teams already trust while locking down mobile access.

The integration advantage

Samsung Knox isn't just a collection of tools—it's a system. Threat signals flow across the device, adapting protections in real time. A phishing alert? That can trigger new firewall rules or even a hardware-backed lockdown. Device health, user context, and threat intelligence all work together—Zero Trust, in practice, not just on paper.

Because Samsung Knox is built into Samsung Galaxy devices, you skip the chaos of multiple agents, vendors, and integrations. SOC 2 certified, GDPR-ready, and fully compatible with leading MDM, UEM, and SIEM platforms—it just works.

Mobile devices aren't endpoints anymore—they're entry points. And if your network security doesn't protect them, it's not just incomplete. It's useless.

Note: This article was written by Lee Radix.





Top Stories This Week


KREMLIN Banking Malware Hijacks Chrome and Edge to Steal Credentials and Session Tokens


Google Gemini Broke Into Real Company Systems After Security Test Domain Mix-Up


Attackers Use Passkey Phishing to Hijack Microsoft Cloud Accounts and Exfiltrate Data


Cisco Warns of New Zero-Day ISE Auth Bypass (CVSS 10.0) Exploited in Active Attacks


China-Linked Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy GRIMWEDGE


New WordPress Click2Shell Flaw Forces Theme Installs, Can Chain to Code Execution


Google Patches Pixel Modem Flaw Amid Signs of Limited Targeted Exploitation


Critical Check Point Management Flaw Lets Unauthenticated Attackers Run Code as Root

LOAD MORE

Featured Resources


Turn Threat Intelligence Into Verified Risk With Threat-Led Penetration Testing


Deploy Browser Security Monitoring in Minutes With a Single Header


Red Teams: Learn How Attack Path Chaining Changes Automated Security Testing


Validation Summit '26: See How Pen Testing, Exposure Validation and BAS Work Together



Securing the Open Android Ecosystem with Samsung Knox

The Hacker News Nov 05, 2025 Mobile Security / Enterprise IT



Raise your hand if you've heard the myth, "Android isn't secure."

Android phones, such as the Samsung Galaxy, unlock new ways of working. But, as an IT admin, you may worry about the security—after all, work data is critical.

However, outdated concerns can hold your business back from unlocking its full potential. The truth is, with work happening everywhere, *every* device connected to your network is a potential security breach point. As threats evolve, so must the tools to defend against them.

Allow me to introduce Samsung Knox—a built-in security platform that combines hardware and software protections on Samsung Galaxy devices. It's loaded with features and is designed to safeguard data, provide IT teams with deeper control, and offer a flexible foundation for enterprise needs.

Let's take a look at some myths about open source and how Samsung can get you on the right path to success.

Myth 1: "Isn't Android more prone to malware and attacks?"

Common concerns around sideloading and third-party apps can be addressed through Samsung Knox's enterprise controls, which let IT admins curate approved apps and prevent sideloading. Plus, AI-powered malware defense adds another layer of protection to help keep the Android ecosystem secure. Here's how:

Proactive protection at scale:

- **Google Play Protect** scans over 200 billion apps daily, ensuring threats are blocked before they spread.
- According to Google, Managed Google Play devices see an exceptionally low rate of potentially harmful app installs, even when company-published apps are included.

Extra defense with Samsung Knox on Samsung Galaxy devices:

- Samsung Message Guard protects Samsung Galaxy devices from zero-click attacks by automatically isolating and scanning suspicious image files received through messaging apps.
- DEFEX (Defeat Exploit) detects abnormal app behaviours and can terminate them before they become active threats.

Key point: Android security isn't about being open or closed—it's about layered, proactive protection. With Samsung Knox on Samsung Galaxy devices, enterprises get exactly that.

Myth 2: "Aren't modern threats about platforms, not people?"

A growing number of breaches today actually stem from *human* vulnerabilities—not just the platform itself! Let's take a look:

- According to Verizon's 2025 Data Breach Investigations Report, an incredible **60%** of breaches involve the human element, including phishing and social engineering.
- The Lookout Mobile Threat Landscape Report – 2024 found that mobile device users face phishing attacks regardless of the platform, with Android devices actually encountering *fewer* incidents in 2024 (surprised?).

