Schneider Electric sichert 50.000 Geräte mit Lookout

Die Herausforderung

Schneider Electric ist ein führendes Unternehmen in der digitalen Transformation des Energiemanagements und der Automatisierung in Wohn- und Gewerbegebäuden, Rechenzentren und Infrastruktur in allen Branchen und entwickelt auf Basis eines modernen, technologieorientierten Konzepts erstklassige Energiemanagement- und Automatisierungssysteme für Kunden. Dem Unternehmen ist bewusst, dass eine kompetente, mobile Belegschaft notwendig ist, die sich auf ihre Mobilgeräte und -anwendungen verlassen kann, um Projekte erfolgreich durchzuführen und die Effizienz vor Ort zu steigern – nur so lassen sich sichere, zuverlässige, effiziente und nachhaltige Energielösungen erzielen.

Da Schneider mittlerweile mehr als 170.000 Mitarbeiter in über 100 Ländern beschäftigt, genießt IT-Sicherheit eine hohe Priorität. Beim Management von Mobilgeräten setzt Schneider auf eine Enterprise Mobility Management-Lösung (kurz EMM), um den Zugriff auf Unternehmensressourcen wie E-Mail und interne Anwendungen zu steuern; ein SIEM-System zur Zusammenführung von Sicherheits-relevanten Informationen, Single Sign-On für vereinfachten Zugang sowie weitere, herkömmliche Sicherheitsmaßnahmen zum Schutz der Unternehmensressourcen. Angesichts all dieser Maßnahmen musste noch ein Bereich abgedeckt werden: Der Schutz von Mobilgeräten und deren Nutzern.

Dieses Projekt wurde von Simon Hardy geleitet, Global Head of Office 365 Services and Enterprise Mobility bei Schneider. Simon Hardy wusste, dass eine MTD-Lösung (Mobile Threat Defense) den Schlüssel zum Schutz der mobilen Belegschaft darstellte. Er musste jedoch eine Lösung finden, die einfach in die bestehende Infrastruktur und die große Flotte an Mobilgeräten implementiert werden könnte. Für diese MTD-Lösung war es immens wichtig, eine einfache Integration in die EMM- und SIEM-Lösungen von Schneider zu ermöglichen, um durch eine Bedrohungserkennung und Unterstützung bei der Einhaltung strikter Compliance-Bestimmungen hinsichtlich Nutzer und interner Berichte durch Schneider unmittelbaren Wert zu schaffen.

Schneider Electric

Kundenprofil

Als führendes Unternehmen im Bereich Energiemanagement und Automatisierung mit Aktivitäten in über 100 Ländern hat Schneider die Vision, Kunden in einer stärker vernetzten, verteilten und intelligenten Welt mit steigendem Energiebedarf mit weniger Ressourcen mehr zu ermöglichen. Schneider Electric ist bestrebt, seinen Kunden durch innovative Technologielösungen und -dienstleistungen die effizienteste und nachhaltigste Nutzung von Ressourcen, Assets, Prozessen und Infrastrukturen zu ermöglichen.

Branche: Versorger/Managed Service

Die Lösung

Lookout Mobile Endpoint Security

Die Ergebnisse

- 50.000 Android- und iOS-Geräte weltweit gesichert
- Nahtlose Integration in bestehende SIEM-, SSO- und EMM-Plattformen
- Einsatz in der weltweiten Flotte im Zusammenspiel mit Microsoft Intune
- Plan für BYOD-Mobilitätsstrategie mit Nutzung von Lookout als standard MTD-Lösung für diese Geräte entwickelt

Sicherheitsspezifische Herausforderungen

- Implementierung eines Cybersicherheits-Tools zum Schutz von Nutzern, die über Office 365 Unternehmensdaten abrufen.
- Beleg für Auditoren, dass Cybersicherheits-Bedrohungen für Mobilgeräte erfolgreich bekämpft werden können, sowie detaillierte Sichtbarkeit der Nutzung von Mobilgeräten durch Mitarbeiter.
- Schutz einer schnell wachsenden weltweiten Belegschaft bei gleichzeitiger Anwendung zweier unterschiedlicher Mobilitätsrichtlinien

Die Sicherheitsstrategie von Schneider basierte auf Zugriffskontrolle statt auf dem Schutz der Geräte und Anwendungen selbst. Zudem wurden Maßnahmen getroffen, um ein sicheres Gateway und eine sichere Verbindung zu Unternehmensressourcen zu gewährleisten. Simon Hardy war jedoch klar, dass eine Absicherung aller Endpunkte erforderlich war, und die Mobilgeräte genossen über die bereits bestehenden Maßnahmen hinaus höchste Priorität bei der Absicherung.

