FORESCOUT

HAWORTH®

Haworth

Weltweit tätiger Hersteller sichert mit Forescout das IT- und OT-Netzwerk und kann so die Rendite deutlich steigern

BRANCHE

Fertigung

UMGEBUNG

12.000 verkabelte und drahtlose Geräte an 20 Produktionsstandorten und 55 Vertriebsbüros weltweit; 6.200 Mitarbeiter

HERAUSFORDERUNG

- Fehlender Überblick über alle Geräte im Netzwerk, einschließlich IoT- und OT-Geräte
- Unzureichende Einsicht in die Sicherheitshygiene neu übernommener Unternehmen
- Bedürfnis kontinuierlicher Betriebsbereitschaft von OT-Umgebungen
- Kleines Sicherheitsteam mit begrenzter Zeit und Ressourcen

LÖSUNG

- Forescout-Plattform
- Forescout Enterprise Manager
- Forescout eyeExtend für Palo Alto Networks Next-Generation Firewall

ANWENDUNGSSZENARIEN

- Gerätetransparenz
- Geräte-Compliance
- Netzwerkzugriffssteuerung
- Netzwerksegmentierung
- Reaktion auf Angriffe

Überblick

Mit einem Fokus auf Innovation und Produktivität ist Haworth Inc. als Designer und Hersteller anpassbarer Büromöbel tätig. Dazu gehören Doppelböden, Stellwände, System- und Sitzmöbel sowie verkabelte und drahtlose Workware™-Technologiegeräte für Echtzeit-Zusammenarbeit. Dieses internationale Unternehmen mit deutschen Niederlassungen in Berlin und Frankfurt beschäftigt 6.200 Mitarbeiter und verfügt über 20 Produktionsstandorte und 55 Vertriebsbüros. Nach der kürzlichen Übernahme mehrerer Firmen für Lifestyle-Design benötigte Haworth Netzwerkzugriffssteuerung (Network Access Control, NAC), mit der nur autorisierte Geräte Zugriff erhalten, die den Sicherheitsstandards des Unternehmens entsprechen.

Um die NAC-Anforderungen zu erfüllen sowie andere Sicherheitslücken (z. B. die Erkennung und Eindämmung nicht autorisierter Geräte) zu schließen, implementierte Haworth die Forescout-Plattform. Dank der detaillierten Transparenz und Kontrollfunktionen konnte die Forescout-Lösung die Sicherheit der IT- und Produktionsumgebungen erheblich verbessern. Die Integration der Unternehmensfirewall erlaubte die Automatisierung der Sicherheitsaufgaben, sodass das Informationssicherheitsteam von Haworth deutlich entlastet wurde. Auch jenseits des Sicherheitsbereichs erwies sich die Forescout-Plattform als nützlich, sodass sie zusätzlich in anderen operativen Bereichen, wiez. B. beim Netzwerk-Management, eingesetzt wird.

Geschäftliche Herausforderung

„In diesen und anderen Anwendungsszenarien benötigten wir nicht nur größere Transparenz und Kontrollfunktionen, sondern auch die Möglichkeit, Geräte zu klassifizieren, Netzwerke nach Geräten zu segmentieren und nach Kompromittierungsindikatoren zu suchen – jeweils in Echtzeit.“

— Joseph Cardamone, Senior Information Security Analyst und Nord-Amerika Privacy Officer bei Haworth

Joe Cardamone ist Senior Information Security Analyst und Nord-Amerika Privacy Officer und in dieser Rolle für die Sicherheitsstrategie bei Haworth verantwortlich. Cardamone ist Teil des 3-Personen-Informationssicherheitsteams und soll gemeinsam mit seinen Kollegen alle globalen Unternehmens- und Produktionsumgebungen von Haworth schützen. Die neuesten Übernahmen zahlreicher autonom geführter Firmen haben diese Herausforderung nur noch weiter vergrößert.

ERGEBNISSE

- Schnelle Rendite: 97 Prozent der Endgeräte wurden innerhalb der ersten sieben Stunden ohne zusätzliche Konfiguration erkannt und kategorisiert
- Echtzeit-Geräte-Transparenz, sobald diese sich mit dem Netzwerk verbinden
- Vereinfachter Schutz von OT-Geräten und dauerhaft mobilen Geräten dank dynamischer Netzwerksegmentierung
- Netzwerkzugriffssteuerung für neu erworbene Unternehmen, die mit dem Unternehmensnetzwerk verbunden werden
- Einsparung von 20 Stunden pro Woche durch Automatisierung von Sicherheitsprozessen
- Weitere Zeiteinsparungen durch die Automatisierung manueller Prozesse zur Suche und Isolation stark gefährdeter Geräte
- Maximierung der Effizienz des 3-Personen-IT-Sicherheitsteams
- Detaillierte Transparenz zur Unterstützung der Sicherheit, IT-Gruppen und des Netzwerkteams
- Erkennung von 60 Prozent mehr Geräten als erwartet

