



CLEW for Network Access Control

The Issue

Organisations face a host of security concerns driven by the power of technology and the vulnerabilities inherent in its use. Information Technology professionals must be vigilant about a number of issues including system penetration threats, hardware portability and employee honesty.

IT Professionals have recognised this and subsequently strengthened security systems but there is still a need to invest in stronger levels of authentication for network access for internal and external use to protect the integrity of the organisation's network information.

Systems that are poorly or inadequately secured (single-level security, easily guessed passwords, unencrypted data, etc.) are an invitation to problems ranging from low data quality to unauthorised infiltration. The ways in which personnel discard access codes and other kinds of personal identification information is also a major problem.

Two-factor authentication systems such as tokens and random pin generators are also susceptible to hackers because they use the same authentication path as the transaction. Biometric systems such as finger scanners have been proven to work but they are extremely expensive for organisations to implement on a wide scale.

Hackers have proven networks can be easily breached due to inadequate levels of authentication for users. It is important that organisations realise this and implement cost-effective multi-factor, out of band authentication systems that will prevent or identify hackers both internally and externally attempting to gain access to the organisation's network.

The Solution

Alacrity's patented Closed Loop Environment for Wireless Technology (CLEW®) allows secure, real time interaction through mobile devices. Alacrity has designed a state of the art multi-factor, out of band authentication system utilising CLEW.

The CLEW system sends a secure alert to authorised users before they can access the network. The user will then receive that alert on their internet connectable mobile device, after securely entering a session via a login and password issued by the organisation. Additional methods of security can be incorporated, if requested by the organisation.

The user then responds to the information and if they are trying to access the network they will approve the alert. If the user is not trying to access the network they will decline the request which will restrict access to the hacker.



Unlike alternative systems CLEW uses out of band authentication which means CLEW uses a different authentication path to the transaction.

The response is held in an irrefutable audit log and can be used for confirmation and reporting requirements. Additionally, unlike SMS, although the client will receive a receipt of the session on their handset once the session is complete, no information remains on the handset.

Business Benefits

CLEW will prevent unauthorised access to networks in an efficient and cost-effective manner. Network access can be initiated and authorised securely by the organisation along with the authorised user. Access can now be promptly and securely authorised or rejected by the user, eliminating the need for costly alternatives.

CLEW provides greater control to network access, risk minimisation and stronger overall confidence in the organisations security systems and processes.