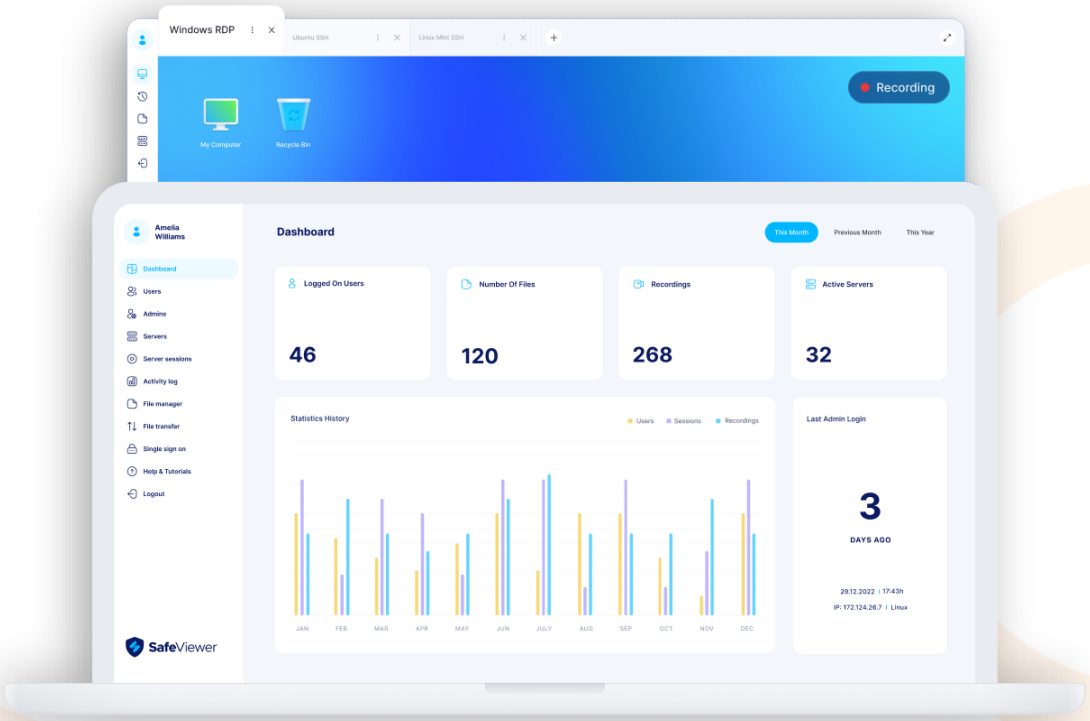
SafeViewer

softwareunited by NOVENTIQ
Global expertise, local outcomes

Implementation and Use of the Safe Viewer Platform in the Ministry of Finance of Serbia



Introduction

For many years, the Ministry of Finance relied on traditional VPN solutions for remote access to its servers. While this solution provided basic access capabilities, there were significant security and operational concerns. The lack of user session tracking and recording capabilities, the absence of features such as session recording and user log tracking, as well as challenging access management led to a need for improvement. Additionally, the need for comprehensive control over file downloads to end servers, detailed tracking of all user-input commands, and the ability to monitor sessions live highlighted the necessity for a transition to a more advanced solution.

In light of these challenges, the Ministry of Finance recognized the need for a robust PAM (Privileged Access Management) solution, which would not only ensure better protection but also offer much more functionality in terms of control, recording, and supervision.

Objective

The aim of this case study is to provide a detailed overview of the Ministry of Finance's transition from a traditional VPN solution to the Safe Viewer platform, emphasizing the key advantages and improvements brought about by the PAM solution. Through this document, specific functionalities of the Safe Viewer platform that enabled the Ministry to achieve a higher degree of security, transparency, and efficiency in its operations will be presented.

Challenges Faced by the Ministry of Finance Before Using the SafeViewer Platform

a) Lack of detailed user session tracking:
Traditional VPN solutions did not offer the capability for detailed tracking and recording of each individual user session. This created a gap in control and supervision, allowing users to undertake activities that might not have been in line with security protocols and remain undetected. Without the ability to record sessions, the Ministry could not effectively respond to potential incidents or investigate suspicious activities.

b) Lack of transparency in file transfers:
Using the VPN, users were able to freely transfer and download files between client machines and servers without any oversight or restrictions. This increased the risk of accidental or intentional spreading of malicious software, leakage of sensitive information, or compromising the system's integrity.

