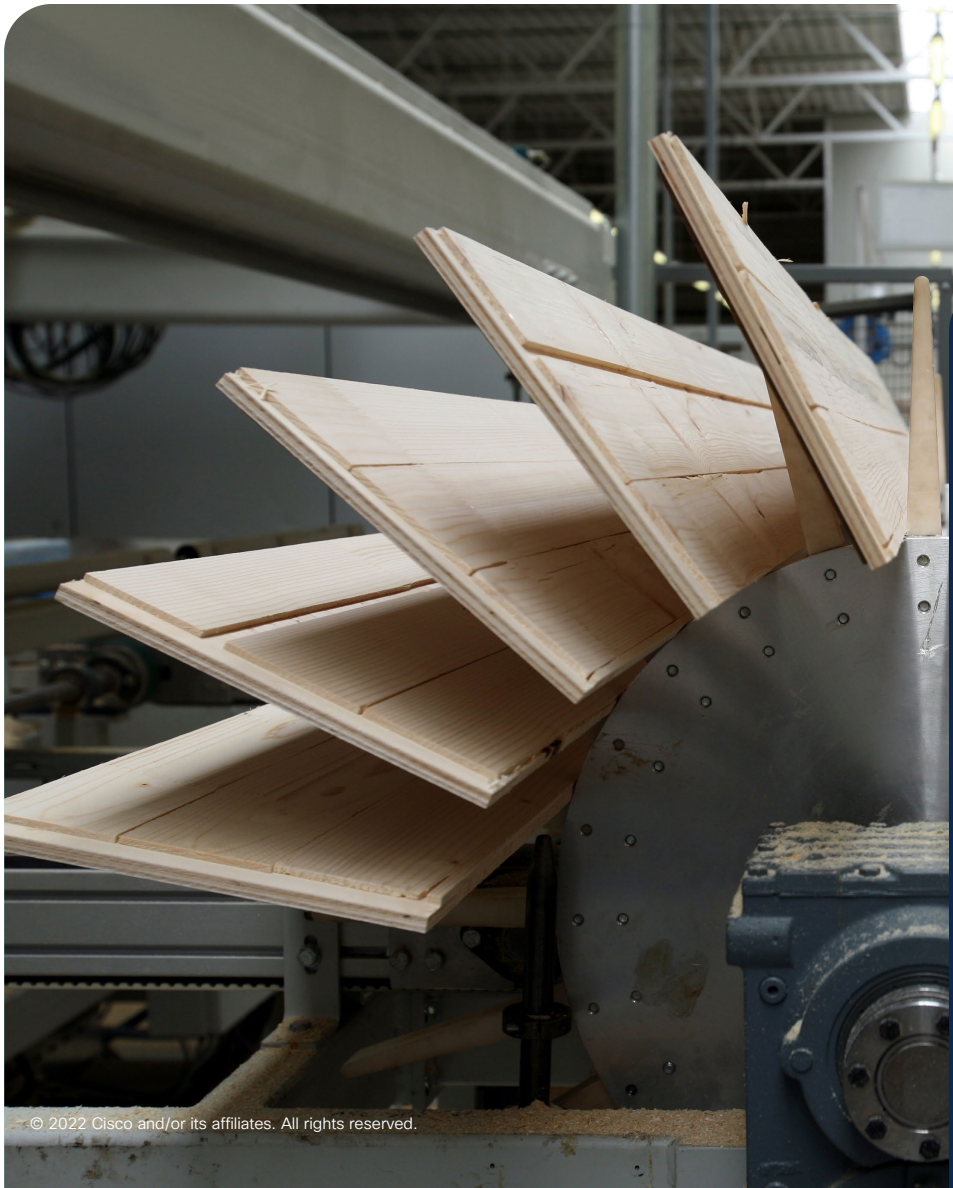
The bridge to possible

Unilin Group

Unilin Secures Its Smart Production

Cisco Cyber Vision creates single view of IT and operational networks to accelerate IoT innovation and mitigate cyber threats



