Your organization's best defense against mobile threats

Digital transformation, cloud adoption and the rise of hybrid work means that sensitive company data is increasingly accessed and stored on mobile devices. This presents information security professionals with a new set of threats to defend against. Communications can be intercepted using a variety of Wifi based attacks. And sophisticated iOS and Android malware, such as Pegasus, Predator and Hermit can be used to gain root privileges on devices.

Corrata addresses these threats with unique mobile endpoint security which is more powerful, more respectful of employee privacy and easier to deploy and manage than competing solutions. Our pioneering on-device network traffic analysis is transforming the way organizations secure their employees' phones and tablets.

Detect and disable malware

Corrata's software works unobtrusively in the background, watching for signs of malware infection and automatically quarantining any compromised devices. Our patented traffic inspection technology detects indicators of compromise buried deep in a device's IP communications.

Block smishing attacks

85% of phishing attacks on mobile take place outside email. Corrata's zero-day phishing protection instantly identifies and blocks attacks over SMS, email, WhatsApp and the whole range of mobile messaging and collaboration applications used by your colleagues.

Implement conditional access policies

Conditional access policies prevent poorly configured phones and tablets from accessing sensitive data. Corrata continually assesses the configuration of devices and alerts employees to update operating system software, remove harmful applications or change settings.

Protect Wi-Fi communications

Public and residential Wi-Fi hotspots are easily hacked. By ensuring that encryption levels are up-to-date and that websites have valid certifications Corrata prevents attackers from snooping on Wi-Fi traffic or impersonating legitimate websites.

Corrata

Corrata inspects over a thousand connection requests per device per day searching for malicious links and suspicious traffic.

Respect for employee privacy

Corrata's innovative approach to mobile threat defense means that employees no longer have to accept intrusive monitoring in order to ensure that their devices are protected. Unlike competing solutions Corrata does not access location information or read the content of messages. Nor does Corrata required employees to grant access to intimidating or obscure permissions.

Uncompromising user experience

Once installed on an employee's phone or tablet, Corrata works silently in the background defending against security threats. Employees receive alerts when sites are blocked and clear instructions to remedy poor security configurations should they arise. When security events arise, Corrata provides IT staff have access to all relevant information.

"Corrata's solution not only provides unprecedented threat prevention but also addresses product shortcomings in its main competitors"

Frost and Sullivan, Mobile Threat Defense Market Report, 2020

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

FIRSTNET
Built with AT&T
VERIFIED

Member of
Microsoft Intelligent
Security Association
Microsoft

About Corrata

Corrata was founded in 2016 with the aim of finding a better way to protect iOS and Android devices from cyber attacks. Today our technology is transforming the way hundreds of organizations protect their employees' smartphones and tablets. Corrata software detects and disables malware, blocks phishing attacks and ensures compromised devices cannot access sensitive data. And all while fully respecting employees' privacy. Corrata is a proud member of the Microsoft Intelligent Security Association and Cyber Ireland and is verified for use with FirstNet, the US Government network for first responders powered by AT&T.

Corrata