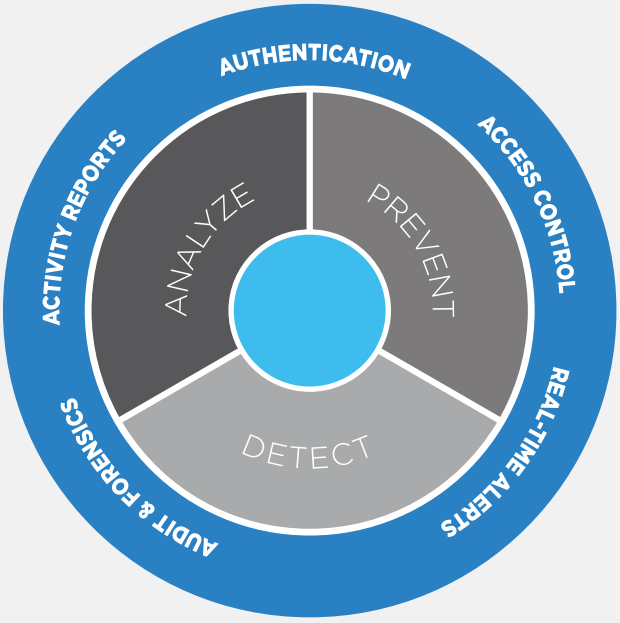


BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

BALABIT
SHELL CONTROL BOX 4 F4

Turnkey appliance for
Monitoring Your Privileged Users

Independent & Transparent Audit Device

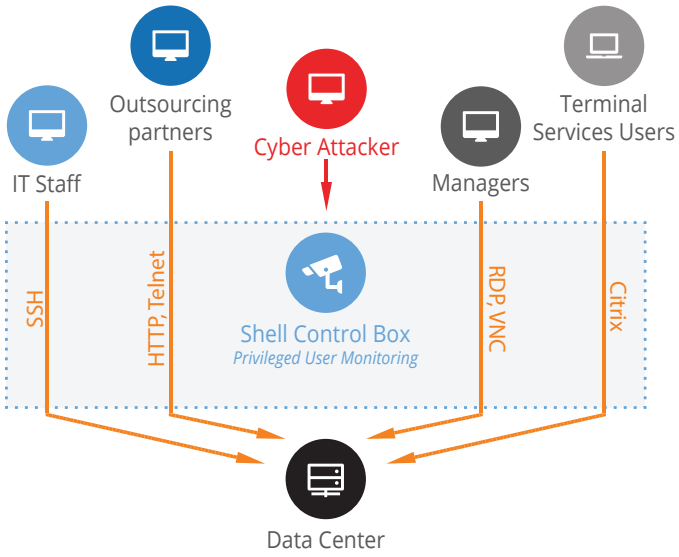
Shell Control Box is an activity monitoring appliance that controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions. SCB is a quickly deployable enterprise solution with extremely low TCO. It is a host independent gateway operating as a router in your network - invisible to the user and to the server. Your existing IT environment requires minimal change and your staff can do their daily jobs without changing their working processes.

- 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

BALABIT PRIVILEGED ACCESS MANAGEMENT CUSTOMER RESEARCH

What percentage did your Shell Control Box reduce the cost of the following challanges?

	Over 90%	61% - 90%	31% - 60%	11% - 30%	Up to 10%
Managing privileged access	12%	25%	38%	6%	19%
IT trouble-shooting & forensics	5%	19%	13%	44%	19%
Internal / External audits	20%	11%	21%	32%	16%
Resolving issues with 3rd parties	0%	37%	26%	16%	21%



WHAT'S NEW IN 4 F4?

- Improved session search and filtering from third-party management applications
- 10Gbit interface to support 10Gbit-only networks
- OS upgrade for improved product reliability and sustainability

"THANKS TO SCB, WE HAVE A TOOL FOR CONTROLLING ADMINISTRATORS' ACCESS TO NETWORK EQUIPMENT WHILE MEETING THE REGULATORY REQUIREMENTS FOR TRACEABILITY."

Pierre Granger, Head of Network Security Operations at Bouygues Telecom.

SC Awards 2016 Europe Magazine Winner · Hewlett Packard Enterprise ArcSight Tested · Cybersecurity Excellence Awards Privileged Access Management Finalist 2016 · Computer Technology Review Top 25 Must Have Software Applications · westcoast labs Performance Validated · vmware Partner Technology Alliance · Citrix ready

SUPPORTED PROTOCOLS

- HTTP/HTTPS
- RDP
- Citrix ICA
- VNC
- Telnet
- TN3270/TN5250
- SSH
- X11
- SCP/SFTP
- TS Gateway
- VMware View

Strong 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 accesses your protected servers. Credentials for accessing the server are retrieved transparently from SCB's local credential store or a third-party password manager. 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 widespread 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 privileged 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.

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 specific patterns 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 „rm" comes into effect.

Industry-leading session recording and auditing

SCB makes all user activities traceable by recording them in high quality, tamperproof 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. Thanks to the Optical Character Recognition (OCR) engine, auditors can do free-text searches in the content of text-based and graphical sessions (e.g. search for typed commands or any text seen by the user). SCB can even list file operations and extract transferred files for review.

In 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.

Balabit's Contextual Security Intelligence™ Platform protects organizations in real-time from threats posed by the misuse of high risk and privileged accounts. Solutions include reliable Log Management with context enriched data ingestion, Privileged User Monitoring and User Behavior Analytics. Together they can identify unusual user activities and provide deep visibility into potential threats. As a privileged user monitoring solution, Shell Control Box is a core component of the Contextual Security Intelligence Platform. It captures the activity data necessary for user profiling and enables full user session drill down for forensic investigation.

LEARN MORE

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

"BALABIT OFFERS INDUSTRIAL STRENGTH SESSION MONITORING AND RECORDING."

The Forrester Wave™: Privileged Identity Management, Q1 2014", Forrester Research, Inc., by Andras Cser.

GLOBAL CUSTOMERS

orange, CEZ GROUP, Tinkoff Bank, SKOLKOVO, MTS, NBK, PADDYPOWER, betfair, alBaraka, NICE, CENTRAL BANK OF THE REPUBLIC OF AZERBAIJAN, Dubai Islamic Bank, e.on, Solvinity, Handelsbanken, RESORTS, EMPH, Bouygues Telecom, FIDUCIA