ActZero

Data Sheet

MDR For Mobile

Protecting against attacks on iOS, Android, and Chrome devices

Use of mobile devices with businesses provides great benefits, providing your employees, partners and supply-chain with instant access to your business-critical applications, anytime and anywhere. However, according to respondents to Verizon's 2021 Mobile Security Index, "*Three-fifths (60%) of respondents said that they think that mobile devices are the company's biggest IT security threat. Of the rest, 85% said that mobile devices are at least as vulnerable as other IT systems*". For a workforce that's highly dependent on use of mobile, that presents a critical gap in security.

Mobile devices have also become widely targeted by adversaries, mainly due to the numerous ways to breach them including a lack of phishing protection, small mobile screens that leave out important details as they prioritize enhancement of the user experience.

Organizations need to better address mobile device security, bringing it in-line with endpoint, network, and cloud security, wherever possible.

Why many mobile solutions fail

In general, SMB and mid-size enterprise cybersecurity teams lack the budgets and tools needed to threats against their data and operations. While solutions like Unified Endpoint Management (UEM), mobile device management (MDM), standalone Mobile Threat Defense (MTD), and enterprise mobility management (EMM) technologies do help, they haven't been widely adopted. Where they have, there exists an overreliance and overconfidence in the tools. The Pegasus spyware incidents in 2020 demonstrated just how easily malware could access a phone via a simple SMS message or WhatsApp call — without any interaction by a user, even with an MDM in place.

To truly protect mobile data, organizations need to ensure that they build holistic security strategies that consider not only the mobile environment, but how threats move across and into endpoints, network and cloud.

ActZero MDR for Mobile

ActZero MDR for Mobile is an AI- and ML-powered MTD solution delivering autonomous threat protection, detection and response to more quickly detect threats like phishing/SMShing, app tampering, keylogging, account takeover attempts, man-in-the-middle (MiTM) attacks, and beyond.

Support for mobile phone and tablets running iOS, Android, or ChromeOS.

Around the Clock, Scalable, Threat Coverage

Through a combination of technology, threat hunting expertise and a deep investment into data science and security engineering, we provide advanced cybersecurity that scales

- ✓ **Fast deployment**: Deploys in minutes by the end user; no complicated configurations
- ✓ **24/7 SOC support**: Provides support when you need it most
- ✓ **On-device agent**: Eliminates reliance on cloud connectivity
- ✓ **Seamless mobile management**: Works with or without an MDM. Easily integrates with MDMs like Intune/Microsoft Endpoint Manager, VMWare WorkspaceOne, Ivanti, and more
- ✓ **Extend protection for endpoints, network, and cloud**: Easily upgrade with our core ActZero MDR solution, unifying support for mobile, endpoints, network, and cloud

Superior Detection & Remediation Outcomes

ActZero's use of AI and ML within our threat hunts sets us apart; helping identify more threats more quickly and with greater accuracy – improving signal-to-noise ratio, and providing less false positives

- ✓ **Phishing/SMSishing protection**: Stop malicious phishing attacks and reduce your attack surface by blocking connections to suspicious URLs, domains, and IPs
- ✓ **Activity-based threats:** Detects known malware and attack chains, app or system tampering, man-in-the-middle attacks, harmful apps, jailbreak/rooting
- ✓ **Device settings-based vulnerabilities and compliance:** Detects screen lock disabled, known OS vulnerabilities, USB debugging or developer options enabled, 3rd-party app store installs allowed, and unencrypted storage.
- ✓ **Enterprise application behavior monitoring**: Monitors app behavior to detect malicious or unwanted activity in business-critical mobile apps
- ✓ **On-device automatic response options including**: Disconnect wifi, Network sinkhole, Disable Bluetooth, Tunnel unsecured traffic

Actionable Intelligence

Maturity improvement advice that helps reduce your risk and improve your maturity over time

- ✓ **Increased Visibility:** Access to ActZero's mobile portal, delivering critical information including detected malicious, unwanted, or accidental access
- ✓ **Tailored Guidance:** Simply reporting stats isn't enough. ActZero's portal provides customers with thorough detection explanations and remediation instructions.