CASE STUDY

ISAE 3000 Compliance with Safeguard for Privileged Sessions

Safeguard for Privileged Sessions

Solvinity develop, implement, host and manage IT environments within the strictest boundaries of security. Solvinity specializes in providing Solvency II compliance services for insurers, managed hosting, vCloud services, virtual private datacenter services and Infrastructure-as-a-Service. In their six years as a company, they've worked on three generations of their cloud platform, and seen consistent growth in both staff numbers and bottom line. Solvinity clients include insurance providers, banks, consultants and free ad placement sites, as well. The company is located in Amstelveen, Netherlands.

Learn more

- Safeguard homepage
- Request callback

The Challenge

Separation of Roles

Solvinity provides global cloud computing services which must follow strict international guidelines. As a services organization, its business processes should be audited and certified by the ISAE 3000 (International Standard on Assurance Engagements) standard. The objective of the ISAE 3000 is to set high-quality auditing and assurance standards for professional accountants with this certification. "Among others, compliance to ISAE 3000 requires separation of roles, which is challenging for a small IT company, like Solvinity, where multiple engineers have privileged access to the majority of resources." - adds Mr. Giray Devlet, Security Officer at Solvinity.

The company previously used traditional logging solutions, which transferred OS and network devices logs to central log- and audit servers. However, the problem was that logging solutions couldn't record every important event, as log collection from Windows systems was limited, and application events were not always forwarded to log servers either. On top of that, log and audit servers were managed by engineers who were supposed to be monitored.

So, driven by these risks identified in an ISAE 3000 audit, Solvinity started to look for a privileged user monitoring solution. The company's key expectations for the solution were smooth integration into the existing infrastructure, transparent operation and easy administration. In addition, they had a specific requirement for full transparency in SSH and RDP administrative sessions.

> "WE WERE UP AND RUNNING IN A VERY SHORT TIME, WHICH IMPRESSED BOTH CUSTOMERS AND AUDITORS. WE WOULD NOT HAVE BEEN ABLE TO ACHIEVE THIS WITH ANY OTHER PRODUCT AVAILABLE ON THE MARKET."
>
> – Mr. Giray Devlet, Security Officer, Solvinity.

The Solution

Safeguard for Privileged Sessions in Data-centers

Monitoring solutions by ObseveIT and Xceedium were considered during the selection process. "The overall technological approach of these solutions, such as the need for agents installed on servers or additional Microsoft SQL license fees were all determining factors against them. We also preferred One Identity's solution, because it controls access on the network level, while the competitors follow a more application level approach." – comments Mr. Devlet. Therefore, the provider opted for One Identity's privileged activity monitoring solution, the Safeguard for Privileged Sessions (Safeguard for Privileged Sessions). Beyond the required technological approach of Safeguard for Privileged Sessions, Solvinity preferred One Identity having used the vendor's free logging product, the syslog-ng Open Source Edition for many years without problems.

Initial deployment was completed in 2011. Solvinity ran a test setup using VMware images before the required appliance arrived. The appliance was configured and put into production in less then one week. Currently, two Safeguard for Privileged Sessions solutions are in use, each in a separate data-center, positioned between the Firewall/ VPN and the internal infrastructure. Safeguard for Privileged Sessions solutions monitor the full activities of 15 engineers accessing resources via SSH or RDP protocols in these two data-centers. In addition, Safeguard for Privileged Sessions can enforce the use of strong authentication methods (public key), and also verify the public key of the admins before they access servers using SSH.

The Result

Impressed Customers and Auditors

Safeguard for Privileged Sessions has been in production since 2011 without any serious issues. Safeguard for Privileged Sessions helped Solvinity fully comply with the ISAE 3000 standard, including the requirements for monitoring privileged users and risk remediation with regards to password policies. In case of a security breach or a major incident, Solvinity can now share related audit records with its affected customer. In this way, Solvinity can quickly eliminate accountability issues, which enhances the company's reputation further.

Safeguard for Privileged Sessions's greatest competitive advantage is that it transparently fits into Solvinity's infrastructure, with just minimal adjustments required in engineers' daily routine. Furthermore, it doesn't require additional settings or changes of any other infrastructure component. "One Identity Safeguard for Privileged Sessions allowed us to quickly and transparently mitigate several risks that were identified by an external audit. We were up and running in a very short time, which impressed both customers and auditors. We would not have been able to achieve this with any other product currently available on the market." - concludes Mr. Devlet.

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