SentinelOne

SOLUTION BRIEF

Securing Chromebooks for K-12

A Singularity™ Mobile Brief

Singularity Mobile

Chromebook security was put to the test in 2020. While the OS proved well fortified, students' Google Workspace was susceptible to phishing, leading to explicit content attacks and more, as well as a long list of school shutdowns.

Malicious adware, phishing, and rogue access points all seek to take advantage of young, trusting, and unwitting students. Student safety is paramount, whether in the classroom, at a coffee shop, or on the home network. Attacks can range from the breach of personally identifiable information (PII), to harassment, and even physical threats. In addition to jeopardizing student mental health and well-being, attacks on Chromebooks distract students and teachers and can lead to school shutdowns. Threat actors can also move laterally from student to instructor's machines, and on to ransom servers and databases. The financial stakes are high: incident response and breach recovery can easily run into the millions of dollars.

Phishing has become the greatest threat to student privacy, so it is no coincidence that SentinelOne's new Singularity Mobile offers the industry's best phishing prevention. Add to that its ability to detect everything from network-based attacks launched from coffee shops to nation state attacks like Pegasus, and there's no better agent to sit between a student and an attacker, ensuring students stay safe and focused on learning.

CHROME OS THREATS

Phishing

Phishing attacks via email or social media snipe student credentials.

Network Attacks

Prying eyes from rogue access points and MiTM attacks in public spaces like coffee shops, where students like to hangout.

Malicious Apps

Such apps misappropriate contacts, to send email blasts, move laterally, and drop malware.

$4.62 m

Average cost of a Ransomware Attack.

2021 Cost of a Data Breach Report

Ponemon Institute & IBM Security

Singularity Mobile

Phishing

Stopping the #1 Cause of Compromised Student Devices

Phishing targets the victim's credentials, which are the fastest type of data to be compromised. In fact, credential theft occurred in over half (51%) of educational breaches in 2020. The critical first line of defense for Singularity Mobile is that all click-through traffic is routed through the Mobile Sentinel Agent, where the Static AI Engine checks whether the destination URL is known to be bad. As an additional measure, the site is examined for risky indicators. In this way, students are doubly protected from adversaries trying to gain access or drop malware after establishing a foothold.

48%

of all EDU breaches involve social engineering.

2021 Data Breach Investigations Report
Verizon

Network Attacks

It's no secret: students like to gather for study groups. Threat actors, camped out at a local coffee shop, can execute a MiTM attack on an unsuspecting study group to intercept and redirect traffic to a URL to deliver a malware payload, or to simply observe and abscond with login credentials. While credential theft threatens data security, the privacy invasion of traffic intercepts can affect well-being or physical safety, such as with explicit content attacks or stalking. With Singularity Mobile, all traffic is routed through the agent, so MiTM and Rogue Access Points are detected in real-time.

KEY CAPABILITIES

Protection against and detection of phishing attacks
Both known and unknown.

On-device agent
Delivers real-time protection without reliance on a cloud connection.

Protection against and detection of rogue access points and MiTM
Protect student learning in public places like coffee shops.

Behavioral AI
Protects Chromebooks from the most sophisticated mobile threats that easily evade signature detection.

SINGULARITY MOBILE

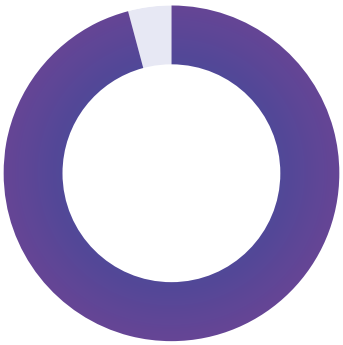
Machine speed protection vs. behavioral malware and mobile phishing

Learn More About Securing Chromebooks at **s1.ai/chromeos**

Singularity Mobile

Malicious Apps

A determined and savvy student can sideload apps on their Chromebook. Such apps are often the source of malware. Some even find their way into the Google Play Store. Malicious apps can siphon contacts' details, to launch phishing emails and text messages, take control of cameras and mics, and siphon GPS coordinates. The best defense is a combination of static and behavioral AI, silently functioning behind the scenes on the student's Chromebook. In this way, known and unknown malicious apps are detected in real-time, at the point of need.



96%

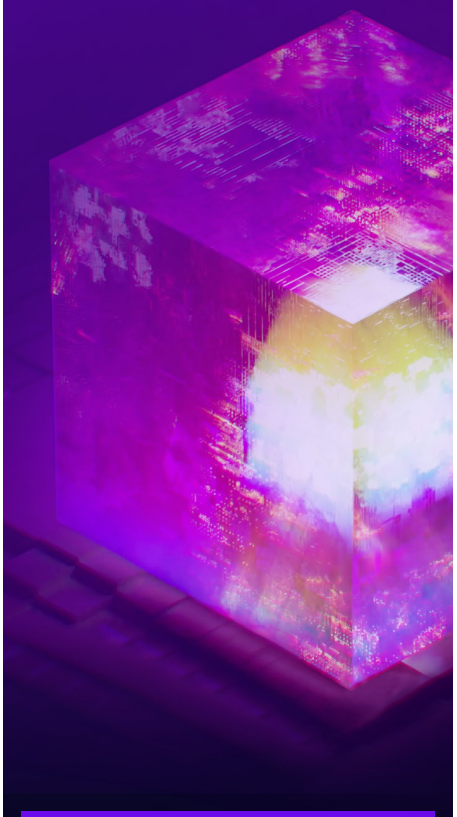
of attacks on educational institutions are financially motivated.

2021 Data Breach Investigations Report
Verizon

Best-in-Class Chromebook Protection

Singularity™ Mobile brings behavioral AI-driven protection, detection, and response to iOS, Android, and ChromeOS devices. Part of the Singularity™ Platform, SentinelOne delivers mobile threat defense that is local, adaptive, and real-time, to thwart mobile malware and phishing attacks at the device, with or without a cloud connection. And because it's mobile, data privacy is built-in at every level.

Singularity Platform



READY FOR A DEMO?

Visit the SentinelOne website for more details.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights 4.9 ★★★★★

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · ISO 27001 CERTIFIED by schellman · TEVORA PCI DSS Attestation HIPAA Attestation

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733