Lösungskriterien

- Integration in bestehende EMM-, SSO-, SIEM- und weitere Sicherheitstools
- Schutz des geistigen Eigentums und Gewährleistung der Einhaltung diverser Compliance-Standards und -Vorschriften.
- Einfache Implementierung, Wartung und Verwaltung mit gleichzeitiger Schulung der Belegschaft zu mobilen Bedrohungen
- Leistungsfähige Bedrohungserkennung auf Grundlage eines großen Datensatzes mit minimalen False-Positives

Die Lösung

Schneider entschied sich für Lookout Mobile Endpoint Security und konnte so ein unmittelbares klares Bild der mobilen Sicherheit und Risikosituation seiner mobilen Nutzer erzielen. In dem Bewusstsein, dass sein Team vor einem umfangreichen Rollout stand, entschied sich Simon Hardy, den Rollout in mehreren Phasen vorzunehmen. Als Erstes wurden Schlüsselpersonen in der Produktion geschützt und dabei bewertet, ob die Lösung den Anforderungen und Erwartungen genügen würde. Nachdem Lookout sechs Monate lang die Erwartungen stetig übertroffen hatte, steigerte Schneider den Umfang der Bereitstellung um das 20-Fache. Nach einem Jahr erweiterte das Unternehmen die Absicherung auf alle 50.000 Geräte der Flotte.

„Lookout ist im Bereich Mobile Security sehr bekannt und schützt bereits über 170 Millionen Geräte. Während unserer Bewertung stellte sich zudem heraus, dass Lookout die reifste Lösung darstellte, und wir waren daher bei unsere Entscheidung, den Marktführer zu beauftragen, sehr zuversichtlich."

Lookout ergänzte nicht nur die bestehenden Sicherheitstools, sondern schloss zudem eine Lücke im Sicherheitsumfeld von Schneider. Durch die Kombination von Lookout mit EMM wird der Zustand des Geräts beim Zugriff auf Unternehmensressourcen kontinuierlich geprüft. So wird sichergestellt, dass nur „gesunde" Geräte auf Unternehmensdaten zugreifen, um das Risiko für das Unternehmen zu minimieren. Durch die Implementierung von Lookout auf Mitarbeitergeräten über EMM und eine einfache Aktivierung konnte Schneider die Lösung für seine umfangreiche mobile Belegschaft problemlos bereitstellen.

Die Ergebnisse

Nun, da 50.000 Android- und iOS-Geräte mittels Lookout geschützt sind, erfüllt Schneider interne und externe Sicherheitsanforderungen und hat einen einzigartigen Einblick in die Risiken im Mobilbereich. Der für Back-End-Administratoren und Nutzer geradlinige Bereitstellungsprozess machte es leicht, bei jedem Schritt der Umsetzung vollständige Abdeckung zu erzielen.

Als weltweites Unternehmen muss Schneider seine Mitarbeiter kontinuierlich vor Angriffen vor Ort schützen. Dies erreicht das Unternehmen durch präzise, unmittelbare Erkennung von Man-in-the-Middle-Angriffen mit einer extrem niedrigen False-Positives Rate und durch die Befolgung der Sicherheits- und Datenschutzgesetze von über 100 Ländern, was über die Erstellung von Richtlinien im Backend der Lookout-Plattform möglich ist.

Nach dem Abschluss des Lookout-Rollouts auf über 50.000 COPE-Geräten plant Schneider nun, ein BYOD-Programm für Mitarbeiter zu starten und weitere 25.000 Geräte mit Lookout zu sichern. Der erwiesenermaßen einfache Umsetzungsprozess und der unmittelbare Nutzen der KI-gestützten Bedrohungserkennung von sowohl App-basierten als auch gerätebasierten Bedrohungen hat Schneider überzeugt, Lookout als integralen Bestandteil bei der Ausweitung seines Mobilitätsprogramms weltweit zu nutzen.

Mit Lookout konnte Schneider eine vollständige mobile Sicherheitsstrategie entwickeln und ein komplexeres Mobilitätsprogramm mit einfacher Bereitstellung, unmittelbarer Sichtbarkeit der App- und Geräterisiken sowie Einhaltung interner und externer Sicherheitsanforderungen weltweit umsetzen