



DATA SHEET

Trellix® Mobile Threat Defense (MTD)

Benefits

- App privacy and security insights help safeguard sensitive data.
- Protect critical business data
- Integrate mobile into your Zero-Trust program
- Mobile forensics accelerate investigation and response.
- Real-time on-device protection reduces mobile risk and stops advanced threats.
- Zero-touch activation enables fast and frictionless deployment
- Integrations streamline response within existing SIEM, IAM, UEM, and XDR workflows.

Trellix Mobile Threat Defense (MTD) is a privacy-first application that provides comprehensive mobile security for enterprises. Trellix MTD is designed to protect an employee's corporate-owned or BYO device from advanced persistent threats without sacrificing privacy or personal data. Leveraging advanced machine learning, Trellix MTD detects threats across the kill chain: device, network, phishing, and app attacks.

Enhanced by artificial intelligence – stay ahead of threats

Trellix MTD's Dynamic Detection Engine scales with the needs of the modern workforce. A key component of the Trellix Mobile Threat Defense, it increases visibility into vulnerabilities and threats. Manage and configure granular security policies – in one place – across teams, groups, and apps. Trellix MTD provides advanced mobile security that enables professionals to work – anytime, anywhere.

Privacy-first approach to mobile device security

With a privacy-first approach, Trellix's MTD enables enterprises to support and secure bring-your-own-device policies alongside corporate-owned endpoints without sacrificing the end user's data privacy.

Integrate seamlessly and respond with accuracy

Forensic data on the device, network connections, and malicious applications give security operations teams visibility into the vulnerabilities and growing mobile threat vectors, enabling them to confidently minimize their total attack surface. Trellix MTD's unmatched forensics prevent a single compromised mobile device from turning into an outbreak, rendering devices inoperable.

Features

- Advanced app analysis to identify security and privacy risks.
- Cross-OS coverage for Android, iOS, and ChromeOS devices.
- Flexible deployment options: cloud, on-premise, or air-gapped.
- Dynamic content filtering to block malicious or risky web activity.
- Mobile vulnerability detection for outdated or non-compliant OS and apps.
- Integrations with SIEM, IAM, UEM, and XDR platforms.
- Full-featured API for workflow automation.

Mobile device requirements

Forensic data on the device, network connections, and malicious applications give security operations teams visibility into the vulnerabilities and growing mobile threat vectors, enabling them to confidently minimize their total attack surface. Trellix MTD's unmatched forensics prevent a single compromised mobile device from turning into an outbreak, rendering devices inoperable.



Apple iOS

Version support
iOS 12 or higher



Android

Version support
Android 6 or higher



Chrome OS

Systems supporting
Android Apps

Learn more about Trellix Mobile Threat Defense at [Trellix.com](https://trellix.com).

Get started with Trellix by [requesting a demo](#).