



A Leading Global Banking Group controls network access and eliminates risk with UserLock[®]



Customer
Global Banking Financial Services company



Industry
Financial Services



Geography
Brazil



Challenge
A global bank needed to eliminate the opportunity for fraud resulting from users sharing logins.



Solution
UserLock eliminates concurrent logins and restricts access, in addition to monitoring and reporting on all session activity throughout the group's Windows network.



Result
Complete login control, eliminating the issue of user login sharing.

Ability to identify, search, report and archive user access for compliance with industry regulations.

Mitigation of risky behavior and insider threat through real-time monitoring of all sessions on the network, enabling an immediate response to suspicious behavior.

“ With 60,000 users conducting financial transactions on a regular basis, we needed to eliminate risks and possible fraud resulting from improper user access. UserLock does that and much more — it even helped us to identify and block employees who used ‘robots’ to automate their tasks on several different workstations, putting both our bank’s and our customers’ data security at risk. ”

Information Security Director

CASE STUDY

A LEADING BANKING GROUP CONTROLS NETWORK ACCESS AND ELIMINATES RISK WITH USERLOCK

The Challenge

Eliminate login sharing and secure the Windows network

One of the largest bank in the Eurozone by market value. This financial institution is primarily engaged in retail banking and operates principally in Spain, the United Kingdom, Portugal, Latin American countries and the United States.

When management at group discovered that user login sharing was compromising their regulatory compliance, they determined the need to implement access security and concurrent login control beyond basic Windows functionality. Operating in such a highly regulated and security-sensitive industry, the bank required complete control of network access for all of their 60,000 users.

Some other UserLock customers

FBI, DEA, UN, Barclays, BNP Paribas, Ministry Interior Saudi Arabia, Bank of Kuwait, South Wales Police, NHS, University of Leeds, NATO, City of Paris, ...

IT needed to monitor and secure network access; most importantly, they wanted to ensure that employees were limited to using only their own personal login information. Equally important was the ability to recognize access attempts from someone other than the legitimate user. Once these re-

quirements were established, they began a search for an effective Windows-based security solution that would be quick to deploy and easy to use.

The Solution

UserLock for access control, regulatory compliance and risk prevention

The group evaluated a few different solutions and quickly came to the conclusion that UserLock best fit its specific requirements. "After analyzing several options, we decided that UserLock was exactly what we needed," said the Information Security Director. "The solution's balance of cost and effectiveness made the decision even easier."

Symmetry (our distributor in Brazil) was key in assisting the bank with the evaluation process, running the Proof of Concept (POC) and also assisting with the software installation.

Because UserLock enabled the group to customize its policy regarding concurrent logins, they were able to configure the solution to best meet their specific needs. Each user login can only be connected to the network once at any given time. If necessary, users can request an exception by opening a help desk ticket, which is then reviewed and either granted or denied.

All exceptions are also reviewed annually to check for trends or suspicious activity.

With UserLock's access security and concurrent login control for their

Windows network, the group has been able to:



Eliminate login sharing. The ability to completely block concurrent user logins allows the group to enforce bank policies by enabling them to control and secure their Windows network. The bank can easily manage who accesses the network, how it is accessed and when exceptions are appropriate.

Ensure compliance with FINRA, SEC Regulation S-P (Safeguards Rule), SOX and other mandates governing data handling. Controlling network access helps the bank secure sensitive and regulated information, prevent data leaks, and comply with regulations.

Recognize and prevent risk. "With 60,000 users, conducting financial transactions on a regular basis, we needed a way to eliminate risks and possible fraud resulting from improper user access. UserLock does that and more – it even helped us to identify and block employees who used 'robots' to automate their tasks on several different workstations, putting both our bank's and our customers' data security at risk."

Download a UserLock FREE TRIAL version
WWW.USERLOCK.COM