Fünf Schritte zur Umsetzung einer Strategie zur Abwehr mobiler Bedrohungen

Der Schutz Ihres Unternehmens gegen mobile Bedrohungen ist ein Wettlauf mit der Zeit. Tun Sie alles, was in Ihrer Macht steht, um einen Angriff abzuwehren?

Haben Ihre Mitarbeiter schon einmal kostenlose WLANs im Hotel, auf dem Flughafen oder im Café verwendet? Was ist mit USB-Anschlüssen? Wie können Sie feststellen, ob die Mitarbeitergeräte gegen eine Man-in-the-Middle-Attacke oder gegen den Diebstahl der Unternehmens-Anmeldeinformationen gesichert sind? Mit welcher Strategie wollen Sie solche Angriffe erkennen und blockieren?

Die fünf Schritte in dieser Anleitung können Sie bei der Entwicklung einer bewährten Strategie unterstützen, die verwertbare Daten liefert und einen sofortigen Schutz gegen heutige mobile Bedrohungen Ihrer mobilen Mitarbeiter ermöglicht. Informieren Sie sich, wie Sie durch Abwehr mobiler Bedrohungen schon auf dem Gerät Geräte, Apps und Daten vor den neuesten Sicherheitsrisiken schützen.

MobileIron

MKT DE-A4 v1.0

Eine mobile Strategie zur Abwehr mobiler Bedrohungen (MTD) ist ein Wettlauf mit der Zeit, weil die Angriffe auf Mobilgeräte rapide zunehmen und zunehmend gefährlicher werden. Die Organisationen hinter diesen Angriffen sind vor allem durch die Gier nach Gewinn motiviert, daher sehr entschlossen und extrem gut in ihren Angriffen. Ein Sicherheitsbericht des Ponemon Institute 2017 stellte fest, dass Unternehmen mit 28%-iger Wahrscheinlichkeit erneut Opfer eines Diebstahls von mindestens 1.000 Datensätzen mit personenbezogenen Informationen über Verbraucher oder Kunden werden dürften – Informationen, die für Cyberkriminelle besonders wertvoll sind.[1] Die Konsequenzen solcher Angriffe können enorm sein: Es geht nicht nur um verloren gegangene oder gefährdete Daten; ein veröffentlichter Datendiebstahl kann Kundenbeziehungen beschädigen, das Unternehmensimage beeinträchtigen, zu Ertragsverlusten, enormen Geldstrafen und Gerichtskosten führen und nicht zuletzt wertvolle Zeit und wertvolle Ressourcen zur Bereinigung des Schadens binden.

Wenn Sie noch nicht alles getan haben, um Ihr Unternehmen gegen solche Risiken abzusichern, ist jetzt der richtige Moment dafür. Mit den folgenden fünf bewährten Schritten können Sie leichter Lücken in Ihrem Sicherheitskonzept identifizieren und für jedes Netzwerk und jeden Arbeitsort der Mitarbeiter einen Komplettschutz aller Mobilgeräte gewährleisten, die auf Unternehmens-Apps und Unternehmensdaten zugreifen.

Übersicht über aktuelle mobile Bedrohungen

75 % DER ANGRIFFE
WERDEN DURCH EXTERNE HACKER AUSGEFÜHRT.

81 % DER DATENDIEBSTÄHLE DURCH HACKER
ERFOLGEN DURCH GESTOHLENE PASSWÖRTER.

73 % DER DATENDIEBSTÄHLE
SIND FINANZIELL MOTIVIERT.[2]

Siehe ICT Security Magazine, „2017 Data Breach Investigations Report, 10th Edition" (Untersuchungsbericht zu Datendiebstählen 2017, 10. Ausgabe)

