



UBS works with highest standards of reliability and confidentiality

THE CHALLENGE

- Replacement of highly mature email filtering system with a new solution
- Reliability, confidentiality, security and compliance
- Swiss-based solution to meet regulations
- Maintenance of productivity in more than 55 countries

THE SOLUTION

- Open Systems
Secure Email Gateway
- 24x7 operations and security monitoring by level-3 engineers

THE RESULTS

- Highly reliable and stable services seamlessly integrated into UBS operations as processes
- Constant, on-going refinement of filter methods between UBS team and Open Systems engineers
- A sound partnership with profound mastery and understanding of the business

The company

The global bank with strong Swiss roots draws on its 150-year heritage to serve private, institutional and corporate clients worldwide, as well as retail clients in Switzerland. The business strategy of UBS is centered on its pre-eminent global wealth management businesses and its leading universal bank in Switzerland. Together with a client-focused investment bank and a strong, well-diversified global asset management business, UBS is expanding its premier wealth management franchise and driving further growth across the Group.

THE CHALLENGE

Over several years, UBS had raised the workflows of its previous email filter system to a very high level of maturity. When it became clear that the email filter system had to be replaced with a new solution, it was important to maintain or even improve the quality for the users. What's more, for reasons of reliability and confidentiality and from a regulatory point of view, it was crucial to find a Swiss-based solution.

In an average month, UBS employees would typically receive more than 130 million emails in total. A good 70% of these, i.e. more than 90 million emails, were spam and thus undesired. It was necessary to make sure that users of the UBS Group's IT infrastructure in over 55 countries around the world were able to work productively while also complying with the technological parameters defined by the Group.

UBS requires the highest standards of reliability and confidentiality. Satisfying these in the global day-to-day business environment is a demanding task for IT.

CUSTOMER STORY

The workplace culture within a financial group is highly intellectual in nature and based on information which nowadays is practically only available digitally. If it is not possible to access some or all of this information, or if there are delays in accessing it, the ability to act is massively restricted.

The regulatory requirements are highly complex and vary from country to country. In simple terms, one can say that the role of the regulators in the individual countries is to monitor that the bank's activities are documented over several years and can be audited. This is something that UBS must also be sure to comply with IT-wise at all times.

To satisfy both internal and regulatory requirements, the data systems on which client data is stored are strictly segregated physically and geographically. Only the employees with the corresponding authorization actually have access to them.

THE SOLUTION

Physically segregated zones

The architecture of the global model is organized so that there are physically segregated zones. For example, a distinction is made between a red zone and a green zone. These are the zones in which UBS has established the highest possible security standards.

Filtering

Emails are filtered by Secure Email Gateway before they are delivered to the user mailboxes. This is a central function through which all unwanted emails, and also those infected with virus signatures, are eliminated and filtered out accordingly. We are talking about more than 70% spam.

Central management of email user data

Management of email user data is performed directly via the central Identity Management System, which is linked to the HR system. It also records who is based where geographically within the company, which functions individual users have, and what authorizations they need to do their job. This additionally serves to regulate the access rights to IT systems, data and information.



“ We demand the highest standards of reliability and confidentiality.”

Markus Lickert, Managing Director
and Head of End User Services, UBS

THE RESULTS

Open Systems services are highly reliable and stable and are ideally integrated into UBS email operations from a process point of view. UBS still has full control over the activities, enabling its End User Services team to react really quickly if need be. From an operations viewpoint, the UBS 24x7 operational organization enjoys a lively exchange with the Open Systems Mission Control Center, which is considered as a good sign.

In conceptual terms, UBS has a strong foundation thanks to Secure Email Gateway. But it's in the nature of things that a service of this kind will continually go on developing. It's a "never-ending story". That's why the End User Services team has joined forces with the Security Engineers at Open Systems in constantly seeking to refine the filter methods and to introduce new processes and mechanisms so that the filter success rate can be improved – along with the user experience – even further. During this collaboration, UBS finds the Security Engineers at Open Systems to be genuine partners, who are highly competent and open to continuously optimizing the existing service.

A sound partner

“Open Systems is a sound partner, with a profound understanding and mastery of the business, that is also conscientious and has the culture required to do a top-quality job,” summarizes Markus Lickert.



Open Systems is a secure access service edge (SASE) pioneer that enables organizations to connect to themselves, to the cloud, and to the rest of the world. With cloud-native architecture, secure intelligent edge, hybrid cloud support, 24x7 operations by level-3 engineers, and predictive analytics, the Open Systems SASE delivers a complete solution to network and security.