Bitdefender

SOLUTION BRIEF May 2023

GravityZone Security for Mobile

Securing ChromeOS, from education to enterprise

Connected devices such as Chromebooks have become essential in educational institutions and enterprises worldwide. However, it's important to note that data risks are still a concern. Like other platforms that have achieved widespread adoption, Chromebooks are susceptible to cyberattacks, which can result in security and compliance concerns for organizations of any size.

Key concerns when it comes to Chromebook devices revolve around mobile privacy and security risks and threats, including:

→ Phishing attacks resulting in stealing the identity of the user

→ Network attacks where personal information is accessed

→ Malicious malware in apps taking control of microphones and cameras

→ Compromised extensions stealing personal and private data

Phishing

Email remains the primary attack medium for phishing attempts, accounting for 90% of attacks, and 60% of these emails are accessed on mobile devices. But mobile phishing may just be the beginning. In 2021, phishing emails were the leading point of entry for ransomware, constituting around 54% of those attacks. (Verizon, DBIR 2022). For example, like many other industries, Educational Services is facing a significant rise in ransomware attacks, which account for over 30% of all breaches. Additionally, the industry must take measures to safeguard against stolen credentials and phishing attacks that could potentially expose the personal information of both students and employees.

How does GravityZone Security for Mobile help? The initial line of defense involves routing all click-through traffic through a local agent, which then checks the destination URL for any known malicious activity. To provide further protection, the site is also analyzed for any risky indicators. This dual-layer approach helps safeguard against adversaries attempting to gain unauthorized access or install malware following a successful breach.

Network Attacks

Bad actors may attempt a Man-in-the-Middle (MiTM) attack to intercept and redirect traffic to a URL that delivers a malware payload or to capture login credentials. The consequences of credential theft are a threat to data security, while privacy breaches through traffic intercepts could result in harm to an individual's well-being or physical safety, such as in the case of explicit content attacks or stalking. However, with GravityZone Security fro Mobile, all traffic is routed through the agent, allowing for real-time detection of MiTM and Rogue Access Points.

AT-A-GLANCE

GravityZone Security for Mobile provides critical security to any enterprise and educational institution using ChromeOS devices, including the following capabilities:

→ Identify and prevent users from accessing phishing sites

→ Filter and limit access to harmful web content

→ Detect malicious WiFi networks and alert users to disconnect from the suspicious network

→ Assess all Android apps for undesired violations of privacy or insecure development practice

KEY BENEFITS

→ Antiphishing. Protection against and detection of phishing attacks, both known and unknown.

→ On-device agent. Real-time protection without reliance on a cloud connection.

→ Network protection. Protection against and detection of rogue access points and Man-in-the-Middle attacks to secure devices used in public places or on the go.

→ Powered by Machine Learning. Protects Chromebooks from the most sophisticated mobile threats that easily evade signature detection.

