Cynet 360 Mobile

Mobile devices are essential for business today – 91% of organizations say they are 'critical' to their operations.[1] While mobile devices boost worker productivity, they significantly expand an organization's attack surface. Because devices provide access to the same content and services as traditional endpoints and also serve as an authentication tool, they are highly attractive to cyber criminals. But the majority of these devices are not secured.

Several factors make mobile devices a unique attack vector, including:

- The majority of work-related email is now opened on mobile devices, and 83% of organizations suffered a successful email phishing attack in 2021[1]
- 30% of zero-day exploits discovered in 2021 targeted mobile devices[2]
- Mobile applications represent another area of risk, as employees can easily access apps that put enterprise data at risk of exposure while the IT team often has limited visibility or control over what is installed on user devices – apps that grant access to sensitive corporate data and resources

Key Benefits

- Protect mobile devices wherever they're located, online or offline
- Prevent mobile threats from infecting corporate networks
- Provide real-time protection against zero-day attacks and other mobile-specific threats
- Stop mobile apps from becoming a threat to data and corporate resources
- Seamless integration with leading MDM / EMM tools
- Hands-off deployment eliminates need for complicated activation steps by the end-user
- Privacy-first approach increases user adoption
- Light weight avoids battery drain

Another risk factor to consider is the increasingly stringent compliance requirements impacting organizations. These mandates extend to all corporate processing and storage of data, including mobile endpoints. However, most mobile devices connecting to corporate networks are unsecured and therefore represent a compliance blind spot.

Some organizations use mobile device management or enterprise mobility management (MDM / EMM) tools to protect sensitive data. These products can enforce corporate compliance policies and also create logical containers on devices to segregate personal and business data but are not designed to detect and prevent mobile threats.

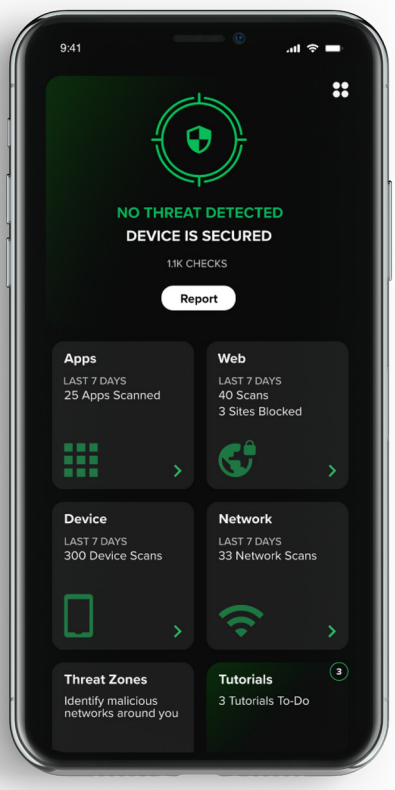
Organizations and their users need a solution that goes beyond device management, providing detection and prevention of device-based threats to personal data and corporate resources.

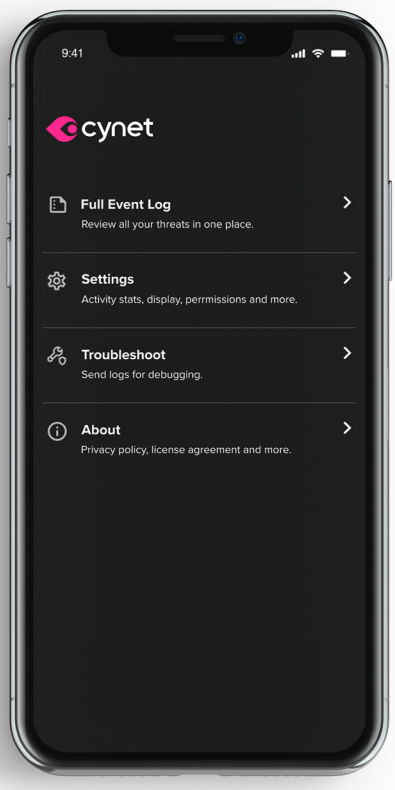
[1]Verizon 2022 Mobile Security Index 2022 report

