CYBERSECURITY BETWEEN HOME OFFICE AND THE CAYMAN ISLANDS IN FINANCIAL SERVICES

> **Open Systems allows us to work securely in a single, shared cloud environment worldwide – fast, reliable, and without compromise.”.**

Chief Operating Officer, Financial Services Company

SUMMARY

The internationally operating financial firm was facing rising cyber risks, increasing compliance requirements, and limited internal IT resources.

With Open Systems, it adopted a comprehensive security architecture combining **ZTNA, cloud proxy,** and **24x7 managed services**. The result: stronger security, reliable global access, simplified management, improved compliance reporting, and significantly fewer security incidents – all at predictable cost.

.

CUSTOMER DETAILS

- Financial Services
- 3 Continents
- ~40 Employees

PRODUCTS USED

- SD-WAN
- ZTNA

RESULTS

100 %
MALWARE PROTECTION
in known cases

24x7
SUPPORT
to reduce staffing needs

100 %
PREDICTABILITY
thanks to all-inclusive flat pricing

0
SECURITY INCIDENTS
even under high threat levels

100 %
CLOUD-FIRST SECURITY
for safe remote work

We sat down with the Chief Operating Officer of a financial services company to discuss the company's past challenges and goals, and how Open Systems provided a comprehensive solution.

WHAT IS YOUR ROLE WITHIN THE COMPANY?

I am the Chief Operating Officer of our corporate group. While we employ around 40 people overall, our organization is internationally distributed. Our headquarters are in Zurich, where a small core team of four to five people is based. Our operational entities are in Ireland and Singapore, each with approximately 16 employees.

As the Group COO, I am primarily responsible for our entire IT infrastructure and for the IT services we provide to our global locations.

WHAT CHALLENGE WERE YOU AIMING TO ADDRESS TOGETHER WITH OPEN SYSTEMS?

Our collaboration with Open Systems started before I joined the company. At that time, we also had an office in the United States, and the main objective was to reliably connect all our locations. From the very beginning, the connectivity between our local servers worked extremely well – and it continues to do so today.

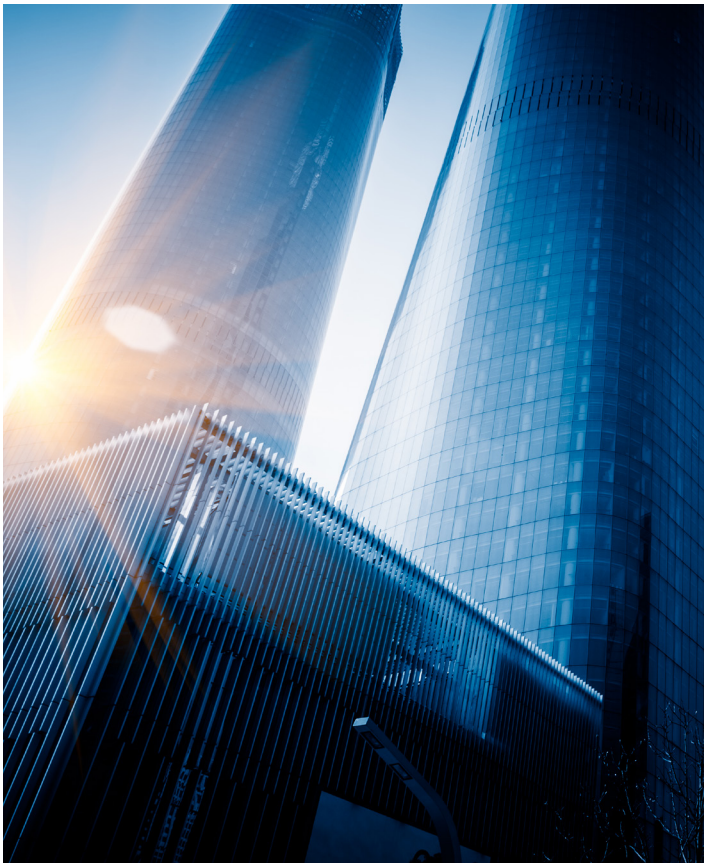
When we later moved to the cloud, this requirement became even more important. Open Systems now ensures that all employees worldwide can access our cloud environment securely and reliably at all times.

WHAT DID YOUR NETWORK AND SECURITY SETUP LOOK LIKE BEFORE WORKING WITH OPEN SYSTEMS?

In the past, we employed two internal IT specialists who handled all IT-related tasks themselves. When I joined the company, only one internal IT employee remained. After that person left, we faced a fundamental decision: either hire a new in-house specialist or fully outsource IT operations.

We chose to outsource. We handed over our internal IT infrastructure to an external cloud provider, while firewall and network responsibilities were assigned to Open Systems. Since then, my role has largely involved coordinating between the different service providers.

This model has clearly proven successful. Today, IT systems must be available and secure around the clock. Since many cyberattacks occur at night or on weekends, 24x7 support was essential for us – and simply not realistic with only two or three internal IT staff. That is why I firmly believe outsourcing these areas is the right approach, and Open Systems has been an ideal partner for us.



