Mobile Threat Defense: Die Mobile Security-Lösung

Die wichtigsten Vorteile von MTD

Gewährleisten Sie konstanten Schutz

MTD verwendet Algorithmen für maschinelles Lernen, die so optimiert sind, dass sie kontinuierlich auf dem Gerät ausgeführt werden - so werden bekannte und Zero-Day-Bedrohungen erkannt und beseitigt, selbst wenn das Gerät offline ist.

Verbessern Sie die Sichtbarkeit von Bedrohungen

Sie erhalten sofortigen und kontinuierlichen Einblick in bösartige Bedrohungen auf allen mobilen Geräten und detaillierte Analysen riskanter Apps.

Erreichen Sie eine 100%ige Benutzerakzeptanz

Für die Aktivierung von MTD auf mobilen Geräten, die bei Ivanti UEM angemeldet sind, sind weder Benutzerinteraktion noch eine neue Anwendungsbereitstellung erforderlich.

Schutz vor mobilen Bedrohungen.

Im „Everywhere Workplace“ von heute sind mobile Geräte wichtige Ressourcen. Mitarbeiter nutzen sie, um auf praktisch alles zuzugreifen. Und da die meisten Benutzer, wenn überhaupt, nur unzureichende Sicherheitsvorkehrungen für mobile Geräte getroffen haben, nutzen Hacker dies aus.

Mit Ivanti Mobile Threat Defense (MTD) können Sie sowohl unternehmens- als auch mitarbeitereigene Android- und iOS-Geräte vor raffinierten Bedrohungen schützen. MTD ermöglicht Organisationen, Geräte zu überwachen, zu verwalten und vor Angriffen zu schützen, die auf Geräte-, Netzwerk- und Anwendungsebene stattfinden, sowie mobile Phishing-Angriffe zu verhindern.

Im Gegensatz zu anderen Lösungen führt Ivanti MTD eine lokale Compliance-Aktion durch, die sowohl bekannte als auch Zero-Day-Bedrohungen auf dem Gerät erkennt und behebt, selbst wenn das Gerät nicht mit einem Wi-Fi- oder Mobilfunknetz verbunden ist. Außerdem ist keine Benutzerinteraktion erforderlich, um MTD auf mobilen Geräten zu aktivieren, die in Ivanti UEM registriert sind. Dies hilft Organisationen, eine 100%ige Benutzerakzeptanz zu erreichen, um sicherzustellen, dass sie vor mobilen Bedrohungen geschützt bleiben.

MTD-Funktionen

Erkennung und Behebung auf dem Gerät

Der auf maschinellem Lernen basierende Schutz vor Angriffen auf Geräte-, Netzwerk- und Anwendungsebene sowie vor Phishing-Angriffen sorgt dafür, dass mobile Geräte auch dann sicher sind, wenn sie nicht mit dem Netzwerk verbunden sind.

Anti-Phishing mit mehreren Vektoren

Das maschinelle Lernen auf dem Gerät und die Phishing-URL-Suche können zur Verbesserung der Effektivität um eine cloudbasierte Suche erweitert werden. Die Anti-Phishing-Funktion der Lösung kann Phishing-Angriffe über alle mobilen Bedrohungsvektoren hinweg erkennen und beheben, einschließlich E-Mail, Text- und SMS-Nachrichten, Sofortnachrichten, soziale Medien und mehr.

Proaktiver Ansatz zur Behebung

Richtlinienbasierte Compliance-Aktionen warnen vor riskantem Verhalten, schalten Angriffe auf dem Gerät proaktiv ab, isolieren kompromittierte Geräte von Ihrem Netzwerk und entfernen bösartige Anwendungen und deren Inhalte, um die Zeitspanne für mögliche Angriffe zu begrenzen und Zero-Day-Angriffe zu stoppen.

Ausführliche Berichte

Dashboards und Berichte helfen Ihnen dabei, einen Überblick über die Risiken von Geräten, Betriebssystemen, Netzwerken und Anwendungen zu gewinnen und geben Ihnen verwertbare Informationen an die Hand, damit Sie schnell und effektiv auf Bedrohungsvektoren reagieren können.

UEM-Integration

Für die Aktivierung von MTD auf mobilen Geräten, die in Ivanti UEM registriert sind, ist keine Benutzerinteraktion und keine neue Anwendungsbereitstellung erforderlich. Das trägt zu einer 100%igen Benutzerakzeptanz bei. Darüber hinaus lassen sich Compliance-Richtlinien erstellen und durchsetzen, um zu verhindern, dass Benutzer MTD deaktivieren oder von ihrem Gerät entfernen.

Beispiele aus der Praxis

MTD schützt vor Angriffen auf Geräte-, Netzwerk- und Anwendungsebene sowie vor Phishing-Angriffen.

Geräteausnutzung

Nachdem MMS-Nachrichten an die Zielbenutzer gesendet wurden, wurde ein Zero-Click-Chained-Exploit ohne jegliche Benutzerinteraktion ausgelöst, der eine Remotecode-Ausführung in Gang setzte, die die Privilegien des Angreifers erhöhte und eine laterale Bewegung im Netzwerk ermöglichte.

Netzwerk-Angriffe

In einem Café in der Nähe ihres Büros wurden Mitarbeiter eines Unternehmens durch einen Man-in-the-Middle (MITM)-Angriff via Wi-Fi auf eine Spear-Phishing-Seite umgeleitet, auf der Unternehmensdaten gestohlen wurden.

