Winkelmann Group

Winkelmann nutzt Forescout, um Risiken zu reduzieren und Audit-Anforderungen zu erfüllen

In 2 Stunden	> 170%	Mehrere Tage
zu umfassender Transparenz	**mehr Geräte entdeckt**	**Zeitersparnis pro Monat für das SecOps-Team**

SEKTOR

Produktion

UMGEBUNG

- 6.800 kabelgebundene und kabellose Geräte auf drei Kontinenten
- 4.300 Beschäftigte

HERAUS-FORDERUNG

- Mangelnde Übersicht über die vernetzten Geräte – IT, IoT und OT
- Einhaltung der TISAX-Sicherheitsanforderungen für die Automobilbranche
- Minimierung der Gefahr von Geschäftsunterbrechungen durch Cyberangriffe

Überblick

Die Winkelmann Group ist ein international aufgestellter, auf hochmoderne Metallbearbeitungsverfahren spezialisierter Hersteller mit Kernkompetenz in der Automobil-, Heizungs- und Wasserindustrie. Durch die Implementierung der Forescout Continuum-Plattform gewann das in Ahlen ansässige Unternehmen umfassende Transparenz über seine Umgebung, die vernetzte IT-, IoT- und OT-Geräte in seinen Produktionsstätten in Europa, Asien und Nordamerika umfasst. Zudem profitiert Winkelmann jetzt von präziser Asset-Inventarisierung in Echtzeit, kontinuierlicher Compliance für alle Geräte, Funktionen zur Netzwerkzugriffssteuerung (NAC) und mehr. All das trägt dazu bei, das Risiko von Sicherheitsverletzungen oder Betriebsstörungen zu minimieren.

„Wir brauchten Netzwerkzugriffskontrolle und Netzwerksegmentierung, doch zuerst mussten wir genau wissen, was sich in unseren Netzwerken befindet."

— Niklas Kaiter, System- und Netzwerkadministrator, Winkelmann Group

Die geschäftliche Herausforderung

Um die Zertifizierung nach TISAX zu erhalten, einem in der deutschen Kfz-Industrie unerlässlichen Prüfverfahren für Informationssicherheit, musste die Winkelmann Group NAC und Netzwerksegmentierung umsetzen. Zudem hatten sich in dem Unternehmen einige Virenvorfälle ereignet, die den Betrieb von Endgeräten und Servern unterbrachen. Zum Glück gelang es dem IT-Team, die Rechner nach diesen Vorfällen vollständig wiederherzustellen. Die Cyberangriffe sowie das Feedback aus Audits veranlassten die Geschäftsleitung jedoch, den Cybersecurity-Ansatz zu überdenken und in geeignete Lösungen zu investieren, um die Benutzer und Geräte besser zu schützen. Erstes Ziel war dabei die Fähigkeit, alle vernetzten Geräte zu sehen.

LÖSUNG

- Forescout Continuum-Plattform
- Forescout eyeExtend

ANWENDUNGS-FÄLLE

- Asset-Inventarisierung
- Asset-Compliance
- Netzwerkzugriffskontrolle

ERGEBNISSE

- Schnelle Wertschöpfung – umfassende Transparenz über alle IT-, IoT- und OT-Assets binnen zwei Stunden
- Erstes präzises Echtzeit-Inventar aller Geräte nach nur einem halben Tag
- Das SecOps-Team spart täglich Stunden bei der Netzwerk- und Geräteverwaltung
- Minimierung des Risikos von Sicherheitsverletzungen dank automatischer, kontinuierlicher Bewertung des Sicherheitsniveaus aller vernetzten Geräte
- Schnellere Erkennung und Behebung von Schwachstellen
- Einfachere Erstellung und Durchsetzung von Richtlinien
- Fundament für Ökosystem-Integrationen und Netzwerk-segmentierung

Warum Forescout?

Nach der Sondierung potenzieller NAC- und Segmentierungslösungen nahm die Winkelmann Group vier Anbieter in die engere Wahl. „Forescout bot ein erheblich breiteres Funktionsspektrum und wesentlich umfassendere Sichtbarkeit als alle anderen Lösungen und war viel einfacher zu implementieren“, erinnert sich Niklas Kaiter, System- und Netzwerkadministrator bei der Winkelmann Group. „Die anderen Lösungen boten entweder zu wenig Funktionen oder waren zu kompliziert und zeitaufwändig in der Implementierung. Die Forescout Continuum-Plattform war deutlich flexibler, mit einem intuitiven Dashboard, leichtem Zugriff auf detaillierte Daten und nahtloser Integration mit zahlreichen anderen Tools und Systemen, die wir einsetzen.“

Geschäftliche Auswirkung

Umfassende Übersicht binnen Stunden, einschließlich IoT und OT

„Wir hatten die Zahl unserer Geräte ursprünglich auf rund 2.500 geschätzt, aber die Plattform von Forescout erkannte schon in der Testphase 5.000 Geräte, darunter IoT- und OT-Assets, die wir noch nie gesehen hatten“, berichtet Kaiter. „In nur zwei Stunden hatten wir weitreichenden Überblick gewonnen, wobei die meisten Assets automatisch klassifiziert wurden. Die Umstellung vom Testbetrieb zum produktiven Einsatz dauerte ebenfalls nur zwei, drei Stunden. Innerhalb eines halben Tages konnten wir mit wenigen Klicks auf dem Forescout-Dashboard ein genaues Echtzeit-Geräteinventar erstellen. Am Ende sahen wir insgesamt 6.800 Geräte – also über 170 % mehr, als wir ursprünglich vermutet hatten.“

