CASE STUDY

Protecting Personal Data and Simplifying Access Management

Safeguard for Privileged Sessions

"SAFEGUARD FOR PRIVILEGED SESSIONS PROVIDED US CLEAN AUDITING AND A SECURE, CENTRAL POINT FOR ACCESS MANAGEMENT."

– Dr. Christoph Biardzki, Head of IT Infrastructure, Server and Service Group, LRZ.

Founded in 1962, the Leibniz Supercomputing Center (LRZ) is one of the oldest computing centers in Germany which provides services to scientific and academic communities in Munich, Germany. Major services include operating the Munich Scientific Network and running IT-Applications. LRZ also operates the fastest supercomputer in Europe and no. 4 in the world.

Learn more

- Safeguard homepage
- Request callback

The Challenge

Protecting student records

LRZ is an institution which traditionally operates an open, scientific environment and usually does not process any sensitive data. However, recently LRZ was requested to host a complex web application which requires a much more stringent approach to IT security than usual, as it directly handles personal data of hundreds of thousands of study applicants. The regulations to protect sensitive personal records required LRZ to implement a process for preventing unauthorized data copies.

Previously, the administrators of the institution used SSH-based access with a password or a SSH key to reach the servers. However, administration and auditing of these accesses was a very complex task as there were countless access controls regulating who is allowed to do what from where and on which server. Consequently, LRZ had to find a solution to easily and securely control and audit access to (Linux) servers storing personal data. This new concept required the separation of server administration and access management roles, as well.

Key Safeguard for Privileged Sessions benefits for LZR

- Central point for access management
- Cheap smartcard-based, two-factor authentication
- Ability to record all activities on servers
- Ability to track sensitive data and file transfers
- Ability to allow or deny server access
- Use of multiple encryption keys for audit trails
- Simple, effective high-availability solution

The Solution

Central access control with Safeguard for Privileged Sessions

In the planning phase, LRZ experts considered different concepts, such as stricter control over all SSH-enabled workstations or the implementation of a Linux-based gateway server. Finally, they chose One Identity's Safeguard for Privileged Sessions activity monitoring appliance.

"We decided to buy Safeguard for Privileged Sessions because it acts as a central access control point to our servers. In addition, compared to a Linux server-based gateway, Safeguard for Privileged Sessions provides gateway functionality without admins needing to have a shell account on a gateway server." – says Dr. Christoph Biardzki, LRZ's Head of IT Infrastructure, Server and Services Group.

LRZ issued a smartcard with an embedded public key to each administrator. The public keys stored on smartcards were entered on Safeguard for Privileged Sessions and administrators were granted access rights based on group membership on Safeguard for Privileged Sessions. Safeguard for Privileged Sessions uses the stored SSH keys to login to the target servers. Target systems include Novell SLES-servers and NetApp filers. As only Safeguard for Privileged Sessions is allowed to access target servers via SSH, securing and auditing network firewalls has become very easy, as the rule sets only include Safeguard for Privileged Sessions and not, like before, many different workstations.

Testing and implementation took approximately one month. Now, Safeguard for Privileged Sessions is in productive operation protecting LRZ's critical servers and storage systems.

It currently controls 10 administrators and 100 servers of the institution. Furthermore, there are plans at LRZ to extend Safeguard for Privileged Sessions operation for additional systems such as network components.

The Result

Secure access management, calm worker's council

Safeguard for Privileged Sessions helped LRZ to implement several IT security best practices like clean assignment of access roles, secure two-factor authentication and auditing.

It also helped to make access administration easier as most access rules are stored centrally and the rest is identical and thus easily auditable on all servers. Additionally Safeguard for Privileged Sessions discourages potential internal attackers from attempting to pull out data from critical servers.

"Most importantly, the turnkey appliance approach made our system less complex. In addition, Safeguard for Privileged Sessions provided a smooth integration with $10 smartcards to get a fully functioning two-factor authentication. Last but not least, the use of multiple encryption keys* for audit trails made easier to us to get implementation approval from the worker's council ("Betriebsrat") which in Germany has to agree to all measures which could be used to monitor employees. Safeguard for Privileged Sessions ensures they are involved if audit logs have to be checked." – concludes Dr. Biardzki.

*Safeguard for Privileged Sessions can use multiple keys to encrypt the audit trails. In this case, multiple decryption keys are needed to replay the audit trails, so a single auditor on his own cannot access every information about LRZ systems.

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