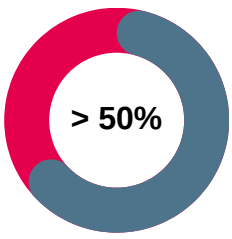
Sneak Peak - Whitepaper

8 Mobile Threat Defense-Systeme im Vergleich

Wie garantiert man die Sicherheit von mobilen Daten?

Dafür gibt es "Mobile Threat Defense" (MTD)-Lösungen, die den gesamten Prozess der Datenverarbeitung betrachten. Sie checken das Betriebssystem, installierte Apps und Daten. Sie erkennen sogar Schadsoftware in installierten Apps und untersuchen den Quellcode der Apps. In Kombination mit MDM/ UEM-Systemen kann man den Geräteschutz sogar erweitern. Diese Lösungen sind in der Lage, den Netzwerkverkehr zu analysieren und können z.B. Phishing-Angriffe erkennen und unterbinden.

Wir haben 8 Anbieter von MTD-Lösungen auf Herz & Nieren getestet. Dabei ist für uns der Ansatz "Aus der Praxis für die Praxis" die optimale Bewertungsgrundlage. Das haben wir mit vielen Praxistests wie folgt umgesetzt.



Im Jahr 2022 waren mehr als 50 % der mobilen Endgeräte einem Phishing-Angriff ausgesetzt.

Smartphones und mobile Endgeräte sind auf Platz 1 der anfälligsten Hardware für Cyber-Angriffe.

SYSTAG GmbH

Gutenbergstrasse 47 D-72555 Metzingen

07123 / 92 02 - 0 franka.theis@systag.com www.systag.com

Die Vorgehensweise

- Online & Dokumentenrecherche
- Befragung der Hersteller mittels Checklisten
- Sicherheitstest, detaillierte Labortests mit lebensnahen Szenarien u. a. PEN-Testing und Hackingmethoden

Untersuchte Lösungen

- CylancePROTECT® Mobile (BlackBerry®)
- Check Point Harmony Mobile
- Cisco Umbrella
- CrowdStrike Falcon for Mobile
- Lookout
- Microsoft Defender Mobile
- Trend Micro™
- Ivanti Neurons for Mobile Threat Defense

Welche Eigenschaften haben wir untersucht und warum?

Das Betriebssystem und die Konfiguration der mobilen Endgeräte (Apps, Verschlüsselung etc.) werden zum **Geräteschutz** analysiert, um Schwachstellen zu bewerten. Die Integration in bestehende **MDM/ UEM**-Systeme ist für die einfache Verwaltung mobiler Endgeräte von entscheidender Bedeutung.

Die Kommunikation zwischen der MTD-Lösung und einem zentralen System (SOC/ SIEM) ist von entscheidender Bedeutung.

Das Zusammenspiel mit dem **SOC** - Security Operations Center (oder, das Team, das darin arbeitet) und **SIEM** - Security Information and Event Management (sammelt und analysiert Geräteprotokolle) muss gewährleistet sein. Denn die Administratoren müssen in der Lage sein, einen Überblick zu behalten, und wenn Risiken auftreten, müssen diese detailliert analysiert werden können. Die Verwaltungskonsole muss dazu die notwendigen Informationen bereitstellen können.

Ebenso wichtig ist, welche **Geräte** und welche Betriebssysteme (iOS oder Android) unterstützt werden (Android for Business und BYOD).
Optimalerweise wird der **Netzwerk**verkehr analysiert und z.B. Netzwerkattacken oder zusätzliche VPNs aufgezeigt.
In Bezug auf die Nutzbarkeit (Usability) wurden in der Studie drei Aspekte untersucht: die **Inbetriebnahme/ Aktivierung**, die Performance und die Offline-Nutzung. Lösungen, die vom Administrator zentral bereitgestellt werden können, ohne dass der Nutzer eingreifen muss (**ZeroTouch**) sind die bevorzugten Lösungen.
Bei der **Performance** werden die Auswirkungen auf die Geschwindigkeit des Geräts und die Akkulaufzeit untersucht. Eine **Offline-Nutzung** ist wichtig, damit der Nutzer auch ohne Netzwerkverbindung geschützt bleibt.
Zum **Appschutz** analysieren MTD-Lösungen installierte Apps auf Schadsoftware. Außerdem bieten sie Funktionen zur Absicherung von geklonten Apps und der MTD-App selbst sowie anderer unternehmenseigener Apps.