The bottom line is, the biggest risks originate from overlooked basics. For example, failing to update devices with the latest security patches and not implementing the necessary IT policies—this applies to *both* open and closed platforms!

Here's how Samsung Knox helps:

- **Know which device to update, when, and why:** Knox Asset Intelligence provides IT admins centralized visibility into such information, and Knox E-FOTA provides precise and stable version control that's hard to match on other platforms.
- **Manage work devices and data according to your business needs:** Samsung Knox enhances the security of Samsung Galaxy devices by providing granular security controls and comprehensive visibility. Users can access these features in multiple ways, including connecting to their own Enterprise Mobility Management systems, using Knox Suite.

Key point: Closed systems don't automatically protect against human error. Enterprises need a layered defense, strong policies, and visibility into device behavior. That's exactly what Samsung Knox delivers!

Myth 3: "Android updates are slower and harder to manage, right?"

With modern Android and Samsung Knox tools, updates are now faster, more flexible, and fully manageable at scale. Let's take a look:

Android innovations:

- Mainline enables critical security and system updates to be pushed directly through Google Play—no wait required for OS upgrades.
- Android's managed system updates allow IT admins to control update timing across work devices, reducing disruption.

Samsung innovations:

The Samsung Knox platform on Samsung Galaxy devices enables hard-to-beat detailed scheduling and stable deployment. **Using Knox E-FOTA, IT admins can access:**

- Target specific firmware versions instead of just the latest release.
- Block all types of user updates, including over-the-air, USB, and unauthorized installations to unintended versions.
- Schedule updates based not only on time but also on factors like battery level and network bandwidth.
- Perform on-prem firmware updates without relying on a cloud network environment.

Key point: With Knox E-FOTA, you gain a strategic level of control that turns mobile updates from a support burden into a predictable, business-aligned process!

The reality: Samsung Knox transforms Android security

Samsung Galaxy devices, secured by Samsung Knox, are redefining what mobile security looks like for enterprises. By addressing old vulnerabilities, tackling human-driven threats, and giving IT strategic update control, Samsung Knox shifts Android from "perceived risk" to enterprise-grade resilience.

The result? Government-grade protection, centralized visibility, and smarter management. Don't take my word for it; find out for yourself by trying Samsung Knox.





Top Stories This Week

- Attacker Hijacks AI Coding Assistant Session, Spreads Shai-Hulud Across About 100 Repositories
- Three Threat Groups Target Russian Enterprises With Backdoors, Ransomware, and Wipers
- Weekly Recap: Rogue AI Agents, WeChat Worm, PaperCut Attacks, AI Espionage, and Rootkits
- Twitch Browser Extension Leaks OAuth Tokens From Nearly 31,000 Users
- China-Linked Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy GRIMWEDGE
- Attackers Use Passkey Phishing to Hijack Microsoft Cloud Accounts and Exfiltrate Data
- LiteSpeed Enterprise Flaw Could Let One Hosting Account Gain Root Access on a Shared Server
- Cisco Warns of New Zero-Day ISE Auth Bypass (CVSS 10.0) Exploited in Active Attacks

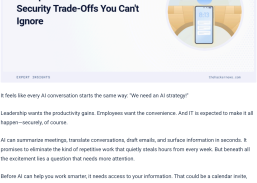
LOAD MORE

Featured Resources

- Red Teams: Learn How Attack Path Chaining Changes Automated Security Testing
- Deploy Browser Security Monitoring in Minutes With a Single Header
- Turn Threat Intelligence Into Verified Risk With Threat-Led Penetration Testing
- Validation Summit '26: See How Pen Testing, Exposure Validation and BAS Work Together

Enterprise Mobile AI: The Security Trade-Offs You Can't Ignore

Samsung
Sep 21, 2026



It feels like every AI conversation starts the same way: "We need an AI strategy."

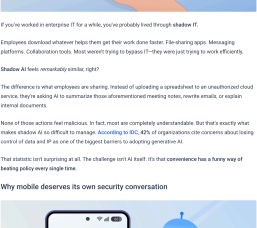
Leadership wants the productivity gains. Employees want the convenience. And IT is expected to make it all happen—securely, of course.

