DATENBLATT

RSA Mobile Lock

Bedrohungserkennung für Mobilgeräte

Vorteile

- **Bedrohungen auf Mobilgeräten erkennen**
- **Vertrauen in nicht verwaltete Mobilgeräte schaffen**
- **Authentifizierung zum Schutz von Ressourcen einschränken**
- **Ausweitung von Bedrohungen während der Untersuchung verhindern**
- **Reaktion des IT-Teams beschleunigen**
- **Mobilgerät und mobile App sichern**
- **Andere Gerätefunktionen unbeeinflusst lassen**

RSA Mobile Lock erkennt kritische Bedrohungen auf Mobilgeräten und schränkt die Authentifizierungsmöglichkeit von Nutzern so lange ein, bis die Bedrohung beseitigt ist. RSA Mobile Lock ermöglicht es der IT-Abteilung Vertrauen zu schaffen, indem sie mobile Geräte über die gesamte Angriffsfläche hinweg verifiziert, systematisch vor Bedrohungen schützt und jedes Gerät sichert, um diese Bedrohungen abzuschwächen.

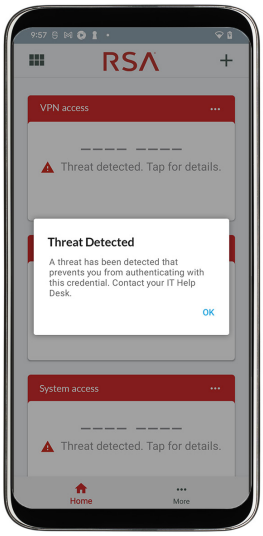
Schnelle und zuversichtliche Reaktion auf Bedrohungen

Im Falle einer Bedrohung ermöglicht RSA Mobile Lock schnelles Handeln, indem es Nutzer warnt und daran hindert, sich in einer gesicherten Umgebung zu authentifizieren und auf Unternehmensdaten, Unternehmenssysteme oder Kundendatensätze zuzugreifen. Bedrohungen können sich so nicht ausgehend von einem kompromittierten Mobilgerät auf alle Unternehmenssysteme und -daten auswirken und mitunter schwerwiegenden Schaden im Unternehmen verursachen.

Sicherheit von Gerät und App managen

Indem RSA Mobile Lock nur die Authentifizierung von Nutzern auf einem Gerät einschränkt, leistet die Anwendung Folgendes:

- Erkennung von Mobilgeräten, die einer Sicherheitsbedrohung ausgesetzt sind
- Inkenntnissetzung von Nutzern über die Bedrohung auf ihrem Mobilgerät
- Benachrichtigung der IT über die Bedrohung
- Aufrechterhaltung der Sicherheit von Geschäftssystemen und -daten



Minderung der Auswirkungen auf Nutzer

Anstatt Nutzer auf ihrem eigenen Gerät zu sperren, verfährt RSA Mobile Lock nach einem gezielten Ansatz, der sich speziell auf die Authentifizierungs-App konzentriert. Während die Authentifizierung bei Vorliegen einer Bedrohung eingeschränkt wird, kann der Nutzer das Gerät weiterhin für Anrufe und andere Zwecke verwenden, die nicht im Zusammenhang mit der Authentifizierung bei gesicherten Ressourcen stehen.

OWN YOUR IDENTITY.

OWN YOUR IDENTITY.

Sicherer Umstieg auf die Cloud

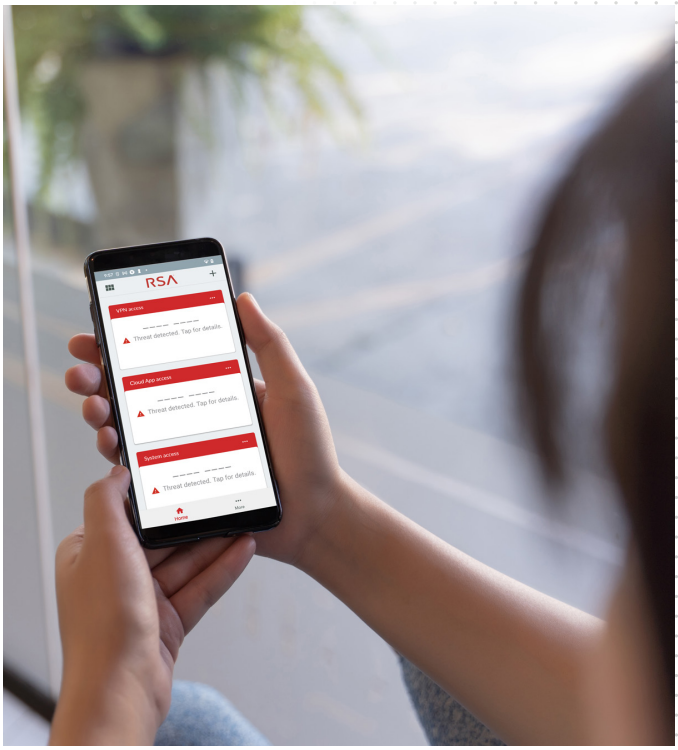
Wenn Ihr Unternehmen auf Cloud-Authentifizierung umstellt, profitieren die Benutzer davon, dass sie sich überall authentifizieren können, oft mit ihren eigenen persönlichen Geräten.. Die Umsetzung von Nutzerwünschen ist aber auch mit Risiken verbunden. So müssen Unternehmen für einen lückenlosen und sicheren Zugriff sorgen. RSA Mobile Lock wird beiden Anforderungen gerecht.

Mehr erfahren

Mehr über die Funktionen von RSA Mobile Lock erfahren Sie unter **RSA.com**.

Über RSA

RSA ermöglicht 12.000 Unternehmen weltweit ein bewährtes Identitäts- und Zugriffsmanagement, betreut 25 Millionen Unternehmensidentitäten und verschafft Millionen von Nutzern einen sicheren und bequemen Zugriff. RSA befähigt Unternehmen, in einer digitalen Welt erfolgreich zu sein, mit umfassenden Funktionen für moderne Authentifizierung, Lifecycle Management und Identity Governance. Ob in der Cloud oder vor Ort, RSA verbindet Menschen mit den digitalen Ressourcen, auf die sie angewiesen sind, wo immer sie leben, arbeiten und spielen. Weitere Informationen finden Sie auf **RSA.com**.



RSA