1 https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states

2 https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

MobileIron

Schritt 1:
Intuitive und unsichtbare Bedrohungsabwehr aktivieren

Einige Lösungen für die Mobilgerätesicherheit erwarten von den Endbenutzern, dass diese ihre Mobilgeräte selbst absichern. Dies ist ein ineffektives und naives Konzept zur Abwehr von MTD-Angriffen. Diese „benutzerabhängigen Sicherheitslösungen" verlangen von dem Benutzer eines Mobilgeräts, sich im App Store des Unternehmens den Client herunterzuladen und mehrere Schritte zur Installation auszuführen, diese zu aktivieren und laufend zu aktualisieren. Darüber hinaus hat die IT-Abteilung nach der Installation des Clients durch den Benutzer nur sehr wenige Möglichkeiten, die Nutzung der Sicherheits-App zu erzwingen – der Benutzer kann die App einfach wieder deinstallieren oder mit einer Wischbewegung deaktivieren und gefährdet damit die Unternehmensdaten. Tatsächlich wurde in einer Studie festgestellt, dass über ein Drittel der Unternehmen Mobilgeräte nicht angemessen absichern, weil das Budget und die Ressourcen fehlen, um moderne Sicherheit im gesamten Unternehmen konsistent durchzusetzen.[3]

IT-Abteilungen können sich oft nur darauf verlassen, dass die Benutzer die neuesten Sicherheits-Apps auf ihren Geräten aktivieren. Wenn die Benutzer ihre Geräte nicht aktualisieren, ist das Unternehmen durch Angriffe gefährdet, wenn nicht alle Endpunkte die Sicherheitsrichtlinien erfüllen. Es ist daher keine Überraschung, dass Dimensional Research in einem Report 2017 feststellte, dass „zwei Drittel der Antwortgeber der Umfrage Zweifel hätten, dass ihre Unternehmen sich gegen eine mobile Cyberattacke verteidigen könnten, obwohl fast alle Sicherheitsprofis der Ansicht sind, dass die Zahl der mobilen Angriffe rapide steigen wird."[4]

Um eine sofortige 100%-ige Sicherheit auf jedem Mobilgerät zu gewährleisten, das auf Unternehmensressourcen zugreift, dürfen die Unternehmen sich nicht darauf verlassen, dass die Benutzer die neuesten Updates installieren. Für eine zeitgemäße, lückenlose Mobilgerätesicherheit empfiehlt die Gartner Group, dass die Unternehmen „die MTD-Lösung in Enterprise Mobility Management (EMM) integrieren".[5] Bei diesem Konzept übernehmen die IT-Administratoren die Absicherung und die Aktualisierung direkt auf dem Gerät über EMM. Das heißt, es ist kein Benutzereingriff erforderlich, um die neuesten Sicherheits-Updates herunterzuladen und zu aktivieren, und die Datenschutzrichtlinien bleiben unverändert. Durch Integration von EMM und MTD kann die IT-Abteilung sich zudem auf strategischere Prioritäten fokussieren und die Belastung mit Routineaufgaben reduzieren, da die Administratoren nicht mehr kontrollieren müssen, ob die Benutzer mit sicheren Geräten arbeiten.

„Zwei Drittel der Antwortgeber in der Umfrage gaben an, dass sie Zweifel haben, ob ihre Unternehmen sich gegen einen mobilen Cyberangriff verteidigen können, obwohl fast alle Sicherheitsprofis der Ansicht sind, dass die Zahl der mobilen Angriffe rapide ansteigen wird."

— Dimensional Research,
„The Growing Threat of Mobile Security Breaches:
A Global Survey of Security Professionals"
(Die wachsende Gefahr mobiler Sicherheitslücken:
globale Umfrage unter Sicherheitsprofis)

3 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
4 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
5 https://www.gartner.com/doc/3789664/market-guide-mobile-threat-defense

Schritt 2:
Alle Arten von Cyberangriffen anzeigen

Die mangelnde Transparenz bei mobilen Bedrohungen ist heute in Unternehmen eine der größten Herausforderungen für die Mobilgerätesicherheit. Tatsächlich gaben mehr als die Hälfte (51 %) der befragten Unternehmen an, dass sie nicht wüssten, ob schon einmal Malware auf die Mobilgeräte heruntergeladen worden wäre, die die Mitarbeiter zur Arbeit mitbringen.[6] Einige Lösungen zur Mobilgerätesicherheit konzentrieren sich nur auf Bedrohungen auf App-Ebene und tragen damit nicht zur Verbesserung der Transparenz bei. Cyberangriffe erfolgen jedoch nicht immer nach dem gleichen Muster. Es gibt verschiedene Angriffsarten, die dieses eingeschränkte Konzept durch andere Mittel umgehen können. Das heißt, Unternehmen dürfen sich nicht nur auf eine Ebene konzentrieren. Sie müssen eine voll integrierte, umfassende Mobilgerätesicherheit gewährleisten, damit Geräte, Netzwerke und Anwendungen („DNA") nicht angegriffen werden können.