AI can summarize meetings, translate conversations, draft emails, and surface information in seconds. It promises to eliminate the kind of repetitive work that quietly steals hours from every week. But beneath all the excitement lies a question that needs more attention.

Before AI can help you work smarter, it needs access to your information. That could be a calendar invite, next quarter's product roadmap, or IP. Think of AI like hiring the world's smartest intern. It can research, summarize, and help organize your otherwise disorganized meeting notes. In other words, you have to hand it your notebook full of your confidential information.

The real question is what happens to that notebook after you've handed it over.

Shadow AI isn't a tech problem. It's a people problem



If you've worked in enterprise IT for a while, you've probably lived through **shadow IT.**

Employees download whatever helps them get their work done faster. File-sharing apps. Messaging platforms. Collaboration tools. Most weren't trying to bypass IT—they were just trying to work efficiently.

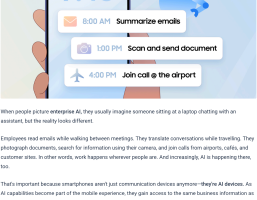
Shadow AI feels *remarkably* similar, right?

The difference is what employees are sharing. Instead of uploading a spreadsheet to an unauthorized cloud service, they're asking AI to summarize those aforementioned meeting notes, rewrite emails, or explain internal documents.

None of those actions feel malicious. In fact, most are completely understandable. But that's exactly what makes shadow AI so difficult to manage. According to IDC, 42% of organizations cite concerns about losing control of data and IP as one of the biggest barriers to adopting generative AI.

That statistic isn't surprising at all. The challenge isn't AI itself. It's that **convenience has a funny way of beating policy every single time.**

Why mobile deserves its own security conversation



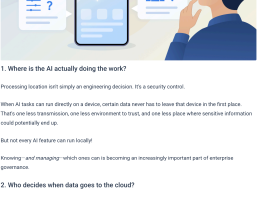
When people picture **enterprise AI,** they usually imagine someone sitting at a laptop chatting with an assistant, but the reality looks different.

Employees read emails while walking between meetings. They translate conversations while travelling. They photograph documents, search for information using their camera, and join calls from airports, cafés, and customer sites. In other words, work happens wherever people are. And increasingly, AI is happening there, too.

That's important because smartphones aren't just communication devices anymore—**they're AI devices.** As AI capabilities become part of the mobile experience, they gain access to the same business information as the OS itself.

That's where things start to get interesting.

The four questions every enterprise should ask



1. Where is the AI actually doing the work?

Processing location isn't simply an engineering decision. It's a security control.

When AI tasks can run directly on a device, certain data never has to leave that device in the first place. That's one less transmission, one less environment to trust, and one less place where sensitive information could potentially end up.

But not every AI feature can run locally!

Knowing – and managing –which ones can is becoming an increasingly important part of enterprise governance.

2. Who decides when data goes to the cloud?

This is the question organizations may underestimate.

Even if cloud processing is necessary, who decides when it happens? The employee? Or IT? And can those policies actually be enforced on every endpoint—including mobile devices?

Those are two very different governance models. Policies are important. **But technical controls are better.** Why? Because relying on thousands of employees to make the right security decision every single time isn't really a strategy.

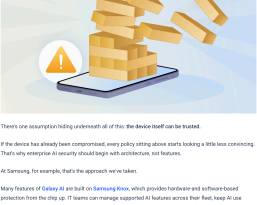
3. Who owns the AI relationship?

When AI activity lives inside a personal account, chat history, generated content, and organizational knowledge can leave with the employee. That's no longer just an identity management issue. **It's a corporate knowledge issue.**

Managed identities help ensure AI remains part of the organization's environment—not someone's personal digital workspace. As AI becomes another place where business knowledge is created, identity architecture becomes just as important as access management.

The fourth question is coming up after a little extra context.

Every governance model rests on one assumption



There's one assumption hiding underneath all of this: **the device itself can be trusted.**

If the device has already been compromised, every policy sitting above starts looking a little less convincing. That's why enterprise AI security should begin with architecture, not features.

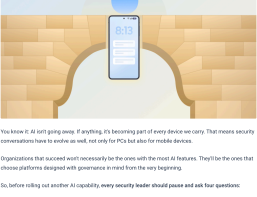
At Samsung, for example, that's the approach we've taken.

