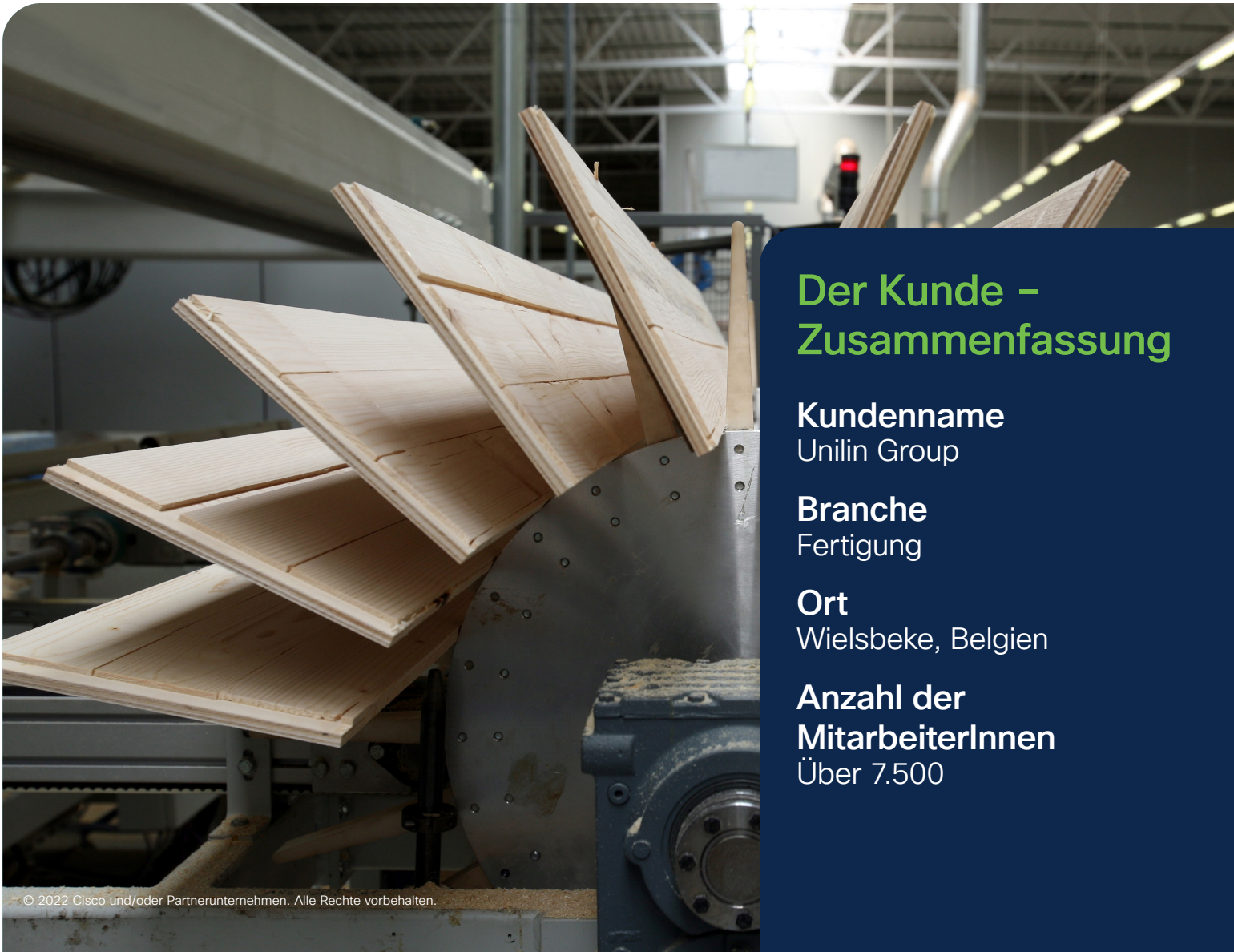


Unilin Group

Unilin schützt seine intelligente Produktion

Cisco Cyber Vision schafft einen zentralen Überblick über die IT und betriebliche Netzwerke, um IoT-Innovationen zu beschleunigen und Cyberbedrohungen abzuwehren



Der Kunde – Zusammenfassung

Kundenname
Unilin Group

Branche
Fertigung

Ort
Wielsbeke, Belgien

**Anzahl der
MitarbeiterInnen**
Über 7.500



Herausforderungen

- Die Automatisierung der Produktion beschleunigen, um die Wettbewerbsfähigkeit zu steigern
- Einblicke in betriebliche Netzwerke erhalten
- Produktionsteams die Möglichkeit bieten, neue IoT-Ideen zu testen