c) Absence of user command tracking functionality:
Without the ability to track and record specific commands entered by users during sessions, it was challenging to establish accountability or determine the exact cause of any technical or security issues. This left the door open for potential misuse by unauthorized users or even internal employees.

d) Limited live monitoring capabilities:
VPN solutions did not offer real-time insight into active sessions. This meant that security teams could not actively monitor and intervene during potentially harmful activities but had to rely on post-event analyses, which often came too late for effective intervention.

e) Lack of comprehensive activity logging:
Traditional solutions did not provide detailed logs of all user activities. Without comprehensive logging, it was challenging to reconstruct events, determine the causes of issues, or provide evidence of activities in cases of security incidents or legal matters.

f) Absence of automatic session recording:
VPN solutions lacked a mechanism for automatically recording each user session with remote servers. This feature is crucial for providing an additional layer of accountability and evidence, allowing the Ministry to quickly and efficiently review and analyze each session, identify irregularities, and respond promptly.

g) Absence of screenshot creation after each interaction:
Without the ability to automatically capture screenshots after every user interaction, it was challenging to swiftly identify and respond to potentially suspicious or unauthorized activities. This level of granularity is essential for providing a complete view of everything a user does during a session, offering an additional layer of security and control.

h) User authentication:
Associating each user with their email address and two-factor authentication. This advanced security measure ensures that every session, without exception, undergoes rigorous identity verification, further reducing the risk of unauthorized access or potential misuse.

In this segment, we highlighted the key challenges the Ministry faced using traditional VPN solutions and detailed the security risks and shortcomings of each of them.

Preparing for implementation

The implementation of SafeViewer in the Ministry of Finance was a comprehensive process that required meticulous preparation, coordination, and testing. Here's how this implementation proceeded step by step:

a) Pre-implementation phase:
Before the process itself began, a detailed review of the Ministry's current network and infrastructure configuration was carried out. This analysis enabled the team to identify key integration points, required resources, and potential challenges that might arise during the implementation.

b) Network Configuration:
Given that this was an On-Premise implementation, it was crucial to configure the Ministry's local network to be compatible with SafeViewer. This included setting up the firewall, opening the necessary ports, and establishing secure connections with all relevant servers within the Ministry.

c) Installation and Integration:
Once the network was prepared, the installation of the SafeViewer software began. With careful adherence to all security protocols, the software was installed, configured, and integrated with all relevant systems within the Ministry.

d) Testing connections and functionalities:
Before the system was launched into production, extensive testing was necessary. This encompassed testing connections between users and remote servers, as well as testing all key functionalities of SafeViewer, including session recording, taking screenshots, monitoring user commands, logging activity, and more.

e) User training:
To ensure that all users could efficiently use the new system, training sessions were organized. During these sessions, users were shown how to access and use SafeViewer, as well as best practices concerning security and session management.

f) Real testing:
After formal testing, SafeViewer was put into trial operation, where users had the opportunity to use the system in their daily work. This phase allowed the team to identify and resolve any minor issues or shortcomings that were not noticed during the initial testing.

g) Review and optimization:
After a 24-hour implementation and testing period, the team conducted a final review, analyzing all aspects of the implementation and adjusting the configuration to ensure maximum efficiency and security.

Implementation

The implementation of SafeViewer in the Ministry of Finance was a comprehensive process that required meticulous preparation, coordination, and testing. Here's a step-by-step breakdown of this implementation:

a) Pre-implementation phase:
Before the process commenced, a detailed review of the Ministry's current network and infrastructure configuration was undertaken. This analysis enabled the team to pinpoint crucial integration points, identify necessary resources, and anticipate potential challenges that could emerge during the implementation.

Required resources:

- Hardware servers with appropriate specifications for SafeViewer (RAM, CPU, disk space).
- Networking equipment (switches, routers, firewall devices).
- Licensed versions of SafeViewer software.
- A qualified internal IT team from the Ministry, specialized in security solutions, providing essential support and expertise throughout the implementation, ensuring the SafeViewer team carried out all phases of implementation efficiently and appropriately.

b) Network Configuration:
Considering it was an On-Premise implementation, it was essential to configure the Ministry's local network to be compatible with SafeViewer.

Detailed network configurations:

- Firewall settings adjusted to allow specific ports necessary for SafeViewer.
- VPN tunnels replaced with direct, but secure access through SafeViewer.

