How a Swiss Asset Manager Reduces Email Security Risks

Enabling Qapital

> **During the test, we clearly saw that up to 40% more suspicious emails were filtered out, and that has a direct impact on reducing our risk.**
>
> Christoph Dreher, Executive Management & Partner

Summary

Enabling Qapital, a FINMA-regulated Swiss impact asset manager, faced the challenge of defending against sophisticated phishing attacks that continued to reach employee mailboxes despite existing security controls. By implementing Open Systems Advanced Email Security, the company added a proactive layer of protection to its security architecture. The result: up to 40% more malicious emails intercepted, significantly reduced risk, and stronger protection of its most critical attack vector.

Customer details

- Financial Services
- Zurich, Switzerland
- 60
- enabling.ch

Product used

- Advanced Email Security
- Secure Email Gateway
- Advanced Threat Protection

Results

- **Up to 40%** more malicious emails intercepted
- **80-90%** of attacks addressed at their primary source (email as the main attack vector)
- **Significantly fewer risky emails** reaching user inboxes
- **Low false-positive rate** despite increased filtering effectiveness
- **Additional security layer** protecting users before threats reach the inbox

Interview

We sat down with **Christoph Dreher**, Executive Management & Partner at Enabling Qapital, to talk through their IT challenges and goals – and how Open Systems enabled a holistic solution.

What is your role within the company, and what responsibility do you carry for IT security and email security?

As COO/CFO, I am responsible for several functions, including IT, HR, and Finance. In the second year after founding our company, we made a conscious decision to elevate IT security to the executive and board level. For us, cybersecurity carries the same importance as portfolio management and business development.

Given our international presence, global investments, and geographically distributed workforce, IT security is a business-critical factor. It is not only about preventing attacks but also about managing the potential impact of a security incident. As an asset manager, we depend on the trust of our clients, and that trust must be reflected in the security of our systems and data.

A security-related incident early in the company's history highlighted the importance of robust cybersecurity measures and the opportunity costs that arise when security is not prioritized consistently. Since then, IT security has been firmly embedded at the highest management level and receives the attention it deserves.

Despite our relatively small size, with around 60 employees and close to USD 1 billion in assets under management, we regularly face attacks such as domain impersonation and targeted phishing campaigns. This reinforces our belief that there is no organization today that is immune to cyber threats.

At the same time, cybersecurity is largely a matter of mindset. Security measures are often perceived as a significant cost factor, while their value remains largely invisible in day-to-day operations. That is why strong executive sponsorship is essential to ensure sustainable investment in security.

> **For us, 80-90% of attacks originate through email. It is by far our most critical attack vector.**
>
> Christoph Dreher, Executive Management & Partner

What importance does email security have for your organization, particularly in the context of your global operations?

Email is our primary attack vector. While our endpoints are protected through comprehensive device management, experience shows that 80-90% of attacks originate through email. Ultimately, the deciding factor is always the human element: whether an attack succeeds depends on the user.

Operating internationally further increases the risk, as our communication partners are located across the globe and do not all adhere to the same security standards. As a result, we see inbound email as the most significant entry point for threats.

Our approach consists of two layers. First, we aim to detect and block as many threats as possible before they reach the inbox. Second, we invest heavily in security awareness training to help employees recognize and respond to potential risks. For us, email security is at least as important as device management.

What specific challenges or risks did you face in email security before working with Open Systems?

One defining incident occurred shortly after the company was founded, before we had invested in more advanced cybersecurity measures. An employee's email account was compromised and misused for communication without immediate detection. The attacker attempted to manipulate a financial transaction.

We also experienced attempts to distribute malware through email. These incidents demonstrated how email can serve both as a direct attack vector and as a mechanism for expanding an attack once access has been gained.

