

CYBEREASON MOBILE

Secure the Latest Targeted Endpoint: Mobile Devices



KEY BENEFITS

- » Unparalleled visibility across all attack vectors
- » Detect, investigate, hunt, and remediate across traditional and mobile endpoints
- » Cybereason expert-managed detection and response (MDR)
- » Native interoperability with UEM technology partners

SYSTEM REQUIREMENTS

ANDROID VERSIONS

5 6 7 9 10

IOS VERSIONS

9 10 11 12 13

[CYBEREASON.COM/DEMO](https://cybereason.com/demo) →

The popularity of mobile devices for enterprise use has surpassed that of desktops and laptops around the world thanks to how they improve workplace productivity. Organizations are undergoing a digital transformation as mobile devices become the preferred platform for many business scenarios and organizations implement Bring-Your-Own-Device (BYOD) strategies. With millions of known malware threats for a growing variety of devices and operating systems alongside the proliferation of cloud and mobile-first applications, the risk to organizations is complex and expanding.

NOT "JUST" A MOBILE CHALLENGE

Cybercriminals are identifying mobile devices as a lucrative target as more people use smartphones, tablets, point-of-sale systems, and other BYOD devices for work. This is compounded by mobile networks rapidly evolving to 5G and the diminishing use of traditional endpoints like desktop computers. Employees are now enabled to work from any device, at any time, and therefore must access corporate data from cloud services outside of traditional security protections.

PERIMETERLESS SECURITY ERA FOR A MOBILE WORKFORCE

Instant access to business-critical applications regardless of the device, location, or time is a requirement for a modern business. The widespread adoption of corporate and personal devices that have different types of hardware, run different operating systems and versions, and use different applications poses an enormous challenge for cybersecurity professionals.

UEM - A FALSE - SENSE OF (CYBER)SECURITY

Unified Endpoint Management (UEM/MDM) solutions have been available for years, but they don't address today's cybersecurity concerns. They offer a starting point, but aren't built to defend against sophisticated attackers. UEM/MDM is meant for device management and policy enforcement, unable to keep up with enterprise needs and mobile cybersecurity risks.

ISOLATED MOBILE & TRADITIONAL ENDPOINT ALERTS

Breaking down the barriers that separate mobile cybersecurity from traditional endpoint cybersecurity is critical to create a seamless security ecosystem. The isolation between existing mobile security products and traditional endpoint security products leads to gaps in enterprise security for hackers to exploit.

CYBEREASON MOBILE

Cybereason is the world's leading endpoint protection platform built to help security teams better prevent, detect, investigate, hunt and respond to advanced attacks. The platform correlates both traditional and next-gen endpoints in a single console for a more efficient and complete incident response process completed by Cybereason's experienced analysts.

AUTONOMOUS PROTECTION

Cybereason Mobile provides on-device, behavior-based protection to uncover a variety of suspicious activity, from malicious mobile app use, abnormal north-south network connections, and operating system vulnerabilities. The app starts protecting mobile devices from day one with no training required. All of this is possible across any device, anywhere, anytime, with no rules, no signatures, and no manual analysis required.

ONE ATTACKER CAMPAIGN, ONE MALICIOUS OPERATION

Instead of using siloed, complex, and disparate alerts, identify a cross-device attack, leverage cross-platform, compromise context across all phases of the attack lifecycle with the Cybereason Mobile malicious operation - Malop™. The Malop is fully aligned with the MITRE ATT&CK for Mobile framework so security analysts can connect and communicate disparate malicious activities across a hybrid of endpoints. Protect against user-targeted or enterprise-focused attacks with fewer false positives and streamlined incident response.

CORRELATE, DETECT, REMEDIATE – RINSE-REPEAT

Cybereason Mobile grasps the full spectrum of mobile risk and the full array of mobile threats to empower security teams to prevent and remediate advanced threats completely missed by legacy endpoint controls. Cybereason Mobile delivers rich context across the operating system, memory, CPU and more, so abnormal behaviors are accurately identified to uncover all affected endpoints, users, and attacker's communications.

WHY CYBEREASON?

Defending traditional endpoints is simply not enough, and the new Cybereason Mobile offering strengthens the Cybereason Defense Platform by delivering complete protection across traditional and endpoints. With the Cybereason Mobile MDR offering, our team will streamline investigation and accelerate response. The Cybereason can handle the huge volume of security data found in today's complex IT environments without heavy installation, maintenance, or analyst oversight.

KEY STATS

"Gartner predicts that 80% of worker tasks will take place on a mobile device by 2020."

GARTNER, "PREPARE FOR UNIFIED ENDPOINT MANAGEMENT TO DISPLACE MDM AND CMT" JUNE 2018

48% are putting speed and profit before mobile security with almost half confirming they had sacrificed security to "get the job done." 46% of those who sacrificed security admitted to suffering a compromise.

VERIZON MOBILE SECURITY INDEX (MSI) REPORT 2019

DO-NO-HARM

Cybereason Mobile's non-intrusive and efficient approach to securing mobile devices protects without compromising device performance, the user-experience, or user privacy.

The lightweight application enforces a do-no-harm policy for mobile performance so network bandwidth and battery life are used efficiently on the device without introducing latency and while safeguarding a user's personally identifiable information (PII).