

BEST PRACTICES:

Grundlagen DER BEDRO- HUNGSAB- WEHR



Was haben Fahrräder, eine Pferdestatue, Hubschrauber und das Porträt einer Frau ohne Augenbrauen gemeinsam? Leonardo da Vinci, natürlich! Der Universalgelehrte der Renaissance schuf diese Gegenstände in irgendeiner Form, wobei er sich mit Malerei, Bildhauerei, Mathematik, Physik, Technik und vielem mehr befassen musste.

Für Organisationen mit begrenzten Ressourcen kann es sich so anfühlen, als müssten Sie der „Renaissance-Mann“ Ihres Unternehmens sein: Geschäftsführer*in, Manager*in, IT-Experte, Buchhalter*in usw. Wir bei Jamf können zwar nicht Ihre Steuern übernehmen, aber wir können Ihnen dabei helfen, die wichtigsten Aspekte der Bedrohungsabwehr kennenzulernen und herauszufinden, was Sie bei der Bewertung Ihrer Strategie zur Bedrohungsabwehr im Hinblick auf bewährte Verfahren beachten müssen.

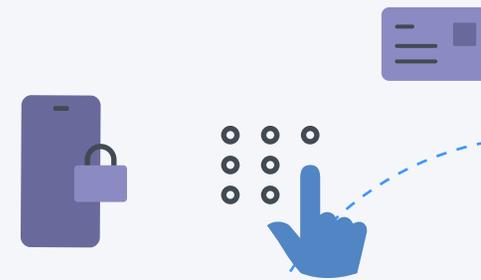


Was ist Gefahrenabwehr?

Die Bedrohungen kommen aus verschiedenen Quellen und mit unterschiedlichen Methoden. Sie können wie ein Anhang in einer E-Mail aussehen, wie eine SMS oder ein Anruf, um sich bei Ihrem Bankkonto anzumelden, wie Websites, die *fast* vertraut aussehen, oder wie gar nichts, wie im Falle von Geräten, auf denen veraltete Software mit Sicherheitslücken läuft.

Die Bedrohungsabwehr arbeitet hinter den Kulissen:

- Schutz vor bekannter Ransomware, Trojanern und anderer Malware
- Einsatz künstlicher Intelligenz zur Erkennung unbekannter Bedrohungen
- Sie auf verdächtige Aktivitäten aufmerksam machen
- Phishing-Angriffe und bösartige Websites blockieren
- Überwachen und protokollieren Sie den Zustand Ihrer Geräte



Braucht meine Organisation eine Bedrohungsabwehr?

Kurze Antwort: Ja! Das gilt unabhängig von der Größe Ihres Unternehmens — wenn Sie Unternehmensdaten haben, müssen diese geschützt werden. Ihr Unternehmen *wird irgendwann* Opfer eines Cybersecurity-Angriffs werden, zumindest gezielt. Deshalb ist es wichtig, das Risiko eines solchen Angriffs und die Auswirkungen auf Ihr Unternehmen zu verringern.

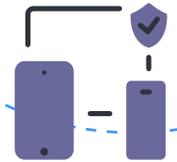


Erste Schritte zur Gefahrenabwehr

Um Bedrohungen vorzubeugen, müssen Sie Ihre Geräte und Ihr Netzwerk schützen. Ein guter Anfang ist es, **sicherzustellen, dass Ihre Geräte auf dem neuesten Stand sind**. **Veraltete** Betriebssysteme und Apps mit ungepatchten Sicherheitslücken machen es böswilligen Akteur*innen viel einfacher, in Ihre Systeme einzudringen.

Die Implementierung eines Antivirus- und Endpoint Detection and Remediation (EDR)-Tools verbessert Ihre Sicherheitslage weiter. Antivirus arbeitet im Hintergrund, um **bekannte Bedrohungen zu identifizieren**, indem es verdächtige Aktivitäten, Informationen in Dateien, die auf Malware hinweisen, bösartige Websites und IP-Adressen und vieles mehr erkennt. EDR geht darüber hinaus, indem es **künstliche Intelligenz und maschinelles Lernen einsetzt, um auf intelligente Weise Bedrohungen zu erkennen**, die noch nicht bekannt sind — Cyberangriffe entwickeln sich jeden Tag zu immer ausgefeilteren und komplexeren Bedrohungen, sodass ein Vergleich mit einer Datenbank bekannter Bedrohungen nicht ausreicht.





Vielleicht ist das zu viel für Sie — wir haben eine Lösung für Sie. Jamf bietet Lösungen für das Gerätemanagement, mit denen Sie Ihre Geräte auf dem neuesten Stand halten und gleichzeitig die Einhaltung der Sicherheitsrichtlinien überwachen können. Und unsere Sicherheitssoftware schützt Ihre Geräte vor bekannten und unbekanntem Bedrohungen, ohne den Benutzer/die Benutzerin zu belasten. Unabhängig davon, ob Sie Jamf für Ihre Verwaltungs- oder Sicherheitslösungen verwenden, sollten Sie diese Best Practices im Hinterkopf behalten:

- 1 Geräte und Software müssen mit den aktuellsten Betriebssystemen (OS) betrieben werden, und die Apps müssen verwaltet, überprüft und aktualisiert werden.
- 2 Verlassen Sie sich nicht einfach auf die sicherste Standard-Hardware. Schützen Sie Ihre Apple Fleet und Ihre Benutzer*innen mit einer auf Apple ausgerichteten Endpoint-Schutzlösung.
- 3 Lassen Sie die Technologie für sich arbeiten, und integrieren Sie KI und maschinelles Lernen mit EDR in Ihre Sicherheitsstrategie.

Möchten Sie mehr erfahren? Unser [E-Book „Bedrohungsabwehr für Einsteiger“](#) bietet einen tieferen Einblick in Taktiken und Lösungen zur Bedrohungsabwehr. Und sehen Sie, wie Bedrohungsabwehr ein integraler Bestandteil von [Trusted Access](#) mit Jamf ist.

Oder wenn Sie bereit sind, [können Sie unsere Software ausprobieren.](#)