The customer summary

Customer name
Unilin Group

Industry
Manufacturing

Location
Wielsbeke, Belgium

Number of employees
7,500+

The bridge to possible

Challenge

- Accelerate production automation to increase competitiveness
- Gain visibility into operational network
- Allow production teams to test new IoT ideas

Solution

- Cisco® Cyber Vision
- Cisco Identity Services Engine
- Cisco DNA Center™
- Cisco Industrial Ethernet (IE) 3400 Series Switch

Results

- Standardized network architectures to drive efficiency
- Built comprehensive view of networks to improve production performance and security
- Created a collaborative workflow

Creating a global network of smart factories

Unilin is a global leader in the flooring industry. You may not be familiar with the name, but there's a good chance you've walked across its products. The business reported revenues of €2.21 billion for 2020. It serves the business and residential markets worldwide, leveraging six business units and 15 brands.

Growth is driven by international expansion, acquisition, and product diversification. Unilin is active in panels, insulation, technologies, and laminate flooring. Innovation and operational efficiency are critical. Unilin boasts of having "the freedom of a start-up with the power of a multinational."

"We are in a very competitive market. We are investing to automate our industrial processes even more and standardize our industrial setups so that all our factories around the globe can benefit from our expertise to increase efficiency and lower their costs," says Pascal Pauwels, Infrastructure Director, Unilin Group.

Unilin's production is global–it has 21 factories worldwide, including Europe, Malaysia, Russia, and the US. But the largest production site remains in Belgium, and it is from here that global production takes its lead. "Our Belgian plant creates a global Industry 4.0 standard for all our factories to deploy," explains Bruno Simoens, Network Architect, Unilin. "We have a lot of projects underway."

> **"Previously, we had firewalls in place, but little visibility of what was behind each firewall. Cisco Cyber Vision gives us the visibility of exactly what devices are connected, their profiles, how much traffic they generate, what they are communicating, and who has remote access to them."**

Pascal Pauwels
Infrastructure Director, Unilin Group

Cisco is central to this relentless innovation. The Cisco Industrial Ethernet (IE) 3400 Series Switch is the cornerstone of this industrial operations standard. It allows Unilin to automate network deployment and management across its production lines, gain visibility on what devices are connected, and enforce security policies as defined with the operations team.

The challenge for Unilin is to ensure that this hyperconnected operational technology (OT), with multiple access points and operating around the clock, remains secure. "These are highly specialized environments with numerous devices having different security requirements, and many vendors and contractors are involved in daily operations," Simoens says. "We need visibility, segmentation, and control."

Security built into the network to protect production and intellectual property

Cisco Cyber Vision gave Unilin the visibility it needed in its industrial environment, enabling further integration with IT networks without compromising security. Built into the Cisco IE3400 switch, Cyber Vision recognizes everything that connects to it and detects anomalous behaviors and cyberthreats to ensure production continuity, resilience, and intellectual property protection.

"Our existing industrial switches didn't always have SPAN ports available to collect traffic and gain visibility on what's happening," explains Simoens. "Cyber Vision runs within the switch, making it very easy for us to collect data from every part of the factory. We don't need to bother OT with complex and costly network setups, and we have comprehensive visibility."

All the information collected by Cyber Vision is shared with other tools such as Cisco DNA® Center and Identity Services Engine (ISE) so that Unilin's IT team can build and enforce security policies that will not disrupt production.

"Previously, we had firewalls in place, but little visibility of what was behind each. Cisco Cyber Vision shows exactly what devices are connected, their profiles, how much traffic they generate, what they are communicating, and who has remote access to them," says Pauwels. "This is a game changer for us. How can you manage or secure something you are not aware of?"