- **Angriffe auf Geräteebene:** Dazu gehören die schwerwiegendsten Bedrohungen, weil erfolgreich genutzte Sicherheitslücken Hackern durch die vollständige Kontrolle des Geräts ermöglichen, verschlüsselten Content zu entfernen. Angriffe auf Geräteebene erfolgen oft durch kostenlos heruntergeladene Apps oder eine SMS-Nachricht, die Malware startet, sobald sie vom Benutzer geöffnet wird.
- **Angriffe auf Netzwerkebene:** Öffentliche Netzwerke sind zwar nützlich und bequem, können jedoch auch die Startrampe für Angriffe direkt auf Mobilgeräte sein. Ein unsauber konfigurierter Zugangspunkt im kostenlosen WLAN des Hotels oder im Café kann beispielsweise eine MITM-Attacke starten und die Kommunikation zwischen dem Gerät und dem Firmennetzwerk abfangen. Der Angreifer kann das Gerät schnell auf bekannte Sicherheitslücken scannen, über die er dann auf das Gerät zugreift und Benutzernamen, Passwörter sowie vertrauliche Unternehmensdaten sammelt, die er dann später für den Angriff auf Unternehmensressourcen nutzen kann.
- **Angriffe auf App-Ebene:** Diese Angriffe erfolgen in der Regel, wenn arglose Benutzer eine App aus einem unbekannten App-Store installieren. Diese App enthält Malware, die auf Benutzerrechte zugreifen, Sicherheitslücken nutzen und in interne Netzwerke eindringen kann, um Unternehmensdaten zu stehlen.

Mit Lösungen, die modernste Algorithmen der künstlichen Intelligenz sowie die verhaltensabhängige Erkennung auf dem Mobilgerät nutzen, können Unternehmen solche bekannten und noch unbekannten (Zero-Day-) Angriffe blockieren. Tools mit künstlicher Intelligenz konzentrieren sich nicht nur auf Apps und damit auf eine einzige Bedrohung, sondern können sofort alle Arten anormaler Aktivitäten erkennen und blockieren, beispielsweise eine nicht genehmigte VPN-Konfiguration oder den Download einer kostenlosen App.

„Mehr als die Hälfte (51 %) der befragten Unternehmen gab an, dass sie nicht wüssten, ob auf Mobilgeräte, die Mitarbeiter zur Arbeit mitbringen, schon einmal Malware heruntergeladen wurde."

— Zimperium,
„Spotlight-Report zur Mobilgerätesicherheit 2017"