SYSTAG GmbH
Gutenbergstrasse 47 D-72555 Metzingen
07123 / 92 02 - 0 franka.theis@systag.com www.systag.com

Unter **Datenschutz** versteht man, wie mit allen personenbezogenen Daten umgegangen wird und welche Einstellungsmöglichkeiten es gibt.

Beim Punkt **Administration** wurde untersucht, wie komplex oder übersichtlich die Verwaltungskonsole ist. Einige Systeme zeigen lediglich einen einfachen "Achtung Risiko"-Status an, ohne eine genauere Erklärung zu geben. Als Administrator ist es jedoch wichtig, auch in großen Umgebungen die Übersicht zu behalten. Wenn Risiken auftreten, müssen diese analysiert werden und die Verwaltungskonsole sollte die erforderlichen Informationen liefern können.

Mit **ZeroTrust** werden alle Aktivitäten nach dem Null-Vertrauens-Prinzip auf verdächtige Vorkommnisse überprüft.

InApp Security (Zusatz) zeigt, wie die Integritätsprüfung der eigenen App stattfindet und welche Technologie dazu verwendet wird.

Der Vergleich

	Lookout	Harmony Mobile	Zimperium	Crowdstrike	Cylance	Trend Micro	Microsoft Defender	Cisco Umbrella
Geräteschutz	★	★	😐	😐	😐	😐	😐	👎
Netzwerk	★	😐	😐	✓	😐	✓	😐	😐
MDM/UEM	👎	★	😐	😐	👎	👎	👎	👎
Endgeräte	✓	✓	✓	✓	✓	✓	✓	✓
SOC/SIEM	★	😐	k.A.	👎	👎	😐	😐	👎
Usability	✓	✓	✓	✓	✓	✓	✓	✓
AppSchutz	👎	✓	★	✓	★	k.A.	✓	k.A.

★ Hervorragende Erfüllung / sehr gut geeignet

👎 ungenügende Erfüllung / eingeschränkt geeignet

✓ Gute Erfüllung / gut geeignet

k.A. k.A. – keine Angabe – der Hersteller gibt dazu leider keine Auskunft

😐 zufriedenstellende Erfüllung / geeignet

Zur vollständigen Studie

SYSTAG GmbH
Gutenbergstrasse 47 D-72555 Metzingen
07123 / 92 02 - 0 franka.theis@systag.com www.systag.com

Fazit

Wenn es um mobile Sicherheit geht, gibt es nicht die eine perfekte, sichere Lösung. Alle getesteten Produkte haben ihre Stärken und Schwächen.

Lookout belegt in dieser Studie eindeutig den ersten Platz. Alle Lösungen gewähren mindestens einen Basisschutz. Je nach der individuellen Gewichtung der bewerteten Eigenschaften können sich die Ergebnisse so verschieben, dass ein anderes System die bessere Lösung sein kann.

Bei der Auswahl der passenden MTD-Lösung empfehlen wir, die gesamten Produktfamilien zu betrachten, denn in diesen Umgebungen haben alle Produkte ihre Stärken und sind auch dort am Markt vertreten.

Diese Sneak Peak gibt einen ersten Eindruck, wie man MTD-Lösungen vergleichen kann und welche Lösungen in Frage kommen. Für ausführliche Informationen und einen tieferen Einblick in die technischen Facetten können Sie hier die Vollversion beziehen.

Sie haben Fragen oder wollen eine MTD-Lösung testen?

Ihre Ansprechpartnerin:

Franka Theis
Strategic Account Manager

SYSTAG GmbH

Gutenbergstraße 47

72555 Metzingen

07123 / 92 02 - 0
franka.theis@systag.com

Zur vollständigen Studie