ZIMPERIUM®
MOBILE THREAT DEFENSE

ZIMPERIUM zIPS™ with Samsung Knox

Advanced Mobile Threat Protection

ADVANCED MOBILE THREAT PROTECTION

Samsung Knox Platform for Enterprise (KPE) is a military-grade mobile solution for IT admins to manage and secure Samsung Android phones, tablets and Tizen watches for business. Zimperium zIPS is the most enterprise-ready and capable mobile threat defense (MTD) solution available. Utilizing the Samsung KPE for MTD API framework, *zIPS with Samsung Knox* option combines KPE's hardware-based capabilities with zIPS' industry-leading machine learning detection to provide users with the most advanced protection against even zero-day, unknown attacks.

SAMSUNG KPE: ADVANCED SECURITY FROM THE CHIP UP

Samsung KPE provides a robust set of features on top of the basic Android Enterprise platform to fill security and management gaps, resolve pain points identified by enterprises, and meet the strict requirements of highly regulated industries. KPE provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features commonplace in today's mobile device market. The Knox platform is the cornerstone of a strong mobile security strategy supporting a wide variety of Samsung devices.

KPE defends against security threats and protects enterprise data through layers of security built on top of a hardware-backed trusted environment. A trusted environment separates security-critical code from the rest of the operating system. This strategic separation ensures only trusted processes that are isolated and protected from attacks and exploits can perform sensitive operations, such as data encryption and decryption. A trusted environment is hardware-backed if hardware protections isolate the environment from the rest of the running system. This isolation ensures that vulnerabilities in the main operating system don't directly affect the security of the trusted environment.

Knox

ZIMPERIUM zIPS: INDUSTRY-LEADING MOBILE THREAT DEFENSE

Zimperium zIPS provides persistent, on-device protection for mobile devices and data in a manner analogous to endpoint protection platforms (EPP) / endpoint detection and response (EDR) solutions. Powered by Zimperium's patented machine-learning engine, z9™, zIPS is the only mobile threat defense (MTD) solution that detects attacks from all four mobile threat vectors – device, network, phishing and apps – on-device and in real-time.

Over the last five years, z9 has detected 100 percent of zero-day mobile exploits without requiring an update. It is also the only machine learning-based engine capable of detecting previously unknown mobile malware and "zero day" phishing attacks on-device in a way that balances security and user privacy.

zIPS WITH SAMSUNG KNOX: UNMATCHED DETECTION & REMEDIATION OF MOBILE THREATS

While Samsung KPE and Zimperium zIPS are the gold standards in their respective capabilities, combining KPE's hardware-based advantages with zIPS' on-device and enterprise-level ones provides unmatched mobile protection. The integrated solution, known as *zIPS with Samsung Knox*, leverages the Samsung KPE for MTD API to provide advanced detections, enhanced group-based remediations and unparalleled forensic details.

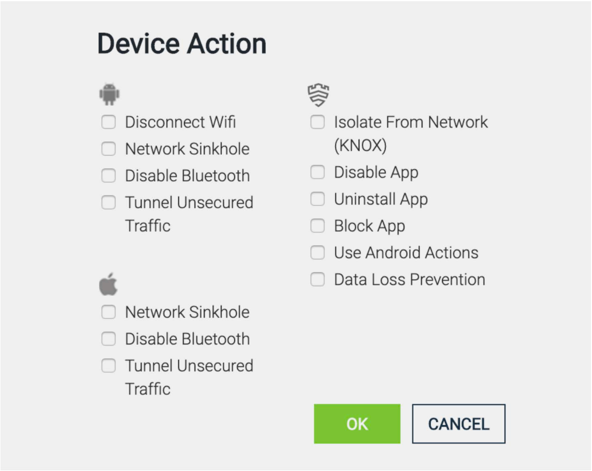
Advanced Detections

On Knox-capable devices, zIPS leverages the KPE for MTD API to facilitate lower level detections than what can be accomplished on other platforms. For example, by leveraging the unique information provided by Samsung KPE for MTD, *zIPS with Samsung Knox* can identify additional system anomalies, elevation of privilege attempts and suspicious network connections made by apps or processes.

Enhanced Group-based Remediations

zIPS with Samsung Knox combines zIPS' granular, group-based policy advantages with KPE's enhanced remediations. Based on privacy/security/compliance policies, admins select the KPE remediations they would like performed for each threat and group in the zIPS management console, zConsole.

zIPS with Samsung Knox's enhanced remediation options include isolating malicious apps or processes from the network, uninstalling or preventing the installation of malicious apps and customized data leakage prevention (DLP) actions to prevent unauthorized data exfiltration (e.g., restricting Bluetooth sharing, preventing SD card transfers, limiting access to the clipboard, disabling screen capture).



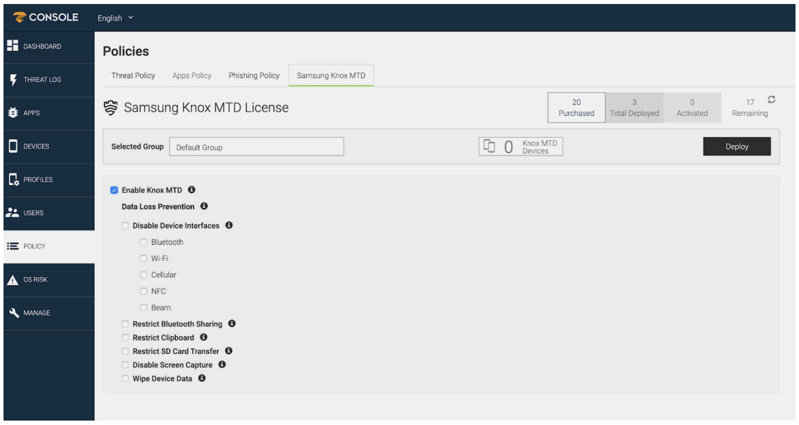
Device Action

- □ Disconnect Wifi
- □ Network Sinkhole
- □ Disable Bluetooth
- □ Tunnel Unsecured Traffic

- □ Network Sinkhole
- □ Disable Bluetooth
- □ Tunnel Unsecured Traffic

- □ Isolate From Network (KNOX)
- □ Disable App
- □ Uninstall App
- □ Block App
- □ Use Android Actions
- □ Data Loss Prevention

Figure 1: Local remediation actions of *zIPS with Samsung Knox*



Policies

Samsung Knox MTD License

20 Purchased | 3 Total Deployed | 0 Activated | 17 Remaining

Selected Group: Default Group

0 Knox MTD Devices

- ☑ Enable Knox MTD
  - Data Loss Prevention
  - □ Disable Device Interfaces
    - □ Bluetooth
    - □ Wi-Fi
    - □ Cellular
    - □ NFC
    - □ Beam
  - □ Restrict Bluetooth Sharing
  - □ Restrict Clipboard
  - □ Restrict SD Card Transfer
  - □ Disable Screen Capture
  - □ Wipe Device Data

Figure 2: Example of *zIPS with Samsung Knox* DLP options

Unparalleled Forensic Detail
For all threats detected, including the advanced ones described above, *zIPS with Samsung Knox* leverages the KPE for MTD API to provide the most granular and detailed threat forensics available today.

Future-proofed Protection
Given the tight integration between the two solutions, additional detections, remediations and forensics will continue to be added into *zIPS with Samsung Knox* on a regular basis. Samsung is both a partner of, and an investor in, Zimperium.

SEE zIPS WITH SAMSUNG KNOX IN ACTION

If you are interested in learning more about the ways *zIPS with Samsung Knox* can help you enhance your mobile security intelligence, please contact us.