6 http://go.zimperium.com/2017-mobile-security-report

Schritt 3:
Bereitstellung von verwertbaren Daten über Sicherheitsbedrohungen

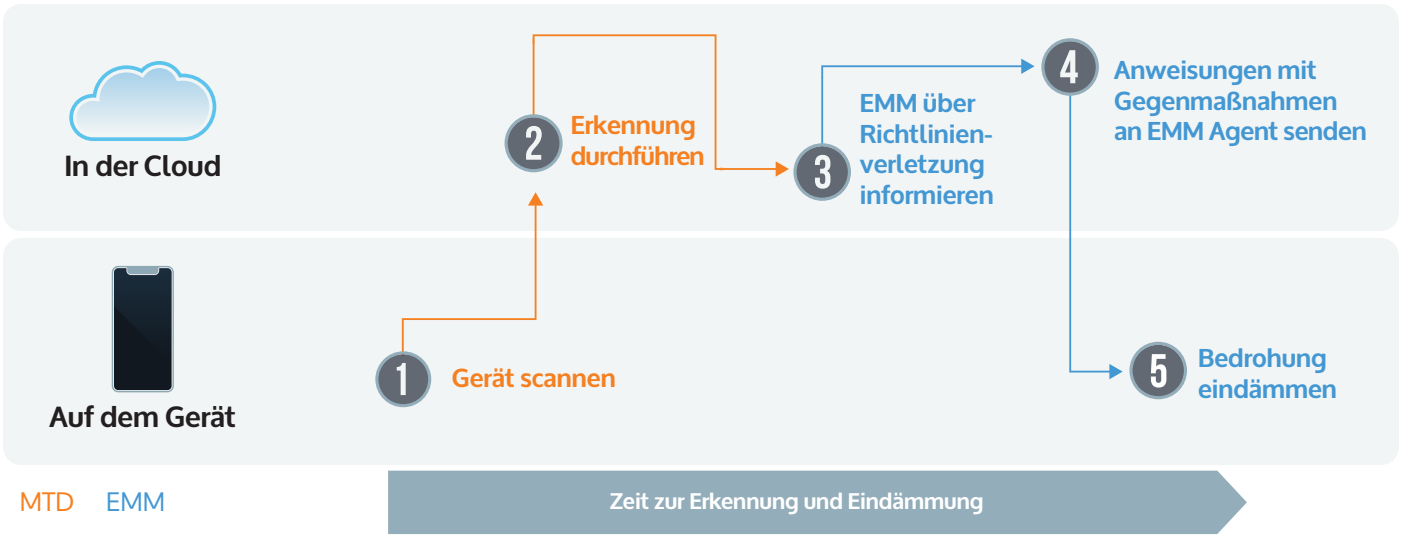
Genauso, wie mangelnde Transparenz dazu führen kann, dass bei der Absicherung Lücken übersehen werden, kann durch ein ständiges Bombardement mit undifferenzierten Warnmeldungen ein Ermüdungseffekt eintreten. Dieser „Ermüdungseffekt" durch Warnmeldungen ohne Priorisierung kann es den Administratoren für Mobilgerätesicherheit erschweren, schnell informierte Entscheidungen zu fällen.

Um verwertbare Daten über Sicherheitsbedrohungen bereitzustellen, müssen die MTD-Lösungen ein Analysemodul enthalten, das mit Algorithmen künstlicher Intelligenz zwischen normalem und verdächtigem Verhalten auf dem Gerät selbst unterscheidet. Durch Analyse kleiner Abweichungen von den Betriebssystemstatistiken des Geräts, den Speicher-, CPU- und sonstigen Systemparametern kann künstliche Intelligenz exakt nicht nur spezifische Angriffe mit Schadsoftware identifizieren, sondern auch detaillierte kriminaltechnische Daten zu Person, Art und Weise, Ort, Zeitpunkt und Ziel eines Angriffs liefern.

Lösungen mit künstlicher Intelligenz auf dem Gerät erkennen Angriffe, selbst wenn die Benutzer nicht mit dem Netzwerk verbunden sind oder die Malware noch unbekannt ist, oder wenn es sich um neue Bedrohungen oder Zero-Day-Angriffe handelt. Solche Lösungen arbeiten schneller als Cloud-Lösungen, weil kein Traffic über Tunnel zur Cloud übertragen werden muss. Experten für Mobilgerätesicherheit können schnell anstehende Bedrohungen identifizieren, diesen eine Priorität zuordnen und bei einem schweren Angriff auf Unternehmensressourcen Sofortmaßnahmen ergreifen.

Erkennung und Eindämmung

Andere MTD- und EMM-Lösungen



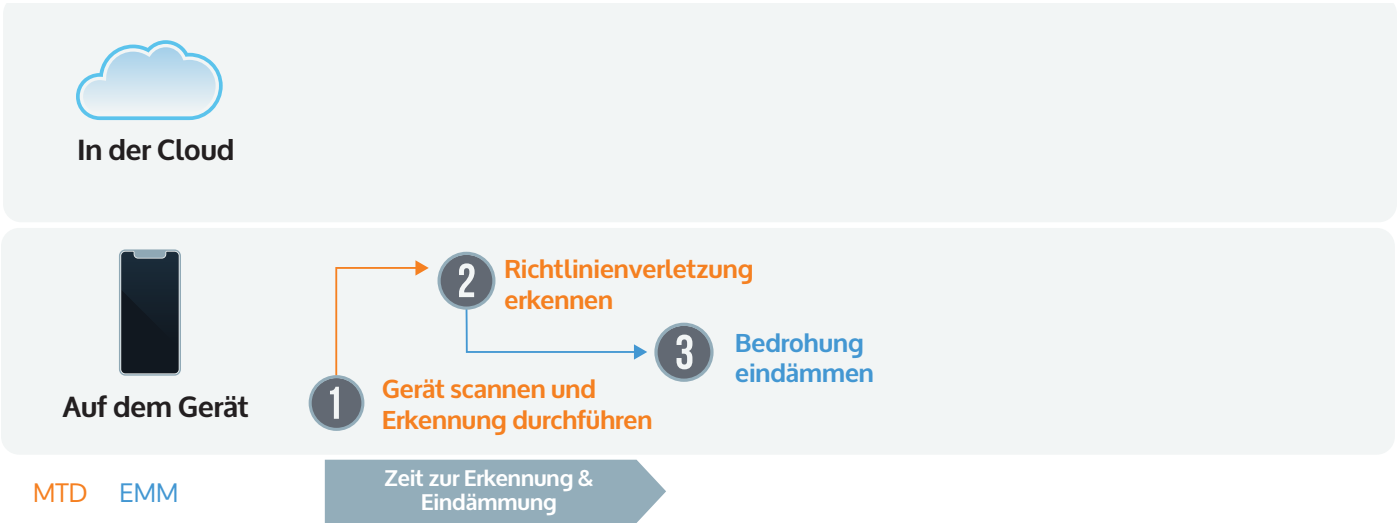
Schritt 4:
Eindämmung von Gerätebedrohungen mit Rechnergeschwindigkeit

