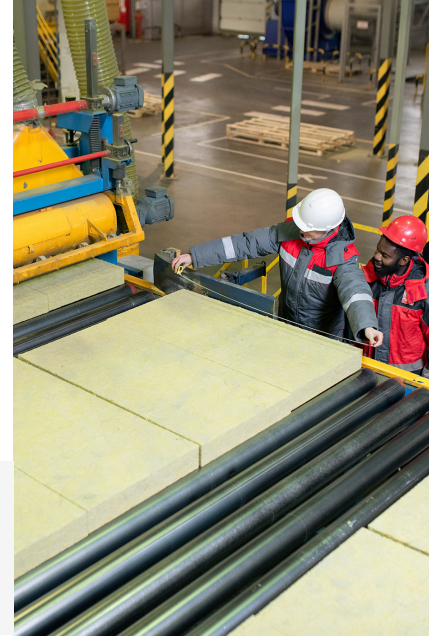




# How Austrotherm Transformed IT Security Across 13 Countries with Unified SASE Architecture



## INDUSTRY

Manufacturing

## HEADQUARTERS

Waldegg/Wopfing,  
Austria

## COMPANY SIZE

1,400 employees

## OVERVIEW

The Austrotherm Group is a family-owned Austrian enterprise. In addition to its headquarters in Wopfing, production sites in Pinkafeld and Purbach and its three locations in Turkey, the leader in insulation is represented by organizations in Germany, Bosnia-Herzegovina, Croatia, Serbia, Bulgaria, Poland, Romania, Slovakia and Hungary. Along with the Baumit and Murexin groups, the Austrotherm group is part of Schmid Industrie Holding.

## OUR SOLUTION

Hybrid Mesh Network Security

Workspace Security

Check Point Services



Check Point gave us everything we need, including SASE for easy remote access, improved endpoint security, zero trust network access design, firewalls, and more.

*Markus Zack Head of Group IT at Austrotherm GmbH*



## CHALLENGE

When Markus Zack took over as head of group IT at Austrotherm GmbH, a European manufacturer of high-quality thermal and acoustic insulation materials, he inherited a security infrastructure that could no longer keep pace with the cyber security needs of a manufacturing company operating 36 production sites across 13 countries. As part of the Schmid Industrie Holding alongside Baunit and Murexin, Austrotherm specializes in energy-saving thermal insulation products and employs approximately 1,400 people across Europe. Despite its significant operational footprint, the company was outgrowing its current IT security capabilities.

The Austrian-based manufacturer faced mounting security challenges across multiple fronts. Perhaps the biggest challenge was its email security, as Austrotherm had been relying on popular antivirus and firewall software. “We were facing substantial phishing attacks,” Zack explained. The volume of suspicious emails began to overwhelm both security and support staff, with help desk tickets frequently requesting that IT verify whether messages were legitimate or phishing attempts.

Remote access created equally serious problems. The company relied on a certificate-based VPN client that proved unreliable. The intermittent connectivity frustrated remote workers and created operational bottlenecks for a workforce that increasingly needed flexible access to manufacturing systems and administrative applications across Europe. With all remote traffic routed through a single access point in Austria, regardless of the user’s actual location, latency issues compounded connectivity reliability issues.

Access control presented additional complexity in Austrotherm’s hybrid technical environment. Austrotherm operates a diverse technology landscape, spanning modern Windows 11 systems in office environments and legacy Windows XP and Windows 98 machines that still run critical manufacturing equipment. This OT/IT convergence requires strict network segmentation to prevent potential security incidents in one environment from cascading into the other. The existing infrastructure provided inadequate visibility and control over which users and systems could access critical production networks.

For Zack’s three-person IT security team, the fragmented toolset meant constant context switching between management consoles. Without centralized visibility, identifying and responding to security incidents required time-consuming, error-prone manual correlation.

The need to enhance cyber security capabilities grew more urgent as Austrotherm pursued aggressive growth, including the 2025 acquisition of Italy’s largest installation materials company, which would add eight production facilities requiring immediate, secure integration. The Austrotherm team began its search for a scalable security platform to enhance overall company security and improve manageability.

## SOLUTION

Following a comprehensive vendor evaluation, Austrotherm selected Check Point’s integrated security portfolio, deploying Check Point SASE (both Internet Access and Private Access packages), Check Point Spark Firewall, and Check Point Email Security across 720 licensed users. “As we looked at Check Point and the competitors, we had great meetings with the Check Point team in Austria, and we learned Check Point gave us everything we need, including SASE for easy remote access, improved endpoint security, zero trust network access design, firewalls, and more,” Zack said.