[2]Zimperium 2022 Global Mobile Threat Report

Device security for today's threats

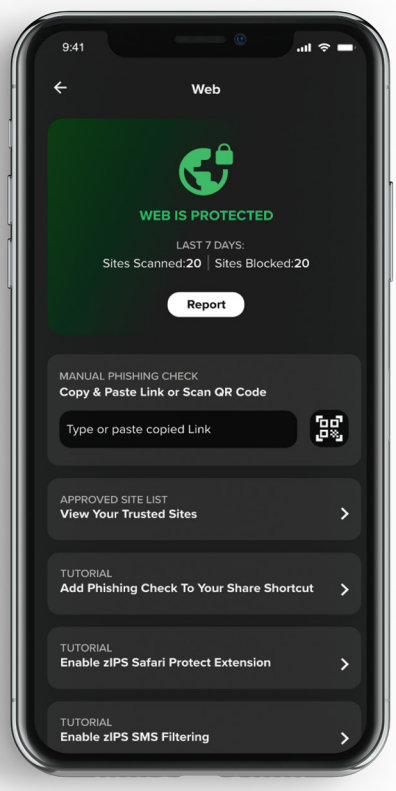
Cynet Mobile prevents security and privacy threats to Chrome OS, Android and iOS devices, and detects applications that put data at risk of exposure and attempt to infiltrate corporate networks. Whether it's zero-days, phishing, network-based or other types of attacks, Cynet Mobile provides persistent, on-device protection of company- and user-owned devices.

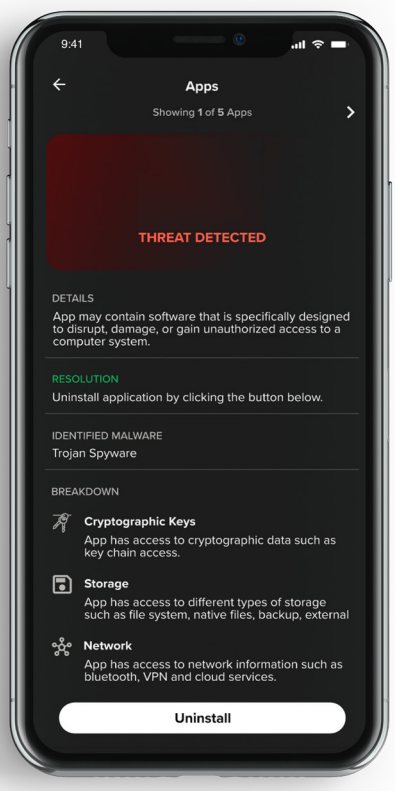




Key features and capabilities of Cynet Mobile include:

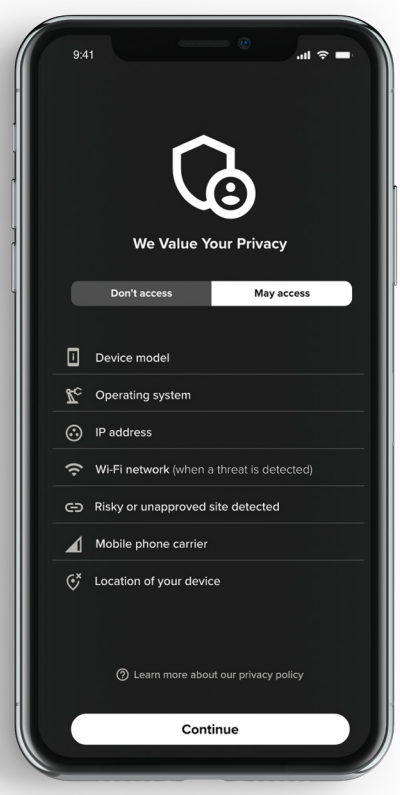
- Extensive anti-phishing capabilities, supported by continuous research and traffic analysis
- Machine learning-based threat detection works whether or not user devices are connected
- Continuous scanning and analysis to prevent connections to malicious networks
- Integration with leading MDM / EMM tools provides comprehensive management and protection
- Integration with SIEM, UEM and SOAR platforms extends the SOC team's visibility and forensic capabilities
- Pre-scans URLs and QR codes for threats, whether sent via SMS or email, or accessed on social sites
- Inspection of app behavior, code, settings and policies that prevents damage before it can occur





Privacy first

Cynet Mobile's prioritizes privacy, giving your users the assurance that the corporate IT team cannot access their personal information, texts, emails, browsing history or documents. The app also does not provide access to the phone's microphone or camera.



Intuitive management console

Cynet Mobile's prioritizes privacy, giving your users the assurance that the corporate IT team cannot access their personal information, texts, emails, browsing history or documents. The app also does not provide access to the phone's microphone or camera.

Cynet Mobile console gives you visibility into all mobile endpoints. The console enables you to:

- See forensics data about threats to specific devices
- Set your threat response, privacy and phishing policies
- Track the timeline of threat trends and changes to your global risk profile
- Check device metrics, including which OSes are in use and which ones are displaying risky behavior or settings