Securing Priceless Data to Drive Manufacturing Advantage

RIETER

"The proof of concept from Palo Alto Networks really impressed us. It was simple to configure, easy to use, and we could integrate with Active Directory, creating different firewall rules based on User-ID – all managed from one point of view."

Markus Fehr | Network Security Engineer | *Rieter Machine Works Ltd.*

Industry
Textile machinery

Challenge
Establish a standardized, efficient approach to network security as business develops and expands globally

Solution
Palo Alto Networks next-generation firewall with URL Filtering, IPS and Threat Prevention, GlobalProtect, and Panorama

Subscriptions
GlobalProtect, URL Filtering, Threat Prevention

Appliances
PA-5050 (2), PA-3020 (2), PA-850, (10 + 7 on-site spares), PA-820 (11 + 7 on-site spares), and PA-220 (17 + 7 on-site spares)

Results
- Established a single platform to manage network security globally
- Simplified secure access for the mobile workforce
- Increased application visibility and control
- Raised protection for industrial patents

Background
Rieter is the world's leading supplier of systems for short-staple fiber spinning. Based in Winterthur, Switzerland, the company develops and manufactures machinery, systems and components used to convert natural and manmade fibers and their blends into yarn. Rieter is the only supplier worldwide to cover spinning preparation processes and all four end spinning processes currently established on the market. With 15 manufacturing locations in nine countries, the company employs a global workforce of some 5,020, about 20 percent of whom are based in Switzerland. Rieter is listed on the SIX Swiss Exchange under ticker symbol RIEN (www.rieter.com).

Story Summary
Much of Rieter's market advantage comes from developing and implementing advances in technology and processes. As such, it needs to closely guard its intellectual property.

Palo Alto Networks® Next-Generation Security Platform allows Rieter to create and maintain a secure, global business. It enables the business to manage 15 production facilities in nine countries, with an empowered mobile workforce. The platform can identify threats to network security while simplifying the user and IT management experience.

Protecting Intellectual Property
Intellectual property spans a broad definition, from visible assets such as the company logo to things such as trade secrets, manufacturing processes and technological advances resulting from intense research and development. This information is highly sensitive and proprietary, and critical to a company's competitive advantage in the market.

In a 2015 FBI survey of 165 private U.S. companies, half reported economic espionage or theft of trade secrets. The economic damage from IP theft runs into the billions of dollars. Theft of industrial IP costs trade revenue and jobs, and diminishes incentive to invest in R&D. Protecting IP encourages more R&D, leading to economic growth.

Safeguarding Industrial Data in a Mobile World
Operating in the new era of Industry 4.0, in which computers and automation come together, gathering machine performance and other sensor data is important to Rieter's future business growth. Customers can use such data to look for insights to improve their yarn quality. The collection of this data, the ability to use it for production improvements, and the protection of company IP from unauthorized access are critical security requirements for the business. Rieter will rely on big data in the future, and the ability to gather big data relies on a safe and secure network.

Over the last ten years, Rieter has expanded around the globe, with the addition of manufacturing capacity in Eastern Europe, China and India. As a result, their network has also expanded around the world, with now more than three-quarters of their workforce located outside of Switzerland. "Our designers are

"We really liked the Active Directory integration in the Palo Alto Networks solution. It is far easier to work with a system that is dynamic."

Markus Fehr | Network Security Engineer | *Rieter Machine Works Ltd.*

working on new drawings and new versions continuously," says Markus Fehr, Network Security Engineer at Rieter, "and these versions are being transferred all around the world, from R&D to production sites to sales teams. Protecting our drawings and designs is one of our most important priorities."

As Rieter's business grew, the company recognized that it had to secure both its online procurement channel and its expanding global network. In order to maintain high standards in security and reduce administrative costs, the company centralized these functions worldwide, with all security managed out of its office in Winterthur, Switzerland. Being able to run security operations on a global scale while accounting for the needs of their user population in different geographies required a solution that could be centrally managed. "In recent years, our focus has been on raising the user experience. That means the best purpose-to-fit hardware, but also the simplest administration," explains Fehr.

Simplify User Integration to Create Dynamic Rules

Until 2012, Rieter used different systems. "For two guys, having different systems to manage and maintain was not ideal; we wanted a solution with everything in one box," says Fehr. It was a proof of concept from Palo Alto Networks that really impressed him: "It was simple to configure, easy to use, and we could integrate with Active Directory, creating different firewall rules based on User-ID – all managed from one point of view."

The Palo Alto Networks Next Generation Security Platform encompasses its Next-Generation Firewall, Threat Intelligence Cloud and Advanced Endpoint Protection. It delivers application, user, and content visibility and control, as well as protection against known and unknown cyberthreats.

Fehr says the main draw of Palo Alto Networks was user integration: "Being able to create firewall rules based on User-ID, rather than changing IP addresses, was a big appeal. As we've started to roll out smartphones and tablets and notebooks, with users moving from wired to wireless networks, working off IP addresses was impractical."

Today, Rieter relies on the Palo Alto Networks family of next-generation firewalls to protect its network perimeter. It has a number of Palo Alto Networks appliances in the Winterthur head office. In addition, Fehr uses the GlobalProtect™ network security for endpoints to secure the mobile workforce with next-generation security for business applications. Panorama™ network security management enables Fehr to control the distributed network of firewalls from a central location. "We have a central view of every firewall. We can configure every firewall from Panorama off set templates, managed centrally and pushed to every local box."

Identifying All Applications Being Delivered to the Business

With the perimeter secured, Fehr's next goal is to secure Rieter's data centers using the Palo Alto Networks platform. Besides the main data center in Switzerland, Rieter operates two regional data centers in India and China. Two PA-3050 clusters will be deployed in India and China in 2017.

"Once complete, we'll be able to identify all services and applications being delivered to the business. We'll create secure and proper firewall rules that allow only the traffic needed to use these applications. With Panorama, we can show the threats, what we've protected, the risk status … we'll be able to demonstrate the measures we've taken to stay safe and secure," Fehr sums up.