

Mobile Threat Defense: The Solution for Mobile Security

Key benefits of MTD

Ensure constant protection

MTD uses machine learning algorithms optimized to run continuously on-device, whether on the cloud or on-premises, enabling it to detect and remediate known and zero-day threats, even when the device is offline.

Improve threat visibility

Gain immediate and ongoing visibility into malicious threats across all mobile devices and detailed analyses of risky apps.

Achieve 100% user adoption

No user interaction is required and no new application deployment is needed to activate MTD on mobile devices enrolled in Ivanti UEM.

Protect against mobile threats

In today's Everywhere Work, mobile devices are essential enterprise resources. Employees use them to access virtually everything. And because most users have subpar, if any, mobile security measures in place, hackers are taking advantage.

Ivanti Mobile Threat Defense (MTD) allows you to protect both corporate and employee-owned Android and iOS devices from advanced threats through the cloud or on-premises deployments. It enables enterprises to monitor, manage and secure devices against attacks that occur at the device, network and application levels as well as prevent mobile phishing attacks.

Unlike other solutions, Ivanti MTD pushes a local compliance action that detects and remediates both known and zero-day mobile threats on-device, even if the device is not connected to a Wi-Fi or cellular network. Additionally, no user interaction is required to activate MTD on mobile devices enrolled in Ivanti UEM. This helps organizations achieve 100% user adoption to ensure they stay protected from mobile threats.



MTD capabilities

On-device detection and remediation

On-device machine learning-based protection against device-, network-, application-level and phishing attacks keeps mobile devices secure even when they are without network connectivity.

In the cloud or on-premises deployment

Designed to safeguard all your devices, regardless of their location. Our on-premises deployment option ensures that every device within your infrastructure, whether connected to the cloud or operating independently, is fully protected. This is particularly crucial for environments that require stringent data control and privacy, such as government, healthcare and financial sectors.

Multi-vector anti-phishing

MTD's on-device machine learning and phishing URL lookup can be expanded to include cloud-based lookup for improved effectiveness. The solution's anti-phishing capability can detect and remediate phishing attacks across all mobile threat vectors, including email, text and SMS messages, instant messages, social media and more.

Proactive remediation approach

Policy-based compliance actions provide alerts of risky behaviors, proactively shut down attacks on-device, isolate compromised devices from your network and remove malicious applications and their content to limit time of exposure for possible exploitation and stop zero-day attacks.

In-depth reporting

Dashboards and reports help you gain visibility and awareness into device, OS, network and application risks and arm you with actionable information so you can respond quickly and effectively to threat vectors.

UEM integration

No user interaction is required and no new application deployment is needed to activate MTD on mobile devices enrolled in Ivanti UEM, helping to drive 100% user adoption. Further, compliance policies can be created and enforced to prevent users from disabling MTD or removing it from their device.



Real-world examples

MTD protects against device-, network-, application-level and phishing attacks.

Device exploitation

After MMS messages were sent to targeted users, a zero-click chained exploit was triggered without any user interaction, launching a remote code execution that elevated the bad actor's privileges and allowed for lateral movement onto the network.

Network attacks

At a coffee shop near their office, a Wi-Fi man-in-the-middle (MITM) attack against a company redirected users to a spear phishing page where corporate data was stolen.

Malicious apps

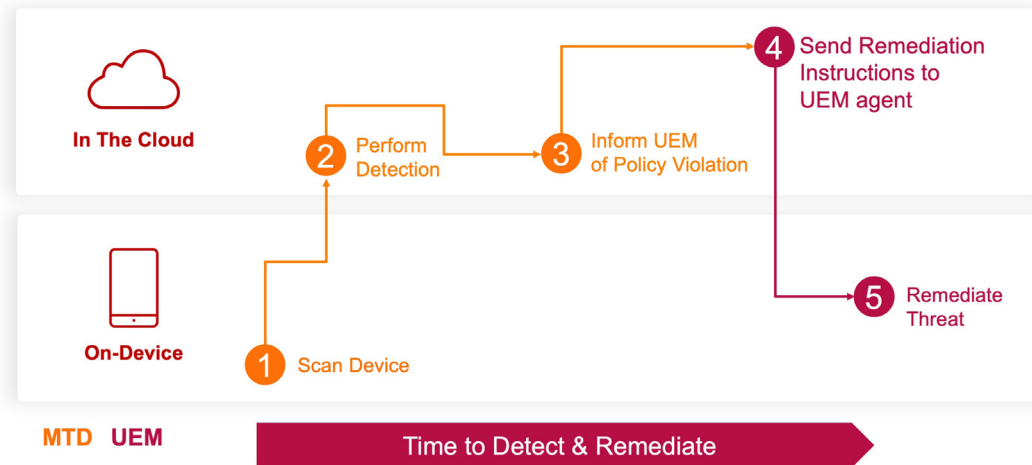
Unsuspecting users installed an app from a third-party app store. The app abused permissions, executed a device exploit, leaked data and was used as a weapon to penetrate internal networks via lateral movement in search for more sensitive data.

Phishing attacks

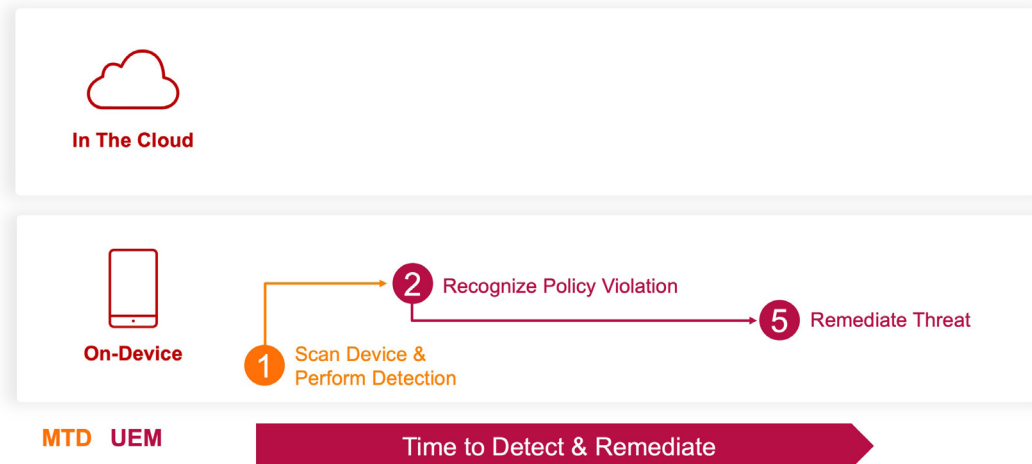
Leveraging social engineering, a bad actor tricked an unsuspecting user into clicking on a link and providing their corporate login credentials. The attacker was then able to log in as the user and access corporate resources.

Detection and remediation

Other threat defense solutions




Ivanti MTD solution



About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the left side of the text block, transitioning from red at the top to orange at the bottom.

For more information,
or to contact Ivanti,
please visit [ivanti.com](https://www.ivanti.com).