STAYING AHEAD OF AI-POWERED EMAIL THREATS

> Stopping threats before they reach employees is crucial for maintaining security and productivity.

Stefan Bast, IT Security Officer, Marquardt

MARQUARDT

SUMMARY

As a global manufacturer of mechatronic systems, Marquardt faced the growing challenge of managing ever-increasing phishing and spam volumes while easing the strain on its IT team. With **Advanced Email Security from Open Systems**, the company implemented a centrally managed solution that fits seamlessly into its infrastructure. The outcome: approximately **25% more suspicious emails blocked, fewer false positives, and a significantly lighter load for the security teams**.

CUSTOMER DETAILS

- Manufacturing
- Rietheim-Weilheim, Germany
- 4 continents
- 9,700
- marquardt.com

PRODUCT USED

- Advanced Email Security
- Standard Email Security
- SD-WAN

RESULTS

810.000 €
PREVENTED
additional damages
(per year)

<0.1%
FALSE POSITIVES

~6 Mio.
EMAILS KEPT OUT
of users' inboxes
(per year)

+25%
BLOCKED
suspicious emails

5.823
PROTECTED
mailboxes (users)

Ca. 16 Mio.
EMAILS
(per year)

We sat down with **Stefan Bast, IT Security Officer, and Philipp Schuster, IT Infrastructure Security at Marquardt**, to discuss the company's past challenges and goals, and how Open Systems provided a comprehensive solution.

WHAT IMPACT DO EMAIL THREATS HAVE ON YOUR SECURITY STRATEGY?

Email threats play a central role in our overall security strategy, as they remain the primary entry point for cyberattacks. Once a malicious message bypasses technical safeguards, security depends on the "weakest link" – the user. Out of ignorance, stress, or carelessness, users may click on manipulated links or infected attachments, unintentionally triggering an attack. That's why email security is one of the most critical components of our defense strategy.

Reports consistently show that phishing attacks are becoming more sophisticated – driven by the use of AI. Realistic emails, targeted social engineering, and the ability to bypass traditional filters pose new challenges even for mature security systems. For this reason, we have adopted a particularly strict approach from the outset. For example, we consistently filter attachments – a time-intensive but effective practice that has already protected us from significant damage on several occasions.

WHAT THREATS, CHALLENGES, OR GOALS LED YOU TO IMPLEMENT AN ADVANCED EMAIL SECURITY SOLUTION?

We wanted to strengthen our defenses against highly targeted and AI-driven email threats, in addition to the strong baseline provided by the Open Systems standard Email Security Service and Microsoft 365 Defender. These advanced threats often seek to manipulate users into revealing confidential information. Purely technical authentication methods such as SPF, DKIM, and DMARC are no longer sufficient.

We therefore conducted a Proof of Concept (PoC) with Open Systems, and the initial results showed that Advanced Email Security filtered at least 15% more dangerous emails.

The threat landscape has intensified dramatically in recent years. Attacks have grown more sophisticated, and new techniques – such as phishing via QR codes – present additional risks. It was clear that action was needed. Ultimately, this is a matter of risk management.

At Marquardt, email security ranks among the top three risk areas, involving both financial and reputational exposure – and is therefore a priority at the executive level.

> **"Attackers use AI to refine their email attacks – so we need AI-powered protection to catch what users can't."**

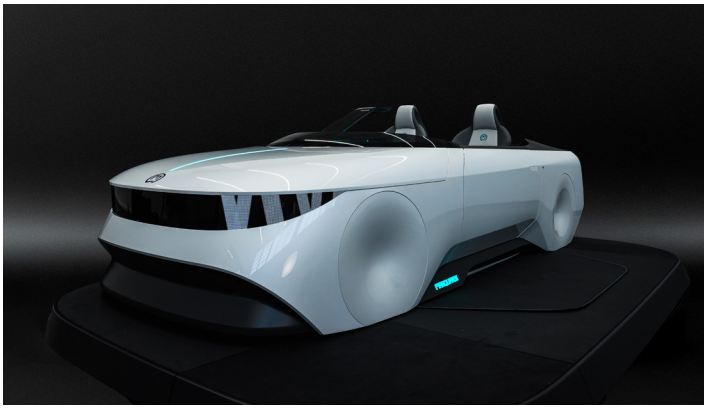
Philipp Schuster, IT Infrastructure Security

WHAT CONVINCED YOU TO CHOOSE ADVANCED EMAIL SECURITY FROM OPEN SYSTEMS?