As a result, we adopted a holistic security strategy. This includes advanced email security capabilities to identify threats at an early stage, combined with additional protection layers such as Managed Detection and Response (MDR) and Managed Vulnerability Mitigation (MVM). Together, these measures enable us to respond quickly and isolate affected systems when necessary.

What role do your international offices and markets play in your security strategy?

We treat all markets as carrying the same level of risk. As a fully cloud-based organization, particularly through Microsoft 365, we do not distinguish between regions. Whether an employee works in Switzerland or Nairobi is irrelevant to our security model.

> **In asset management, trust is everything. That is why IT security carries the same importance as portfolio management or business development.**
>
> Christoph Dreher, Executive Management & Partner

Our strategy focuses on establishing clear boundaries between internal and external systems while maintaining strict access controls. Looking ahead, we are moving toward a Zero Trust approach based on the assumption that any system could potentially be compromised and that every access request must be explicitly authorized.

What prompted you to introduce Advanced Email Security in addition to your existing solution?

Despite existing protection mechanisms, we observed that certain threats were still reaching users. These included attacks disguised as messages from platforms such as DocuSign or LinkedIn, as well as malicious attachments embedded in PDFs and QR codes.

A major limitation of traditional solutions is their reliance on known patterns and threat databases. As a result, new and highly targeted attacks often go undetected. Open Systems' Advanced Email Security provides a significant advantage through machine learning and relationship-based communication analysis.

Because a large portion of our email communication occurs with established business partners, the system can quickly identify unusual behavior and anomalies within normal communication patterns.

The combination of multiple protection methods significantly reduces risk. These include AI-based analysis of attachments, links, and QR codes, as well as sender reputation checks and behavioral analysis of communication patterns. Each message is evaluated against numerous signals and interpreted within the specific context of our organization, allowing threats to be identified early. The system continuously learns and adapts to emerging attack techniques.

During the testing phase, we observed a substantial increase in the number of potentially dangerous emails detected and filtered out.

> **The service provided by Open Systems is outstanding: fast, highly competent, and delivered at a level that is difficult to find elsewhere.**
>
> Christoph Dreher, Executive Management & Partner

Why did you choose to take this step with Open Systems?

Beyond technical capabilities, the quality of the partnership is critical for us. We place great value on trusted relationships and aim to keep vendor management as simple as possible.

Open Systems' service, particularly through Mission Control, stands out because of its rapid response times and high level of expertise. Unlike some outsourcing models, Open Systems provides around-the-clock access to experienced professionals who can make informed decisions independently.

Regulatory considerations also played an important role. Open Systems has an excellent reputation with FINMA and holds relevant ISO and SOC1/ISAE certifications. Having a provider based in Switzerland is also an important factor for us as a regulated company.

What role did compliance requirements and data sovereignty play?

Compliance and regulatory requirements are central to our business. As a regulated organization, we must ensure that our cybersecurity solutions meet the expectations of regulators and auditors.

Open Systems' certifications and strong market position significantly simplify both audits and regulatory discussions.

Data sovereignty is another important consideration and was carefully assessed as part of our risk analysis. As a Microsoft 365 customer, we operate within a certain level of regulatory complexity, including considerations related to the CLOUD Act. However, we deliberately rely on Microsoft's enhanced customer agreements for the Swiss financial sector, often referred to as the "Swiss Cloud." These agreements provide the framework needed to meet regulatory requirements while still benefiting from cloud technologies.

What insights did you gain from the proof of concept?

The results were highly encouraging. One key observation was that many emails that would previously have been delivered at least to the spam folder were now blocked entirely before they could reach users.

Overall, the proof of concept demonstrated that approximately 30-40% more emails were filtered out compared to the previous solution.

Given that we regularly conduct phishing simulations, both automated and manually designed, we know how easily even well-trained employees can be deceived by sophisticated attacks. Minimizing the number of potentially dangerous emails that reach employee inboxes is therefore essential.

