CASE STUDY

TANIUM

How insurer Zurich shields against cybercrime

ZURICH

Industry
Financial services

Size
50,000+ employees

Headquarters
Zürich, Switzerland

The results of Zurich collaborating with Tanium.

Faster patching

Zurich saves up to 100 resource hours a month with an automated patching capability built on top of Tanium's patching tools.

More cybersecurity & IT operations cooperation

Tanium helps Zurich solve IT issues that could otherwise slip through the cracks between IT and operations. The platform enables the groups to work together seamlessly.

Greater cyber resilience

Paige and his team know it's not if an attack happens, but when. Yet with Tanium's multiple capabilities, Zurich is ready for whatever comes.

With more than 100,000 endpoints worldwide, the insurer needed a higher level of protection.

Zurich Insurance Group has been in business for 150 years with a global presence in 210 countries and territories and well-known brands including Farmers Insurance. Zurich provides property and casualty (P&C) and life insurance products and services to individuals, small and mid size businesses, and multinational corporations. In 2021, Zurich generated a business operating profit of $5.7 billion, a year-on-year increase of 35%.

But success also attracts cybercriminals. With more than 100,000 digital endpoints in a geographically distributed and highly heterogeneous environment, Zurich must keep those endpoints safe and secure.

"We're fighting cyber bad guys on an everyday basis" says Paige Adams, Zurich's global chief security officer. "So, our key measure for success is: Are we protecting Zurich, our customers, and our customers' data? It's a simple yes-or-no question."

Paige first learned about Tanium eight years ago, when he joined Zurich as the incident-response leader in North America. The team he was assigned to had already been investigating Tanium, and they were eager to get his sign-off. "I was told that Tanium is kind of a Swiss Army knife of IT tools" Paige recounts. That's compelling! We're a Swiss company, so a Swiss Army knife sounds great to have."

Paige met with Tanium customers, who explained its real-world capabilities and benefits. That helped him understand the offerings as well as the role of Tanium solutions in security and operations.

"It's always a sweet spot when you can find a set of capabilities that delivers value to multiple teams" he says.

> “Our key measure for success is: Are we protecting Zurich, our customers, and our customers’ data? It’s a simple yes-or-no question.”

Paige Adams,
Global chief security officer, Zurich Insurance Group

> “I was told that Tanium is kind of a Swiss Army knife of IT tools. I said, ‘That’s compelling! We’re a Swiss company, so a Swiss Army knife sounds great to have.”

Paige Adams,
Global chief security officer, Zurich Insurance Group

Paige realized Tanium could help on the security side with incident response. In the event of an attack, Zurich can determine what occurred, when and where it happened, which devices were affected, and how attacked endpoints can be isolated, mitigated, and then returned to safe operation. Paige and his team now have full visibility into their endpoints. Prior to using Tanium, Zurich lacked tools that could both provide visibility into endpoints and manage them. With Tanium, Zurich now not only has those capabilities, but also has them in a centralized dashboard and set of tools.

“In that regard,” Paige says, “Tanium was a game-changer.”

Tanium not only helps Zurich keep its endpoints protected with up-to-date patches, but also helps save time. Paige estimates the savings at up to 100 resource hours a month, based on the automated patching capabilities Zurich has built on top of Tanium’s patch tool.

Tanium also helps Zurich with use cases that cross the border between IT operations and security teams. “We’ve been able to leverage Tanium in unique ways that fulfill use cases that sit in between the IT ops team and our cyber response team,” Paige says. “This helps us resolve issues like internal misconfigurations, or to spin up a response effort to handle IT severity incident” he adds.

Initially, Zurich used Tanium mainly for security use cases. But once the operations team saw Tanium’s security capabilities up close, they asked if they could use some of its capabilities, too. The answer was a resounding ‘yes.’ That later led Zurich to create what it calls The Enterprise Command Center, and new capability that uses Tanium to handle IT and incident management, performance analysis, and monitoring.

“It’s always a nice, sweet spot when you can find a set of capabilities that multiple teams find of value” Paige says. “We’ve gotten good saturation of Tanium usage, on both the cyber side of the house and the IT operations side. It’s a set of capabilities that everybody loves.”

Ultimately, Tanium is helping Zurich become cyber-resilient. “It starts with a simple question: What do we do when this happens? Not if this happens, but when,” Paige says. In practically any scenario, Tanium’s capabilities help.

Tanium, the industry’s only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That’s the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.