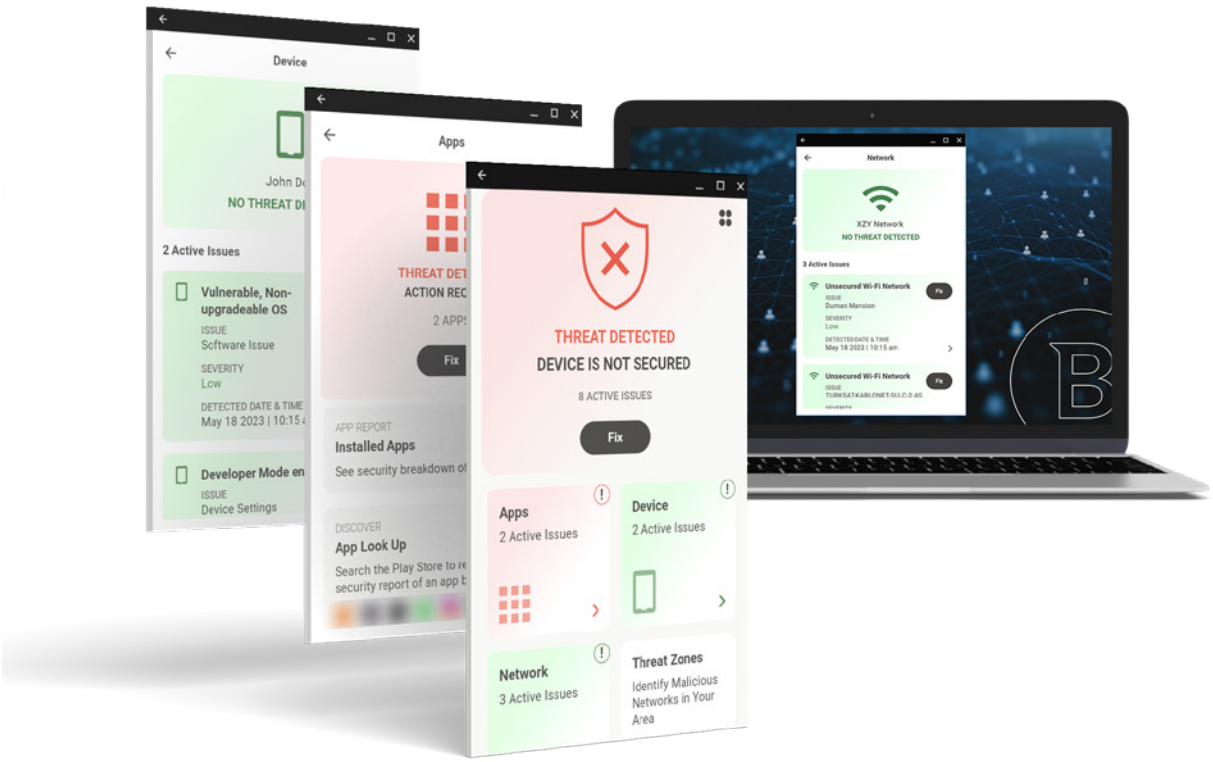
→ One console for all security related aspects. Integrated with the GravityZone console for end-to-end visibility and endpoint security, across all platforms.

Malicious Applications

Apps can be installed on Chromebook devices through sideloading. Unfortunately, these apps are frequently the source of malware, and some even make their way onto the Google Play Store. Malicious apps can extract contact details, launch phishing emails and text messages, take over cameras and microphones, and collect GPS coordinates. The optimal defense comes from the machine leaarning technologies which runs silently in the background of the Chromebook device. This way, both known and unknown malicious apps can be detected in real-time as needed.

Malicious Extensions

Browser extensions have historically been a security risk for all platforms, but ChromeOS is especially vulnerable because of how heavily it depends on the Chrome browser. The accidental installation of harmful extensions by users is one of the biggest security concerns that ChromeOS faces. These malicious extensions can utilize browser exploits to spread malware, steal cookies or login information, record keystrokes, mine cryptocurrency on the victim's computer, inject malicious javascript code into websites, and more after being installed. A Chrome extension that may detect threats in other extensions and remove harmful extensions is included with GravityZone Security for Mobile. It can identify and stop phishing attempts by using a variety of approaches, including website URL analysis, tracking suspicious behavior, and comparison to existing phishing databases, enhancing user security by alerting and blocking potential phishing threats encountered during web browsing.



GravityZone Security for Mobile

As Chromebooks continue to gain popularity across various industries, they require the same level of advanced technology and rigorous security measures as other endpoints. GravityZone Security for Mobile offers advanced mobile threat defense capabilities to ChromeOS and provides essential protection to organizations and educational institutions that rely on this always-connected endpoint.

Security for Mobile offers crucial security capabilities through on-device detection and determination, including:

→ Preventing users from accessing phishing sites

→ Filtering and restricting access to harmful web content

→ Identifying and alerting users to disconnect from malicious WiFi networks

→ Assessing all Android apps for privacy violations or insecure development practices

Overall, Security for Mobile provides vital security to any enterprise or educational institution that uses Chromebooks.

GravityZone Cloud MSP Security for Mobile

GravityZone Cloud MSP Security for Mobile provides Managed Service Providers (MSPs) with the tools they need to secure and protect mobile devices from potential threats. This comprehensive security solution features a single, easy-to-use multi-tenant console and a flexible, monthly usage-based licensing model. With usage-based billing, MSPs have complete control over their revenue streams, as customers are only charged for the services they actually use, eliminating the risk of overpayment for unused Chromebooks. This capability, coupled with GravityZone's advanced protection features, makes it the ideal solution for protecting mobile devices.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-SOLG-Sec4Chrome-SP-creat4977-en_EN