Lösungen

- Cisco® Cyber Vision
- Cisco Identity Services Engine
- Cisco DNA Center™
- Cisco Industrial Ethernet (IE) Switches der Serie 3400



Ergebnisse

- Standardisierte Netzwerkarchitekturen zur Steigerung der Effizienz
- Umfassender Überblick über Netzwerke zur Verbesserung der Produktionsleistung und Sicherheit
- Schaffung eines kollaborativen Workflows

Schaffung eines globalen Netzwerks aus Smart Factorys

Unilin ist ein weltweit führendes Unternehmen im Bereich Fußbodenbeläge. Auch wenn Ihnen der Name nicht geläufig ist, sind Sie mit großer Wahrscheinlichkeit schon einmal über eines seiner Produkte gelaufen. Für das Jahr 2020 meldete das Unternehmen einen Umsatz von 2,21 Milliarden Euro. Mit sechs Geschäftsbereichen und 15 Marken bedient das Unternehmen Geschäfts- und Privatkundenmärkte weltweit.

Das Wachstum wird durch internationale Expansion, Übernahmen und Produktdiversifizierung vorangetrieben. Unilin ist in den Bereichen Paneele, Isolierung, Technologien und Laminatfußböden tätig. Innovation und betriebliche Effizienz sind entscheidend. Unilin ist stolz darauf, „die Freiheiten eines Start-ups mit der Macht eines globalen Konzerns“ zu verbinden.

„Wir befinden uns in einem extrem wettbewerbsintensiven Markt. Wir investieren in eine noch stärkere Automatisierung unserer Fertigungsprozesse und in die Standardisierung unserer Fertigungsanlagen, damit alle unsere Werke weltweit von unserem Know-how profitieren können. So steigern wir die Effizienz und senken die Kosten“, so Pascal Pauwels, Infrastructure Director, Unilin Group.

Unilin produziert weltweit an 21 Standorten, unter anderem in Europa, Malaysia, Russland und den USA. Die größte Fertigungsstätte befindet sich jedoch nach wie vor in Belgien und von hier aus wird die weltweite Produktion gesteuert. „Unser belgisches Werk schafft einen globalen Industrie 4.0-Standard für alle unsere Standorte“, so Bruno Simoens, Network Architect bei Unilin. „Wir haben eine Menge Projekte am Laufen.“

„Zuvor hatten wir Firewalls im Einsatz. Doch wir hatten nur wenig Einblick in das Geschehen dahinter. Cisco Cyber Vision zeigt genau, welche Geräte angeschlossen sind, ihre Profile, wie viel Traffic sie erzeugen, was sie kommunizieren und wer Remote-Zugriff auf sie hat.“

Pascal Pauwels
Infrastructure Director, Unilin Group

Für diese kontinuierliche Innovation ist Cisco von zentraler Bedeutung. Der Cisco Industrial Ethernet (IE) Switch der Serie 3400 ist das Fundament dieses Standards für industrielle Verfahren. Damit kann Unilin die Netzwerkbereitstellung und -verwaltung in seinen Produktionslinien automatisieren, einen Überblick über die angeschlossenen Geräte gewinnen und die mit dem Betriebsteam festgelegten Sicherheitsrichtlinien durchsetzen.

Die Herausforderung für Unilin besteht darin, dafür zu sorgen, dass diese dicht vernetzte Betriebstechnologie (Operation Technology, OT) mit mehreren Access Points und Dauerbetrieb sicher bleibt. „Es handelt sich um hochspezialisierte Umgebungen mit zahlreichen Geräten und unterschiedlichen Sicherheitsanforderungen und viele Anbieter und Auftragnehmer sind in den täglichen Betrieb eingebunden“, so Simoens. „Wir benötigen Transparenz, Segmentierung und Kontrolle.“

In das Netzwerk integrierte Sicherheit zum Schutz der Produktion und des geistigen Eigentums

Cisco Cyber Vision verschaffte Unilin die nötige Transparenz in seiner Produktionsumgebung und ermöglichte eine stärkere Integration mit IT-Netzwerken, die nicht auf Kosten der Sicherheit ging. Cyber Vision ist in den Cisco IE3400-Switch integriert, erkennt alle angeschlossenen Geräte und erfasst anormale Verhaltensweisen und Cyberbedrohungen, um die Kontinuität der Produktion, die Ausfallsicherheit und den Schutz von geistigem Eigentum zu gewährleisten.