HOW HAS USING OPEN SYSTEMS SD-WAN CHANGED YOUR DAY-TO-DAY OPERATIONS?

For a company of our size, operating a proxy firewall is somewhat unusual. It does make the setup more complex, but it also significantly improves security. We discussed for a long time whether the added effort was justified. In hindsight, I can clearly say that it was.

In at least two cases, the proxy firewall prevented malware from establishing a connection to its command-and-control servers – exactly what this solution is designed to do.

About two years ago, we implemented a major change. In Zurich, roughly half of our team works remotely, and at the time we were still using a physical firewall at the office. Today, we rely entirely on ZTNA and additionally use cloud proxies. This combination has proven to be extremely effective for us. Internet access is now provided locally through the cloud proxy, which works very well in Zurich.

In Singapore and Ireland, we continue to operate physical firewalls at the office, supplemented by ZTNA for remote work. Overall, the

> **ZTNA has significantly improved our security while reducing complexity. Access can be configured more precisely, and the solution is truly 'always on.'**

transition has made a lot of sense and has significantly strengthened both our network and security architecture.

WHY DID YOU MOVE FROM MOBILE ENTRY POINT (MEP, CLIENT VPN) TO ZTNA?

Before making the switch, we experienced numerous hacking attempts, and user accounts were frequently locked. That was a clear indication that our attack surface was too large. At the same time, it became evident that our existing setup was unnecessarily complex and that ZTNA would offer clear advantages.

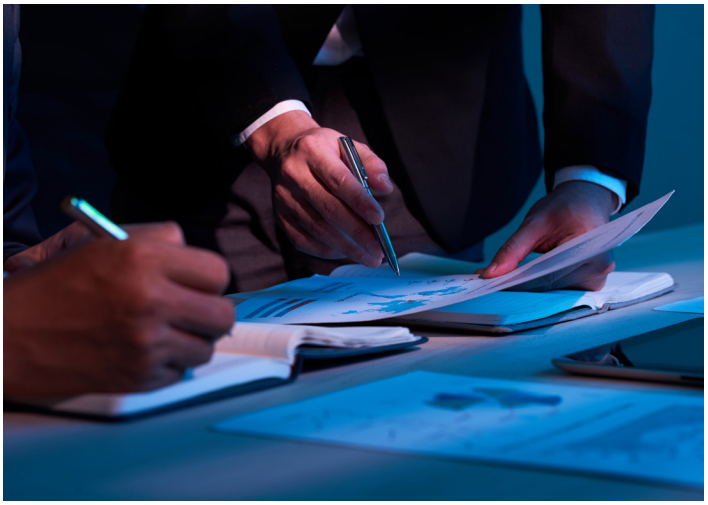
ZTNA not only improves security but also reduces reliance on local infrastructure. When working from home, we previously needed MEP and often a locally hosted proxy, which led to certain limitations. With ZTNA combined with cloud proxies, we gain much greater flexibility. Because Open Systems operates globally distributed Points of Presence (PoPs), the impact on performance is significantly reduced.

What we value most about ZTNA is the granular access control and the ability to implement a true always-on security model.

WHY DID YOU CHOOSE ZTNA FROM OPEN SYSTEMS?

We were already an Open Systems customer and had consistently positive experiences. It also made sense for us to source all security-relevant services from a single provider, as that greatly simplifies collaboration. In addition, the price-to-performance ratio was very compelling.

We particularly appreciate the all-inclusive approach. Transparent flat-rate pricing allows us to plan our IT costs reliably and maintain full cost visibility at all times.



DID FINANCIAL INDUSTRY REQUIREMENTS INFLUENCE YOUR DECISION?

We are an attractive target for cyberattacks, which is evident from the large volume of phishing emails we receive every day. As a financial services company that regularly processes high-value transactions, attackers often attempt man-in-the-middle attacks.

They may compromise customer email accounts or try to gain access to our systems in order to send fraudulent invoices with manipulated bank details. We encounter such attempts on an ongoing basis, which makes constant vigilance essential. That is exactly why we rely on Open Systems' security solutions – they help us consistently and effectively reduce these risks.

WHAT ROLE DOES THE 24X7 MANAGED SERVICE PLAY IN DAILY OPERATIONS?

It plays a critical role for us. When a security incident occurs – and experience shows that this often happens in the evening or on weekends – it is extremely valuable to have access to true 24x7 support.

Our cloud service provider also offers round-the-clock assistance, and in critical situations these services work seamlessly together. This gives us confidence that we will receive fast and reliable support whenever it is needed.

WHAT CONCRETE IMPROVEMENTS HAVE YOU SEEN FROM THIS COLLABORATION?

I am aware of at least two specific incidents where our proxy firewall prevented malware from connecting to a host. Such risks arise constantly – for example, when someone accidentally opens a malicious file.

