SAMSUNG

PARTNER LOGO HERE

	Isn't Galaxy based on Android OS which is open source, so less secure?	Aren't some devices known for having better data protection?	Isn't Android's security fragmented, more costly and difficult to control?	Isn't it slower and harder to handle software updates on Android devices?	Isn't Android more prone to malware and attacks?
Respond	Galaxy runs Knox-hardened Android, which adds powerful enterprise controls on top of the flexible, open foundation. And against modern threats, openness is what enables the adaptive protection that business needs.	In reality, Knox-hardened Android covers the commonly promoted data protection capabilities. And for needs beyond baseline security, such as AI risks, theft, or business data, Galaxy is a stronger fit.	A one-size security may sound convenient, but it has limits for enterprise needs. With Android Enterprise and Knox, you can choose the level of security that aligns with how your teams really work.	Android adds ways to expedite critical security updates. And for work devices, what truly matters is making updates predictable and controlled. Galaxy and Knox powers IT to achieve that without compromising security or stability.	Such perception used to come especially from open app ecosystem, but such risks are now greatly reduced especially on work devices. When modern attacks target people, not platforms, Knox helps businesses fortify protection.
Reframe with Context	**Galaxy runs hardened, multi-layered security. Open source is just the base.** - Android Enterprise raises the security baseline across work devices. - Samsung adds Knox, our government-grade security platform, baked into the hardware and software of Galaxy. **"Walled garden" is not the cure to modern threats. Vigilance is.** Closed alone doesn't stop attacks, and may be facing limits. - Lookout 2024 Annual Mobile Threat Report notes how enterprise devices encounter phishing regardless of platform, with Android facing less. - Per the Digital Markets Act, devices in the EU allow side-loading from 2024. **Openness drives the transparency and flexibility enterprises need. Knox can enable both.** - Galaxy helps you be ready for Zero Trust, with OEM-level Knox security signals feeding into SOC workflows. - Open means customizable for highly-regulated security needs, such as Galaxy Tactical Edition (US) running custom ROM for military use.	**The commonly promoted data protection capabilities are largely baseline. Galaxy has them covered.** - File and data encryption by default - End-to-end encryption with Samsung Cloud's Enhanced Data Protection - RCS Messaging encryption with Google Messages - Credentials in a secure chipset with Knox Vault **Beyond baseline, we provide innovative protection against modern risks.** - Some Galaxy AI features can be set to run on-device only, ensuring data control. Configurable for work devices. - Android's theft detection features help keep your device and data safe. **Galaxy gives real control over work data, whatever your business task is.** - **On fully managed devices,** Knox security platform powers the granular controls. - **On BYOD/COPE devices**, Android Work Profile can separate work data from personal. - **Even on unmanaged devices**, block compromised devices from accessing corporate data via Knox-integrated MAM or ZTNA.	**One-size doesn't always mean cheap across teams with varying needs.** - Limited device range (size, form factor) and support for flexible use cases may add cost/friction at scale. - Choosing familiarity over customized security may cause bigger risk. **Android Enterprise provides mature security standards for work devices.** -Android Enterprise Recommended reduces inconsistencies across OEMs, raising the security baseline. - Android Work Profile enables flexible control over work data across various ownership models (e.g. BYOD, COPE). **Knox unlocks the flexibility and controls that can drive business.** - Knox security platform is built in to our diverse portfolio: Galaxy S and A series, rugged, foldable, and even customized for tactical use. - Knox platform fuels the granular security controls, accessible via our Knox services or just plugged in to your own EMM. - Our flexible ecosystem can help cut costs while meeting security standards. Chicago PD adopted Galaxy, DeX, and Knox, saving cost and time.	**Android enables fast and flexible updates, especially for enterprise use.** - Project Mainline allows Android to push critical updates via Google Play, independent from full OS updates. - Managed system update enables IT to postpone/window/auto-install updates as soon as available. **Knox brings strategic control over updates to Galaxy work devices.** - Knox E-FOTA gives precise and stable updates: . Block user updates incl. USB/OTA . Push the version you tested, not just the latest . Push based on time/battery/network . On-premise update support - Get up to 7yr of updates from global launch on Galaxy S24 and later models. **Effective update management starts with visibility and a clear cadence.** - Knox Asset Intelligence helps IT know which device needs urgent updates, with vulnerability context. . See OS versions, patch levels, and attestation checks in one place. - Paired with Knox E-FOTA, IT can create a full loop of update system.	**Google and Samsung proactively protects from malware.** - Google Play Protect scans 200B+ apps daily. It's exceptionally rare to see a potentially harmful app on a managed Android. - Samsung Auto Blocker can block side-loading, and enables Message Guard to block malware via messages. **Threats today target people, not just platforms.** - Human elements are involved in 60% of breaches. Phishing and pretexting are among the costliest. (Verizon 2025 Data Breach Investigations Report) **Security hygiene and device controls take priority. Knox helps fortify both.** Biggest risks come from overlooked basics, such as not having the latest security patches and not setting the right policies. Knox helps you: - Know which device to update, when, and why. - Plan strategic updates and push without hurting workflow. - Keep work devices and data under control, across managed, BYOD, and even unmanaged devices.