Angriffe erfolgen mit Rechnergeschwindigkeit. Sicherheitsfunktionen müssen genauso schnell reagieren. Nur in der Cloud installierte MTD-Lösungen können die Erkennung und Eindämmung der Bedrohungen auf Mobilgeräten verzögern, weil der EMM-Plattform eine Sicherheitsverletzung erst bekannt wird, nachdem das Gerät gescannt wurde und Warnmeldungen über die Cloud versendet worden sind. Dies kann dazu führen, dass kritische Reaktionszeit für Gegenmaßnahmen bei einer möglicherweise verheerenden Attacke verloren geht, beispielsweise bei einem MITM-Angriff, bei dem ein Gerät über einen kostenlosen WLAN-Zugang attackiert wird. Bei solchen Attacken nutzt der Hacker eine Sicherheitslücke, die das mobile Gerät gefährdet und dem Hacker eine umfangreichere Kontrolle des Gerätes erlaubt, als es dem Benutzer möglich ist. Beispielsweise kann der Hacker alle Benutzerkontakte herunterladen, E-Mail-Nachrichten stehlen und sich als Benutzer anmelden, um eine Phishing-E-Mail an den CEO zu senden – und damit wiederum ein massives Sicherheitsproblem für das gesamte Unternehmen auslösen.

Eine auf dem Gerät installierte MTD-Lösung reagiert auf Bedrohungen mit Rechnergeschwindigkeit, weil keine weiteren Schritte zur Erkennung und Eindämmung der Bedrohungen erforderlich sind. Weil die entsprechende Software auf dem Gerät installiert ist, kann sie eine Verletzung von Richtlinien sofort erkennen und die Bedrohung auf dem Gerät blockieren, selbst wenn es sich um einen MITM-Angriff handelt. In dem Wettlauf mit der Zeit erhalten Sie so einen entscheidenden Vorteil gegenüber Hackern und verhindern viele weitere Folgeprobleme.

Erkennung und Eindämmung

Die Lösung Threat Defense von MobileIron



Schritt 5:
Detaillierte Berichte vereinfachen die Einhaltung der Compliance

In jedem internationalen Unternehmen müssen zur Erfüllung der Regulierungsvorschriften eindeutige Audit- und Berichtsprozesse beispielsweise zu den Bestimmungen der Datenschutzgrundverordnung, den US-amerikanischen PCI-Datensicherheitsstandards (PCI DSS) sowie zum US-amerikanischen Gesetz zum Schutz und zur Portabilität von Patientendaten (HIPAA) sowie zu meldepflichtigen Datenschutzverletzungen (NDB) existieren, um nur einige zu nennen.

