ANALYZE · REAL-TIME ALERTS · ACCESS CONTROL · PREVENT
AUDIT & FORENSICS · MONITOR · ACTIVITY REPORTS
eCRIME SCENE
eCSI OFFICERS ONLY
2

BalaBit
IT Security

BALABIT SHELL CONTROL BOX 4 LTS

Turnkey appliance for monitoring privileged users

- Central access policy enforcement
- Closer employee & partner monitoring
- Prevention of malicious activities
- Lower troubleshooting and forensics costs
- Faster, cost-effective supervisory audits
- Advanced protection of sensitive data
- Improved regulatory compliance

Application areas

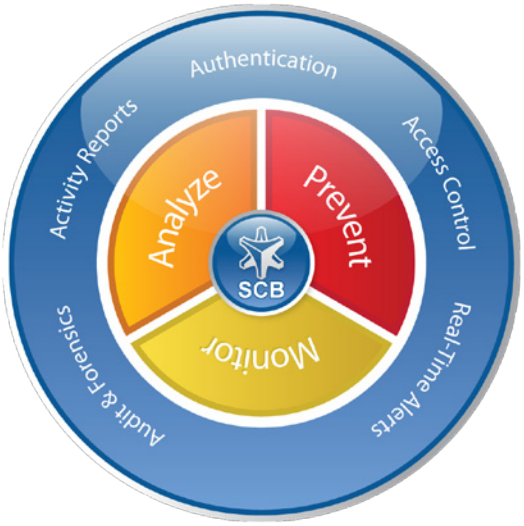
- Monitor IT administrators and developers
- Control outsourcing and cloud partners
- Audit Citrix and VMware View users
- Meet local laws and international standards (PCI DSS, ISO2700x, etc.)
- Improve IT incident management

Unlimited “Power” of Privileged Users

Users at different departments of your company have the possibility to access and manipulate sensitive information, such as financial or CRM data, personnel records or credit card numbers. These users can vary from legal department employees, through HR managers to accountants or customer service people. Beyond these “privileged” employees, there can be several superusers (administrators, IT contractors, executives, and so on) as well, who practically have unrestricted access to your company’s information assets. Controlling these users’ activity with traditional methods (for example with logging or with written company policies) is quite difficult. As a result, the question of “who did what?” is almost impossible to answer, and often leads to accusations along with the time and money wasted on investigating incidents.

Independent & Transparent Audit Device

The Shell Control Box (SCB) solves exactly these problems by introducing an independent auditor layer to oversee the working sessions of your privileged users. Shell Control Box is an activity monitoring appliance that controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions. SCB is a quickly deployable enterprise security solution with the widest protocol coverage on the market. Your existing IT environment requires no change and your staff can do their daily jobs without changing their working habits.



Privileged Activity Monitoring with SCB

> “WE FOUND THAT BALABIT SCB IS THE ONLY SERIOUS PRODUCT ON THE MARKET THAT IS CAPABLE TO SECURELY MONITOR SSH SESSIONS.” - *Øyvind Gielink, IT security Officer, Telenor Group*