Mehr Sicherheit durch leichtere Umsetzung der Gerätekonformität

Die Winkelmann Group hat die Sicherheit erhöht, indem sie das Sicherheits-niveau aller vernetzten Geräte – IT, OT und IoT – durch die Continuum-Plattform automatisch und kontinuierlich bewerten lässt. Sobald ein Gerät versucht, sich mit dem Netzwerk zu verbinden, prüft die Plattform, ob auf dem Gerät eine Antiviren-Software installiert ist und läuft, ob die Windows-Firewall aktiviert ist, ob das Gerät über die neuesten Windows-Updates verfügt und ob es sich im richtigen VLAN befindet. Wenn beispielsweise die Antiviren-Software nicht läuft, versucht die Plattform, sie zu aktivieren. Falls sich die Einhaltung der Richtlinien nicht automatisch erreichen lässt, wird ein Administrator benachrichtigt, der dann manuell eingreifen kann, beispielsweise durch Verschieben des Geräts in ein anderes VLAN.

„Neben Problemen mit der Gerätehygiene deckt Forescout auch gravierende Schwachstellen und Bedrohungen auf. Dazu zählen etwa die Nutzung von Anwendungen, die auf der Blacklist stehen, oder Zugriffe firmenfremder Laptops auf unser Netzwerk via VPN“, so Jan-Erik Strauss, ebenfalls System- und Netzwerkadministrator. „Wir stoßen immer noch fast wöchentlich auf neue Dinge, die wir ohne Forescout niemals bemerkt hätten.“

„Forescout deckt gravierende Schwachstellen und Bedrohungen auf ... Wir stoßen immer noch fast wöchentlich auf neue Dinge, die wir ohne Forescout niemals bemerkt hätten."

— *Jan-Erik Strauss, , System- und Netzwerkadministrator, Winkelmann Group*

Geringerer Aufwand für das Netzwerkmanagement

Zudem erleichtert die Continuum-Plattform dem kleinen Team aus Sicherheits- und Netzwerkadministratoren bei Winkelmann die Aufgaben und spart so mehrere Tage Arbeit pro Monat. Um nur ein Beispiel zu nennen: Nachdem das Unternehmen in den letzten Jahren von einer lokalen Antiviren-Lösung auf eine cloudbasierte umgestiegen war und dabei Agenten deinstalliert und neu installiert wurden, fehlte nun auf einigen Endgeräten der Virenschutz. „Mit Forescout konnten wir nicht nur leicht erkennen, wie viele Geräte betroffen waren, sondern auch genau feststellen, welche es waren und wem sie gehörten", berichtet Strauss. „Die detaillierten Geräteinformationen, die Forescout liefert, sind enorm wertvoll und sparen uns in vieler Hinsicht Zeit."

„Die Forescout Continuum-Plattform ist enorm leistungsfähig und dabei sehr einfach einzurichten und zu nutzen", so Strauss weiter. „Bei der Konfiguration der Plattform brauchten wir kaum externe Hilfe. Das Dashboard ist intuitiv bedienbar, und neue Gruppen, Richtlinien und so weiter lassen sich sehr leicht erstellen."

„NAC, aber noch viel mehr"

Auch wenn die Winkelmann Group mit Forescout vom ersten Tag an Nutzen erzielte, hat sie die ganzheitlichen Funktionen der Continuum-Plattform noch längst nicht ausgeschöpft. Künftig will Winkelmann weitere Sicherheitsprozesse automatisieren, Netzwerksegmentierung implementieren und vom Monitoring zur Durchsetzung von Richtlinien übergehen, sowohl für die IT-Assets als auch die Maschinen im Fabrikeinsatz. Das Unternehmen hat die Plattform bereits in seine VMWare-Infrastruktur, die Firewalls und Active Directory integriert und erwartet, die Vorteile der nahtlosen Integration auch mit anderen Systemen in seiner IT-Umgebung nutzen zu können.

Auf die Frage, wie er die Continuum-Plattform im Gespräch mit Kollegen bewertet, antwortet Kaiter: „Man kann auch nur ein Viertel dessen investieren, was wir für die Plattform von Forescout aufwenden, aber dann erreicht man auch nur ein Viertel der Sicherheit oder noch weniger. Man hat dann einfach nicht den Funktionsumfang, den Forescout bietet ... Wir haben Forescout für die Netzwerkzugriffssteuerung angeschafft, doch jetzt nutzen wir die Lösung auch tagtäglich für das Gerätemanagement und können uns für die Zukunft viele weitere Anwendungsfälle vorstellen. Ja, es ist eine NAC-Lösung, aber eben noch viel mehr."

FORESCOUT

Forescout Technologies, Inc.

Gebührenfrei (US) 1-866-377-8771
Tel (intl) +1-408-213-3191
Support +1-708-237-6591

Erfahren Sie mehr auf Forescout.com