Dabei waren die Geräte der neuen Partner nicht die einzigen Assets, für die mehr Transparenz und Kontrolle erforderlich waren. Das Team benötigte zum Beispiel eine bessere und schnellere Möglichkeit, stark gefährdete IoT-Geräte zu erkennen und zu verhindern, dass diese Kommunikationen ohne Befugnis erhalten oder übertragen. Außerdem mussten die IT-Sicherheitsverantwortlichen problemlos in der Lage sein, die eigenen proprietären digitalen Workware-Zusammenarbeitsgeräte zu identifizieren und abzusichern, da sich diese konstant zwischen verschiedenen Standorten bewegen und häufig aktualisierte Software und Hardware erhalten.

Gründe für Forescout

Ein leicht implementierbares, anwenderfreundliches Informationszentrum

Cardamone und sein Team führten Proof-of-Concepts für die Forescout-Plattform und die Lösung eines anderen Anbieters durch, der bereits intensiv im Unternehmen eingesetzt wurde und ursprünglich vom Haworth-Netzwerkteam präferiert wurde. Forescout ging hier als klarer Gewinner hervor.

„Die Forescout-Plattform ist ein Informationszentrum, das im Gegensatz zu unserer Alternative leicht implementierbar und sehr anwenderfreundlich ist“, meint Cardamone. „Ich erhalte eine zentrale Übersicht über unsere gesamte Umgebung – mit genauen Details und der Möglichkeit, den Schutz mit einem Mausklick zu verwalten. Die Benutzeroberfläche ist sehr intuitiv und die präsentierten Informationen sind selbst für neue Teammitglieder und nicht sicherheitsbezogene Abteilungen, wie beispielsweisedem Netzwerkteam, nützlich.“

Auswirkungen auf das Unternehmen

Schnelle Bereitstellung und Rendite mit Standardkonfiguration

Die Bereitstellung der Forescout-Plattform nahm weniger als einen Tag in Anspruch „Wir starteten die Implementierung zur Mittagszeit, und als ich meinen Computer am gleichen Abend hochfuhr, waren 97 Prozent unserer Umgebung bereits erkannt und klassifiziert“, erinnert er sich. „Innerhalb von sieben Stunden erhielten wir also einen vollständigen Überblick über unsere globale Umgebung. Das ist beeindruckend.“

Vorteile umfassender, detaillierter Transparenz von Anfang an deutlich

Sofort nach der Implementierung wurden die Vorteile des genauen Überblicks durch die Forescout-Plattform deutlich. „Wir dachten, dass wir etwa 7.500 Geräte in unseren Netzwerken hätten. Die Forescout-Plattform entdeckte jedoch mehr als 12.000 IP-Adressen“, erklärt Cardamone. „Zudem stellten wir bislang unbekannte Sicherheitslücken fest, zum Beispiel dutzende drahtlose Zugriffspunkte in unseren Ausstellungsräumen. Dank dieser neuen Transparenz konnten wir diese Geräte blockieren und die Administratoren vor Ort anweisen, sich darum zu kümmern.“

„Doch das ist nur die Spitze des Eisbergs“, ergänzt Cardamone. „Der Umfang der Daten, die wir von der Forescout-Plattform erhalten, ist einfach unglaublich. Während viele andere Tools lediglich die IP-Adressen der Endgeräte erkennen, ist das die bei weitem beste Lösung zur Erkennung, Identifizierung und Kontrolle von Systemen, die ich bisher gesehen habe. Sie hat ihren Mehrwert für uns deutlich bewiesen.“

> *„Der Umfang der Daten, die wir von der Forescout-Plattform erhalten, ist einfach unglaublich. Während viele andere Tools lediglich die IP-Adressen der Endgeräte erkennen, ist sie das bei weitem beste Tool zur Erkennung, Identifizierung und Kontrolle von Systemen, die ich bisher gesehen habe. Sie hat ihren Mehrwert für uns deutlich bewiesen.“*
>
> **— Joseph Cardamone, Sr. Information Security Analyst und Nord-Amerika Privacy Officer, Haworth**

„Die Maßnahmen für Endgeräte lassen sich meist automatisieren, doch auch manuelle Eingriffe erfordern lediglich einen einfachen Mausklick“, fährt Cardamone fort. „Ich kann Mitarbeitern der Stufen 1 oder 2 im Notfall auch Aktionen der Stufe 3 freischalten, ohne ihnen Zugriff auf privilegierte Funktionen gewähren zu müssen. Die Forescout-Plattform verfügt bereits in der Standardkonfiguration über leistungsstarke Funktionen und ist zudem weiter anpassbar. Unsere Möglichkeiten sind damit praktisch unbegrenzt.“