› SSL/TLS encryption for all communications.
› Network segmentation to ensure that only certain segments of the network are accessible via SafeViewer.
› Configuration of access rules for different user groups within the Ministry.

c) Installation and Integration Process
Following the optimal preparation of the network infrastructure, the team proceeded to the main phase - the implementation of the SafeViewer platform. Adhering to stringent security standards and protocols, the software was successfully installed and meticulously configured to integrate with the existing systems of the Ministry. Significant efficiency in this step was achieved thanks to an automated and well-tested installation procedure for SafeViewer, reducing the implementation time to just an hour. In addition to the primary installation, the team also conducted a series of checks to ensure the stability and proper functioning of the software platform in the Ministry's real-world environment.

d) Testing of Connections and Functionalities:
Before the system was deployed into production, extensive testing was indispensable. This encompassed testing the connections between users and remote servers, as well as evaluating all key functionalities of SafeViewer, including session recording, screenshot creation, and user command tracking, among others.

e) User Education:
To guarantee flawless and efficient utilization of the newly installed system, thorough user training sessions were conducted. Through these educational sessions, users were demonstrated how to operate the SafeViewer platform, with a particular emphasis on best security practices and session management. In addition to direct training, users had access to continuously available tutorials covering all aspects of the SafeViewer platform's usage. These resources enable users to revisit key functionalities and procedures at any given time. The primary objective of this phase was to empower users, equipping them with the necessary knowledge and skills, to fully leverage all the advantages SafeViewer offers.

f) Production Testing:
After the completion of initial tests, SafeViewer entered a trial phase within the real operational environment. This step was fundamentally crucial, as it allowed users to become intimately familiar with the system's functionalities within the context of their daily tasks. This phase was also pivotal in identifying and rectifying minor difficulties or oversights that might have remained unnoticed during basic tests. To ensure full functionality and security, test connections were established with specific test servers, guaranteeing that everyday critical services remained undisturbed. Through this process, it was ensured that the production environments were safeguarded and secure from any potential disruptions or damages.

g) Review and Optimization:
Following a 48-hour implementation period and thorough testing, the expert team conducted a comprehensive review, methodically analyzing every segment of the deployed system and, where necessary, making additional adjustments to ensure optimal performance and uncompromised security. Upon completing this phase, users were electronically provided with a license activation certificate. The certificate precisely indicated the duration of each license and the specifications of all active licenses. Additionally, users received details about the technical support offered by the license manufacturer.

h) Launching into Production:
With all preceding steps successfully completed, SafeViewer was officially launched into production, providing the Ministry with a new level of security and control over its remote sessions.

Key Features of the SafeViewer Platform in the Ministry of Finance

- **Administrative Control Panel:** Provides a comprehensive overview of all platform activities, allowing for efficient monitoring and management.
- **User Management:** A centralized platform for managing user profiles, access, and permissions, ensuring the proper assignment of access rights.
- **Session Management and Recording:** Each session is meticulously documented, offering added protection and transparency for all remote activities.
- **Log Logging:** Precise record-keeping of all user activities during sessions enables inspection and audit of access whenever necessary.
- **File Quarantine:** A tool that enforces strict control over downloads and transfers to servers. Every download must be approved by the main administrator of the Ministry of Finance, further strengthening data security.
- **Reports:** Automatic report generation offers a quick and clear insight into all activities on the SafeViewer platform, guaranteeing timely information and the ability to respond to potential anomalies.
- **Real-time Session Termination:** During live monitoring of any session, the main administrator has the capability to terminate the session and block the active user, ensuring an instant reaction to potential irregularities.
- **User Authentication:** Linking every user with their email address and two-factor authentication. This advanced security measure ensures that every session, without exception, undergoes rigorous identity verification, further reducing the risk of unauthorized access or potential misuse.

Conclusion

By introducing the SafeViewer platform, the Ministry of Finance has set a new standard in IT security, offering a high level of transparency and control when accessing its servers. This advanced system allows the Ministry to precisely manage and oversee both external and internal users when they access key system resources.

By implementing the SafeViewer platform, the Ministry of Finance not only enhanced its security protocols but also achieved significantly greater efficiency in the work of its IT team. In addition to increased security and transparency, the Ministry has also acquired a more powerful monitoring and management tool, further strengthening its defence against potential threats.

The Ministry's decision to implement the SafeViewer platform is a clear demonstration of their commitment to preserving the integrity of their IT infrastructure, and confirmation that they are ready to use the latest technical solutions to protect their resources and ensure the optimal functioning of their system.