SentinelOne®

DATA SHEET

Singularity Mobile

AI-Powered Mobile Threat Defense

The work landscape is rapidly evolving, with a growing reliance on devices running iOS, Android, and ChromeOS across various form factors such as handhelds, tablets, pads, and Chromebooks. As organizations embraced remote work, mobile devices became the gateway to enterprise resources for many - housing corporate apps, authenticators and other credentials employees use to gain access to internal resources. In recent notable breaches, adversaries have targeted employees on mobile devices to harvest credentials or tokens to gain a foothold for a broader attack campaign. As mobile devices increasingly become integral to zero trust authentication and enterprise resource access, it is crucial to address their security needs.

Many organizations have turned to Mobile Device Management (MDM) solutions to tackle this challenge. However, MDM offers limited attack protection, focusing primarily on device management, configuration, and policy enforcement. MDM and MTD serve different yet complementary roles in ensuring mobile security. MDM focuses on managing devices and enforcing policies, while MTD is dedicated to detecting and mitigating threats targeting mobile devices.

Singularity Mobile, an AI-powered MTD solution, provides autonomous threat protection, detection, and response for iOS, Android, and ChromeOS devices. As an on-device behavioral AI product, it dynamically detects unprecedented malware, phishing, exploits, and man-in-the-middle (MiTM) attacks. Protecting mobile devices and users is critical, considering that the 2022 Verizon Mobile Security Index revealed that 45% of surveyed companies experienced a compromise involving a mobile device leading to data loss, downtime, or other negative outcomes.

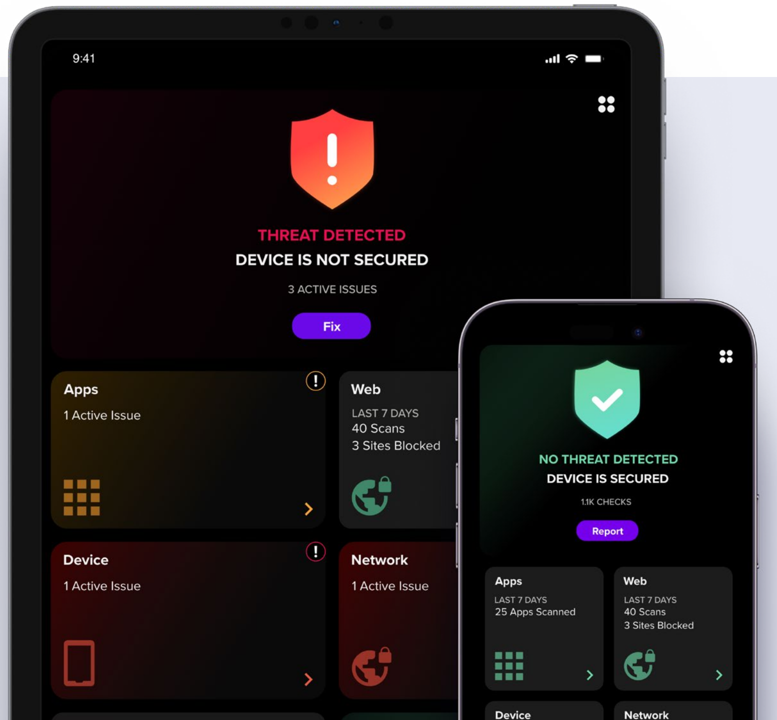
SINGULARITY MOBILE BENEFITS

+ **Autonomous AI Protection and Visibility:** Best-in-class protection, visibility, and response for mobiles and Chromebooks
+ **Mobile Phishing Protection:** Secure credentials from phishing and smishing attacks
+ **Supports all major platforms:** iOS, Android, and ChromeOS
+ **Efficient:** Zero-touch deployment
+ **Designed for Privacy:** Balances data privacy with security
+ **MDM Optional:** Works with leading MDMs like Intune and VMware WorkSpace One. Works without an MDM for BYOD devices

