PRIVILEGED ACCESS CONTROL

Shell Control Box Use Case

The Challenge - Unlimited “Power” of Administrators

System administrators and other “superusers” are the most privileged users in a company’s IT environment. They have very high or even unrestricted access rights on operating systems, databases and application layers, as well. Having superuser privileges on servers, administrators have the possibility to directly access and manipulate the company’s sensitive information, such as financial or CRM data, personnel records or credit card numbers. Furthermore, several administrators typically access the same privileged account, sharing the account password, which could not be treated as secure from this point. Consequently, it is very hard to answer the question of “who did what?” and even more difficult to provide proof of any misuse. Nevertheless, regulations like the PCI-DSS, the ISO 2700x, or the COBIT all mandate the control of information system access to prevent unauthorized use of sensitive data.

Although many information systems generate access log entries, this only enables reactive measures. In addition, administrators can easily erase the traces of their actions from these logs. Another problem about privileged access is the increasing tendency of IT outsourcing. If a company outsources the administration of its servers to an external company, it effectively means that complete strangers have omnipotent access to all business data of the company. Although, there are activity monitoring technologies available on the market (e.g. network sniffers or agent-based solutions), these all have limitations in terms of granular access control capabilities.

Key Shell Control Box benefits for access control

- control SSH, RDP, VNC, Citrix ICA, Telnet and other protocols
- integration with AD/LDAP/RADIUS directories
- granular access control policies (e.g. based on time periods or group membership)
- credential store (e.g. automatic password-based authentication on target systems)
- two-factor authentication
- 4-eyes authorization
- real-time session following with the possibility of instant termination

The Solution - Privileged Access Control

In such situations it is reassuring to have an independent device that can reliably control and record access to sensitive data, and can securely store these records for later review. BalaBit Shell Control Box (SCB) is an activity monitoring appliance that restricts access to remote servers, virtual desktops, or networking devices, and records the activities of the users accessing these systems. The finest granularity of access management helps you control who can access what and when without having any doubt. SCB organizes the recorded activities into sessions called audit trails, making easy to replay the actions of individual users. Monitored user activities can optionally be forwarded to external intrusion detection systems for further inspection. Being an enforcement point for company policies, only authorized personal can access critical assets fulfilling regulatory requirements related to access control.

In addition, SCB has its own Credential Store to store user credentials (for example, passwords, private keys, certificates) and use them to login to the target server without the user having access to the credentials. In addition to storing credentials locally, SCB can integrate smoothly to third-party privileged identity management solutions.

To avoid accidental misconfiguration and other human errors, SCB supports the 4-eyes authorization principle as well. This is achieved by requiring an authorizer to allow remote administrators to access the server. The authorizer also has the ability to monitor the work of the administrators in real-time, as if they were watching the same screen. This also means that SCB offers independent tamper-proof auditing of accesses with customizable reporting capabilities.

Technical Implementation

SCB allows you to define policies: access to a server is possible only from the listed client machines. Access can be restricted by various connection parameters such as the time when the server can be accessed, user-groups, authentication method or type of channels permitted in the protocol.

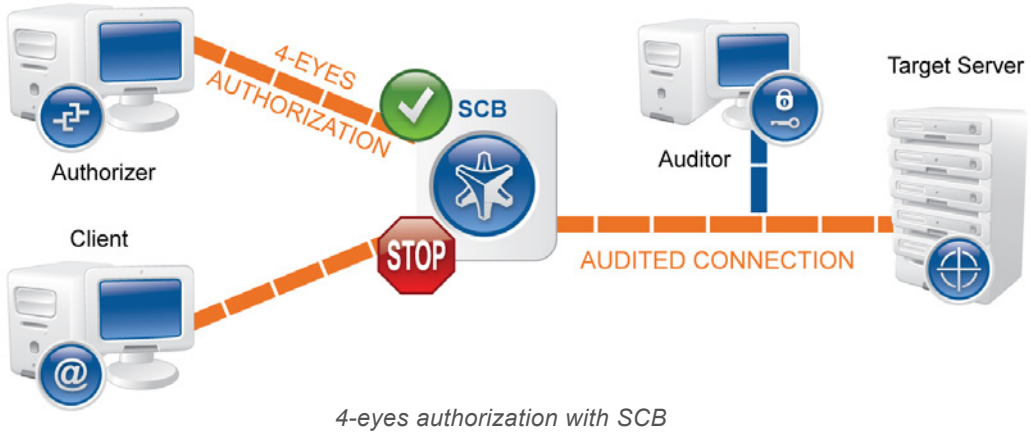
SCB can require the users to perform gateway authentication, meaning that the user must authenticate on SCB, as well. To improve access security further, SCB can enforce the use of strong authentication methods (public key), and also verify the public key of the users.

With SCB user-mapping policies defining access privileges to the remote server for specific user-names can be established and implemented; only members of the specified local or LDAP user-groups can use the specified user-name on the server.

Recorded audit trails are encrypted, digitally signed and timestamped and access to them is granularly controlled by SCB to prevent unauthorized manipulation of sensitive data.

Learn More

- Shell Control Box homepage
- PCI and ISO 27001 compliance and forensics in auditing remote server access
- Are you providing VPN access for your consultant?
- Request an evaluation version
- Request a callback



4-eyes authorization with SCB

About BalaBit

BalaBit IT Security is an innovative information security company, one of the global leaders in developing privileged activity monitoring, trusted logging and proxy-based gateway technologies to help customers be protected against insider and outsider threats and meet security and compliance regulations. BalaBit, the second fastest-growing IT Security company in the Central European region concerning Deloitte Technology Fast 50 list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Its R&D and global support centers are located in Hungary, Europe.

More information: www.balabit.com