The decisive factor was Open Systems' comprehensive, integrated approach: all services come from a single source, operate within a unified infrastructure, and are part of a managed service with 24x7 coverage. This is further supported by Customer Success Managers who have worked with us for years.

Had we implemented an additional standalone email security tool, the effort would have been substantial – from integrating it into existing email flows to ensuring availability and eliminating redundancies. That would have created a heavy operational burden. With Open Systems, it was simply a matter of activating another module on the existing platform.

The solution integrates seamlessly into our current environment. Through the Open Systems Portal – which includes incident tracking, change management, and other features – we have a single, centralized point of contact alongside the responsive Operations Center Mission Control. For us, this is the true essence of a managed service: minimizing internal effort while fully leveraging the provider's expertise.



HOW DOES THE MANAGED SERVICE FROM OPEN SYSTEMS SUPPORT YOUR IT TEAM?

We operate in the automotive industry, which is currently facing economic challenges. As such, we monitor labor costs closely – especially in high-wage countries like Germany.

That's precisely why a managed service like Open Systems' is so valuable. Reaching the same level of quality internally, in a short time, would be nearly impossible. We also greatly appreciate the continuous 24x7 support with Level 3 expertise, which clearly distinguishes Open Systems from competitors that only provide on-call support outside business hours.

HOW DID IMPLEMENTATION GO, AND HOW WELL DID THE SOLUTION INTEGRATE?

Implementation went very smoothly thanks to the Learning Mode. During this phase, the system runs in an "observation mode" for one to two months: suspicious emails are detected and flagged but not yet blocked. This allowed us to see exactly which messages would have been filtered – without interrupting normal email operations. As a result, the system went live without any legitimate messages being mistakenly blocked.

Afterward, we reviewed concrete cases together in a workshop. It became clear that Advanced Email Security had identified additional suspicious messages that had previously bypassed other mechanisms. For us, that was clear evidence of its added protection. False positives were extremely rare – under 0.1%. Over time, the engine has learned to classify such cases automatically, eliminating the need for manual whitelisting. This eases the workload for our service centers and increases employee satisfaction, as users no longer have to wait for email approvals.

End users barely noticed the transition. Only if an email was missing – for example, due to a false positive – would they realize anything had changed. Our service desk was trained to quickly check and escalate such cases when needed.

> **"Advanced Email Security is an excellent example of how Open Systems continually evolves its own service portfolio and integrates new technologies and solutions, thereby increasing the value-add for its customers."**

Guido Wettemann, Director Global Operations IT-Systems

WHAT IMPROVEMENTS HAVE YOU OBSERVED SINCE IMPLEMENTATION?

Since deploying Advanced Email Security, approximately 25% more emails are now being reliably intercepted. Notably, many mass mailings and phishing attempts that previously slipped through are now effectively blocked. In the past, we often had to send out company-wide warnings urging employees to delete dangerous emails immediately – this is now rarely necessary.

Overall, Advanced Email Security has greatly strengthened our defenses and prevents dangerous messages from ever reaching users.

HOW HAS YOUR EMAIL SECURITY POSTURE EVOLVED – INCLUDING EMPLOYEE SAFETY AND AWARENESS?

End users rarely notice email security in their daily work because suspicious messages are filtered silently in the background. As a result, awareness of email threats could decline, which is why our CISO continues to provide regular user training.

For the IT Security team, however, the introduction has been a clear success. Significantly more threats are intercepted, and the number of support tickets has dropped sharply. Previously, employees frequently asked whether suspicious messages were spam – today, such emails rarely reach them. This relieves both users and the security team.

Currently, we still maintain an additional control layer: users cannot self-release quarantined emails; approval is required from the IT Service Desk. This ensures an added level of protection, as users may still overlook forged messages.

The combination of multiple protection mechanisms has substantially reduced overall risk. We are particularly impressed by the AI capabilities – analyzing attachments, links, QR codes, sender reputation, icons, and communication patterns. Advanced Email Security correlates hundreds of signals per email, evaluates them in context, and continuously learns and improves.