In both cases, the antivirus system triggered an alert, and the firewall reliably blocked the connection. Incidents like this likely occur more often than people realize. You can regularly see in the log files which threats are being stopped. For us, this clearly demonstrates how effective these security measures are.

HOW DOES ZTNA SUPPORT YOUR REGULATORY REQUIREMENTS (BAFIN, GDPR, ISO 27001, ETC.)?

ZTNA plays a major role in helping us meet compliance requirements and significantly simplifies the completion of numerous questionnaires. Our local entities in Ireland and the Cayman Islands are subject to strict regulatory standards, and many of our clients also require formal proof of compliance.

Insurance is another important factor. Today, it is becoming increasingly difficult to obtain a policy unless you can demonstrate substantial investment in cybersecurity. Fortunately, this has not been an issue for us, as we have continuously strengthened our security posture over the years – and these investments have clearly paid off.

HOW WOULD YOU DESCRIBE THE USER EXPERIENCE TODAY COMPARED TO THE PAST?

The user experience, including the Mission Control Portal, continues to improve. Implementing ZTNA requires a significant upfront effort, as configurations must be very precise. However, that same effort results in a much higher level of security.

Our Technical Account Manager at Open Systems is a major advantage here, as he has deep knowledge of our specific setup. As part of the managed service, we are currently modernizing the environment together so that future updates – such as changes introduced by Microsoft – are applied automatically.

> **ZTNA helps us significantly meet our compliance requirements – especially for our locations in Ireland and the Cayman Islands, where extensive regulatory questionnaires are required.**

This approach also makes day-to-day management much easier. In the past, employees often found it confusing when different firewall rules applied at the office versus at home. By standardizing access through ZTNA, usability has improved significantly.

WHAT DO YOU VALUE MOST ABOUT WORKING WITH OPEN SYSTEMS?

Working with Open Systems is consistently efficient. When we need support, we receive solutions quickly – even in critical situations. I particularly appreciate that complex technical topics are explained clearly and in plain language. This makes collaboration very straightforward, especially for me as someone with a background in finance rather than IT. Even without deep technical expertise, I can easily manage and oversee all processes together with the Open Systems team.

WHAT ARE YOUR NEXT STEPS IN THE ZERO TRUST JOURNEY?

At the moment, we do not have specific next steps defined. Over the past two to three years, we have already implemented a great deal. Our current focus is on consolidation. Once that is complete, we will evaluate which additional measures it makes sense to pursue.

WHERE DO YOU SEE THE NEXT STEP IN YOUR NETWORK OR SECURITY STRATEGY?

Right now, we are looking closely at CASB (Cloud Access Security Broker) solutions. Our employees increasingly use online tools – such as PDF converters – and we want to either block these tools or at least control them more effectively. I expect this need to grow significantly as the use of AI continues to increase.

I am personally a strong advocate of AI and use it extensively. At the same time, this is where the challenge lies. AI applications can make systems more permeable in many ways. While you try to protect data, information often flows out in uncontrolled ways, which creates risks.

> **We're an attractive target for hackers, but with Open Systems we've strengthened our security foundation so much that we're now very well protected.**

We have not yet identified the ideal solution. In many cases, you have to rely on the security standards of individual providers – much like many organizations do with Microsoft, assuming that "What Microsoft does will be ok." With tools such as Perplexity combined with the new Comet browser, for example, it is difficult to understand exactly what data is being transmitted, making it harder to control sensitive information.

WHAT ADVICE WOULD YOU GIVE TO OTHER COMPANIES FACING SIMILAR CHALLENGES?

I firmly believe that investing sufficiently in cybersecurity is always worthwhile. A single major incident can be enough for a small or mid-sized company to lose customer trust. That is why it is critical to invest in security early and consistently to minimize these risks.

IS THERE ANYTHING ELSE ABOUT WORKING WITH OPEN SYSTEMS YOU WOULD LIKE TO HIGHLIGHT?

What stands out most is the 24x7 managed service, which provides a reliable point of contact at all times. Even on weekends, tickets are handled promptly if an issue arises.

At the same time, we benefit from a strong local presence. Not only product development and account management, but also many support staff are based in Switzerland or operate according to Swiss quality standards – and those standards are exceptionally high.

AT A **GLANCE**

THE CHALLENGE

Internationally regulated, a frequent target of phishing and fraud attempts, and operating across distributed locations, the financial firm faced the challenge of meeting the highest security and compliance requirements efficiently and reliably.

THE SOLUTION

With SD-WAN, ZTNA, and managed services from Open Systems, the financial firm unified secure access worldwide. 24x7 support and reduced complexity deliver strong security with ease of use.

THE RESULT

- Significantly **stronger security** paired with **improved user experience**
- **High compliance and audit readiness** despite international regulation
- **Less operational IT effort** through unified access and services
- **Reliable 24x7 operations** with **predictable costs** and fast support

Open Systems delivers co-managed SASE operating models that combine secure connectivity, Zero Trust access and transparent 24×7 operations for complex hybrid and multi-cloud enterprise environments across operations in more than 180 countries.

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