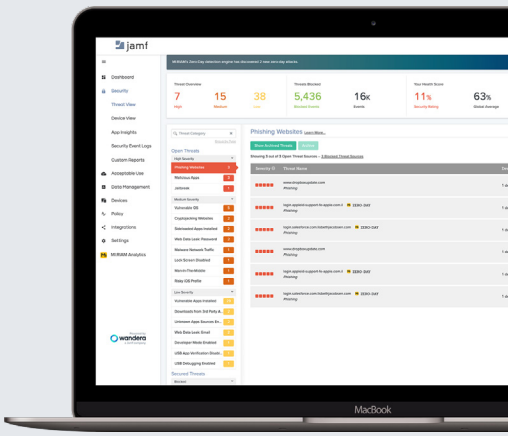
jamf

JAMF THREAT DEFENSE

Schützen Sie Ihre Geräte, Benutzer und Apps vor Cyberbedrohungen



Jamf Threat Defense bietet Sicherheit aus der Cloud, die im Gerät und im Netzwerk wirkt.

Leistungsstarke Endgeräte-Sicherheit

Threat Defense erkennt und behebt ein breites Spektrum an Endgerätebedrohungen, darunter Geräteschwachstellen, Malware und riskante Apps. Umfassende Risikobewertungen werden kontinuierlich ausgeführt, um Bedrohungen zu identifizieren. Dadurch können Sicherheitsrichtlinien in Echtzeit durchgesetzt werden.

Netzwerkschutz für Benutzer und Daten

Angriffe mithilfe von netzwerkinternen Verteidigungsfunktionen verhindern bevor sie eintreten können. Content-Schutz blockiert schädliche Websites einschließlich völlig neuer Zero-Day-Phishing-Websites, die das Ziel haben, geschäftliche Anmeldeinformationen zu erfassen. Darüber hinaus verhindert Threat Defense Command-and-Control und Datenexfiltration, indem die Konnektivität mit riskanten Websites unterbunden wird. Verbindungen werden automatisiert gesichert, wenn Angriffe festgestellt werden.

Adaptiver Zugriff auf Ihre Anwendungen

Verbessern Sie Ihre Sicherheitsaufstellung, indem Sie nur sicheren und vertrauenswürdigen Geräten erlauben, auf Geschäftsanwendungen zuzugreifen. Threat Defense überwacht kontinuierlich eine breite Palette von Sicherheitsdaten und kontextuelle Inputs, mit denen der Anwendungszugriff verhindert werden kann, wenn ein Endgerät gefährdet oder mit einem hohen Risiko verbunden ist. Adaptive Zugriffsrichtlinien können mit Zero-Trust-Netzwerkzugriff oder Jamf Pro, der Verwaltungslösung von Jamf, durchgesetzt werden.

jamf

Umfassende Bedrohungserkennung und -prävention

Zero-Day-Netzwerkschutz

Threat Defense identifiziert und blockiert selbst hochkomplexe Angriffe auf das Netzwerk einschließlich Zero-Day Phishing-Versuche, Command-and-Control-Communication und Cryptojacking. Dieser Service funktioniert mit jeder Anwendung, einschließlich Webbrowser, E-Mail, sozialen Medien und SMS.

Risikobewertung in Echtzeit

Threat Defense bewertet ständig das Risiko für Endgeräte – von Schwachstellen im OS bis zu schädlichen Profilen – was es Organisationen ermöglicht, schnell Geräte zu identifizieren, die gegen die Compliance verstoßen und echte Zero Trust Access Richtlinien durchzusetzen.

Detaillierte Einblicke in Apps

Threat Defense bietet fortgeschrittene App Intelligence, die sowohl für Workflows zur Prüfung von Apps als auch für Sicherheitsuntersuchungen verwendet werden kann. Für jede App wird eine Risikobewertung bereitgestellt, zusammen mit einem detaillierten Bericht, der die Berechtigungen und eingebetteten URLs verstellt, die Benutzer und Unternehmensdaten gefährden.

Dynamische Datenverschlüsselung

Threat Defense verhindert durch Echtzeitverschlüsselung, dass eine kompromittierte WLAN-Infrastruktur vertrauliche Daten offenlegt. Dieser Service läuft ruhig im Hintergrund und erfordert keine Benutzerinteraktion.

Wichtige Sicherheitsfunktionen und Fähigkeiten

Ständig aktive Endgerätesicherheit

Threat Defense schützt Telearbeiter und Geräte durch eine Endgeräte-App, die Schadsoftware, gefährliche Einstellungen und riskante Verbindungen identifiziert, bevor ein Datenleck auftreten kann.

Echtzeit-Meldungen und Richtlinienkontrollen

Die Unified Policy Engine ermöglicht es Administratoren, eine Sicherheitsrichtlinie schnell zu konfigurieren. Diese wird sofort durchgesetzt, wodurch Richtlinien im laufenden Betrieb optimiert und modifiziert werden können. Detaillierte Berichte können im Portal „Threat Defense“ eingesehen werden, oder über benutzerfreundliche Integrationen in Tools von Drittanbietern exportiert werden.

Bedingte Zugriffsrichtlinien

Verhindert den Zugriff auf Unternehmens-Apps, wenn die Risikoschwelle vordefinierte Werte übersteigt. Bedingte Zugriffsrichtlinien können nativ innerhalb des Threat Defense Netzwerks oder durch Integration in Jamf oder einen Identity Provider durchgesetzt werden.

Einheitliche Operationen und Verwaltung

Threat Defense integriert sich direkt in die Verwaltungsinfrastruktur, wodurch der Service schnell für verwaltete Geräte bereitgestellt werden kann. Die Integration erleichtert auch die Überwachung von Ereignissen und die Suche nach Bedrohungen für ThreatOps, indem sie den Meldungen durch Menschen lesbare Namen hinzufügt.

Jamf Threat Defense funktioniert nahtlos mit Ihren bestehenden IT Services und Technologien.

Umfassende Integration in Microsoft, Google, Cisco und mehr helfen Ihnen, den Wert Ihres existierenden Technologie-Stacks zu erhöhen.

jamf

www.jamf.com/de

Weitere Informationen darüber, wie Threat Defense Benutzer, Mobilgeräte und Unternehmensdaten schützen kann, finden Sie unter www.jamf.com/de