ONE IDENTITY
by Quest

Real-time administrator oversight with instant replay

БКС
ФИНАНСОВАЯ ГРУППА

Broker Credit Service improves security and services by monitoring and recording privileged users' remote sessions

Customer:

Broker Credit Service

Industry:

Financial services

Country:

Russia

Website:

https://bcs.ru/

3,000 simultaneous users across global offices monitored

Real-time issue detection and video capture

2 days to deploy

0 interruptions to application response times

Boosts security

Improves uptime and service levels

Cuts risk and costs

Challenge

To deliver competitive financial services and protect clients' information from hackers, BCS needed to securely facilitate and monitor remote administrative access.

Solution

- One Identity Safeguard

Protecting client information from unauthorized access and ensuring fast, continuous service availability are organizations' top priorities. To achieve both, administrators need remote access to systems so they can immediately mitigate any issue, without having to drive to an office. However, remote access increases risk: if hackers gain access to an administrative account, they can view confidential information, download files and make system changes, often without detection.

BCS, a top financial institution and winner of the Stock Market Elite award in 2020, held off on granting administrators remote system access until the organization could do so, while still meeting its security and performance requirements. Security personnel needed a privileged access management (PAM) solution that enabled them to monitor and record administrators' remote-access sessions, so that they could quickly detect any breach to administrators' accounts. The PAM tool had to be tamper-proof as well as highly flexible, to meet evolving business requirements and ensure interoperability with disparate technologies. And because micro-seconds count in the financial industry, the solution had to operate seamlessly in the background, without degrading the response times of business applications.

Superior security with zero hits to application server performance

When BCS evaluated One Identity Safeguard along with other PAM technologies, the organization chose Safeguard and moved forward with enabling remote access for administrators. Safeguard provides real-time session monitoring and recording, plus the solution's architecture is faster and more secure than the alternatives. Safeguard runs on a dedicated proxy server, which sits as a standalone, security-hardened appliance between clients' devices and application servers. The competitive PAM tools that BCS evaluated increase risk surface-areas because they use software agents that run on individual application servers.

Alexander Pirogov, Head of Department of Technical Means of Protection at BCS Group, says, "Proxy solutions like Safeguard have the least impact on the operation of systems and they minimize risk. Agents use server resources one way or another. For highly loaded systems, this can reduce performance. There is also a risk that someone could disconnect the recording of a privileged user's session," when the process is managed by agents on the application server. In addition, "We received very good feedback from our colleagues in other financial institutions who use One Identity Safeguard," he says. "It is very stable—and it requires minimal administration, support and hardware."

> **"Controlling the actions of privileged users with Safeguard drives business efficiency. ... It gives us the insight and control we need on all levels to meet our security, performance and budget requirements."**
>
> **Alexander Pirogov**
> **Head of Department of Technical Means of Protection, BCS Group**

> "The initial setup of Safeguard took about 20 minutes, and it took two days to test configuration options and fully deploy the solution."
>
> Alexander Pirogov
> Head of Department of Technical Means of Protection, BCS Group

Increases ROI with a two-day deployment and minimal maintenance

Two system administrators quickly deployed Safeguard, opting for virtual appliances to increase flexibility and stability. They configured the solution so that it audits and records administrators' remote sessions facilitated by Remote Desktop Protocol on Windows-based systems. They also have Safeguard log administrators' sessions initiated from UNIX-based systems that use the SSH file protocol. To build automated reports that detail information about remote access, administrators integrated Safeguard with the company's existing event management solution. "The initial setup of Safeguard took about 20 minutes, and it took two days to test configuration options and fully deploy the solution," Pirogov explains. "Everything was easy. The solution is well-documented and quite understandable."

Today, administrators spend minimal time on solution management. "During the four years we've used Safeguard, we have not encountered a single system crash or failure," says Pirogov. "And One Identity's technical support is excellent. They answer any and all questions we ask, quickly and efficiently."

Speeds issue mitigation, boosting uptime and security

By facilitating remote access for administrators, BCS boosted uptimes and customer service levels. "We increased the reliability of our IT systems by enabling remote administrative access with Safeguard," Pirogov says. "Administrators do not need to come to the office to check on events in monitoring messages and alerts. This significantly reduces their response times, and contributes to greater compliance with internal SLAs."

At the same time, "We have minimized risks and avoided security issues with Safeguard," explains Pirogov. That's because security personnel have the insight they need to immediately know about any anomalies in administrators' remote sessions—and take appropriate steps for rapid resolution. In addition, Safeguard can automatically close an administrator's session if specific types of events occur.

> "Security personnel can review recordings of administrators' sessions. Safeguard provides the **large amount of information** they need to conduct investigations."
>
> Alexander Pirogov
> Head of Department of Technical Means of Protection, BCS Group

Cuts risk with real-time administrative oversight

From the Safeguard dashboard, security personnel can see all the data collected about an event, including who the user was, when the event took place and a summary of the anomalies that triggered the event. Anomalies can include a change in the IP address an administrator logs in from, the time they spent working remotely or unusual system access. "If more details are needed about events than what is on the dashboard, security personnel can review recordings of administrators' sessions. Safeguard provides the large amount of information they need to conduct investigations of suspicious events."

To save time, Safeguard starts the video playback at the exact time the event occurred. However, investigators can play back videos starting from any point in time. They can search for frames with specific information, such as commands users typed and text that appears on screens they viewed. Investigators can also list users' file operations and extract any files they transferred.

Rapidly scales to support 3,000 simultaneous users

When the COVID-19 pandemic erupted, BCS needed to quickly ensure global employees could work from home using secured and monitored connections. Because the organization already had Safeguard in place, it contacted One Identity for new licenses. "It took us two days to add more Safeguard appliances, including additional virtual CPUs, memory and storage disks," Pirogov explains. "The whole process turned out to be very simple. We now use Safeguard as a remote access control tool for all users of the company network. During peak times, we have up to 3,000 simultaneous users connected through different instances of Safeguard, safely working from home."

Because BCS enabled remote access with Safeguard, the learning curve for employees was minimal. "Our remote-access users do not understand or see that they are connecting through One Identity Safeguard," Pirogov says. "The solution operates transparently in the background."

Simplifies video storage management and minimizes costs

Manually moving video files between storage platforms can be extremely time-consuming. And determining when it makes financial sense to transfer files from local storage, which provides the fastest playback times, to long-term storage, which is slower but more cost effective—can be difficult.

BCS estimates that recording the sessions of 1,000 users generates 80 gigabytes of data in eight hours. To avoid having to manually move these files between storage platforms, BCS takes advantage of Safeguard's automated workflows for exporting video from Windows- and UNIX-based systems to shared network storage. In addition, the organization uses a calculator from One Identity to make decisions that maximize ROI. "The storage calculator provided to us by One Identity gives us the information we need to determine when it's time to move files to a less expensive file server," says Pirogov.

Commenting on the overall benefits BCS has realized by using Safeguard, he says, "Controlling the actions of privileged users with Safeguard drives business efficiency. The solution requires minimal costs and resources to deploy and manage—and it gives us the insight and control we need on all levels to meet our security, performance and budget requirements."

> "We increased the reliability of our IT systems by **enabling remote administrative access** with Safeguard."
>
> **Alexander Pirogov**
> **Head of Department of Technical Means of Protection, BCS Group**

About One Identity

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com.