ChromeOS

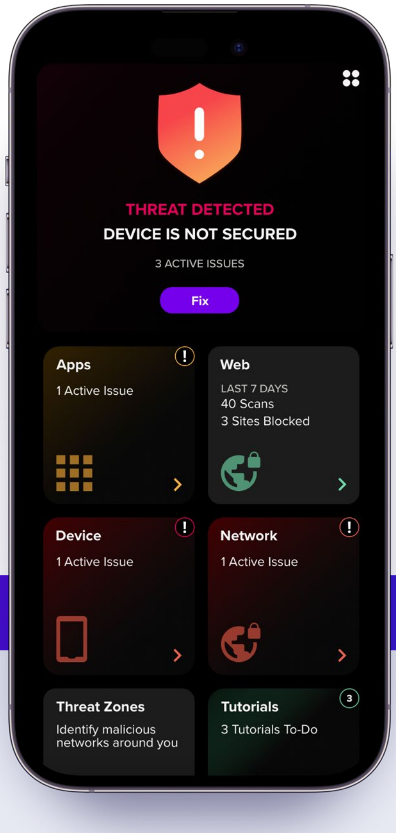
iOS

Android



Key Capabilities

- **Behavioral AI** protects iOS, Android, and ChromeOS devices from the most advanced mobile threats.
- **Protection and detection of mobile malware**, both known and zero-day attacks.
- **Protection and detection of phishing attacks**, both known and unknown.
- **On-device agent** eliminates reliance on cloud connectivity.
- **Minimal battery consumption** for optimal end-user experience.
- **Zero touch deployment** designed for busy teams.



THREAT DETECTED
DEVICE IS NOT SECURED
3 ACTIVE ISSUES
Fix

Apps
1 Active Issue

Web
LAST 7 DAYS
40 Scans
3 Sites Blocked

Device
1 Active Issue

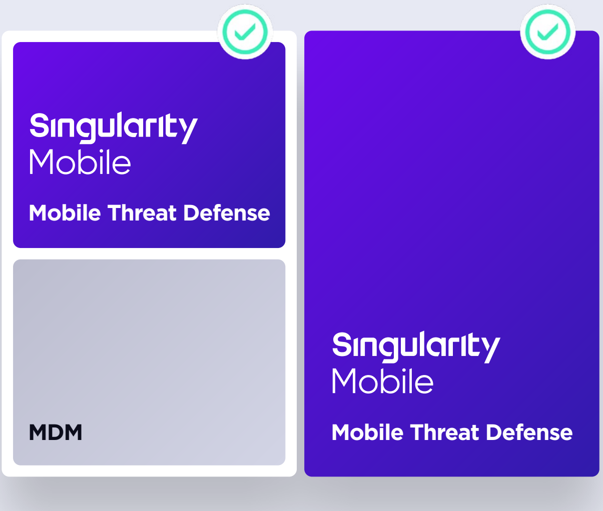
Network
1 Active Issue

Threat Zones
Identify malicious networks around you

Tutorials
3 Tutorials To-Do

Learn More at **S1.ai/mobile**

MTD That Builds on Your MDM



Singularity Mobile works with or without an MDM. Already own an MDM? Bring mobile security to the next level with easy integration to these MDM products:

- Intune / Microsoft Endpoint Manager
- VMWare WorkspaceOne
- MobileIron
- and more