„Unsere vorhandenen industriellen Switches waren nicht alle mit SPAN-Ports ausgestattet, um den Traffic zu erfassen und einen Überblick über sämtliche Aktivitäten zu erhalten“, so Simoens. „Cyber Vision wird im Switch ausgeführt, was es uns sehr einfach macht, Daten aus allen Bereichen des Werks zu erfassen. Wir müssen OT nicht mit komplexen und kostspieligen Netzwerkeinrichtungen belasten und wir erhalten einen umfassenden Überblick.“

„Es handelt sich um hochspezialisierte Umgebungen mit zahlreichen Geräten und unterschiedlichen Sicherheitsanforderungen und viele Anbieter und Auftragnehmer sind in den täglichen Betrieb eingebunden. Wir benötigen Transparenz, Segmentierung und Kontrolle.“

Bruno Simoens

Network Architect, Unilin Group

Alle von Cyber Vision gesammelten Informationen werden mit anderen Tools wie Cisco DNA® Center und Identity Services Engine (ISE) geteilt. So kann das IT-Team von Unilin Sicherheitsrichtlinien erstellen und durchsetzen, ohne die Produktion zu behindern.

„Zuvor hatten wir Firewalls im Einsatz. Doch wir hatten nur wenig Einblick in das Geschehen dahinter. Cisco Cyber Vision zeigt genau, welche Geräte angeschlossen sind, ihre Profile, wie viel Traffic sie erzeugen, was sie kommunizieren und wer Remote-Zugriff auf sie hat“, so Pauwels. „Das war ein echter Game-Changer für uns. Wie kann man Geräte verwalten oder schützen, von denen man nichts weiß?“

Da Cyber Vision nun alle industriellen Endpunkte identifiziert, können IT- und OT-Teams bei der Erstellung von Sicherheitsrichtlinien zusammenarbeiten. Mit DNA Center kann das IT-Team Sicherheitsvorlagen direkt an den Switch senden und so ein Zero-Touch-Netzwerk schaffen. Die Netzwerkkonfiguration kann nun automatisiert werden, um das Risiko von Fehlern zu verringern und die Bereitstellung und das Änderungsmanagement zu vereinfachen. Dadurch wird der Aufwand für die OT-Teams reduziert und das Netzwerkteam kann global daran arbeiten, die Kosten weiter zu senken.

„Ohne die Hilfe des OT-Teams hätten wir das nicht geschafft. Das Team kennt die Fertigungsprozesse und die Geräte. Aber ohne die IT wäre ihm das nicht möglich gewesen. Der Aufbau zuverlässiger und sicherer Netzwerke ist unser Spezialgebiet“, so Pauwels.

Transparenz erhöht die Sicherheit und die Produktionseffizienz

Cisco Cyber Vision ermöglicht eine gemeinsame Vision des OT-Netzwerks und des Fertigungsprozesses. Auf diese Weise kann Unilin die Fertigungseffizienz verbessern und die Risiken von Sicherheitsbedrohungen eindämmen, die über das IT-Netzwerk in die Produktionsumgebung gelangen und umgekehrt.

„Glücklicherweise hatten wir bislang keine Sicherheitsprobleme“, so Simoens. „Cyber Vision hat uns jedoch gezeigt, wie anfällig unser industrielles Netzwerk ist. Die Lösung hat sofort eine lange Liste von Software-Schwachstellen in unseren Industriegeräten entdeckt. Außerdem wurde uns aufgezeigt, wie flach unsere Netzwerkarchitektur war. Die IT- und OT-Teams treffen sich nun wöchentlich, um all diese Punkte gemeinsam zu besprechen. Diese Transparenz hat uns geholfen, Vertrauen aufzubauen und so die Zusammenarbeit zu verbessern.“

„Vor allem aber unterstützt Cyber Vision unser Betriebsteam bei der Behebung von Produktionsproblemen“, so Simoens. „Wir hatten zum Beispiel das Problem, dass ein Lieferant Änderungen an einem Bauteil vorgenommen hat, die sich auf die Leistung des Fertigungsprozesses auswirkten. Mit Cyber Vision konnten wir diese Änderungen leicht als Ursache identifizieren, sodass wir sie schnell rückgängig machen konnten.“

