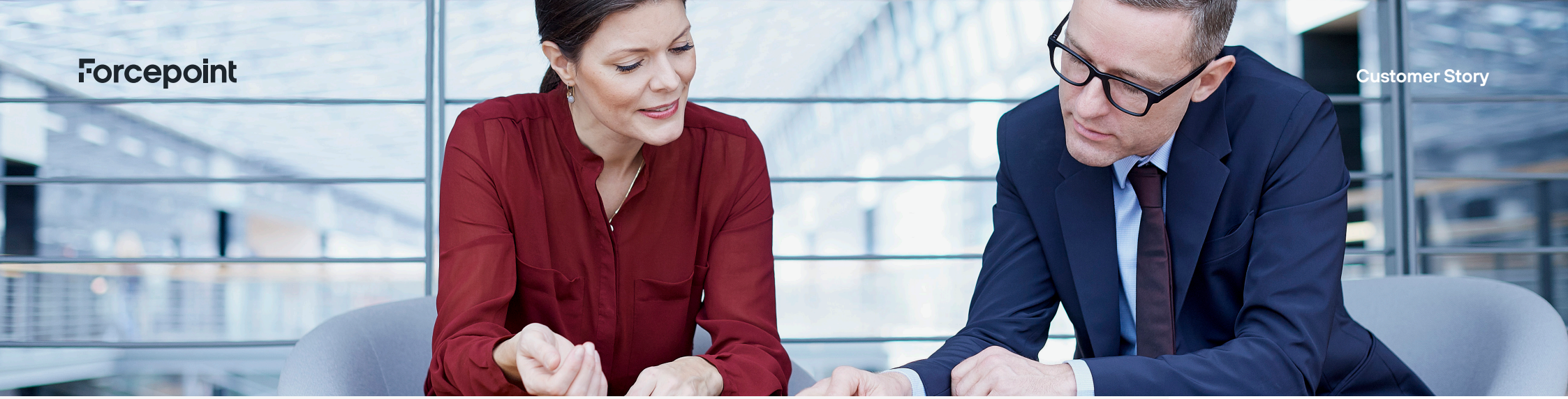

A Fast-Growing Bank Meets Strict Swiss Security Standards, While Maintaining World-Class Customer Service, with Forcepoint

This entrepreneurial Swiss bank relies on a combination of agility and reliability to serve its customers, and relies on Forcepoint DLP to help maintain its reputation as a trusted institution, without getting in the way of its business.

Despite operating in one of the most strictly regulated financial marketplaces in the world, this entrepreneurial Swiss Bank experienced rapid growth with its unique approach to client management. Continued growth requires a diligent effort to maintain a balance of agility and reliability. And with the introduction of FINMA, it needed to find a way to increase security without slowing its growth.

CUSTOMER PROFILE:
Leading private Swiss bank.

INDUSTRY:
Financial Services

HQ COUNTRY:
Switzerland

PRODUCT:
Forcepoint Data Loss Prevention

Since the early 20th century, private Swiss banks have thrived based on their reputation for stringently protecting the private banking information of the world's most wealthy. But the industry has faced daunting challenges in the 21st century: low interest rates and less financial market volatility have lowered profits, while the fastest growing client bases are now farther away, in China and emerging markets. While this caused turmoil in the more traditional banking industry, this startup Swiss bank saw an opportunity to take a different approach with hands-on, proactive customer account managers who can stay on top of rapidly evolving market forces and act decisively when conditions demand. This style of customer service has been so successful with clients the bank has grown quickly in just a few years, from startup to global leader.

While the bank was growing its customer base, Swiss banking regulations became even more stringent with the introduction of the Swiss Financial Market Supervisory Authority (FINMA) in 2007. FINMA has authority over banks, insurance companies, stock exchanges, and other financial institutions, and its data privacy requirements are stricter than the European Union's General Data Protection Regulation (GDPR) mandates.