Bösartige Apps

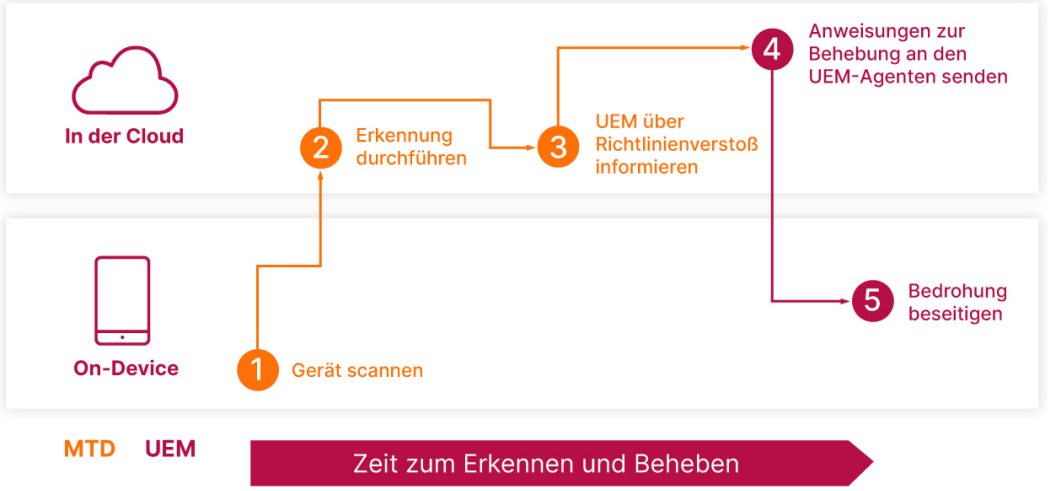
Ahnungslose Benutzer installierten eine App aus einem App-Store eines Drittanbieters. Die App missbrauchte Berechtigungen, führte einen Geräte-Exploit aus, ließ Daten nach außen dringen und wurde als Waffe eingesetzt, um über laterale Bewegungen in interne Netzwerke einzudringen und nach weiteren sensiblen Daten zu suchen.

Phishing-Angriffe

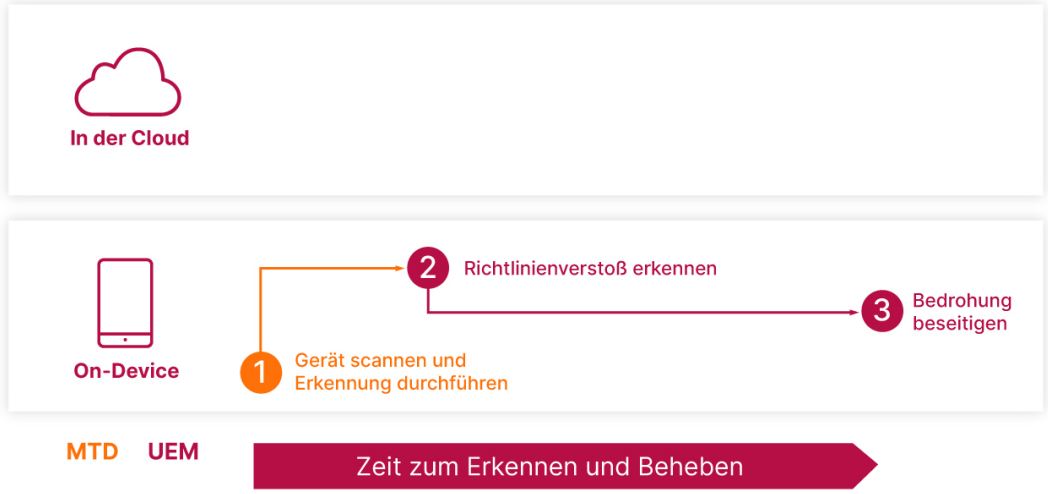
Mit Hilfe von Social Engineering brachte ein Angreifer einen ahnungslosen Benutzer dazu, auf einen Link zu klicken und seine Anmeldedaten für das Unternehmen anzugeben. Der Angreifer war dann in der Lage, sich als Benutzer anzumelden und auf Unternehmensressourcen zuzugreifen.

Erkennung und Behebung

Andere Threat Defense-Lösungen



MTD-Lösung von Invanti



Über Ivanti

Ivanti macht den Everywhere Workplace möglich. Im Everywhere Workplace nutzen Mitarbeiter unzählige Geräte, um über verschiedene Netzwerke auf IT-Netzwerke, Anwendungen und Daten zuzugreifen und so von überall aus produktiv arbeiten zu können. Die Ivanti-Automatisierungsplattform verbindet die branchenführenden Unified-Endpoint-Management-, Zero-Trust-Sicherheits- und Enterprise-Service-Management-Lösungen des Unternehmens und bietet Organisationen eine zentrale Plattform für das Self-Healing und Self-Securing von Geräten sowie für den Self-Service von Endanwendern. Mehr als 40.000 Kunden, darunter 96 der Fortune 100, haben sich für Ivanti entschieden, um ihre IT-Assets von der Cloud bis zum Edge zu erkennen, zu verwalten, zu sichern und zu warten und ihren Mitarbeitern ein hervorragendes Endbenutzererlebnis zu bieten, egal wo und wie sie arbeiten. Für weitere Informationen, besuchen Sie ivanti.com

ivanti.com
1 800 982 2130
sales@ivanti.com