„Es war wichtig, dass wir die Zustimmung der Mitglieder des OT-Teams hatten“, so Simoens. „Das ist ihre Umgebung und das sind ihre Switches. Als wir dem OT-Team zeigten, dass das Cisco Netzwerk Einblicke in die Vorgänge in der Fertigung ermöglichte, anhand derer das Team Fertigungsprobleme leichter lösen konnte, war es zum Austausch seiner vorhandenen Netzwerktechnik bereit. Dadurch konnten wir gleichzeitig die Sicherheit verbessern.“

„Als wir dem OT-Team zeigten, dass das Cisco Netzwerk Einblicke in die Vorgänge in der Fertigung ermöglichte, anhand derer das Team Fertigungsprobleme leichter lösen konnte, war es zum Austausch seiner vorhandenen Netzwerktechnik bereit. Dadurch konnten wir gleichzeitig die Sicherheit verbessern.“

Bruno Simoens

Network Architect, Unilin Group

Aufbau einer flexibleren und sichereren Produktionsumgebung

Der Einsatz von Cisco Cyber Vision kam für Unilin zu einem entscheidenden Zeitpunkt. Das Betriebsteam arbeitete an mehreren Industrie 4.0-Projekten, die neue Sicherheitsbedrohungen mit sich brachten. Und die Coronapandemie führte zu zahlreichen Störungen, die Unilin zwangen, seine Produktionsumgebung schnell anzupassen.

„Zu den größten Herausforderungen gehört derzeit die kontinuierliche Belieferung mit Material“, so Pauwels. „Die Verwaltung einer komplexen, globalen Lieferkette ist nicht einfach. Durch die Pandemie wurden viele Unbekannte geschaffen. Als Unternehmen müssen wir schnell reagieren.“

Industrie 4.0 ermöglicht es Unilin, seine Produktion zu optimieren, Material zu verfolgen und die Kapazität bei Bedarf zu erhöhen. Gleichzeitig ist es aber auch erforderlich, Maschinen mit neuen Anwendungen zu verbinden, Daten an externe Server zu senden und das Betriebsnetz für das Internet zu öffnen.

„Das OT-Team tat alles, was es konnte, um die Produktionsleistung zu erhöhen und die wachsende Kundennachfrage zu befriedigen“, so Simoens. „Als wir aber begannen, Cyber Vision zu nutzen, stellten wir fest, dass wir eine Menge Traffic von öffentlichen IP-Adressen in die Produktionsumgebung und eine Menge unkontrollierter Remote-Zugriffe auf Maschinen hatten. Das stellte eine große Bedrohung für unsere Produktionsabläufe, aber auch für unsere IT-Umgebung dar.“

Dank dieser Transparenz konnte Unilin Sicherheitsrichtlinien für die Verbindung von Geräten, Remote-Benutzern und Anbietern erstellen, um den Netzwerkzugriff offen und dennoch sicher zu halten und Innovationen in Zeiten der Pandemie umzusetzen.

„Mit Cisco Cyber Vision können wir auch kleinere Projekte in Angriff nehmen, um neue Benutzer und Industrieanlagen zu verbinden, und zwar auf sichere Weise,“ so Simoens. „Dass die Integration so einfach ist, gibt dem OT-Team und den BedienerInnen der Produktionsanlagen das nötige Vertrauen.“

Sicherheit, so Simoens weiter, ist nie ein Nullsummenspiel. Auch wenn das Netzwerk sicherer gemacht wird, ist das Risiko einer Sicherheitsverletzung nicht völlig ausgeschlossen. „Das ist wie bei Feuer- oder Rauchmeldern. Wir haben beides, aber das bedeutet nicht, dass es bei uns nie brennen kann. Mit Cisco Cyber Vision können wir zumindest das Ausmaß der Bedrohungslandschaft in unserem Netzwerk erkennen und entsprechend handeln.“

Produktliste

- [Cisco Cyber Vision](#)
- [Cisco Identity Services Engine \(ISE\)](#)
- [Cisco DNA Center](#)
- [Cisco Industrial Ethernet \(IE\) Switches der Serie 3400](#)

Weitere Informationen

Besuchen Sie: [cisco.com/go/iotmanufacturing](https://www.cisco.com/go/iotmanufacturing)