In 2018, FINMA sent a letter to all Swiss banks with recommendations for technical approaches to safeguarding data. The bank could check all the boxes except one: a data loss prevention solution. In order to address the gap, without impacting the firm's continuing growth and its customer relationships, it turned to Forcepoint.

Safeguarding a wealth of data

Swiss banks don't just contain money. They hold a wealth of data on customers, employees, and business partners—none of which is allowed to leave the country, according to Swiss banking regulations. In addition, banks contain intellectual property on their structured banking products that would be of tremendous value in the hands of competitors. One major challenge to safeguarding this bank's data: tremendous growth. The potential for an outside threat like malware, phishing, and social engineering preying on an internal weakness keeps the bank's Head of Information Security up at night. "Having almost doubled our staff over the last years, the exposure has doubled as well," he explained. "We trust in the integrity of our employees 100%. Nevertheless, one is never immune from an accidental data breach. Such a breach would both damage the reputation of our bank and cause enormous costs."

> "Having almost doubled our staff over the last years, the exposure has doubled as well. We trust in the integrity of our employees 100%."
>
> HEAD OF INFORMATION SECURITY, PRIVATE SWISS BANK

Protection and control down to the endpoint

The IT team ran a benchmarking process to identify the most suitable DLP software on the market. The shortlist included two providers, which were examined in a proof-of-concept with sophisticated security tasks. "The Forcepoint solution achieved far better results in the test and was also able to demonstrate more scope of services. In addition, the system performs controls directly on users' workstations, ensuring maximum efficiency, another benefit," recalls the Head of Information Security (IS). "For these reasons, we immediately decided to use Forcepoint Data Loss Prevention (DLP)."

Challenges

Swiss bank to move swiftly to serve its customers, while maintaining their trust.

A doubling of staff over the last few years increased the risk to customer data as well as valuable information on proprietary, structured banking products.

Swiss banking regulations require that customer, employee, and partner PII not leave the country, while the bank must also comply with multiple data regulations across the many countries it operates in.

Approach

Implement Forcepoint Data Loss Prevention to prevent accidental and malicious data loss.

A powerful centralized solution in a distributed data environment

The biggest implementation challenge related to the mandatory storage of sensitive data. In addition to Swiss law, the bank is under the control of many regulators worldwide, whose laws usually stipulate that affected data must be stored within the respective national borders. Therefore, the bank's IT managers initially planned a completely decentralized use of the software. However, this procedure proved too complex and expensive to maintain. Ultimately, Forcepoint Security Manager allowed the bank to host the system in Switzerland centrally, but gives branch offices the ability to customize guidelines to align with the regional authority.

After the go-live, the benefits of the investment quickly became apparent. The firm is now able to stay attuned to data flowing seamlessly across all channels—especially those that cannot be blocked. Several administrative areas can be defined so the bank can create separate guidelines for different global locations and delegate administration to them.

Protecting data by protecting people

The bank's head of information security believes that the implementation of a DLP solution in itself has raised employee awareness of data security. They handle information more consciously and cautiously, taking more responsibility for data security, he explained.

Even so, accidental mishandling can never be ruled out. When this happens, Forcepoint DLP prevents employees from unintentionally emailing or knowingly copying protected data to external and removable media. Outgoing messages are scanned completely, and the system is able to automatically recognize classified data and block its transfer.

In addition, the solution controls the private data employees can take with them when leaving the company. The review of this data was previously conducted manually, allowing the risk of data leakage in the process. Now, these files are systematically scanned with the solution's discovery capabilities.

Long-term security for data and reputation

"Forcepoint DLP is now a key component of our security architecture. We are able to protect our sensitive data from abuse, ensure the privacy of our clients as a strategic goal, and secure the bank's reputation in the long term," the Head of IS summarized. "It has taken our entire data and information security management abilities to a whole new level."

Results

With the addition of DLP, employees have become more sensitized to data security.

Manual review of files leaving the company when an employee leaves has been replaced with a systematic scan by the solution's discovery capabilities.

Forcepoint DLP is now considered a key component of the bank's security architecture.