BELDEN

CASE STUDY

NAC in der Automobilindustrie – Das zusätzliche Maß an OT-Netzwerksicherheit und -kontrolle

Die praxiserprobte, herstellerunabhängige NAC-Lösung von Belden sichert die Betriebsnetzwerke eines der größten Automobilhersteller weltweit

Zusammenfassung

Weltweit stehen Firmen im Fokus von Cyberkriminellen, die versuchen sich Zugang zu Produktionsnetzwerken zu verschaffen – eine Gefahr, vor der sich Unternehmen schützen müssen, um wettbewerbsfähig zu bleiben. In einem global agierenden Unternehmen mit verteilten Produktionsstandorten, internationalen Sicherheitsstandards und hybriden Infrastrukturen bietet Belden mit macmon NAC (Network Access Control) eine praxiserprobte, herstellerunabhängige Lösung.

Über den Kunden

Bei dem Kunden handelt es sich um ein international tätiges Unternehmen aus der Automobilindustrie. macmon NAC von Belden wird in einer der modernsten Produktionsstätten der Welt eingesetzt.

macmon nac

Herausforderungen des Kunden

Der Kunde verwendet Profinet, ein in der Automatisierungsbranche weit verbreitetes Ethernet-basiertes Kommunikationsprotokoll.

Es bietet eine hohe Bandbreite und Echtzeitfähigkeit, was es für viele Anwendungen attraktiv macht. Die Verwendung von Profinet kann jedoch die Sicherheit gefährden, da es eine größere Angriffsfläche als herkömmliche Feldbussysteme bietet.

Definition der Lösung

macmon NAC von Belden wurde speziell für den Schutz von Profinet-Netzwerken vor Cyber-Attacken entwickelt und bietet die folgenden Funktionen:

- Beschränkung des Zugriffs auf Netzwerkressourcen auf autorisierte oder vertrauenswürdige Geräte
- Integration in bestehende Sicherheitslösungen
- Isolierung oder Quarantäne von problematischen oder kompromittierten Geräten mit der Herausforderung, die Produktion nicht zu unterbrechen

Implementierung / Projektpfad

Die spezifischen Anforderungen des Kunden wurden in einem Proof of Concept (POC) ermittelt und von den Cybersecurity-Experten von Belden in kurzer Zeit umgesetzt. Zusätzliche Investitionen in Hardware und Beratung waren nicht erforderlich. Spezielle Funktionalitäten wurden in nur wenigen Tagen in das Produkt integriert.

Eine Herausforderung bestand darin, eine einfache Möglichkeit zu schaffen, einen Produktionsbereich oder eine “Produktionsblase” für unbekannte Endgeräte vollständig abzutrennen.

Eine Herausforderung bestand darin, eine einfache Möglichkeit zu schaffen, einen Produktionsbereich oder eine „Produktionsblase“ für unbekannte Endgeräte vollständig abzutrennen.

Das bedeutet, dass alle Maschinen innerhalb der Blase weiterhin produzieren können, es sei denn, es erfolgt ein unmittelbarer Angriff auf ein bestimmtes Endgerät. Dadurch wird sichergestellt, dass sich potenzielle Bedrohungen nicht auf andere Bereiche einer Anlage ausbreiten können, indem ein künstliches Air Gap geschaffen wird. Außerdem sind weitere Teile des Systems in diesem Use Case nicht betroffen, bis das Problem behoben ist. macmon NAC basiert nicht auf einer obligatorischen Anwendung von RADIUS/802.1x. Es gibt andere Strategien zur Erkennung unerwünschten Verhaltens im Netzwerk für Systeme, die RADIUS/802.1x nicht verwenden können.

Funktionen von Advanced Security

macmon NAC Advanced Security von Belden bietet Kunden die folgenden Funktionen:

- Identifizierung der Betriebssysteme von Geräten, die mit dem Netzwerk verbunden sind
- Standortname des Geräts (physischer Standort)
- Identifizierung von offenen und geschlossenen Ports (TCP & UDP)
- Überprüfung der erfolgreichen Anmeldung
- Systemname
- Active Directory Domänenname
- Zertifikatsautoritäten
- Fingerprinting
- Verhinderung von Sicherheitsvorfällen wie ARP-Spoofing, MAC-IP-Mismatch, MAC-Adressen-Flooding und MAC-Spoofing

Die wichtigsten Vorteile

macmon NAC von Belden verwendet mehrere Technologien, um Informationen über das Betriebssystem, den Domänennamen und die Netzwerk-Ports eines Endgerätes zu sammeln.
Dies verbessert die Netzwerktransparenz und hilft dem Administrator, Endgeräte besser zu klassifizieren, zu identifizieren und zu lokalisieren.

macmon NAC vergleicht die gesammelten Informationen mit vorhandenen Daten, um ARP-Spoofing und Angriffe zu verhindern. Es erkennt und stoppt Man-in-the-Middle-Angriffe, schlägt Alarm und isoliert Geräte mit doppelten IP-Adressen.

