

Transforming Email Security: 60% Fewer False Positives, Faster Response, Better Protection, Happier Clients



INDUSTRY

Technology Solutions

HEADQUARTERS

Vienna, Austria

COMPANY SIZE

11 Employees

OVERVIEW

ristl.IT GmbH is an Austrian Managed Service Provider based in Vienna. The company provides medium-sized enterprises with comprehensive IT services from a single source: from planning and implementing secure IT infrastructures to cloud migration (Microsoft 365, Azure) to Managed Security Services with multiple partners. ristl.IT is ISO/IEC 27001 certified and places special emphasis on information security.

OUR SOLUTION

Workspace Security



Check Point Email Security is unbelievably great. We can use it in a multi-tenancy environment and roll it out without issues to different clients with similar configurations.

Christian Schertl, director of operations at ristl.IT



CHALLENGE

Florian Ristl, founder and current managing director and CEO of an eleven-person Austria-based managed IT services provider ristl.IT, began his career as a professional poker player. Those 10 years provided Ristl with much of the experience needed to be a successful entrepreneur: risk management, emotional discipline, pattern recognition, and strategic thinking under uncertainty.

ristl.IT's success largely stems from its focus on business-minded IT management, with the services provider and client sharing the same goal: zero problems enabled by transparent fixed pricing and proactive monitoring. Over time, however, ristl.IT noticed a challenge emerging with their existing email security system, which was increasingly showing signs of aging and diminishing effectiveness.

For instance, the IT security services team was forced to spend up to 20 minutes investigating each quarantined email, while the mail gateway also generated excessive false positives. This frustrated clients and eroded trust in the system.

The email security frustration also reached ristl.IT's services team as they worked to investigate and understand the nature of attacks threatening their customers. "We had to look in four different portals — the defender portal, the mail flow, and we had to hunt for emails and piece all of that together," said Christian Schertl, director of operations at ristl.IT.

Even the most straightforward of emails quarantined for review that clients ultimately requested for release to client recipients because they turned out to be legitimate took 15 to 20 minutes to resolve and required discrete remote connections that were time-consuming to establish. "When clients get hit with too many false positives, they don't catch actual threats because they are fatigued from getting so many of those false positives," Schertl said.

The team also observed a trend of man-in-the-middle attacks via phishing emails on the rise, particularly fake Microsoft sign-ins designed to bypass multi-factor authentication.

Following the frustrated calls for change from one especially frustrated client, the ristl.IT team set out to evaluate multiple modern email security platforms to identify the most suitable replacement.

SOLUTION

The ristl.IT team would select the winning platform on three critical criteria: seamless integration, an MSP-friendly architecture, and proven accuracy. Ultimately, after piloting Check Point Email Security with ristl.IT first—a great practice to fully become familiar and understand the client experience—ristl.IT began migrating all its clients to Check Point Email Security within two months.

Regarding the first of the three success criteria ristl.IT established for itself, the team appreciated Check Point Email Security's seamless integration, enabled by the email and cloud collaboration security platform's hybrid architecture that combines API-based connectivity with inline mail flow inspection. Combined, these deliver multi-layered security without requiring proxies, appliances, or endpoint agents. "The integration with Microsoft 365 was perfect," Schertl added.

When it came to service provider-friendly architecture, the ristl.IT team found Check Point Email Security to be exceptional. "Check Point Email Security is unbelievably great. We can use it in a multi-tenancy environment and roll it out without issues to different clients with similar configurations," Schertl said.

Check Point Email Security also proved much more accurate than their legacy system. Check Point Email Security lowered false positives dramatically. “We are delighted with the results. We really fell in love with Check Point Email Security,” Schertl said.

The ristl.IT team wanted the new email security system to reduce false positives, enable faster threat investigation, better identify phishing attacks, enhance automation, and minimize client interruptions while maintaining strong security.

OUTCOME

Exactly how much more accurate did Check Point Email Security prove to be? Schertl said that the accuracy slashed support tickets, client frustration, and eliminated alert fatigue that had been undermining security. “The number of false positives is 50% to 60% lower,” he said.

Investigation time was also reduced from 20 minutes per suspicious quarantined email to making a valid judgement on email legitimacy to “almost instantly”. “For all our technicians, it’s a relief to get an informed decision so quickly. We can check for phishing and make a rapid decision. Also, there is an effective preview in the sandbox that proves crucial to making those knowledgeable decisions quickly,” Schertl said.

Technicians now make decisions “without bothering the client, and the need to connect to the client and see the email,” Schertl added.

Check Point Email Security additional security layers successfully addressed man-in-the-middle attacks. The geolocation feature for unusual sign-ins became “a very crucial additional security tool in terms of phishing emails and the associated man-in-the-middle attacks,” Schertl said. “We feel more secure because we know we can react more quickly. We get more information very quickly.”

Check Point Email Security integration with the ticketing system streamlined workflows. “The requests from clients for the release of quarantined emails being directed into our ticket system works very well for us,” he said. For one high-volume client, the optional Incident Response as a Service add-on reduced workload and improved the client’s experience by enabling faster access to their emails. “The less you have to interrupt the client, the better. More silence leads to much better customer satisfaction,” Schertl said.

ristl.IT established clear success criteria: significantly reduce false positives, enable faster threat investigation without hunting across multiple portals, better identify sophisticated phishing attacks, enhance automation through ticketing system integration, and minimize client interruptions while maintaining strong security.

“The experience was so good that as future security needs come up in other areas, we will definitely look at what Check Point is offering,” Schertl said.



We are delighted with the results. We really fell in love with Check Point Email Security.

Christian Schertl, director of operations at ristl.IT



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (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

