

THIRD-PARTY DEVELOPER CONTROL

Shell Control Box Use Case

The Challenge

Omnipotent application development partners

In a global environment, application development and management responsibilities are inevitably connected to outsourced or sub-contracted departments. These third-party developers, including independent software vendors (ISVs), contractors or offshore application management providers are essential to business operations. This also means that they require connection to your corporate network, can remotely manage your business-critical applications and – as privileged users – they have the possibilities to access your sensitive financial databases or customer records. Typical methods for providing developer access include IPSec VPN, SSL VPN or jump hosts. These solutions provide complex firewall rules, but they lack granular access control options. In addition, controlling external developers' activity with traditional administrative methods (e.g. internal company policies) is quite difficult. Consequently, giving responsibility to a third-party developer is always a security risk.

SLA verification

You may control the partnership in your developers' contract but monitoring their employees is hardly manageable with a standard Service Level Agreement (SLA). Nowadays, companies don't have a secure and easy-to-use solution for validating SLAs and verifying billable activities. Measuring Key Performance Indicators (KPI) such as response times or restricting external developers access to sensitive data is also a challenging exercise. That's why it's essential to monitor these third-party accesses, in order to know which developer doing what once they connect to your systems.

Key Shell Control Box benefits for application developer 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)
- credential store (e.g. password-based authentication on target systems)
- two-factor authentication
- 4-eyes authorization
- real-time session following with the possibility of instant termination
- automatic and customizable reporting

The Solution – Shell Control Box

SLA control

In such situations it is reassuring to have an independent device, such as the BalaBit Shell Control Box, that can reliably monitor all external application management activities. It gives organizations the possibility to oversee and audit external developers, and is also a great tool to evaluate their effectiveness. For example, SCB records as external administrators configure your CRM database, or maintain your mission critical SAP application at night. Thereby, control over SLAs - and billable activities – can be improved, as the fulfillment of the services can be verified.

External user management

SCB can also restrict external developers' access to your sensitive databases. Its granular access management functionality helps you control who can access what and when in your IT systems. As a tamper-proof access control tool, it also helps organizations pass compliance audits of IT outsourcing processes.

Quick audit & forensics

SCB provides detailed information in troubleshooting and forensics situations to quickly uncover the root causes of incidents. The recorded audit trails can be replayed like a movie to review the events exactly as they occurred. Consequently, the

audit trails can be used as evidence to settle any accountability issues about the remotely managed applications, which is in the common interest of both the customer and the application vendor as well. For instance, if an unexpected application breakdown occurs, by replaying the recorded audit trails, you can easily identify if the failure was caused by your external vendor (e.g. misconfiguration, upgrade, etc.) or it was a hardware failure.

Technical Implementation

SCB is a proxy gateway: the transferred connections and traffic are inspected on the application level (Layer 7 in the OSI model), giving control over protocol features like authentication and encryption methods or permitted channels. SCB operates transparently in your network and extracts information into audit trails directly from the communication of the remote client and the server, providing reliable, easy-to-access content. The content of the audit trails can optionally be indexed to make searching for events and automatic reporting possible. To make integration into your network infrastructure smooth, SCB is available both as hardware and virtual appliance, and supports several different operation modes.



Third-party developers control 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

Learn More

- [Shell Control Box homepage](#)
- [Are you providing VPN access for your consultant?](#)
- [Request an online demo](#)
- [Request a callback](#)