Gartner peerinsights™

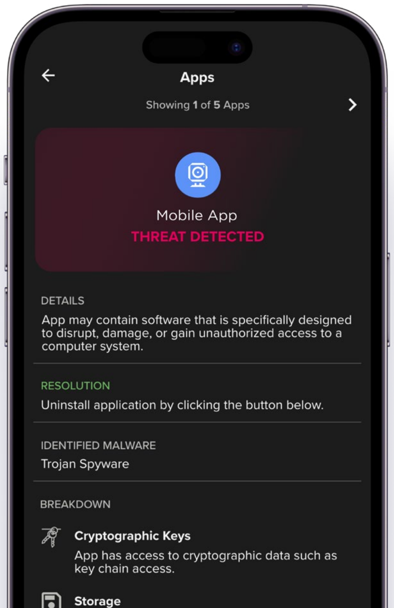
> SentinelOne provides the easiest to use but most comprehensive toolset for endpoint. ~February 11, 2021
>
> ★★★★★
>
> **HEAD OF SECURITY ARCH. & STRATEGY**
> **Telecommunications, 10B-30B USD**

Use Cases

Mobile Malware

Mobile malware is specifically designed to target and exploit vulnerabilities in mobile devices, such as smartphones and tablets. These threats can range from data-stealing apps to ransomware that locks users out of their devices until a ransom is paid.

Singularity Mobile Threat Defense (MTD) is a powerful solution designed to protect against both known and zero-day mobile malware attacks. By leveraging advanced techniques like machine learning, behavioral analysis, and threat intelligence, Singularity Mobile can proactively detect and block malicious activities before they can cause harm.



Apps
Showing 1 of 5 Apps

Mobile App
THREAT DETECTED

DETAILS
App may contain software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

RESOLUTION
Uninstall application by clicking the button below.

IDENTIFIED MALWARE
Trojan Spyware

BREAKDOWN

Cryptographic Keys
App has access to cryptographic data such as key chain access.

Storage

Mobile Phishing & Smishing

Mobile phishing targets mobile devices, such as smartphones and tablets, to deliver malicious content. Phishing has been around for some time, with adversaries using email messages and web pages as their primary method of attack. However, with the popularity of mobile devices and advent of AI-generated phishing tools and phishing-as-a-service (PaaS) providers, mobile phishing has become an increasingly common way for cybercriminals to access sensitive information. Types of mobile phishing include:

- **Clickable links within applications:** Attackers can embed malicious links within popular apps, social media platforms, or messaging services. Unsuspecting users who click on these links may be directed to fraudulent websites designed to steal their login credentials or personal information.
- **Text message and SMS phishing (smishing):** Smishing involves sending text messages containing deceptive content and links to malicious websites. These messages often appear to come from legitimate sources such as banks, government agencies, or well-known brands, enticing users to click on the link and enter their sensitive information.

Singularity Mobile protects mobile users from phishing attacks, both from known phishing URLs and behaviorally identifies novel attacks. Singularity Mobile alerts users to potentially dangerous links and SMS messages, preventing credential theft and more. Mobile credential theft remains a primary attack vector for mobile users, and Singularity Mobile fills the void.

BYOD Security

Bring Your Own Device (BYOD) programs allow employees to use their own personal devices for work purposes. While this can increase productivity and reduce costs, it also presents a number of security challenges that must be addressed. As personal devices are often used to access sensitive company information, it is essential that organizations have measures in place to prevent unauthorized access or accidental data leakage.

Singularity Mobile is a comprehensive MTD solution that offers optimal security for Bring-Your-Own-Device (BYOD) environments without compromising user privacy. Easily enroll BYOD devices without collecting browsing histories, passwords, local files, or personal data.

76%

of companies faced smishing attacks last year

2023 Proofpoint State of the Phish

66%

of organizations surveyed recently have active BYOD programs in place, with 11% looking to implement the policy over the next year

2022 Zimperium Global Mobile Threat Report

10%

of the applications installed on the average BYO mobile endpoint are enterprise-focused, from multifactor authentication (MFA), data access tools, and communications

2022 Zimperium Global Mobile Threat Report

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP

TEVORA PCI DSS Attestation HIPAA Attestation

AICPA SOC

STAR LEVEL ONE

VB 100 VIRUS virusbtn.com

SE Labs BEST Innovator WINNER 2021

SE Labs AAA

Trusted Cloud Provider CSA

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733