Computer Technology Review Top 25 Must Have Software Applications 2014

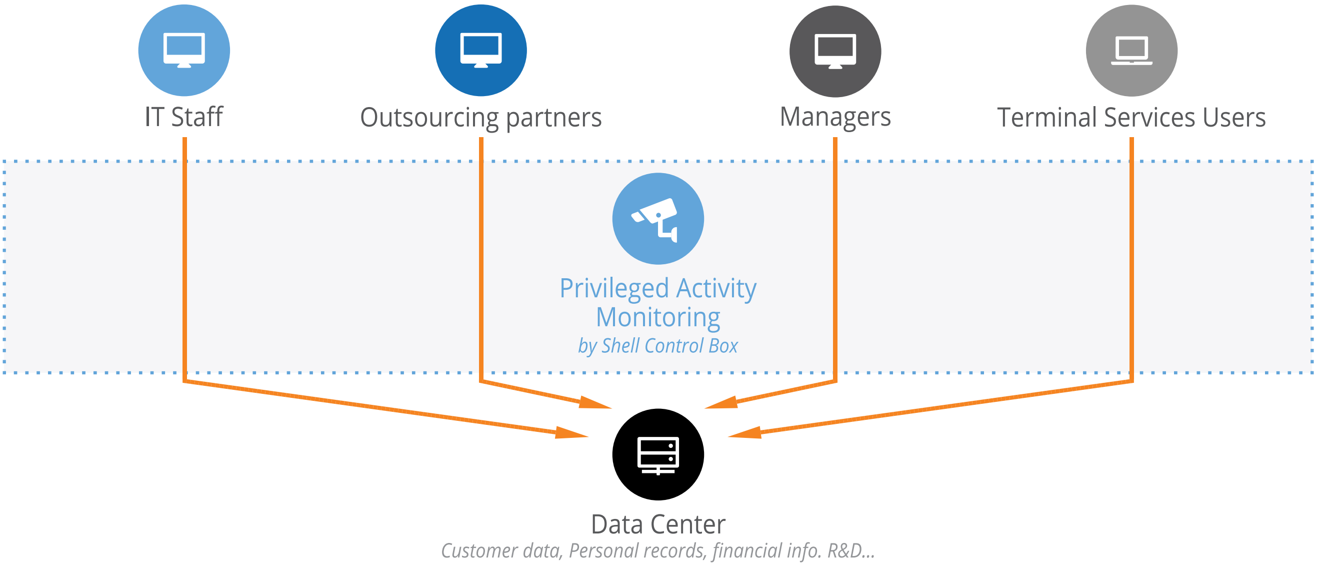
westcoast labs PERFORMANCE VALIDATED

vmware PARTNER TECHNOLOGY ALLIANCE

CiTRIX ready

Supported protocols

- HTTP/HTTPS
- Citrix ICA
- VMware View
- VNC
- Telnet/TN3270
- SCP/SFTP
- X11
- TS Gateway
- SSH
- RDP



Central Authentication

SCB acts as a central authentication gateway, enforcing strong authentication before users access your sensitive IT assets. SCB can also integrate to user directories (for example, a Microsoft Active Directory) to resolve the group membership of the user who access your protected servers. Credentials for accessing the server are retrieved transparently from SCB's local credential store or a third-party password management system by SCB impersonating the authenticated user. This automatic password retrieval is crucial as this method protects the confidentiality of passwords as users never get access to them.

Granular Access Control

SCB is a turnkey solution to control and audit all access over the most wide-spread protocols, including encrypted ones, such as SSH, RDP or HTTPs. The detailed access management helps you to control who can access what and when on your servers. It is also possible to control advanced features of protocols, like the type of channels permitted. For example, you can disable unneeded channels like file transfers or file sharing, reducing the security risks on the servers. With SCB you can enforce policies for all access in one single system, which guarantees a high level of security throughout your whole infrastructure at minimum costs.

4-eyes authorization

To avoid accidental misconfiguration and other human errors, SCB supports the 4-eyes authorization principle. This is achieved by requiring an authorizer to allow the administrators to access the server. The authorizer also has the possibility to monitor – and terminate - the work of the administrator real-time, as if they were watching the same screen.

Learn More

- Shell Control Box homepage
- Request an online demo
- Request a callback

Real-time prevention of malicious activities

SCB can monitor the network traffic in real time, and execute various actions if a certain pattern (for example, a suspicious command, window title or text) appears on the screen. SCB can also detect numbers such as credit card numbers. In case of detecting a suspicious user action, SCB can send you an e-mail alert or immediately terminate the connection. For example, SCB can block the connection before a destructive administrator command, such as the „delete" comes into effect.

High quality auditing & forensics

SCB makes all user activities traceable by recording them in high quality, tamper-proof and confidential audit trails. SCB replays the recorded sessions just like a movie – all actions of the users can be seen exactly as they appeared on their monitor. The Audit Player enables fast forwarding during replays, searching for events (for example, typed commands or pressing Enter) and texts seen by the user. SCB can even list file operations and extract transferred files for review. In the case of any problems (database manipulation, unexpected shutdown, etc.) the circumstances of the event are readily available in the trails, thus the cause of the incident can be easily identified. By generating custom activity reports, audit process is supported further and corrective actions can be made.

What's new in 4 LTS?

- Citrix XenDesktop 7.0 and XenApp 6.5 support
- Real-time content monitoring, alerting and blocking in Citrix sessions
- Content recognition of more than 100 languages incl. Russian, Arabic and Japanese
- New web-based search interface and improved auditor view
- Integration interface to third-party workflow & ticketing systems
- Virtual appliance support on MS Hyper-V
- New, more robust hardware appliances

Global customers