CASE STUDY

Internal and External Security Compliance at Adobe

Safeguard for Privileged Sessions

"ONE IDENTITY SAFEGUARD FOR PRIVILEGED SESSIONS HELPS US MEET A PORTION OF OUR COMPLIANCE AND INTERNAL SECURITY REQUIREMENTS RELATED TO ACCESS MANAGEMENT."

– Matt Magleby, Sr. Computer Scientist at Adobe.

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.

Learn more

- Safeguard homepage
- Request callback

The Challenge

The Adobe Experience Cloud business unit had several internal policy- and compliance-related security requirements, such as the ISO 27001 and SOC 2 reporting. Key requirements included multi-factor authentication (MFA) for accessing production systems and logging of all administrative sessions. Adobe wanted to consolidate bastion hosts into a central access management gateway to reduce their operating costs. For usability and manageability reasons, Adobe also wanted a network-level solution that didn't require installing agents on clients or servers. In addition, they needed a user-friendly solution that would 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

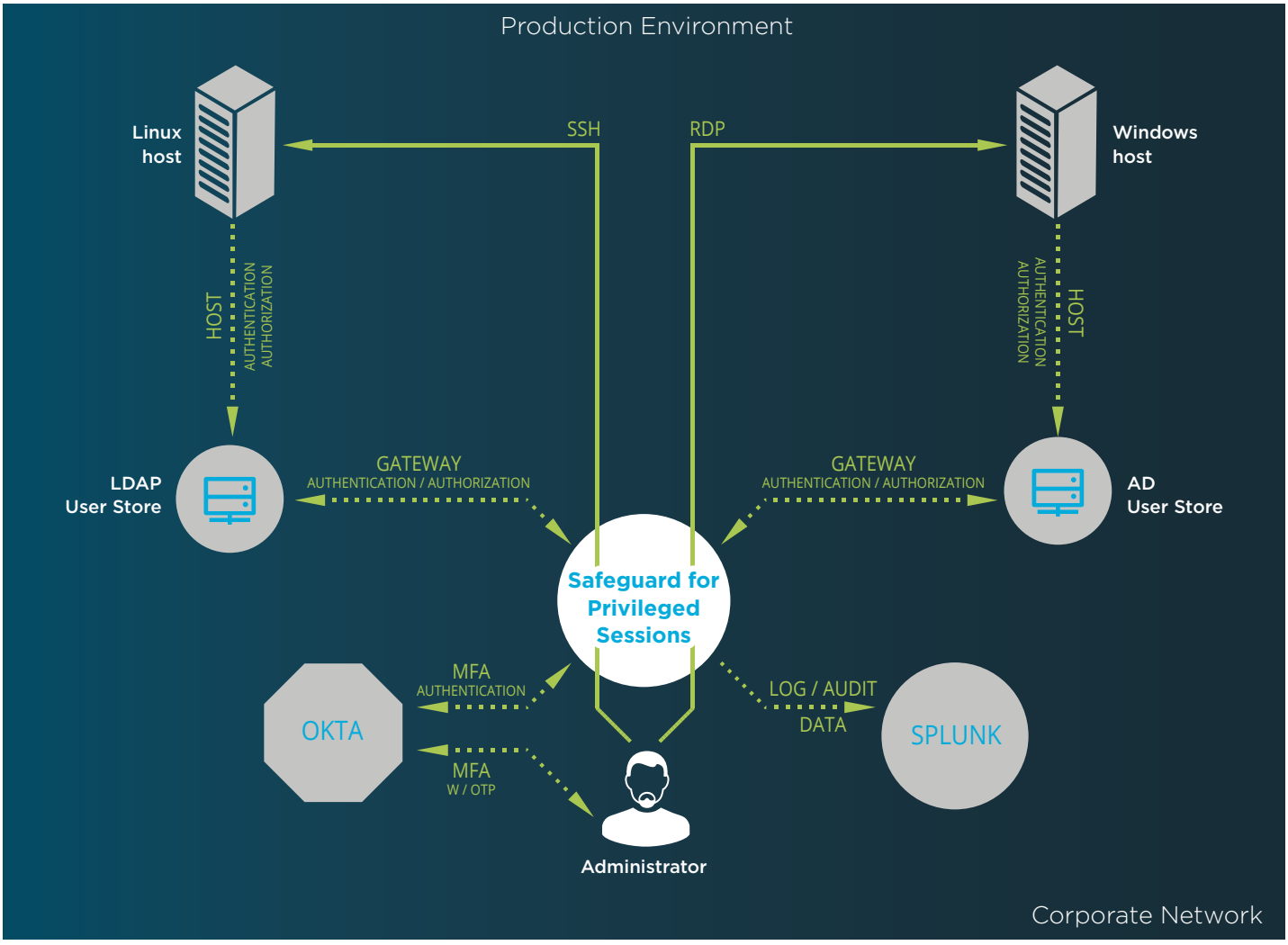
The Solution

During the selection process, Adobe evaluated virtual terminal-based access management systems and other privileged identity management (PIM) solutions. 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 One Identity's privileged session management solution, Safeguard for Privileged Sessions (formerly known as Shell Control Box).

"We chose Safeguard for Privileged Sessions because it's a proxy-based gateway architecture and easy implementation was 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 great implementation support from One Identity'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 Safeguard for Privileged Sessions. The full rollout took a few weeks. In the beginning they ran Safeguard for Privileged Sessions in parallel with the existing bastion hosts and eventually decommissioned the old systems.

Adobe deployed three high availability Safeguard for Privileged Sessions 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, Safeguard for Privileged Sessions is operational in Adobe's production environment. It monitors hundreds of administrative users and helps protect tens of thousands of systems.



Safeguard for Privileged Sessions architecture at Adobe

"We were looking for a low maintenance and horizontally scalable solution. We expected that it could be customized to our needs with a high level of quality and responsiveness from the vendor."

says Matt Magleby, Sr. Computer Scientist of the Core Services Team at Adobe.

Third-party Integrations

OKTA

Safeguard for Privileged Sessions is integrated with identity management service Okta, which supports multi-factor authentication scenarios. Prior to establishing an SSH or RDP connection the Safeguard for Privileged Sessions 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

Safeguard for Privileged Sessions exports 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 security-related log data from Safeguard for Privileged Sessions 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 Safeguard for Privileged Sessions provides.

Benefits

Safeguard for Privileged Sessions helped Adobe to meet compliance requirements for its Experience Cloud business unit by providing multi-factor authentication and auditing technology, a core component to gaining SOC2 compliance. Implementing a central, proxy-based access management gateway instead of distributed bastions helped streamline administrative tasks and decrease support tickets. The enforcement of a second-factor authentication and the availability of session recordings made access of high-risk users more secure.

"One Identity Safeguard for Privileged Sessions helps us meet a portion of our compliance and internal security requirements related to access management. Our administrative users readily accepted it as it is not disruptive to their existing workflows. Safeguard for Privileged Sessions is a reliable and straightforward solution, which integrated seamlessly into our existing identity management system and is able to support 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 the benefits Safeguard for Privileged Sessions has been able to provide, and the ease in which we were able to adopt it." – concludes Magleby.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com

© 2018 One Identity LLC ALL RIGHTS RESERVED. One Identity, and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.oneidentity.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.