Compliance to Local Finance Laws with One Identity's Safeguard for Privileged Sessions

Safeguard for Privileged Sessions

"ONE IDENTITY IS THE FIRST COMPANY IN IT BUSINESS THAT PROVIDED A SOLUTION IN PROMISED TIME WITHOUT ANY OBVIOUS FAULTS"

– Michael Fendt, System & Network Engineer, Fiducia IT AG.

▲ FIDUCIA
Ihr IT-Partner

Fiducia IT AG is the leading IT provider of financial companies and one of the ten largest IT service providers in Germany. The company provides IT outsourcing and data-center services for 775 cooperative banks, 53 private banks, as well as central government institutions. Its data-center services are served by innovative mainframe technologies and supported by leading data protection and IT security solutions.

In addition, it develops and sells an integrated, multi-banking solution called "agree", which is one of Germany's leading core banking systems. The company's headquarter is located in Karlsruhe and it has a branch office in Munich. The number of employees reached 2,400 in 2012.

Learn more

- Safeguard homepage
- Request callback

The Challenge

Compliance to BaFin

In Germany, the Federal Financial Supervisory Authority (BaFin) recently announced new regulations which further extend the Minimum Requirements for Risk Management (MaRisk) for financial institutions. Among others, MaRisk requires full audit of administrative access to private banking information. To fulfill these strict requirements, Fiducia had to look for a solution capable of recording all database access by system/database/security administrators and replaying the records for forensic purposes in case there is suspicion of non-compliance. In addition, as the Fiducia data-center environment consists of approximately 8,000 UNIX and Linux servers, finding an adequately robust auditing solution was increasingly challenging. For a long time, the provider couldn't find any competitive offerings on the market. Finally, it discovered a solution that met its requirements: Safeguard for Privileged Sessions.

Key Safeguard for Privileged Sessions benefits for regulatory compliance:

- Control SSH, RDP, VNC, Citrix ICA, Telnet and protocol-specific channels
- Granular access control policies (e.g. based on time period or group membership)
- Strong authentication methods
- Tamper-proof audit trails for privacy and compliance
- Movie-like audit trail playback and search for quick forensics
- DLP-integration for file transfer analysis
- Compliance reports

The Solution

Full Audit of Internal and External Connections

The provider involved its strategic system partner AS Computer Consulting & Service in the implementation project. The experts at Fiducia and AS Computer spent about five months to thoroughly test Safeguard for Privileged Sessions down to its tiniest pieces. "Finally, we chose the One Identity product as it was the only offering fulfilling our particular requirements and promised the development of a custom solution with a competitive time frame and costs." - explains Mr. Michael Fendt, System & Network Engineer of Fiducia IT AG.

Fiducia started to use Safeguard for Privileged Sessions in production in 2008. The integration of the Safeguard for Privileged Sessions appliances has been smooth; however, the organizational integration of SSH auditing into administrative processes of Fiducia was more complex. Originally, they used Safeguard for Privileged Sessions for auditing only SSH administrative sessions, but later they extended its coverage for RDP-sessions. Recently, they've added Citrix ICA and TN3270 protocols to the list and started to evaluate the audit of encrypted TN3270 connections as well. (TN3270 is a Telnet protocol used to communicate with IBM mainframes.) Fiducia has continuously extended its Safeguard for Privileged Sessions footprint since 2008. Currently, they use 2 High-Availability (HA) Safeguard for Privileged Sessions clusters for the audit of internal employees, 1 additional cluster for the PCI DSS environment, and 2 HA clusters for auditing external customers' connections.
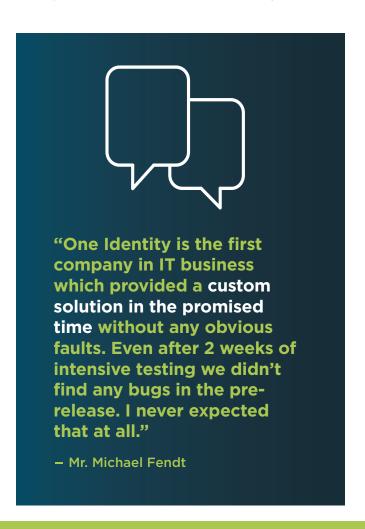
Involvement of all stakeholders

Since Safeguard for Privileged Sessions logs contain very sensitive and sometimes personal data, the requirements of the worker's council and the Personnel Department were also involved from the beginning. Due to continuously coordinated actions of all related parties, they were able to extend the labor management contract. It also defined that only a very limited group of people can request an analysis of the archived administrative sessions. Actual evaluations are in the rarest cases needed. Indeed, the mere fact that all administrative activities are recorded audit proof already deters most of the potential attackers.

The Result

Passing Supervisory Audits

By implementing Safeguard for Privileged Sessions, Fiducia is now capable of fulfilling the relevant specifications of German finance laws and regulations.

The provider has recently passed the audit of the supervising authority without negative comments. If needed, with Safeguard for Privileged Sessions it is possible to fully review who, when, on which system exactly what kinds of changes have been made. In addition, FIDUCIA's specific needs were also completed by One Identity by the development of a custom module within half a year.

> **"One Identity is the first company in IT business which provided a** custom solution in the promised time **without any obvious faults. Even after 2 weeks of intensive testing we didn't find any bugs in the pre-release. I never expected that at all."**
>
> **– Mr. Michael Fendt**

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