

CASE STUDY

# Internal and External Staff Control at Leading Telecom Operator

Safeguard for Privileged Sessions



France Telecom-Orange is one of the world's leading telecommunications operators with annual sales of 43.5 billion euros and has 170,000 employees worldwide. Present in 32 countries, the group has a total customer base of approximately 231 million customers, including 172 million mobile customers and 15 million broadband internet (ADSL, fiber) customers worldwide. Orange is one of the main European operators for mobile and broadband internet services and, under the brand Orange Business Services, is one of the world leaders in providing telecommunication services to multinational companies.

## Learn more

- [Safeguard homepage](#)
- [Request callback](#)

## The Challenge

### Protection of Critical Telecom Assets

Like any major telecom provider, Orange Romania also operates sensitive front-end applications, service-delivery platforms and specific network devices. As usual in the telecom sector, such info-communication systems are accessed by privileged employees, consultants and suppliers, as well. Auditing the activities of this internal and external workforce was a key technical challenge for Orange. Therefore, Orange's IT experts started to search for a device capable to audit remote access over commonly used protocols, such as SSH, SFTP, SCP, RDP, Telnet and VNC.

## The IT experts specified the following key expectations about the new solution:

- ✓ Transparency - users do not have to change their usual client applications to connect to remote systems
- ✓ Scalability - the product must adapt to increasing enterprise needs both in user number and working load
- ✓ OCR-ing and indexing the content of graphical protocols to completely audit RDP-based accesses from security reasons
- ✓ File transfer control and
- ✓ Ease of configurability and use.

"I RECOMMEND ONE IDENTITY'S SAFEGUARD FOR PRIVILEGED SESSIONS FOR ITS OCR AND AUDIT TRAIL SEARCH CAPABILITY. I ALSO LIKE THIS SOLUTION BECAUSE IT IS FULLY TRANSPARENT."

- Bogdan Mistrapau, Middleware Infrastructure Administrator, Orange Romania.

## The Solution

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

During the selection process One Identity Safeguard for Privileged Sessions and 2 competitive products were considered.



**“We finally chose Safeguard for Privileged Sessions because this solution offered full transparency on the network and the capability of searching in the audit trail content. Safeguard for Privileged Sessions has been a quite secure product, as bypassing the audit system is almost impossible.”**

**says Mr. Bogdan Mistrapau,  
Middleware Infrastructure  
Administrator of Orange Romania**

One Safeguard for Privileged Sessions appliance was implemented for auditing 10 external suppliers and consultants accessing Orange’s “VAS” (Value Added Services-) platforms and other systems via a VPN tunnel. Several SSH and RDP connections were configured to be audited and an indexing service was also set up on an external server to make searching in audited content possible. Safeguard for Privileged Sessions operates in router mode.

In the second environment, a high-availability Safeguard for Privileged Sessions cluster was implemented for auditing privileged access to the billing system, which is a menu-based OpenVMS-application accessible via Telnet terminal. External indexing service was also set up. In this deployment, Safeguard for Privileged Sessions operates in bridge mode.

## The Result

### Transparent Audit and Forensics

Orange Romania can now audit several user activities over commonly used remote access protocols. Thanks to Safeguard for Privileged Sessions’s OCR function, the security staff can conduct free-text searches even in audit trails storing graphical content. “Safeguard for Privileged Sessions is non-intrusive because the users doesn’t have to change anything in the way they are connecting to remote systems. Unlike other solutions on the market, with Safeguard for Privileged Sessions, our users can use their usual client application and do their daily job without changing their working habits. Safeguard for Privileged Sessions doesn’t restrict the preferred authentication method either.” – summarizes Mr. Mistrapau.

Orange intends to extend Safeguard for Privileged Sessions’s audit coverage to further external consultants and suppliers in the near future.

## 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](https://www.oneidentity.com)