Many features of Galaxy AI are built on Samsung Knox, which provides hardware-and software-based protection from the chip up. IT teams can manage supported AI features across their fleet, keep AI use connected to managed corporate identities, and apply controls for how supported features and cloud services process business data. This helps organizations give employees access to AI while maintaining visibility and control.

That's the interesting part: not that AI can summarize a meeting. Lots of AI can do that. The real question is whether your organization can confidently answer where that summary was processed, who controlled the policy behind it, and where that information now lives.

Those are architecture questions. Not AI questions.

The future belongs to trustworthy AI



You know it: AI isn't going away. If anything, it's becoming part of every device we carry. That means security conversations have to evolve as well, not only for PCs but also for mobile devices.

Organizations that succeed won't necessarily be the ones with the most AI features. They'll be the ones that choose platforms designed with governance in mind from the very beginning.

So, before rolling out another AI capability, **every security leader should pause and ask four questions:**

1. Can sensitive tasks stay on-device whenever possible?
2. Can cloud processing be governed centrally?
3. Is AI tied to managed corporate identities?
4. **Does all of it sit on a trusted device foundation?**

Here's the thing: The smartest AI in the world won't matter much if nobody trusts it with the notebook. That's why many features of Galaxy AI on Samsung Galaxy devices are built on a foundation of Knox security—helping organizations adopt AI with confidence. **That's the conversation enterprise security should be having.**

Top Stories This Week


Claude Opus 5 Helped Researchers Take Over OpenAI Staff Accounts via Chained Flaws


Google Gemini Broke Into Real Company Systems After Security Test: Human Mix-Up


OpenAI Reveals Six Model Incidents Involving Hidden Failures and Unauthorized Uploads


Public Exploits Released For Four Linux Kernel Flaws That Enable Local Root


New WordPress Click2Shell Flaw Forces Theme Installs, Can Chain to Code Execution


Critical Check Point Management Flaw Lets Unauthenticated Attackers Run Code as Root


ThreatsDay: Self-Rewriting Agents, 800+ Flaws Patched, Insider SIM Swaps and 22 More New Stories


Critical Unbound DNSSEC Validator Flaw Could Allow RCE via a Malicious DNS Zone


Cisco Warns of New Zero-Day ISE Auth Bypass (CVSS 10.0) Exploited in Active Attacks


Three Threat Groups Target Russian Enterprises With Backdoors, Ransomware, and Wipers


Attacker Hijacks AI Coding Assistant Session, Spreads Shai-Hulud Malware Across 180 Repositories


Google Patches Pixel Modem Flaw Amid Signs of Limited Targeted Exploitation


KRBUM: AI-Ranking Malware Hijacks Chrome and Edge to Steal Credentials and Session Tokens


LiteSpeed Enterprise Flaw Could Let One Hosting Account Gain Root Access on a Shared Server


China-Linked Hackers Exploit Chromium Windows Zero-Day Chain to Deploy GRAMDROP

Cisco Secure Email Gateway Flaw Exploited in the Wild, Enables Root Command Execution

New DDRip Attack Breaks Intel TDX and AMD SEV-SNP Confidential Computing

1 Weekly Recap: Hyper AI Agents, WatNet Worm, PaperCut Attacks, AI Espionage, and Rootkits

Twitch Browser Extension Leaks OAuth Tokens From Nearly 20,000 Users

Attackers Use Passkey Phishing to Hijack Microsoft Cloud Accounts and Exfiltrate Data

Nitro PhishKit Targets US and EU Businesses, A New Challenge for Identity Security

An Abandoned CDN Domain Was Re-Registered. Thousands of Sites Still Call It.

How to Evaluate a Unified Security Platform Using a Dev-Incident Test

Stop Trying to Control AI Behavior; Control What AI Can Reach

Featured Resources

Validation Summit '26: See How Pen Testing, Exposure Validation and BAS Work Together

Red Teams: Learn How Attack Path Chaining Changes Automated Security Testing

Turn Threat Intelligence Into Verified Risk With Threat-Led Penetration Testing

Replay Browser Security Monitoring in Minutes With a Single Header