

RC WILLEY DERIVES WIDESPREAD BENEFITS FROM “FLAWLESS” NETWITNESS® PLATFORM UPGRADE



Home furnishings retailer RC Willey has been a customer of NetWitness for many years. In 2015, the Salt Lake City, Utah-based company began using NetWitness® Packets to monitor potential threats on its network. Following the successful implementation of NetWitness Packets (now known as NetWitness Network), RC Willey deployed NetWitness Logs and NetWitness Endpoint to expand its threat detection capabilities.

Rich Sheridan, RC Willey’s IT manager, says NetWitness Logs, Network and Endpoint, which make up the NetWitness Platform evolved SIEM, are essential to the company’s security infrastructure. “Without these tools,” he says, “we wouldn’t have half the visibility we need to detect threats on our network and endpoints.”

When NetWitness Platform 11 was released during the second half of 2017, RC Willey was eager to explore the SIEM’s new features and capabilities. NetWitness set up a free trial, and the network traffic analysis solution immediately identified large amounts of unknown traffic on RC Willey’s network. “This enabled us to discover multiple anomalies that could have been exploited if left unresolved,” says Sheridan. “We got immediate value just from the trial.”

During the trial, Sheridan and his colleagues were also impressed with the platform’s modern user interface (UI) and data visualization capabilities—two important focus areas for NetWitness. When developing the UI for NetWitness Platform, NetWitness committed to raising the bar for usability in SIEM platforms across the industry. While some SIEM providers focus on creating pretty dashboards, the goal at NetWitness was to create a UI that truly enhanced the efficiency and effectiveness of the analysts who would be using the platform. To that end, NetWitness enlisted dozens of security analysts who devoted hundreds of hours to usability testing the platform.

Sheridan says the company’s tenacious work on the UI paid off. “It’s amazing,” he says. “NetWitness Platform is an exceptional representation of NetWitness’s commitment to its customers, to cybersecurity and to innovation.”

With the trial complete, RC Willey was ready to upgrade.



CUSTOMER VITAL STATISTICS

Industry: Retail

Number of employees: 2,500

NetWitness product: NetWitness® Platform 11

What I like about NetWitness:

- Visibility across entire IT infrastructure, including cloud-based, virtual and hybrid environments
- Enhanced visualization capabilities enabling much faster and more accurate decisions
- Guidance and expertise from NetWitness Risk & Cybersecurity Practice

A FLAWLESS TRANSITION

There are multiple ways for existing NetWitness Platform customers to transition to the latest version, from self-managed options to highly structured consulting packages delivered by the professional services team from the NetWitness Risk & Cybersecurity Practice. RC Willey opted to work with the NetWitness Risk & Cybersecurity Practice for a number of reasons, including positive experiences RC Willey had had with them in the past.

“We have a modestly sized IT and security group; enlisting experts from the NetWitness Risk & Cybersecurity Practice enabled us to become operational—and secure—in the shortest amount of time,” says Sheridan. “Because NetWitness Platform is at the heart of our security stack, we wanted to be sure it was optimally configured and implemented; we knew working with NetWitness consultants would give us that confidence.”

During the upgrade, which took place over the course of just three days in April 2018, members of the NetWitness Risk & Cybersecurity Practice sat in a conference room with RC Willey IT staff, and together they executed every step in the process. The end result: An “uneventful” and “flawlessly executed” upgrade with zero loss of any of the data RC Willey had accumulated in its earlier version of NetWitness Platform, according to Sheridan.

RESULTS

While RC Willey had always benefited from the visibility its earlier version of NetWitness Platform provided, the new version of RSA NetWitness Platform is delivering even greater visibility, investigative insights and productivity benefits, according to Sheridan.

For one, NetWitness Platform 11 is capable of aggregating and analyzing logs from cloud-based systems and virtual infrastructure, which gives customers like RC Willey new-found visibility into a rapidly growing portion of their infrastructure that attackers are increasingly trying to exploit. “Like many companies, we’re adopting more and more cloud-based systems, and to prevent cloud-based threats, we need visibility into that infrastructure,” says Sheridan.

In addition, NetWitness Platform 11 offers user and entity behavior analytics (UEBA) capabilities designed to provide security teams with high-fidelity alerts signaling the suspicious behaviors associated with insider threats and external attacks. It also features orchestration and automation capabilities to streamline and accelerate investigations and incident response.

Finally, the UI and visualization capabilities are driving dramatic productivity benefits for Sheridan and his team. “It used to take me one-and-a-half to two hours each morning to run through security alerts from different systems,” says Sheridan. “But now, because of the integration with NetWitness Platform, it only takes me 15 to 20 minutes. The user interface and advanced visualizations bring security data from disparate systems to life in this one single platform. As a result, I’m able to make much faster and more accurate decisions, and I’ve freed up a significant portion of my day.”

To ensure RC Willey continues to get the most out of NetWitness Platform 11, Sheridan’s team meets quarterly with the NetWitness Risk & Cybersecurity Practice to discuss the platform’s continually expanding feature set and to glean industry best practices. Additionally, RC Willey has an incident response retainer in place with NetWitness to ensure RC Willey has access to rapid investigation and remediation services should a cyber attack occur. “The reason we’re so successful is because of the NetWitness Risk & Cybersecurity Practice. We’re a small team and we would never have been so successful without them,” says Sheridan.

“The reason we’re so successful is because of the NetWitness Risk & Cybersecurity Practice. We’re a small team and we would never have been so successful without them.”

– Rich Sheridan, IT Manager, RC Willey Home Furnishings

“It used to take me one-and-a-half to two hours each morning to run through security alerts from different systems, but now, because of the integration with NetWitness Platform, it only takes me 15 to 20 minutes. The user interface and advanced visualizations bring security data from disparate systems to life in this one single platform. As a result, I’m able to make much faster and more accurate decisions, and I’ve freed up a significant portion of my day.”

– Rich Sheridan, IT Manager, RC Willey Home Furnishings

ABOUT NETWITNESS

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats.

For more information, go to netwitness.com

“Because NetWitness Platform is at the heart of our security stack, we wanted to be sure it was optimally configured and implemented; we knew working with NetWitness consultants would give us that confidence.”

– Rich Sheridan, IT Manager, RC
Willey Home Furnishings