splunk>

CASE STUDY

PostFinance Delivers Improved Fraud Detection and Enhances Customer Experience

PostFinance
Surpassing support.

Executive summary

PostFinance is the third largest retail bank in Switzerland with just under three million customers. It provides a full range of financial products to both consumers and merchants with an established position as the number one payments provider in Switzerland. The bank needed to improve visibility into its payments processing and online banking services to be more proactive in addressing threats and protecting customers from potentially fraudulent activity. Since deploying Splunk Enterprise, PostFinance has seen benefits including:

- Improved debit card fraud detection
- Real-time Operational Intelligence across its online banking platform
- Better overall visibility into its payments architecture

Why Splunk

Protecting its customers' financial assets and personal data from criminal elements is a top priority for PostFinance. With a large quantity of machine data generated and stored due to government regulation, the bank recognized that this resource could be used to drive greater value, with particular focus on fraud prevention and security.

Splunk Enterprise is used by the fraud management team at PostFinance to provide insight into the online shopping solution used by 11,000 merchants in Switzerland. It monitors the technology at each stage of the buying process, providing useful data for the team to analyze. Around 50 automated fraud searches feed data into a dashboard that enables the fraud management team to track activity, as well as allowing for ad hoc searches and reporting according to the team's needs.

The Splunk platform also monitors the company's online banking portal, which is used by 1.6 million customers. When the online security team is alerted to a potential attack, they mimic the actions of a customer to get more information. Each attack stage is monitored through Splunk

Industry

- Financial Services

Splunk Use Cases

- Security and Fraud
- Application Delivery

Challenges

- Absence of operational visibility across the online shopping solution
- Need to build an in-house fraud security solution for PostFinance debit cards
- Changing security landscape required an improved ability to respond to potential phishing attacks

Business Impact

- Streamlined fraud detection across online and in-store transactions
- Introduction of operational visibility enables the security team to quickly identify and respond to phishing attacks and other online threats
- Improved ability for product management teams to respond to merchant needs

Data Sources

- E-commerce applications
- Web server logs
- Middleware logs
- DB logs (Oracle and MSSQL)
- Online banking logs
- Network devices and appliances
- Reverse proxies
- Unix, Solaris and Windows Server

Splunk Products

- Splunk Enterprise

Enterprise, providing details such as the pattern for fraudulent activity and whether further action is needed.

Insights shine a light on debit card fraud

PostFinance had to develop its own security and fraud detection system to protect customers using debit cards within the bank's payments processing solution. PostFinance relies on Splunk Enterprise to monitor this system, streamlining and improving its security and fraud detection capabilities. Previously, the fraud management team would have to manually create a complex multi-tier database and application stack in order to find anomalies or patterns in merchant transactions. Using the Splunk platform, PostFinance now automates a large part of this process, saving time and resources that can be deployed to other critical areas of IT operations. With the extra layer of operational insight provided by data generated through debit card transactions, the fraud management team can now proactively address potential issues by operationalizing a fraud workflow that reviews data. Detection mechanisms can then be added to the system within minutes including access to historical verification. This allows for the identification of new fraud patterns such as a suspiciously large number of new customers visiting a merchant, enabling PostFinance to escalate issues to law enforcement.

Better visibility across data results in better customer protection

As well as upgrading the fraud detection capabilities around debit card use, PostFinance has seen benefits from the Splunk platform across its online banking website and app, E-Finance. Before the deployment, attempts to track online security attacks had been hindered by a lack of holistic visibility into the data being produced at different stages of the attack.

"Our use of the Splunk platform has grown dramatically and it is now an integral part of our IT operations, providing insights in areas from e-commerce to security and fraud. Ultimately, with Splunk Enterprise, we have improved the protection we offer our customers."

Patrick Hoffman, Head of IT Infrastructure
PostFinance

With Splunk Enterprise, all the data generated from, for example, potential phishing attacks can be tracked and mapped, so they can be identified and mitigated faster. Through this improved operational visibility, PostFinance is now able to offer a better online banking service to its customers, ensuring they are more secure against the growing volume of online threats.

Improved insight into merchant success and performance

With greater visibility into merchant data, the PostFinance product management team has been able to innovate its services and offer new tools and products to meet customer needs. One example is that the team can now view transactions and revenue of merchants using its payments services over a set period of time through a Splunk dashboard. This allows the team to make decisions based on previously inaccessible data, offering customers a value added service. This dynamic approach to customer service has contributed to the continued leadership of PostFinance in the payments field in Switzerland.