CASE STUDY

# Privileged Account Management at Leading Telecom Operator

Safeguard for Privileged Sessions

"THANKS TO ONE IDENTITY'S SAFEGUARD FOR PRIVILEGED SESSIONS, BOUYGUES TELECOM HAS A TOOL FOR CONTROLLING ADMINISTRATORS' ACC ESS TO NETWORK EQUIPMENT WHILE MEETING THE REGULATORY REQUIREMENTS FOR TRACEABILITY."

– Mr. Pierre Granger, Head of Network Security Operations at Bouygues Telecom

Founded in 1994, Bouygues Telecom has operations worldwide in mobile and fixed-line communications, television, the Internet and cloud computing. The company has been well known for its innovative products and high quality of customer service, serving 11.1 million mobile customers and 2 million broadband customers of which over 1.5 million are business customers and over 1.7 million are B&YOU customers.

The operator currently has over 9,000 staff members, including 2,000 customer advisors working in its six call centers in France and 2,500 sales consultants in its network of retail stores.

## Learn more

- Safeguard for Privileged Sessions homepage
- Request callback

## The Challenge

**Security of Privileged Accounts**

Bouygues Telecom is well aware of cybersecurity issues and has always paid special attention to protecting the data of its users and customers. In addition, as part of its "Jump-host" project for allowing all system administrators to access the operator's 18,000 network devices and servers, Bouygues Telecom wanted to implement policy management for privileged accounts.

Before the implementation of the "Jump-host" platform, Bouygues Telecom had traditional IT solutions (Solaris and Windows TSE) for channeling the network flows to the core production systems. However, this architecture neither provided enough logging details, nor did it offer a centralized security policy.

Bouygues' ultimate goal was to centralize administrative network access and to retain access data for all equipment (mobile and ISP telecom network) at critical security levels with a solution that can support most administrative protocols. Last but not least, the operator wanted to control administrators' access and secure the usage of shared accounts on critical systems, primarily through providing effective password management.

## The key advantages of Safeguard for Privileged Sessions for Bouygues Telecom

- Global management of privileged accounts
- Centralization of network accesses
- Compliance with regulatory requirements for traceability
- Controlling administrative access to network equipment
- Scalable solution for the provisioning of managed devices

## The Solution

**Tracing of administrative access to 18,000 devices**

Bouygues Telecom called for a tender, and Finally chose the Safeguard for Privileged Sessions (Safeguard for Privileged Sessions) appliance from One Identity. The Safeguard for Privileged Sessions provides secure administrative access to all telecom devices of the operator – routers, network switches, Unix and Windows servers, the core mobile data (GGSN and xGSN) and voice data communications devices (HLR, HLRv, MSC, IMS).

> **"We needed a high-performance industrial solution in our project. Being more user-friendly than our old solution, Safeguard for Privileged Sessions lets us freely manage our devices and protect them in the same time."**
>
> says Pierre Granger, Head of Security Operations at Bouygues Telecom

Because of the significant load of simultaneous connections (400 SSH connections and 100 simultaneous RDP connections per appliance), Bouygues Telecom appreciates both the performance of Safeguard for Privileged Sessions and the range of protocols supported. "It was important for us that the solution could cover a huge number of protocols – not only SSH and RDP, but also VNC, Telnet and Citrix." - states Pierre Granger.

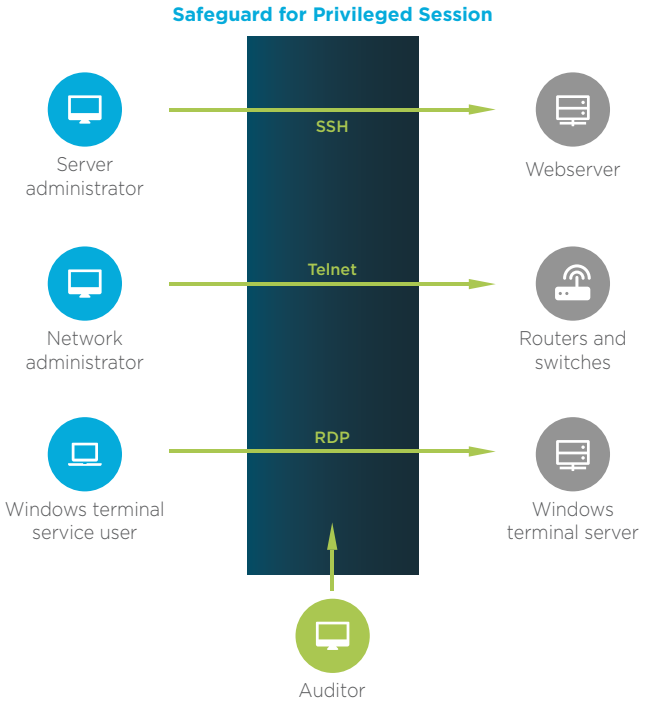
## Benefits

**Advanced security of privileged access**

With Safeguard for Privileged Sessions, Bouygues Telecom is able to manage privileged accounts and improve the security of administrative access to all critical equipment.

With the help of the system integration partner "I-Tracing", which defined the architecture of the solution, Bouygues Telecom was able to limit the impact of integrating the "jump-host" platform on the connections used to access devices.

"With the performance of Safeguard for Privileged Sessions we can protect a significant number of devices, and reach our goals in terms of access control and traceability. In addition, the indexing service on recorded sessions lets us carry out text searches easily using the OCR engine." - adds Pierre Granger.




*Controlling and monitoring remote administrative 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