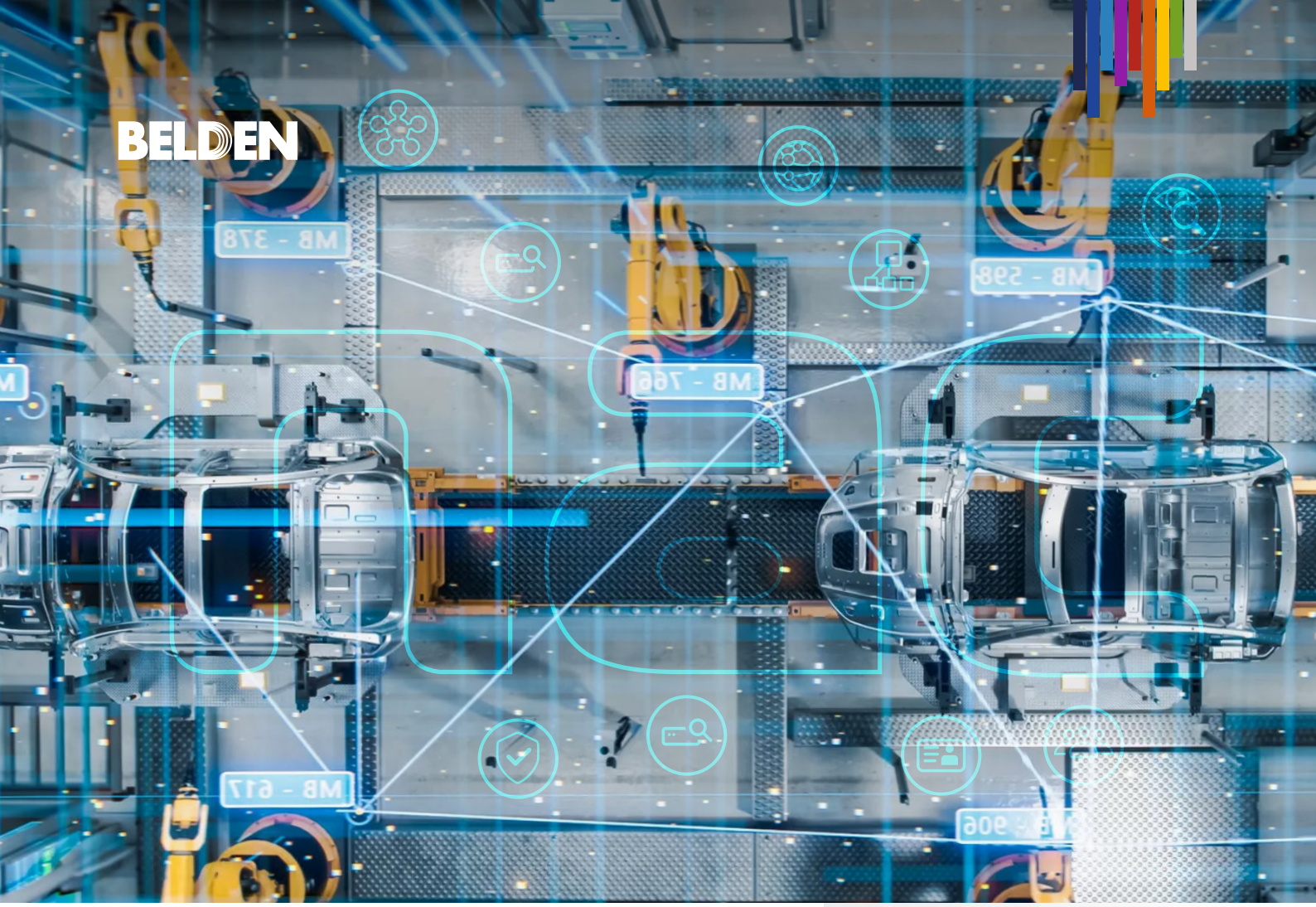
Mit macmon NAC Advanced Security wird jedes Gerät untersucht, das in das Netzwerk gelangt. Es kann mit Geräten über deren IP-Adresse kommunizieren. Es kann auch überprüfen, ob das Endgerät dasselbe oder ein ähnliches ist wie jenes, das zuvor autorisiert wurde. Ist dies nicht der Fall, kann es das Gerät aus dem Netzwerk entfernen oder in ein Quarantäne-Netzwerk verschieben.

Dort kann der Bedrohungsgrad und die Aktivität des Geräts in einer sicheren Umgebung überprüft werden. Alternativ kann das Ereignis auch einfach gemeldet oder protokolliert werden

Eine andere Möglichkeit, das Gerät zu überprüfen, ist SSH, ein Fingerprinting-Protokoll.
Der SSH-Fingerabdruck kann jeden Client eindeutig identifizieren. TLS (Transport Layer Security) wird für zusätzliche Zertifikatsprüfungen verwendet. Weitere Protokolle sind für die Überprüfung verfügbar.

macmon NAC von Belden kann periodisch überprüfen, ob die Geräte noch auf dem neuesten Stand sind, indem ein Zeitwert in der Weboberfläche hinterlegt wird, z. B. 60 Minuten.

Durch den Einsatz von Beldens macmon NAC Advanced Security hat das beschriebene Unternehmen ein zusätzliches Maß an OT-Netzwerksicherheit und -kontrolle für seine Fertigungsprozesse erreicht – ohne negative Auswirkungen auf die Verfügbarkeit der Produktionsumgebung.



Über Belden

Belden Inc. liefert die Infrastruktur, die den digitalen Wandel einfacher, intelligenter und sicherer macht. Unser Fokus liegt nicht nur auf der Verbindungstechnik, sondern auch auf dem, was wir durch ein leistungsorientiertes Portfolio, zukunftsorientiertes Know-how und maßgeschneiderte Lösungen möglich machen. Mit mehr als 120 Jahren Erfahrung in Sachen Qualität und Zuverlässigkeit verfügen wir über ein solides Fundament, auf dem wir auch in Zukunft aufbauen können. Wir haben unseren Hauptsitz in St. Louis und verfügen über Produktionsstätten in Nordamerika, Europa, Asien und Afrika. Für weitere Informationen, besuchen Sie uns auf www.belden.com und folgen Sie uns auf Facebook, LinkedIn und X/Twitter.

Mehr erfahren

Für weitere Informationen zu unseren Netzwerksicherheitslösungen besuchen Sie uns unter: www.belden.com/networksecurity