FORESCOUT

Winkelmann Group

Winkelmann Reduces Risk and Meets Audit Requirements with Forescout

2 hours
to achieve comprehensive visibility

> 170%
more assets discovered

Days
saved each month by SecOps

INDUSTRY

Manufacturing

ENVIRONMENT

- 6,800 wired and wireless assets across three continents
- 4,300 employees

CHALLENGE

- Lack of visibility into all connected assets on the network, including IT, IoT and OT
- Meet TISAX security regulations for automotive industry
- Minimize risk of business disruption from cyberattack

Overview

The Winkelmann Group is a multinational manufacturer specializing in technologically advanced metal forming processes, with core business in the automotive, heating and water industries. By implementing the Forescout Continuum Platform, the Ahlen, Germany-based company gained comprehensive visibility across its entire organization, including IT, IoT and OT connected assets in its production facilities in Europe, Asia and North America. The company also gained accurate, real-time asset inventory, continuous asset compliance, network access control (NAC) capabilities and more, all of which help minimize the risk of a breach or business disruption.

> "We needed network access control and segmentation, but first we needed to know exactly what was on our networks."
>
> *— Niklas Kaiter, System and Network Administrator, Winkelmann Group*

Business Challenge

To receive TISAX certification, a security standard required for German automotive manufacturers, Winkelmann Group had to implement NAC and network segmentation. In addition, the company had experienced a few virus incidents that disrupted operations of endpoints and servers. Thankfully, the company's IT staff was able to fully restore the machines after these events. However, these cyberattacks, combined with audit feedback, led executives to rethink its cybersecurity approach and commit to investing in the right solutions to better secure its users and assets – starting with being able to see everything on their networks.

SECURITY SOLUTION

- Forescout Continuum Platform
- Forescout eyeExtend

USE CASES

- Asset inventory
- Asset compliance
- Network access control

RESULTS

- Rapid time to value – comprehensive visibility within two hours, across IT, IoT and OT assets
- Initial real-time, accurate asset inventory after only half a day
- Security operations saves hours daily regarding network and asset management
- Minimized risk of breach with automatic, continuous posture assessment across all connected assets
- Accelerated time to detect and remediate vulnerabilities
- Facilitated policy creation and enforcement
- Has laid the foundation for ecosystem integrations and network segmentation

Why Forescout?

After its initial research into potential NAC and segmentation solutions, the Winkelmann Group down-selected four vendors. "Forescout offered a much broader feature set and much more comprehensive visibility than any of the others, and Forescout was much easier to implement," recalls Winkelmann Group System and Network Administrator Niklas Kaiter. "The competitors either did not have enough functionality or were too complicated and time-consuming to deploy. The Forescout Continuum Platform was much more flexible, with an intuitive dashboard, easy access to granular data, and seamless integration with many of the other tools and systems we use."

Business Impact

Comprehensive visibility in hours, including IoT and OT

"We initially guessed we had approximately 2,500 assets, but even the initial trial of the Forescout platform showed 5,000, including IoT and OT assets, which we had never seen before," says Kaiter. "We had wide-ranging visibility in just two hours, with most of the assets classified automatically. Expanding from trial to production deployment also took only two or three hours. Within half a day in full deployment, we could produce a real-time, accurate asset inventory with just a few clicks on the Forescout dashboard. Ultimately, we saw a total of 6,800 assets – over 170% more assets than we originally guessed we had."

Upleveling security posture with easier device compliance

Winkelmann boosted its security by using the Continuum Platform to automatically and continuously assess the security posture of all connected assets – IT, OT and IoT. When an asset attempts to connect to Winkelmann's network, the platform checks to make sure that antivirus software is installed and running, Windows Firewall has been enabled, Windows updates are current and that the asset is on the correct VLAN. If the antivirus software is not running, for example, the platform attempts to reactivate it. If the asset cannot be brought back into compliance automatically, an administrator is alerted for manual remediation, such as moving it to another VLAN.

"Besides asset hygiene issues, Forescout has uncovered serious vulnerabilities and threats, such as the use of blacklisted applications or a non-corporate laptop accessing our network via VPN," notes Jan-Erik Strauss, also a system and network administrator. "We still see new things almost every week that we would never have seen otherwise."

"Forescout has uncovered serious vulnerabilities and threats … We still see new things almost every week that we would never have seen otherwise."

— *Jan-Erik Strauss, System and Network Administrator, Winkelmann Group*

Reducing network administration burden

Deploying the Continuum Platform also saves Winkelmann's small team of security and network administrators multiple days each month and makes their jobs easier. Just one example: in the past few years, after the company shifted from an on-premises antivirus solution to one in the cloud, as agents were uninstalled and reinstalled, some endpoints ended up without any antivirus protection. "With Forescout, it was easy to see not only how many assets needed attention but exactly which ones and who they belonged to," explains Strauss. "The depth of asset information available is incredibly useful and saves us time in multiple ways.

"The Forescout Continuum Platform is exceedingly powerful yet quite easy to set up and use," says Strauss. "We were able to configure the platform without much external help. The dashboard is intuitive, and it's very easy to create new groups and policies and so on."

"NAC but also so much more"

Although the Winkelmann Group saw value from Forescout on Day One, it has just begun to leverage the holistic capabilities that the Continuum Platform offers. In the future, Winkelmann plans to automate more security processes, add network segmentation and move from monitoring to policy enforcement for IT assets as well as machines on the factory floor. It has already integrated the platform with its VMWare infrastructure, firewalls and Active Directory and hopes to take advantage of seamless integrations with other systems in its environment as well.

When asked what he tells peers about the Continuum Platform, Kaiter replies: "You can invest one-quarter of what the Forescout platform costs but then you'll only have one-quarter of the security, or even less. You just won't have the breadth of functionality you get with Forescout. … We bought Forescout for NAC, but we use it daily for asset management and foresee many future use cases. Yes, it's a NAC solution, but it is also so much more."

FORESCOUT

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com