BALABIT

INTERNAL AND EXTERNAL SECURITY COMPLIANCE AT ADOBE

Shell Control Box Case Study

"BALABIT SHELL CONTROL BOX ALLOWED US TO MEET ALL OF OUR COMPLIANCE AND INTERNAL SECURITY REQUIREMENTS." *– Matt Magleby, Sr. Computer Scientist, Adobe.*

Adobe gives everyone—from emerging artists to global brands—everything they need to design and deliver exceptional digital experiences. Adobe is passionate about empowering people to create beautiful and powerful images, videos, and apps, and transforming how companies interact with their customers across every screen.

THE CHALLENGE

The Adobe Marketing Cloud business unit had several internal policy- and compliance-related security requirements, such as the ISO 27000 and the Service Organization Control (SOC 2) reporting. Key requirements included multi-factor authentication (MFA) for accessing production systems and logging of all administrative sessions. Previously, Adobe used distributed and heterogeneous bastion hosts for access that lacked MFA and session logging and were difficult to manage. So, mainly driven by TCO considerations, Adobe wanted to consolidate bastion hosts into a central access management gateway. For usability and manageability reasons, Adobe preferred a network-level solution that does not require installing agents on clients or servers. In addition, needed a user-friendly solution that did not disrupt the daily workflow of system administrators.

FROM A TECHNICAL PERSPECTIVE, ADOBE WAS SEARCHING FOR A SOLUTION THAT:

- Supports in-line MFA
- Supports SSH and RDP protocols to access both Linux and Windows servers
- Logs and audits administrative network traffic
- Integrates with existing LDAP user directory
- Supports SSH keys for authentication
- Can forward user logs into Splunk for long-term storage and analysis
- Provides high availability

THE SOLUTION

During the selection process, Adobe evaluated virtual terminal-based access management systems and other "all-in-one" privileged identity management (PIM) solutions as well. However, these solutions did not integrate well with Adobe's existing identity management infrastructure and would have required significant changes in administrator workflows. When searching for alternatives, they found Balabit's privileged user monitoring appliance, Shell Control Box (SCB).

"We chose SCB because its proxy-based gateway architecture and the easy implementation were important for us. The MFA support, the integration with LDAP and the least disruption to workflows were additional advantages of the product. In addition, we got a great implementation support from Balabit's pre-sales team." – says Magleby.

After an initial Proof-of-Concept phase, Adobe created a test environment to conduct extensive testing and plan the implementation of SCB. The full rollout took a few weeks. In the beginning they ran Shell Control Box in parallel with the existing bastion hosts and eventually decommissioned the old systems.

