Case Study

European Bank Ensures Compliance and Combats Insider Threats

The challenge

Our customer is a large financial organization that works in several European countries. They rely on complex IT infrastructure to deliver their services and rely on a server monitoring system to ensure data security. As the organization grew, they found it increasingly challenging to monitor their infrastructure and protect sensitive data with their existing software.

That's why they started looking for a more scalable and easier to use cybersecurity solution that would help them perform the following tasks:

- **Ensure secure data processing on terminal servers**

  The customer stores sensitive financial data on several terminal servers and needs to know that all employees handle that data securely.

- **Stay compliant with industry IT requirements**

  The financial industry is highly regulated by various laws, standards, and requirements (including the GDPR and PCI DSS) that compel financial organizations to protect sensitive data, monitor user activity, manage access, etc. Non-compliance with any of them can lead to massive fines and reputational losses. That's why it was extremely important for our customer to maintain a high level of data security.

- **Rapidly audit compliance**

  Complex IT infrastructure and a growing amount of sensitive data made it challenging for our customer to conduct internal audits and assess compliance. Audits started taking too much time and effort from security officers.

- **Prevent insider threats**

  Banking institutions store sensitive financial data that may attract malicious insiders and create additional security risks. Our customer had faced insider threats in the past and was well aware of the damage they can inflict. That's why they were looking for a solution that would allow them to detect and stop malicious insider activity in a timely manner.

The customer

Organization type:

Banking institution

Location: EU

Must comply with: GDPR, PCI DSS, Payment Services Directive 2, European Central Bank recommendations

Pending issue:

- Ensure the security of sensitive data
- Comply with IT requirements and corporate policies
- Conduct rapid audits
- Detect and stop insider threats

To choose the software that would cover these needs in the best possible way, our customer-to-be tested several monitoring solutions. After half a year of evaluation, they chose Syteca.

During the pandemic, the customer needed to switch lots of employees to remote work while maintaining the required level of data protection. They discovered that they could ensure secure data access and processing for remote workers with the Syteca platform.

Customer's needs	The result	Our solution
Ensure secure data processing on terminal servers	Insights into user activity on terminal servers	Deployment of monitoring agents on terminal servers
		Alerts and notifications on security incidents
Stay compliant with industry IT requirements	Ability to maintain cybersecurity compliance	Continuous user activity monitoring
		Secure management of user credentials
		Ability to manage user access to sensitive data
Rapidly audit compliance	Fast and efficient internal audits	Accessing audit data via an easy-to-use web management tool
		Scheduled and ad-hoc reports
Prevent insider threats	Ability to detect and stop malicious insider activity in real time	Ability to monitor the activity of in-house and remote users
		Alerts on suspicious activity
		Manual and automated incident response to insider threats

The results

In the first months after deployment, our customer found that the Syteca platform fully fit their key requirements and was easy to use and maintain. After the deployment, they were able to:

- ✓ Get insights into user activity on terminal servers
- ✓ Ensure fast and efficient internal audits
- ✓ Maintain cybersecurity compliance
- ✓ Detect and stop malicious insider activity in real time

How we did it

The Syteca platform helps our customer monitor complex and constantly changing infrastructure. They find these capabilities and features especially useful:

Deployment of monitoring agents on terminal servers

Our customer is focused on protecting sensitive data stored on remote servers by deploying monitoring agents on these servers instead of on user machines. Agents can detect security issues on their servers in real time or review records of any user action.

Alerts and notifications on security incidents

The customer's security officers receive an alert each time Syteca detects user activity that violates the security rules. Using the alert and real-time review of a user session, officers can investigate security incidents fast.

Continuous user activity monitoring

By deploying user activity monitoring, our customer enhanced compliance with the GDPR and PCI DSS, which require continuous monitoring of all activity with sensitive data. Predefined and custom security rules and alerts on suspicious activity help them detect and respond to insider threats in real time, protecting sensitive data.

Secure management of user credentials

According to PCI DSS and PSD2, financial organizations have to manage user credentials securely. Syteca helps them to do so by providing a password manager that automatically creates, stores, handles, and terminates credentials.

Ability to manage user access to sensitive data

The ability to granularly manage user access rights allows our customer to ensure that only users that need to work with financial data can access it. To limit access to the most sensitive resources, they provide users with access only during working hours.

Ability to access audit data via an easy-to-use web management tool

During an internal audit, security officers have to review hundreds of user actions that may endanger sensitive data. That's a time-consuming process. With Syteca's simple web management tool and built-in YouTube-like video player, they are able to review users' sessions quickly and efficiently.

Scheduled and ad-hoc reports

Reporting is an essential part of internal and external audits. Syteca helps security teams automate this process and save a lot of time by generating reports in a couple of clicks.

After several years of cooperation, our customer has also come to appreciate Syteca's flexibility to cover their needs when scaling infrastructure and adding new platforms or licenses.

Request a free demo to see how Syteca helps you ensure data security and stop insider threats!

www.syteca.com

Syteca

info@syteca.com