In mobilen Unternehmen sind die damit verbundenen Herausforderungen deutlich höher, da die Benutzer nicht mehr an die von der IT kontrollierten Desktops gebunden sind; sie greifen auf Unternehmens-Apps und Unternehmensdaten über diverse private und firmeneigene Mobilgeräte und verschiedene Netzwerke zu. Einer der Berichte stellte dazu fest: „Eine der Herausforderungen zur Einhaltung der Datenschutzgrundverordnung wird die Absicherung personenbezogener Daten auf Laptops und anderen Mobilgeräten sein. Der Schutz solcher Informationen lässt sich schwerer erreichen, und es besteht ein höheres Risiko, weil diese Informationen sich nicht hinter der Firewall des Unternehmens befinden."[7]

Die Fähigkeit, alle Geräte und Apps zu erfassen und zu verwalten, ist unverzichtbar für die Einhaltung der Compliance, weil damit ein transparentes Bild der mobilen Bedrohungen und Risiken insgesamt gepflegt wird. Wenn Administratoren schnell Audit-Reports generieren, Bedrohungsprotokolle anzeigen sowie den Zugriff und die bisherige Nutzung verfolgen können, können sie schnell potenzielle Schwachstellen identifizieren und sicherstellen, dass alle Benutzer, Geräte und Apps die Anforderungen erfüllen. Auf diese Weise können Unternehmen die Richtlinien zur Einhaltung der Compliance erfüllen und alles in ihren Kräften stehende tun, um das Unternehmen gegen mobile Risiken zu sichern.

„Eine der Herausforderungen für die Einhaltung der Datenschutzgrundverordnung wird die Absicherung personenbezogener Informationen auf Laptops und anderen Mobilgeräten sein. Der Schutz solcher Informationen lässt sich schwerer erreichen, und es besteht ein höheres Risiko, weil diese Informationen sich nicht hinter der Firewall des Unternehmens befinden."

Datenschutzgrundverordnung: Report, „Einhaltung der Datenschutzgrundverordnung für mobile Mitarbeiter", Oktober 2017

7 https://gdpr.report/news/2017/10/13/gdpr-compliance-mobile-workers

MobileIron THREAT DEFENSE

MobileIron Threat Defense: Die Lösung für einfache, transparente Sicherheit auf Mobilgeräten

MobileIron weiß, dass Cyberkriminelle laufend an ausgefeilteren Möglichkeiten arbeiten, Daten mit allen erforderlichen Mitteln zu stehlen. Aus diesem Grund arbeiten wir laufend an innovativen Lösungen, damit unsere Kunden den Wettlauf mit der Zeit gewinnen und den neuesten mobilen Sicherheitsbedrohungen immer voraus sind. Als Teil dieser Bemühungen unterstützt MobileIron Threat Defense die fünf kritischen Schritte zur Bereitstellung einer zeitgemäßen Sicherheit auf Mobilgeräten. Unsere Lösung mit einer einzigen, integrierten App hat mehrere entscheidende Vorteile:

- Eine einzige voll in EMM integrierte App zum Schutz vor Bedrohungen.
- Keine Benutzeraktion erforderlich, um die Sicherheit auf dem Gerät zu aktivieren oder zu aktualisieren.
- Die zeitgemäße, mobile Sicherheitslösung blockiert bekannte und unbekannte Bedrohungen für iOS- und Android-Geräte, ohne dass eine Internetverbindung erforderlich ist.
- Algorithmen mit künstlicher Intelligenz erkennen sofort Bedrohungen des Geräts, der Apps und des Netzwerks und dämmen diese ein.

Damit wird transparent und unkompliziert eine Gerätesicherheit gewährleistet, die verwertbare Daten liefert und alle mobilen Mitarbeiter sofort vor Bedrohungen des Geräts, der Apps und des Netzwerks schützt. Sie können damit eine zeitgemäße, mobile Sicherheitsstrategie umsetzen, die auf der soliden Basis der EMM-Plattform aufbaut und diese durch zusätzliche Schutzmaßnahmen gegen mobile Bedrohungen ergänzt. Das heißt, Sie können sich auf das konzentrieren, was für Ihr Unternehmen am wichtigsten ist: die ständige Produktivität der mobilen Mitarbeiter, damit Ihr Unternehmen seinen innovativen Wettbewerbsvorsprung behält.

Weitere Informationen über unsere vollintegrierte Lösung zur Erkennung und Eindämmung mobiler Bedrohungen finden Sie unter www.mobileiron.com/threatdefense.

MobileIron

401 East Middlefield Road
Mountain View, CA 94043, USA
globalsales@mobileiron.com
www.mobileiron.com
Tel.: +1 877 819 3451
Fax :+1 650 919 8006