Now that Cyber Vision identifies all industrial endpoints, IT and OT teams can work together to build security policies. DNA Center allows the IT team to push security templates directly to the switch, creating a Zero-Touch network. Network configuration can now be automated to reduce the risk of errors and simplify deployment and change management. This limits the effort needed from the OT teams and allows the network team to work on a global scale to further reduce costs.

"We couldn't do this without the help of the OT team. They know the industrial processes and the machines. But they couldn't do it without IT. Building reliable and secure networks is our expertise," explains Pauwels.

> "These are highly-specialized environments with numerous devices having different security requirements, and many vendors and contractors are involved in daily operations. We need visibility, segmentation, and control."
>
> **Bruno Simoens**
> Network Architect, Unilin Group

The bridge to possible

Visibility drives security and production efficiency

Cisco Cyber Vision enables a shared vision of the OT network and the industrial process, enabling Unilin to improve manufacturing efficiency and control risks of security threats reaching the production environment through the IT network, and vice versa.

"Fortunately, we've had no security issues," says Simoens. "But Cyber Vision revealed how vulnerable our industrial network was. It immediately detected a long list of software vulnerabilities in our industrial devices. And it highlighted how flat our network architecture was. IT and OT teams now have weekly meetings to address all these points together. This visibility helped us build trust to better work together.

"More importantly, Cyber Vision is helping our operations team fix production issues," says Simoens. "For example, we had a situation where a vendor made changes to a component and impacted the performance of the industrial process. Cyber Vision made it easy to identify those changes as the root cause so we could revert quickly."

"It was important we had the buy-in of the OT team," explains Simoens. "This is their environment; these are their switches. When we showed operations that the Cisco network could give them visibility into what's happening in their manufacturing plant so they could solve production issues, they were ready to replace their existing network equipment. And this helped us improve security at the same time."

Building a more agile and secure manufacturing environment

The use of Cisco Cyber Vision arrived at a critical moment for Unilin. The operations team had several Industry 4.0 projects introducing new security threats. And the COVID-19 pandemic created many disruptions, forcing Unilin to quickly adapt its manufacturing environment.

"One of the biggest challenges at the moment is a consistent supply of raw materials," says Pauwels. "It is not easy managing a complex, global supply chain. COVID has created many unknowns. As a business we need to react quickly."

Industry 4.0 allows Unilin to tweak its production, track raw materials, and scale up capacity when needed. But it also requires connecting machines to new applications, sending data to external servers, and opening the operational network to the internet.

"OT was doing everything they could to increase production outputs and meet growing customer demand," explains Simoens. "But when we started to use Cyber Vision, we realized we had a lot of traffic from public IP addresses into the industrial environment and a lot of uncontrolled remote accesses to machines. This was a major threat to our manufacturing operations, but also to our IT environment."

"When we showed operations that the Cisco network could give them visibility into what's happening in their manufacturing plant so they could solve production issues, they were ready to replace their existing network equipment. And this helped us improve security at the same time."

Bruno Simoens
Network Architect, Unilin Group

The bridge to possible

Gaining this visibility helped Unilin build security policies to connect devices, remote users, and vendors, so it could keep network access open yet secure and continue to innovate throughout COVID.

“Cisco Cyber Vision gives us the confidence to try smaller projects, to connect new users and industrial assets, securely,” says Simoens. “The simplicity of the integration gives confidence to the OT team and the production line operators.”

Security, Simoens adds, is never a zero-sum game. Making the network more secure doesn’t completely rule out the risk of a security breach. “It’s like fire or smoke detectors. We have invested in both, but that doesn’t mean we can never have a fire. Cisco Cyber Vision at least means we can see the scale of the threat landscape across our network, and act accordingly.”

Product list

- Cisco Cyber Vision
- Cisco Identity Services Engine (ISE)
- Cisco DNA Center
- Cisco Industrial Ethernet (IE) 3400 Series Switch

Learn More

Please visit: cisco.com/go/iotmanufacturing

01/22