Adobe deployed three high availability SCB clusters in three locations. The clusters control SSH- and RDP-based access to Linux and Windows hosts located in multiple, geographically distributed datacenters and cloud-based environments. Today, SCBs are fully operational in Adobe's production environment. They monitor hundreds of administrative users and protect tens of thousands of hosts.
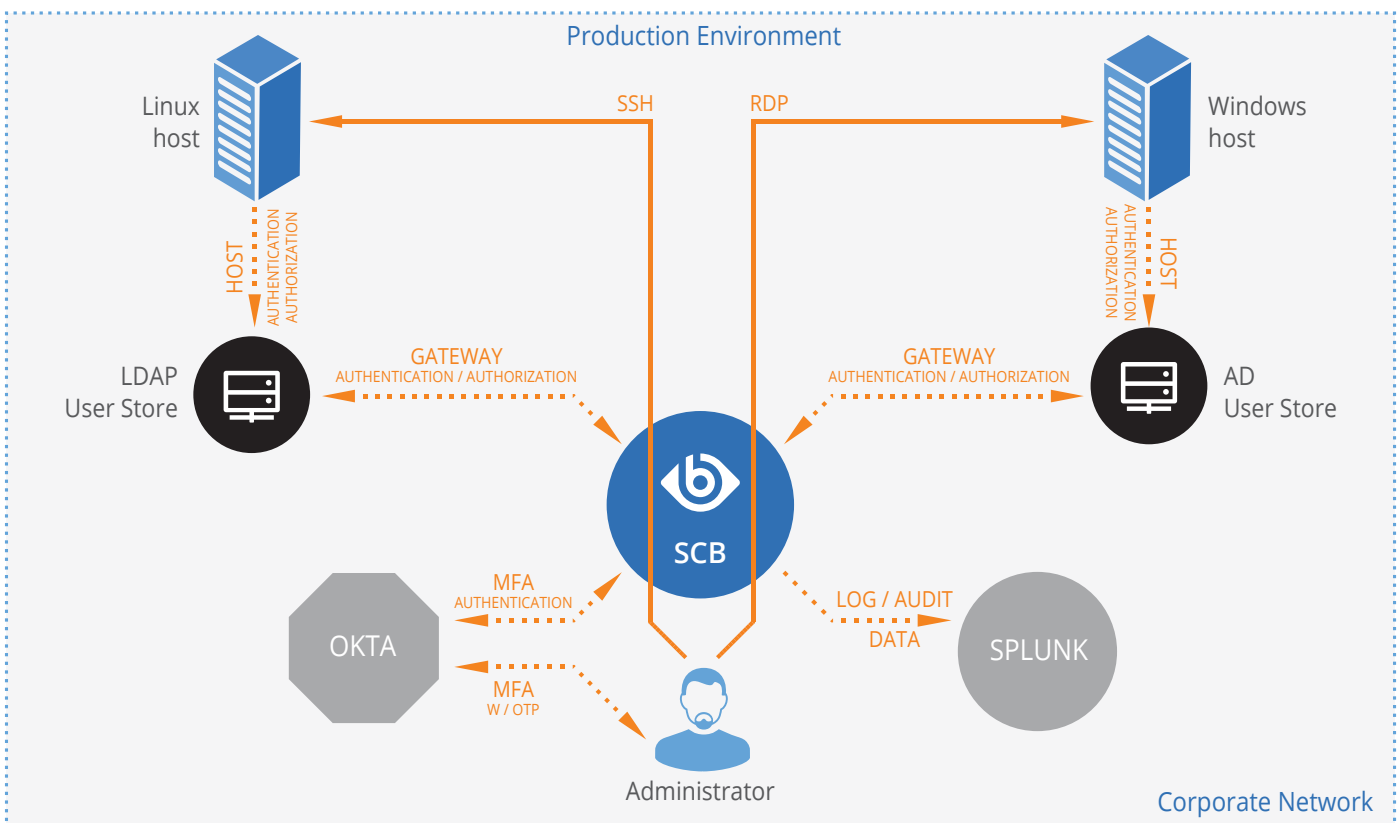
SCB-based privileged user monitoring architecture at Adobe

THIRD-PARTY INTEGRATIONS

OKTA

The Shell Control Box is integrated with identity management service Okta, which supports multi-factor authentication scenarios. Prior to establishing an SSH or RDP connection the SCB AA plugin framework invokes Okta Verify OTP (one-time password) or PUSH authentication. This allows Adobe to leverage an additional out-of-band factor (typically through the user's registered smartphone) when authenticating the user. The additional factor is processed in-line with the connection setup, so users don't have to go to an external application to process the additional factor. This results in an efficient end-user experience that is readily accepted by the users.

SPLUNK

SCB exports all audit data for both SSH and RDP sessions and sends them directly into Splunk using the Splunk's HTTP Event Collector. This allows Adobe to leverage Splunk as the aggregator for all security-related log data from SCB as well as other applications, hosts and devices. Thus, they can use their existing SIEM tool for monitoring, correlating and investigating security events with additional critical information that SCB provides.

BENEFITS

With the help of Shell Control Box, Adobe could procure necessary compliance certifications critical in retaining their existing customers and acquiring new ones. Implementing a central, proxy-based access management gateway instead of distributed bastions decreased support requirements. The enforcement of a second-factor authentication and the availability of session recordings made access of high-risk users more secure.

"Balabit Shell Control Box allowed us to meet all of our compliance and internal security requirements. Our administrative users readily accepted it as it is not disruptive to their existing workflows. SCB is a reliable and straightforward solution, which integrated seamlessly into our existing identity management system and is able to support all of our needs for both Linux and Windows server access. Implementation went very smoothly as it did not require any changes to our network or servers. We are happy with all the benefits SCB has been able to provide, and the ease in which we were able to adopt it." – concludes Magleby.

ABOUT **BALABIT**

Balabit is a leading provider of Privileged Access Management (PAM) and Log Management solutions with a mission to help businesses reduce the risk of data breaches associated with privileged accounts. Founded in 2000, Balabit has a proven track record, with 25 Fortune 100 customers and more than 1,000,000 corporate users worldwide. The company operates globally with offices across the United States and Europe, together with a network of reseller partners.

LEARN MORE

Shell Control Box homepage

Request online demo

Request callback