Login Enforcer

Control computer login through electronic door access.

Background

Login Enforcer provides innovative convergence between physical and logical security by controlling computer login through electronic door access. Forming an essential part of any organization's security strategy, it provides an easy way to implement more stringent IT security policies and mitigate security breaches.

49% of organizations (2006 Global Security Survey - Deloitte Touche Tohmatsu) have experienced a security breach. Breaches include: 28% insider fraud, 18% leakage of customer data, 10% internal network, 3% wireless network, and 6% undetermined internal breaches. 72% of organizations breached internally estimated the costs to be around US $1 million and 2% estimated the costs were over US$5 million.

Despite evidence to the contrary the perception of internal threats is misguidedly low.

Login Enforcer will:

- Better protect valuable data, information and systems from the growing threat of illicit internal access
- Reduce the headache and cost of enforcing stringent computer security policies and regulatory compliance guidelines
- Simplify the control of when users have access to computer resources, yet provide significantly improved computer security
- Maximize the investment already made in your physical security infrastructure

Finance	**Trading rooms:** Login Enforcer ensures only authorized traders can use computers in trading rooms and only when they are allowed to. **Branch computers:** Through Login Enforcer's physical location based login control, the risk of illicit access to teller and account managers' computers is greatly reduced.
Airports	**Control centers:** Login Enforcer ensures airport control centers (air traffic control, security monitoring) have the highest level of computer login security. **Customs:** To prevent customs fraud and potential computer compromise Login Enforcer can be deployed to ensure only valid Customs Officers can access specified computers. **Check-in and gate control:** Being located in semi-public areas check-in and gate control computers are at real risk of illicit attempts to login. Login Enforcer can be deployed in these environments so that only valid staff members who have gained legitimate physical access to their workplace are allowed to log in to their computers.
Education	**Computer labs:** Most higher education facilities have computer rooms for students to perform coursework and attend computer based courses. Login Enforcer provides strict control over both who and when users can access computers in these labs.
Call centers	**Operator login control:** Many call centers have large numbers of staff many of whom are transient (e.g. from external workforce agencies). Combine this with different shifts and workdays for each employee, and there is real potential for misuse of computer resource by non -employees and non-scheduled employees. Login Enforcer provides the solution to this problem as only employees with valid security access (including shift) will be granted login rights to call center work stations.
Server rooms	**Server login protection:** Servers invariably contain both an organization's most sensitive information and most critical software applications. Login Enforcer provides additional security for server administrators requiring them to physically be in a server room in order to login .

Installation

Login Enforcer is easy to install comprising two Windows software packages:

- Login Enforcer Badge Monitor — links to the access control platform to monitor security badging events, and send these to the Login Enforcer Directory Updater
- Login Enforcer Directory Updater — links to your Domain Controller to change user login based on a user's security door access.

With Login Enforcer there is no requirement for additional network devices or specialized PC hardware (such as USB fingerprint or smart card readers), and because Login Enforcer is entirely server based there is no need for any workstation software to be installed.

Configuration

Through the Login Enforcer administration console you can select which accounts Login Enforcer will control by configuring individual domain users or domain groups. Users can be configured with the following options to determine how Login Enforcer will control their computer logins:

- Account Control — Login Enforcer enables and disables a user account as that person enters and exits a work area respectively
- Group Membership Control — Login Enforcer adds additional Active Directory groups to users when they enter access controlled areas and removes these once the person leaves. In this way users are given elevated computer privileges when they are physically present in an area, which are automatically revoked again when the person leaves.
- Log off on exit — When a person leaves a work area Login Enforcer will automatically log that person off.

Easy login security

Once a user is configured their account is immediately under the control of Login Enforcer. When a user enters a work area through an electronic access control door, Login Enforcer will control whether that user's login is active and which additional Active Directory groups are assigned.

Login Enforcer is completely transparent to normal domain user authentication. When a user gains valid door security access they will log in normally to Windows and be unaware that their account is under Login Enforcer control. However, when a user gains invalid security door access (e.g. tailgating and/or by-passing security entrance points) Login Enforcer will restrict access accordingly.

Easy logoff

Many organizations concerned about computer security will automatically lock a computer when it enters screen saver mode. While this is good practice, unless the screen saver timeout is annoyingly short, there is a time period when a user leaves their computer that it is un-secured.

In Login Enforcer users can be configured so that the workstation automatically logs off when a person exits the secure area, thereby ensuring that a workstation remains secure at all times. It can also help ensure that computers are available for other users when a person exits a work area.

Login Enforcer features

Fault tolerant	Can detect faults in the access platform and either grant or lockout computer login as appropriate.
Scalable	Supports any number of domain controllers in larger networks.
Active Directory replication 'aware'	Updates all replication partners simultaneously to ensure instantaneous Windows login control.
All Group Policy and Active Directory options supported	Login Enforcer is designed to work with all standard Active Directory options and Domain Group Policy settings.
Supports a standard workstation image	Requires no workstation software installation so organizations can continue to use their standard desktop build.
Access control scheduling	Access control platforms typically have excellent scheduling, often including built-in support for shift control or specific time scheduling patterns. Login Enforcer allows this same scheduling to control Windows login.
Enforces security access policy	Users will need to use access control devices in order to use computers, which will reinforce the use of readers to gain physical door access. Sharing of access cards is reduced as this can invoke workstation lock-out. Personnel tracking for evacuation, health and safety, and time and attendance is improved.
No additional hardware	Login Enforcer is a software only package. There is no need for specialized hardware devices.
High encryption as standard	Login Enforcer uses TripleDES encryption to protect all data communications.

Specifications

Supported Access Control	Facility Commander Wnx 7.5 & 7.6
Supported Domain Controllers	Windows 2000 Server Windows Server 2003 (all versions) Windows Server 2008 (all versions)
Login Enforcer Badge Monitor: **System Requirements**	1 GB of RAM 50 MB of Available Disk Space Operating Systems: Windows XP Professional Windows 7 (Professional, Enterprise, Ultimate) Windows Server 2003 (all versions) Windows Server 2008 (all versions)
Login Enforcer Directory Updater: **System Requirements**	2 GB of RAM 100 MB of Available Disk Space Operating Systems: Windows 2000 Server Windows Server 2003 (all versions) Windows Server 2008 (all versions)

REDCRATER

Contact: Peter Neil

p:	+64 7 829 5345
m:	+64 21 896 305
s:	peter.neil
e:	peter.neil@redcrater.co.nz
w:	redcrater.co.nz