XM Cyber | Case Study

Manufacturing

XM Cyber and Kärcher: Protecting a Global Innovator With Continuous Visibility

Kärcher, the global leader in cleaning equipment and systems, uses XM Cyber, running on STACKIT's secure European cloud, to safeguard its worldwide operations, retain crucial digital sovereignty, and maintain proactive control over its constantly expanding digital environment.

The Challenge:

Protecting Innovation Through Visibility and Control

Based in Winnenden, Germany, Kärcher is a household name worldwide, offering products and systems for homes, industries, and cities—from pressure washers and industrial vacuums to digital cleaning platforms and more. Its equipment is used across manufacturing, logistics, retail, and facility management, supported by more than 17,000 employees across 85 countries.

As Kärcher connected more of its machines and services through IoT and cloud systems, the company recognized that every new connection broadened the potential attack surface. The adoption of AI tools and remote service platforms added even more complexity.

This trend led Kärcher Chairman of the Board Hartmut Jenner to place a special focus on cyber security. According to Jenner, "Through our networked work with customers, suppliers and the various tools, we offer attackers more and more space. The attack surfaces are larger than ever before and are growing almost exponentially. Every additional digital tool creates new vulnerabilities that allow attackers to find gateways. And this is precisely why cyber security is an issue that concerns us all and will continue to do so in the future."

Kärcher needed a solution that could deliver continuous visibility into its massive global digital infrastructure, help accurately prioritize risks, and ensure compliance with strict European data protection standards while preserving organizational independence and control.

KÄRCHER

Customer:
Kärcher

Industry:
Manufacturing

Location:
Winnenden, Germany

Challenge:
Protecting a global digital ecosystem while preserving data sovereignty

Solution:
XM Cyber exposure management platform on STACKIT infrastructure

Results:
Continuous visibility, proactive prevention, and a secure, sovereign foundation for digital growth

The Solution:

A Continuous and Sovereign Defense with XM Cyber

Kärcher chose XM Cyber to replace backward-looking, periodic pentests with a continuous, automated exposure management approach. Running on STACKIT's sovereign European cloud, the platform continuously maps attack paths, identifies critical vulnerabilities, and helps strengthen defenses proactively before attacks can materialize.

Jenner highlighted the profound shift from their previous methods: "Up to now, we have carried out pentests, but with a backward-looking approach and not really looking forward. With XM Cyber, we now have automated, continuous processes that allow us to take a holistic view. Vulnerabilities can be analyzed much better. We can detect potential attacks in advance. That's a completely different approach."

The implementation was fast and disruption-free. XM Cyber was deployed quickly across Kärcher's workstations and servers, delivering immediate visibility into existing exposures. Running on STACKIT also ensured that the deployment fully met all sovereignty and European data protection requirements.

Benefits and Outcomes:

Operational Stability Through Proactive Prevention

Kärcher now benefits from continuous insight into its global exposure landscape and the ability to act before threats can escalate. The XM Cyber live dashboard gives teams real-time security awareness and drives ongoing improvement across all systems and global sites.

“In the past, we were rather reactive. For pentests, we had to request a quote, place an order and then rectify the weak points. Today, we can always find out about the current status of our security in XM Cyber's live dashboard.”

This approach has successfully coalesced Kärcher’s IT and security teams around a shared, attacker-aware view of risk, significantly improving collaboration and bolstering operational stability across its worldwide network.

Recommendation and Outlook:

Security as a Foundation for Innovation

Chairman of the Board Hartmut Jenner views cybersecurity as a central duty of leadership: “For a globally networked, innovative company like ours, which uses more and more digitalized methods and tools, there is an exponential risk potential. For me as CEO, it is fundamentally important to protect the company and its assets. I have to protect the customers, the suppliers, the employees. There is therefore no question that cyber security is a matter for the management.”

He emphasized that maintaining digital sovereignty means keeping control of company data and shaping their own digital architecture. With XM Cyber on STACKIT, Kärcher can manage risk continuously while advancing its use of cloud and AI technologies with full oversight and control.