

Security for Mobile

Mobile Threat Defense for iOS, Android, and Chromebook Devices

Smartphones and tablets have transformed the way we maintain remote access for work. Along with convenience, new risks have been introduced into the workplace as employees access communication channels like email, SMS messaging, apps and rich messaging apps. Many have access to much of the same data through their mobile devices as they would in the office: sensitive customer information and critical corporate systems. A compromised mobile device can pose a significant risk to an organization's customer data, intellectual property, and core systems.

Security for Mobile protects mobile devices so that employees can access corporate data in a safe and secure way. It detects both known and unknown threats, including zero-day, phishing and network attacks. The solutions protects devices against primary attack vectors, even when the device is not connected to a network.

Mobile devices need protection

- Emails are the number one attack vector for phishing attacks (90%) and 60% of emails are opened on mobile devices
- 18% of clicked phishing emails come from a mobile device
- 79% of people admitted using a work device for personal tasks, such as checking personal email, shopping or streaming

Features

- Application Protection – Leverages Artificial Intelligence technologies on and off the device to detect malicious apps (Android and iOS).
- Application Vetting – Out of compliance application detection.
- Web Protection – Anti-phishing and web access control.
- Network Protection – Detects network borne threats, recon attempts, weak security connections, and man-in-the-middle attacks.
- Device Protection – Detects OS vulnerabilities, devices that cannot be updated, missing encryption, jailbreak or root, system tampering, etc.

At-a-Glance

GravityZone Security for Mobile provides organizations with insight into their mobile device footprint and associated risks to prevent and protect against attacks, detect and respond to compromised devices, and integrate mobile devices into overall security structures.

Key Benefits

- Visibility into, and protection against, mobile threats.
- Advanced cyber security protection across apps, web traffic and devices.
- Broad detection with granular control for compliance policies.
- Device and platform agnostic security for iOS, Android, and ChromeOS.
- End-to-end insight and control across all platforms.
- Reduces the risk of data theft, credential loss, and non-compliance.