WHAT ADVICE WOULD YOU GIVE TO OTHER COMPANIES SEEKING TO IMPROVE EMAIL SECURITY?

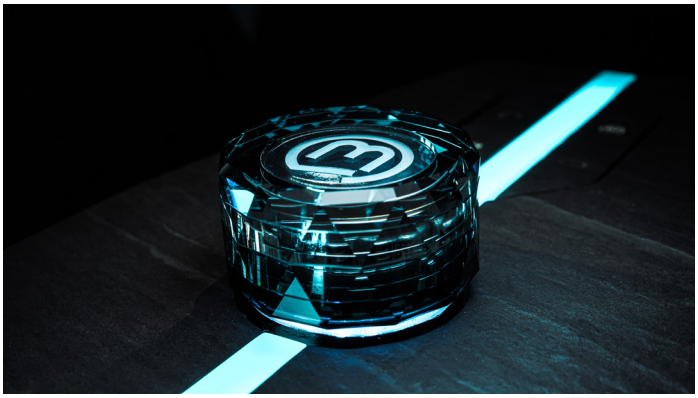
Definitely consider Advanced Email Security – and above all, run a Proof of Concept. That's the only way to obtain concrete, verifiable data. Gut feelings or fear-based arguments don't convince management; numbers do.

It's crucial to make the risks clear: a successful attack can have existential consequences. In our case, the PoC results, the CISO's prioritization, and the board's awareness of risk led to approval – despite the difficult economic environment.

> **Email security is the most critical attack vector. Investing here is one of the most effective ways to reduce overall exposure.**

Heiko Wirth, Chief Information Security Officer

Because security budgets are limited, priorities must be set. For us, email security is a top priority: it's the most common attack vector and one every employee can relate to, since everyone uses email daily.



WOULD YOU LIKE TO SHARE ANYTHING ELSE ABOUT YOUR EXPERIENCE WITH EMAIL SECURITY OR OPEN SYSTEMS?

A key success factor for us is Open Systems' all-inclusive service, which consistently operates at a high standard and offers a wide range of solutions on a single platform. Having dedicated Technical Account Managers who know our environment is extremely valuable and contributes greatly to the efficiency and security of our email communication.

We operate globally and previously had separate solutions at each location. Although we had defined uniform rules for handling email, implementation was inconsistent – standards varied, and processes differed.

With Open Systems' centralized solution, we now benefit from a unified platform and 24x7 support. This means we're no longer woken up at night; instead, local teams can contact Open Systems directly, have incidents reviewed, and obtain guidance whenever needed.

Stefan Bast
IT Security Officer
Marquardt

Philipp Schuster
IT Infrastructure Security
Marquardt

A FINAL **SUMMARY**

THE CHALLENGE

Phishing attacks are becoming increasingly sophisticated – fueled in part by AI, which enables highly realistic emails, targeted social engineering, and the evasion of traditional filters. To counter the rising flood of phishing and spam emails, Marquardt set out to strengthen its defenses – even with existing protections in place such as Secure Email Gateway (SEG) and Microsoft 365 Defender. At the same time, the company aimed to reduce operational workload.

THE SOLUTION

Marquardt chose Advanced Email Security from Open Systems, a centralized, fully managed solution that integrates seamlessly into the company's existing infrastructure. With 24x7 support, a unified platform, and intelligent protection engines, Marquardt was able to significantly enhance its email security posture.

THE RESULTS

Today, roughly 25% more potentially harmful emails are reliably blocked, while false positives have dropped to under 0.1%. Ticket volumes have declined noticeably, and Marquardt enjoys stronger protection against phishing attacks – reducing both reputational and financial risk. The IT Security team and IT Service Centers have also seen a marked decrease in workload.

About Marquardt

The family-owned Marquardt Group, headquartered in Rietheim-Weilheim, Germany, has been developing and producing mechatronic switch and control systems since 1925 – serving industries such as automotive, household appliances, and power tools. With around 10,000 employees at 21 global locations, the group generated approximately €1.4 billion in revenue in 2024.

Open Systems provides Managed SASE solutions that combine networking and security functions on a cloud-native platform, securely connecting hybrid IT environments for greater efficiency, enhanced security, and maximum scalability.

Discover more at **open-systems.com** |