Advanced Email Security showed clear strengths in analyzing communication patterns and detecting sophisticated attack techniques, including QR code-based attacks. It filtered significantly more threats while maintaining a low false-positive rate.

> **Many organizations see email security as a cost factor, until something happens and the true cost becomes visible.**
>
> Christoph Dreher, Executive Management & Partner

What measurable improvements do you expect?

We expect a significant increase in phishing detection rates, particularly for targeted attacks and previously unseen threat patterns, while maintaining low false-positive rates.

A key objective is to quantify how many additional malicious emails are intercepted and to track this performance over time. These metrics are monitored and reviewed regularly.

How would you describe your collaboration with Open Systems?

> The partnership is characterized by openness, direct communication, and deep technical expertise. Despite our size, we have dedicated contacts in both account management and technical support.
>
> Compared with other providers, we experience considerably faster response times and a much higher quality of support. That level of service creates significant value for us.
>
> Overall, we regard the collaboration as consistently excellent.

How does the team support you on a day-to-day basis?

> Mission Control serves as our primary operational point of contact. Requests and reports, including false-positive cases, are handled quickly and professionally.
>
> For us, the most important differentiator is the combination of fast responsiveness and technical expertise.

Why would you choose Open Systems again?

> Three factors stand out: exceptional service, deep expertise, and technologically advanced solutions. We also value the company's clear innovation roadmap and focus on the security challenges that matter most.

What insights did you gain from the FINMA audit, particularly regarding your security posture compared to other organizations?

> For us, the outcome of the latest IT audit provided strong confirmation that our security strategy is on the right track. Being ranked among the top 5% demonstrates that we not only meet key requirements but achieve an above-average level of security in critical areas.
>
> At the same time, this strengthens our clients' confidence that their data is being protected to the highest standards. IT security has therefore become an integral part of our quality commitment and customer trust proposition.

What advice would you give to other organizations?

> Email security should be regarded as one of the most important pillars of any cybersecurity strategy. It extends far beyond traditional spam filtering and has a major impact on an organization's overall risk profile.
>
> Companies should be willing to invest in preventive controls rather than relying solely on standard security solutions. In our view, security measures that filter threats before they reach users are essential.
>
> Our experience also shows that even established solutions such as Microsoft 365 Defender do not reliably detect every attack. A layered security approach that combines multiple technologies is therefore critical to reducing risk sustainably.

Christoph Dreher
Executive Management & Partner
Enabling Qapital

A Final Summary

The Challenge

As a globally active and Swiss-regulated financial institution, Enabling Qapital is exposed to a consistently high level of cyber risk. Email represents the organisation's most significant attack vector, as many attacks rely on user interaction to succeed. Despite existing security measures, sophisticated phishing emails continued to reach employee inboxes, increasing the risk of fraud, data loss, and financial damage.

The Solution

With Advanced Email Security, Enabling Qapital strengthened its existing security architecture with an additional layer of protection before messages reach end users. Using heuristic analysis, AI-powered threat detection, and contextual intelligence, the solution identifies and blocks both known and previously unseen attack techniques, particularly targeted phishing attempts.

The Results

The proof of concept demonstrated a clear improvement in email security effectiveness. Up to 40% more potentially malicious emails were detected and blocked, while significantly fewer risky messages reached employee inboxes. As a result, Enabling Qapital benefits from substantially stronger protection against its most critical threat vector while maintaining a low false-positive rate.

About Enabling Qapital

Enabling Qapital Ltd. (EQ) is a FINMA-regulated, leading Swiss impact asset manager dedicated to a world where investments generate financial, social, environmental, and economic returns. With over USD 900 million under management, EQ invests through private debt and listed bonds, pursuing strategies focused on microfinance, access to energy/clean cooking, as well as emerging market bonds.

Open Systems is an AI-powered SASE platform provider that combines secure access, networking, and AI-driven operational processes. This enables organizations to run complex hybrid and multi-cloud environments securely, efficiently, and with full visibility.