CASE STUDY

Managing Third-Party Access at T-Mobile Austria

Safeguard for Privileged Sessions

T-Mobile Austria is the second largest mobile telecommunications provider in Austria with more than 4 million customers and approximately 1,300 employees. The T-Mobile and tele.ring brands target various customer groups – from smartphone consumers to sole proprietorships and even large enterprises.

As part of the Deutsche Telekom group T-Mobile benefits from the innovative capacity and financial stability of the group, one of the biggest global players in the telecommunications market. In the fiscal year 2015 the group reported a turnover of 69.2 billion Euros. T-Mobile Austria serves, amongst other functions, as a machine to machine communication (M2M) expert for the Deutsche Telekom group. T-Mobile offers a wide range of cloud-based solutions to its business customers.

Learn more

- Safeguard homepage
- Request callback

The Challenge

"One Identity Safeguard for Privileged Sessions enables me to sleep easy with its fine-grained access control, supervision, and audit of shell access to our critical systems."

As a major mobile provider, T-Mobile Austria operates a heterogeneous communications network consisting of thousands of third-party devices and systems. These systems are supported and maintained by numerous vendors requiring remote access to T-Mobile's network. Although the provider has traditional perimeter defense such as firewalls and VPNs in place, these lack fine-grained access control and monitoring of vendor activities. In the past, T-Mobile had to manually enable predefined firewall rules for SSH-based shell connections to grant temporary access (i.e. maintenance windows) for the vendors arriving from a specific IP range. Granting Service Management Center (SMC) personnel permission to configure firewalls was an additional disadvantage of the old solution. Consequently, the IT security experts articulated the need for a security device capable of controlling, monitoring and auditing the remote access of third-party vendors.

"We wanted to maintain the scalability, availability and quality of the carrier-network; that's why we needed a tool capable of reliably interoperating with the production systems serving our 4 million customers. And, of course, we wanted secure, controlled, and auditable access for a large number of supplier engineers." – explains Georg Petzl.

"ONE IDENTITY SAFEGUARD FOR PRIVILEGED SESSIONS ENABLES ME TO SLEEP EASY WITH ITS FINE-GRAINED ACCESS CONTROL, SUPERVISION, AND AUDIT OF SHELL ACCESS TO OUR CRITICAL SYSTEMS."

– Georg Petzl, Chief Security Officer at T-Mobile Austria

The Solution

The T-Mobile Austria experts heard about One Identity's privileged user monitoring technology, Safeguard for Privileged Sessions, back in 2011. They tested the solution and were very pleased with it. As the investment cost was affordable they decided to purchase it.

"We chose the Safeguard for Privileged Sessions because it simply fulfilled our needs for reasonable cost. Later, when our needs changed, One Identity responded quickly and very satisfactory." – adds Georg Petzl.

First T-Mobile Austria provided limited shell access to vendors' engineers: they could remotely access internal systems only for initial installation and configuration purposes.

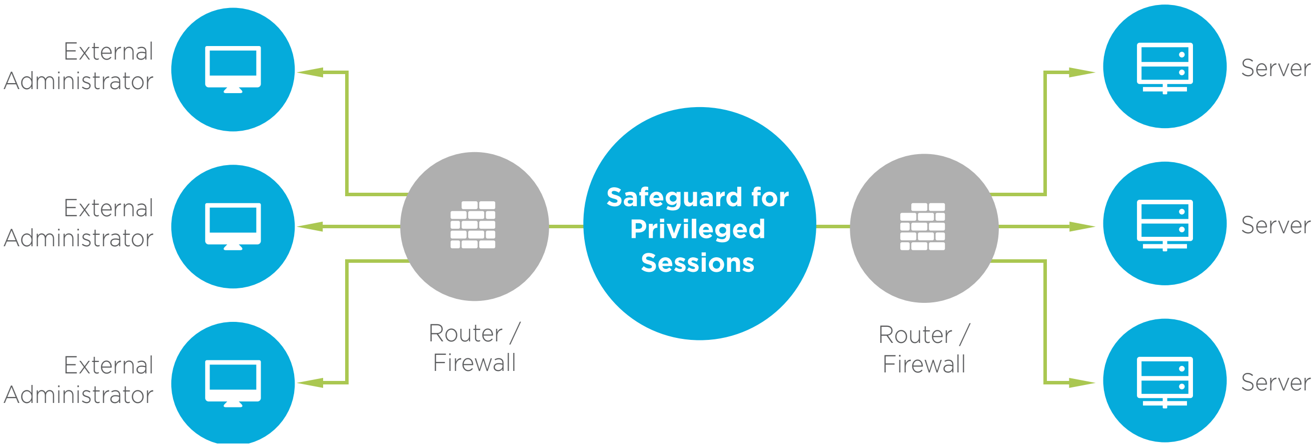
T-Mobile Austria has used One Identity Safeguard for Privileged Sessions in production since 2011. In March 2016, the license was upgraded from 150 to 500 hosts and the number is growing...

Benefits

For shell access, Safeguard for Privileged Sessions proved to be a great solution for T-Mobile Austria. Beyond the access control of third-party vendors, Safeguard for Privileged Sessions has an added value for the provider: it offers a convenient way for the provider's on-call support engineers to connect to the systems they are responsible for.

T-Mobile also likes the transparent and platform-independent nature of the Safeguard for Privileged Sessions – the engineers don't have to install or change anything on their client machines; they can continue to use any SSH-capable client software. The white- or blacklisting of commands permitted to use on remote systems and the recording and playback of privileged sessions also impressed the provider.

"Managing access of a large number of third-party vendors and their support engineers is a nightmare for every security manager. One Identity's Safeguard for Privileged Sessions enables me to sleep easy with its fine-grained access control, supervision, and auditing of shell access to our critical systems. We are very satisfied with sales and technical support of One Identity."



Monitoring third-party access by Safeguard for Privileged Sessions

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