CASE STUDY

Privileged User Monitoring and Auditing for a US-based Financial Services Company

THE CHALLENGE

Our customer works with highly sensitive data: financial records, cardholder data, personal information of end customers. Therefore, they must comply with a number of local and international cybersecurity standards including PCI DSS, SWIFT CSP, and NIST 800-53. A large portion of the data our customer works with is stored in their own private data centers. To secure this data, access to the data centers is severely limited and can only be obtained via a jump server.

Our customer needed a cost-efficient solution for thoroughly monitoring and auditing the activity of privileged users on their jump servers. They also had two other vital requirements:

Customer requirements for privileged user monitoring

- Support for both Windows and Linux
- Support for offline updates

1) **The monitoring solution needed to support —** both Windows and Linux.

2) **The solution needed to allow offline updates,** as the server it was to be installed on has no direct access to the internet.

Previously, the customer used a different popular insider threat management solution, but that product didn't fully meet these two critical requirements. After considering several alternative solutions available on the market, they decided to deploy Ekran System.

THE CUSTOMER

Our customer is a US-based financial services company that operates globally. They provide a wide range of financial services, including transferring funds and processing electronic payments.

THE SOLUTION

Ekran System is a full-cycle insider threat management platform. It enables continuous monitoring and logging of user activity through the installation of Ekran System Clients on servers, jump servers, and workstations that need to be monitored. Ekran System can record data both offline and online and then sends it to Ekran System Server for safekeeping.

In this way, Ekran System helps organizations manage insider threats and meet the requirements of cybersecurity standards and financial industry regulations.

Ekran System is a **cross-platform solution** that can be used for monitoring user activity on servers running both Windows and Linux — precisely what our customer needed.

Our customer's network includes several data centers with critical data and applications requiring strict protection. Privileged users — remote workers and third parties — can only access these data centers through protected jump servers via a VPN. Therefore, we offered to **install the Ekran System Client only on the customer's jump servers.** In this way, the customer acquired full visibility into privileged user activity with a minimal deployment and minimal maintenance.

In contrast to other insider threat management solutions, Ekran System **supports two ways of updating the software:** scheduled online updates and manual updates in offline mode. As our customer wanted to keep the server collecting monitoring data as secure as possible, they disabled any direct internet connections to the Ekran System Server. To keep the monitoring software on the server up to date and performing well, they perform updates manually.

CASE STUDY

Privileged User Monitoring and Auditing for a US-based Financial Services Company

BENEFITS AND RESULTS

Deploying Ekran System for monitoring privileged user activity on a critical jump server was beneficial to our customer for several reasons:

Benefits of using Ekran System for privileged user activity monitoring

Fast deployment and secure use	Full visibility into critical data and systems
Fast incident response	Compliance with cybersecurity regulations
Full desktop and server OS support	Low total cost of ownership

- **Fast deployment and secure use —** Our customer had Ekran System up and running in less than half an hour. Ekran System has a knowledge base containing detailed guides on the platform's functionality, features, and configuration. Thanks to the software's intuitive interfaces, our customer has found Ekran comfortable and easy to work with. The platform also enables offline updates for Ekran Server, allowing our customer to closely protect their most critical data.

- **Full visibility into critical data and systems —** Ekran System records all user actions within the protected perimeter, so our customer can know exactly who does what and when in their network. Context-rich recordings are securely stored on the Ekran System Server and can be exported in a tamper-proof format for further investigation.

- **Fast incident response —** Ekran System allows users to deter, detect, and disrupt insider threats in a timely and efficient manner thanks to a user and entity behavior analytics module and a library of ready-to-use rules for incident response. Our customer expanded this library with custom rules for alerts and notifications that were a better fit for their needs.

- **Compliance with cybersecurity regulations —** Our platform provided our customer with the functionalities they needed to meet the requirements of PCI DSS, NIST 800-53, and other standards.

- **Full desktop and server OS support —** As Ekran System is a cross-platform solution, it supports the most popular desktop and server operating systems. Our customer was mostly interested in Windows and Linux, but Ekran System also supports UNIX, X Window System, Citrix, VMware, and other operating systems.

- **Low total cost of ownership —** Thanks to floating endpoint licensing, our customer can reassign Ekran System licenses between different servers and workstations, significantly reducing the total cost of platform ownership.

Ekran System has enabled our customer to secure jump servers running different operating systems with a single solution and gain the needed level of visibility into user activity on these jump servers. Our customer is fully satisfied with the capabilities that Ekran System gives them and plans to continue working with the platform.

> **"Ekran System was the only solution that allowed us to monitor servers running different OSs and install critical updates offline. Getting the same monitoring functionality for a reasonable price was an unexpected benefit of this cooperation.**
>
> - Feedback from the customer