“Check Point Portal—a unified management console that would eliminate the screen-hopping that plagued daily operations placed Check Point clearly over the top. Check Point Portal provides us one place where we can configure every security tool and a complete overview of where we stand,” Zack explained.

“The consistent interface across product families dramatically reduced the learning curve and made onboarding the team very straightforward,” he said. This proved essential for a small security team managing infrastructure across 13 countries.

Check Point SASE addressed the remote access challenges through a zero-trust network access (ZTNA) architecture. Rather than backhauling all traffic through Austria, Austrotherm could now deploy multiple gateway locations across Europe, enabling staff to connect to the nearest point of presence. Check Point SASE also provided granular firewall rules and access controls, ensuring that only authenticated users on compliant devices could access specific network resources. For third-party support vendors who needed temporary access to manufacturing equipment, Check Point SASE provided a secure, auditable alternative to traditional VPN credentials.

For email security, Check Point Email Security replaced the underperforming prior email security software. Side-by-side comparisons during their evaluation revealed that their previous system was allowing significant quantities of phishing emails to reach users’ inboxes. Check Point Email Security is integrated directly with Microsoft 365, requiring minimal configuration - “it’s complete in five minutes,” Zack said. Users gained self-service access to quarantined messages through an intuitive dashboard, while IT administrators received detailed context on sender history and communication patterns to make informed release decisions.

The hybrid architecture combined cloud-delivered SASE services with on-premises Check Point Spark Firewall at larger sites. VLAN segmentation separated office networks from production environments, with jump hosts providing the only authorized pathway for IT staff to access legacy manufacturing systems. Check Point virtual firewalls extended protection into Austrotherm’s Microsoft Azure environment, creating consistent security policy enforcement across cloud and on-premises resources.

Implementation partner Bacher Systems, a Check Point services provider in Austria, assisted with detailed design and configuration following Austrotherm’s selection of Check Point. However, the platform’s intuitive interface enabled Zack’s team to manage ongoing operations independently, with Check Point’s responsive support team available as needed.

“



My team can now focus on other projects and other topics, because Check Point products require so little work each day.

*Markus Zack Head of Group IT at Austrotherm GmbH*

”

## OUTCOME

The transformation delivered quantifiable improvements across multiple dimensions. Email security witnessed the most dramatic change. Check Point Email Security blocked 20-30% more phishing attempts than the previous email security software, while help desk tickets requesting verification of suspicious emails dropped by 70%.

“We can trust that most of the phishing attacks are blocked,” Zack said. The company’s remote access connectivity issues essentially disappeared. Over six months following full deployment, Austrotherm’s IT team received zero tickets related to VPN connection issues or remote access failures. “The users are very happy,” Zack reported. “They turn on their computer, and they have internet and are immediately connected to the network, and they can conduct their work everywhere.” Throughput performance improved dramatically as distributed gateways eliminated the latency previously caused by routing all traffic through Austria. “It’s nearly as if you’re working in the office at the moment,” Zack said, as he highlighted the seamless experience now available to remote workers.

The unified management console delivered operational efficiency gains, freeing the small IT security team to focus on strategic initiatives rather than daily firefighting. “My team can now focus on other projects and other topics, because Check Point products require so little work each day,” Zack explained. Because of that freed time, other IT projects now progressed more quickly because the team wasn’t constantly troubleshooting security infrastructure.

Business agility improved significantly, demonstrated most dramatically during the recent acquisition integration. During those efforts, Austrotherm needed to connect eight geographically dispersed facilities—from Northern Italy to Southern Italy—whose core systems were all located in a single data center. “We made the connection in one day, the entire connection,” Zack reported. The rapid deployment occurred while the company simultaneously migrated computers and file systems, a process that could have introduced significant security risks.

Austrotherm has expanded its Check Point footprint beyond the initial deployment, adding Check Point Browser Security for AI data protection as employees increasingly use tools like ChatGPT. The comprehensive security platform has positioned the manufacturer to pursue continued growth while maintaining robust protection across its expanding European operations.

## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leading protector of digital trust, utilizing AI-powered cyber security solutions to safeguard over 100,000 organizations globally. Through its Infinity Platform and an open garden ecosystem, Check Point's prevention-first approach delivers industry-leading security efficacy while reducing risk. Employing a hybrid mesh network architecture with SASE at its core, the Infinity Platform unifies the management of on-premises, cloud, and workspace environments to offer flexibility, simplicity and scale for enterprises and service providers.

[LEARN MORE](#)

### Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

### U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065

[www.checkpoint.com](http://www.checkpoint.com)

