EFG Bank

HP Enterprise Security Customer Case Study

"I'm simply amazed at the speed of ArcSight Logger. We collect about five million events per day and are now able to run reports across our entire dataset in a matter of seconds, not minutes or hours. I never thought it was possible to get reports so quickly. This is just fantastic."

—Claude Bilat, former Chief Information Officer, EFG Bank

HP Enterprise Security Customer Case Study:
ArcSight allows EFG Bank to pinpoint the exact location of any issues on its network and respond immediately with specific, policy-based actions.

Industry:
Banking

Customer Brief

EFG Bank is the private banking arm of EFG International, a global banking group offering private banking and asset management services. Headquartered in Zurich, Switzerland, EFG International's group of private banking businesses currently operates in 50 locations in over 30 countries, with approximately 2,000 employees. EFG International is a member of the EFG Group, which is the third-largest banking group in Switzerland.

Product(s)

- ArcSight SIEM Platform
- ArcSight ESM
- ArcSight Logger
- ArcSight TRM
- ArcSight Connectors

Business Benefits

- ArcSight Logger helps EFG meet key requirements of Switzerland's banking laws fast and cost-effectively
- ArcSight ESM enables EFG to protect customer data and combat security threats
- ArcSight SIEM Platform allows EFG to act like a much larger organization, with far fewer people

EFG Bank Business Challenge

Customer data is the main asset of EFG Bank, so it must be safeguarded at all costs. The bank needed an efficient, reliable and automated security management system that could keep external threats at bay, as well as protect against any possible insider threats and data breaches.

Because Switzerland is highly regulated when it comes to banking, Swiss banks like EFG must also maintain their records and event logs for up to ten years. Due to this long-term data retention requirement, EFG needed a cost-effective way to collect, secure and store audit-quality log data in an easily accessible log repository.

Another challenge is the sheer volume of event logs that EFG generates on a daily basis. Each year, EFG collects and stores over two billion events originating from numerous sources ranging from networking equipment and security devices to databases and homegrown applications. Given the wide variety of log formats and the ever-growing volume of logs generated, EFG needed a log management infrastructure that could support the rapid collection of large log volumes.

The ArcSight Solution

On the security front, EFG Bank implemented the full ArcSight SIEM Platform including ArcSight ESM, ArcSight TRM, ArcSight Connectors and ArcSight Logger. In particular, ArcSight TRM allows EFG Bank to pinpoint the exact location of any issues on its network and respond immediately with specific, policy-based actions.

For example, if anyone logs onto the EFG network and then tries to access its central banking application from a non-approved laptop or desktop, ArcSight TRM will automatically deny access and throw that person off the network, thus adding an extra layer of protection to EFG's banking operations.

On the compliance front, ArcSight Logger allows EFG to quickly and easily capture, analyze and store audit-quality log data. It also ensures that the data it collects cannot be modified in any way, which was a major requirement for EFG. ArcSight Logger not only preserves logs in their original form, it is able to prove that after logs are captured, they are not subsequently tampered with or modified, thus satisfying a key aspect of Switzerland's banking law.

"This is a feature that really attracted us to ArcSight Logger in the first place," says Claude Bilat, former Chief Information Officer of EFG Bank. "There are so many reports we have to produce to demonstrate compliance with banking regulations. We simply could not do this without ArcSight Logger. The product was just what we needed to solve our long-term storage issue and meet our compliance requirements."

The ArcSight Impact

EFG is benefitting greatly from the blazing speed of ArcSight Logger. The product is capable of capturing raw logs at sustained rates in excess of one hundred thousand events per second per appliance.

"I'm simply amazed at the speed of ArcSight Logger," says Bilat. "We collect about five million events per day and are now able to run reports across our entire dataset in a matter of seconds, not minutes or hours. I never thought it was possible to get reports so quickly. This is just fantastic."

EFG has also implemented ArcSight ESM to protect its perimeter from hackers and guard against fraud and insider threats. In one case, EFG connected all its printers, scanners and photocopiers to ArcSight ESM. If, for example, an employee copies or prints out a suspiciously large amount of customer account data, EFG can correlate this action against other factors to see if it is facing a potential issue, such as industrial espionage or fraud.

ArcSight also allows EFG to do more with less. This is critical because EFG operates a very lean IT organization and does not have the resources to manually monitor its network for security events. Instead, EFG can rely on ArcSight solutions to automatically pinpoint suspicious behavior on its network and automate time-consuming processes related to compliance requirements. "With ArcSight products, we can have far fewer people doing the job of a much larger organization," says Bilat.

ESP-CCS004-101708-02, Created August 2011