Überblick über Gerätehygiene der übernommenen Unternehmen

Die Forescout-Plattform liefert Transparenz zu den übernommenen Unternehmen sowie zur jeweiligen Gerätehygiene. „Wenn die Geräte seit längerer Zeit nicht gepatcht wurden, sehen wir das und können Maßnahmen ergreifen“, erklärt Cardamone. „Die Forescout-Plattform prüft außerdem den Patch- und Virenschutz-Status sowie das Betriebssystem aller Partnergeräte, die sich mit dem Unternehmensnetzwerk zu verbinden versuchen. Wenn die Geräte unsere Kriterien nicht einhalten, werden sie blockiert.“

Vereinfachte und gleichzeitig stärker anpassbare Netzwerksegmentierung

Mit dem Forescout eyeExtend für Palo Alto Networks® Next-Generation Firewall-Modul konnte Cardamone die Forescout-Plattform schnell mit der Unternehmensfirewall integrieren, und ermöglicht somit die spontane Netzwerksegmentierung basierend auf den genauen, kontextbezogenen Echtzeit-Informationen der Forescout-Lösung. „Dank der Forescout-Palo Alto Networks-Integration basiert unsere Segmentierung nicht mehr nur auf einfachen Eigenschaften wie IP- oder VLAN-Adresse“, erläutert Cardamone. „Wir haben deutlich mehr Optionen als nur mit 802.1X, da die Segmentierung auf einem detaillierteren und umfassenderen Endgeräteprofil basieren kann.“

So verwendet Cardamone die Forescout-Plattform zum Beispiel auch in der Haworth-Fertigungsumgebung zur Identifizierung und Klassifizierung aller besonders gefährdeten IoT-Geräte. Das sind vor allem die Geräte, die vom Hersteller nicht mehr unterstützt werden, da sie zum Beispiel mit Windows® XP- oder Windows 2000-Betriebssystemen laufen. Die dynamische Netzwerksegmentierung verhindert anschließend automatisch, dass diese Geräte – außer unter streng reglementierten Umständen – Daten empfangen oder übertragen können.

Erhebliche, quantifizierbare Zeiteinsparungen durch Integration und Automatisierung

Durch die Forescout-Palo Alto Networks-Integration konnte Haworth aufwändige manuelle Prozesse automatisieren. Ein Beispiel hierfür sind die Haworth Workware-Technologiegeräte, die sich in den Haworth-Zentralen und den Ausstellungsräumen in aller Welt befinden. Diese Geräte nutzen VLANs und erhielten in der Vergangenheit statische IP-Adressen, damit sie durch die Firewall mit dem Gastnetzwerk kommunizieren können. Allein in den Unternehmenszentralen befinden sich 130 dieser Geräte, sodass manuelle Prozesse zur Aktualisierung sowie Anpassung der Hardware und Software sowie physische Standortwechsel, die mit neuen IP-Adressen einhergehen, zu langsam waren, um angemessene Netzwerkzugriffsteuerungen zu ermöglichen.

Heute werden diese Geräte von der Forescout-Plattform erkannt, klassifiziert und in eine dynamische Zugriffsgruppe sortiert, die mit einer Firewallrichtlinie verbunden ist und den zugehörigen IP-Adressen die Kommunikation mit dem Gastnetzwerk über die erforderlichen Ports und Anwendungen erlaubt. „Wenn das Gerät also nach China oder Deutschland verschickt und dort eingesetzt wird, wird es von Forescout erkannt und die Firewall legt die korrekten Einstellungen fest“, sagt Cardamone. „Der bisherige kontinuierliche, fast unmöglich umsetzbare manuelle Prozess wurde vollständig automatisiert.“

„Wenn ich all die Zeit zusammenrechne, die wir seit der Installation der Plattform und der Integration mit unserer Firewall in den verschiedenen Anwendungsszenarien gespart haben, komme ich auf etwa 20 Stunden pro Woche bzw. eine halbe Vollzeitstelle“, sagt Cardamone. „Dadurch kann unser kleines Sicherheitsteam unsere Umgebung mit weniger Aufwand besser schützen.“

Vorteile der Forescout-Transparenz jenseits der Sicherheit

Auch die operativen Haworth-Mitarbeiter profitieren von der Forescout-Plattform. Das Techniksupport-Team kann damit den physischen Standort der Geräte feststellen, die Softwareverwaltung prüft Geräte auf nicht konforme Anwendungen und das Netzwerkteam ruft einmal wöchentlich Informationen zu allen Ports und Switches ab. Und es kommen noch weitere Anwendungsmöglichkeiten hinzu. So wird Forescout eine wichtige Rolle spielen, wenn das Unternehmen zukünftig zu einer BYOD-Richtlinie wechseln wird.

Weitere Informationen finden Sie unter **www.Forescout.de**

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Telefon (International):
+1-408-213-3191
Support: +1-708-237-6591