

Swiss IT Service Provider Uses Check Point to Protect New Data Centers and Maintain Strict Customer SLAs

Check Point Next Generation Security Gateway enables Wagner AG to flex customer loads across locations, with advanced network protection and centralized security management



Customer Profile

Wagner AG is an IT service provider based in Switzerland. It specializes in outsourcing and consultancy services.

Challenges

- Strengthen threat prevention capabilities at two, connected data centers
- Improve visibility of threat landscape, with consolidated monitoring and granular reporting
- Provide smooth handling of customers by ensuring business continuity

Solution

- Check Point Next Generation Security Gateway
- Check Point R80.10 Security Management

Benefits

- Provides advanced threat protection and detection, identifying cyber security attacks in their infancy
- Allows for scaling to support growth in managed services at both locations
- Enables the business to securely spread customer loads between two data centers

“What we appreciate most about R80 is the clear and simplified administration of our policies. Being able to administrate policies by several users simultaneously makes daily work much easier.”

— Thomas Eltschinger, Head of Managed Backend Services, Wagner AG

Overview

Wagner AG

Wagner AG is a provider of IT services, based in Switzerland. It has customers in a range of market sectors, including financial, food and healthcare. The business was founded in 1996 and has over 100 employees.

Business Challenge

Building the infrastructure to accommodate growth

Wagner AG provides managed IT services to corporate customers in Switzerland. As businesses look to outsource their IT to a specialist, reducing management complexity and stabilizing costs, Wagner AG had drawn up plans for two new data centers. Located 120kms apart with two 40GB connections, the investment would provide room to grow and strengthen redundancy.



“The cluster functionality of the Check Point solution fits very well with other network components. It is a definite advantage.”

— Thomas Eltschinger, Head of Managed Backend Services, Wagner AG

“This was a sizeable, strategic investment, built from the ground up,” says Thomas Eltschinger, Head of Managed Backend Services, Wagner AG. “We wanted to incorporate the latest technology. As we’re delivering managed services, with strict SLAs, we needed clustered firewalls at both locations.

“We want to be able to offer our customers the best possible protection with today’s modern options. We can do this with the various blades and the flexible license model of Check Point.”

Solution

Maximized uptime with advanced protection

The Check Point Next Generation Security Gateway combines the most comprehensive security protection with data center grade hardware to maximize uptime while safeguarding enterprise and data center networks. The solution ensures high performance protection against the most advanced cyber-attacks.

Eltschinger says the Check Point solution offered the best fit in terms of features, and enables the business to meet industry compliance in terms of security and traceability. Check Point Next Generation Security Gateway offers unique ‘first time prevention’ for the most sophisticated zero-day attacks. It is optimized for inspecting SSL encrypted traffic and its centralized management control and Lights Out Management (LOM) improves serviceability. It is also modular, and can be expanded if necessary.

In addition, Check Point R80.10 Security Management provides fully integrated visibility and clearer security insights. R80.10 SmartConsole allows Wagner AG to create unified policies for all network and cloud environments, all managed centrally.

“Automation and API options are useful features in R80.10,” says Eltschinger. “We’re standardizing our customer environments, which means the existing API becomes more important for automation. The TCO becomes smaller and costs can be saved.”



“The documentation and Secure Knowledge on the Check Point site is excellent. It was simple to find answers to any technical questions.”

— Thomas Eltschinger, Head of Managed Backend Services, Wagner AG

Benefits

Scale, with latency and redundancy

“Implementation went smoothly. It was done manually, working through all the old rules, creating new ones, and cleaning things up. We didn’t want to bring across any unwanted security rules from old devices,” says Eltschinger.

Eltschinger further explains that the implementation was done alongside their Check Point partner, BNC Business Network Communications AG, and any issues were quickly resolved: “The documentation and Secure Knowledge on the Check Point site is excellent. It was simple to find answers to any technical questions.”

Today, the two data centers house around 50 Wagner AG customers, with up to 3,000 users and 5,000 different firewall objects. “The fact that I can have these objects run in either location means we can spread the load evenly. We can connect customers by geography, but still retain latency and redundancy,” says Eltschinger. “The cluster functionality of the Check Point solution fits very well with other network components. It is a definite advantage.

“However, what we appreciate most about R80 is the clear and simplified administration of our policies. Being able to administrate policies by several users simultaneously makes daily work much easier.

“Feedback from customers,” he adds, “has been positive. Everything is running smoothly, which wasn’t the case with the old solution.”

Eltschinger explains Wagner’s plan is to introduce SandBlast™ Threat Emulation and Threat Extraction by the end of 2018.

“The ultimate aim is to have no malware on the network, to allow things onto the network unhindered, and to catch problems as close to the entry point as possible. The Check Point SandBlast function offers that.”



For more information, visit:
<https://www.checkpoint.com/products/sandblast-network-security/>