CASE STUDY

IS Decisions
Secure & Master your Windows Infrastructure™

UserLock® empowers Pernambuco State Traffic Department

to better protect sensitive information for over 2000 employees

Customer

Detran-PE: Pernambuco State Traffic Department

DETRAN-PE

Industry

Government

Geography

Brazil

Challenge

Sensitive data on the Windows-based network was being put at risk by unauthorized user access and uncontrolled user behavior.

Solution

With UserLock, a customized access policy can be set and enforced to permit or deny user logins. Concurrent sessions can be prevented and access restricted to specific workstations or devices, time, business hours and connection type (including Wi-Fi).

Result

Reduced risk to the organization's data through effective network access management and monitoring.

Password sharing between users has been stopped through the prevention of concurrent logins,

Up to 90% less time is spent manually monitoring and auditing user activity on the network.

An effective control of time for when the network can be accessed

> *"With UserLock, we have an effective network access management tool that is very simple to manage and easy to understand. It has helped simplify IT's work by reducing between 70 to 90% the time spent monitoring and auditing network access of all users."*

Antônio Fernandes S. Oliveira
Network Manager
Pernambuco State Traffic Department

CASE STUDY

USERLOCK EMPOWERS PERNAMBUCO STATE TRAFFIC DEPARTMENT TO BETTER PROTECT SENSITIVE INFORMATION

The Challenge

State Traffic Department need to control and secure 'traffic' to the network

Pernambuco State Traffic Department in Brazil is a very busy organization, having, amongst other tasks, to monitor all the state's traffic, issue driver's licenses and vehicle license plates. The IT department is no less busy, with responsibility for approximately 2000 users spread over more than 100 different divisions.

In such an organization like the State Traffic Department, unauthorized access to information, whether it is from inside or outside the organization, can have serious consequences. It is therefore of utmost importance for the department to be able to enforce security rules that control network and data access.
To meet these needs with native Active Directory security, several Group Policies were in place for software restriction and approved audit, a strict password setting policy (based on size, history and complexity) was enforced and all admin access was restricted to only support users.

Despite these measures the IT department noted several on-going security risks linked to user behavior and their network access, often without the users even being aware of the risks at hand. For example, access to the network out of business hours, connection from unauthorized external locations, and, very frequently, password sharing.

"Before UserLock we did not have an effective access login management, and because of that anyone could access the network at any place and time, and as many times as they wanted."

"Network security is a critical problem for most companies, and security in Windows-based networks relies heavily on a user's login credentials", said Antônio Oliveira, Network Manager. *"The problem is that native Windows-based network controls does not limit the number of possible logins for a single user. On many occasions, users give their passwords to colleagues or other people, without being aware that this can cause them serious trouble: a user's login is their signature and any problem related to it becomes their responsibility. By limiting the number of concurrent logins, the network is better protected."*

Solving these issues required a whole new level of access security and user login management, in order to eliminate these risk factors and better protect information on the group's network.

The Solution

UserLock addresses very specific but important gaps in managing the security of Windows infrastructures.

The team set out the following objectives a new solution would accomplish:

- Location management - to prevent unsecure connections from outside locations.
- Time management - to avoid users connecting to the company network outside of designated hours.
- Improved network access reporting - to help with the daily management of users.
- Concurrent login management - to reduce the risk of users sharing their passwords.

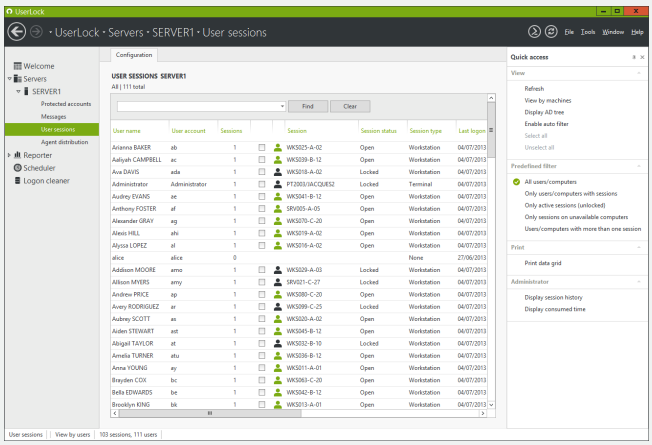
Having been able to put the software to the test in their own specific environment, they found that UserLock met exactly the department needs to be able to restrict access of network users, limit access per user, and prevent concurrent logins. The team also found the solution extremely effective in helping with the audits conducted by the organization.

In addition, the ability to receive alerts on suspicious

access events, coupled to the possibility to take control via remote session when needed, also proved to be a significant plus.

With its simple deployment process, the team rapidly installed UserLock and started controlling user access and protecting the network. *"It took us about 48 hours to deploy. First on the server and then across all locations through the automatic deployment system provided by the software."*

During their daily use of the software, Antônio Oliverira and his team did note one possible improvement; to end users sessions, once the time limit was exceeded. This feedback was taken on by the development team at IS Decisions, who added this feature to their software within the next product release.
"The support given by IS Decisions was excellent, especially because they are open to new ideas. We contacted them to address the matter of ending the sessions of users exceeding their network access time limit, and after our feedback a new function was added in the subsequent version."



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, ...

The Benefits

Reduced risk to the organizations data through effective network access management and monitoring

In using UserLock, Antônio Oliveira states that Pernambuco State Traffic Department can now deliver effective network access management across all its locations. *"Before UserLock we did not have an effective access login management, and because of that anyone could access the network at any place and time, and as many times as they wanted."*

UserLock has helped reduce the risk of security breaches to the organization's data and realize time savings when it comes to monitoring, auditing and reacting to suspicious access events.

- Through the prevention of concurrent logins for 95% of their users, password sharing between users has now been stopped.
- Access to users can now be restricted and limited based on multiple criteria, including workstation or devices, time, business hours and connection type.
- All user access can be monitored in real-time with IT able to remotely and instantly react to any suspicious events.
- Time spent manually monitoring and auditing network access has been reduced by up to 90%, freeing up resources for other tasks.

"With UserLock, we have an effective network access management tool that is very simple to manage and easy to understand. It has helped simplify IT's work by reducing between 70 to 90% the time spent monitoring and auditing network access of all users"

Download a UserLock FREE TRIAL version
WWW.USERLOCK.COM

IS Decisions
Secure & Master your Windows® Infrastructure™

www.isdecisions.com | info@isdecisions.com
Technopôle IZARBEL - Créaticité Bât. A
BP12 - 64210 Bidart - FRANCE
Phone: +335.59.41.42.20 - Fax: +335.59.41.42.21

Microsoft Partner
Silver Application Development