CASE STUDY

Tightening control of privileged access without additional overhead

Cloud service provider 3DS OUTSCALE streamlines privileged access management and strengthens security by automating monitoring, recording and password control with One Identity Safeguard

Key Facts

- **Company**
  3DS OUTSCALE
- **Industry**
  Cloud Service Provider
- **Country**
  France
- **Website**
  https://en.outscale.com/

Challenges

- Investigating privileged access incidents was a full-time job for one member of staff
- Repetitive monitoring and reporting tasks were error-prone
- Lack of real-time data prevented proactive incident management
- Passwords were shared to avoid time-consuming requests and resetting processes

Results

- Automated privileged access monitoring saves one full-time equivalent
- Privileged session recording and replay are constantly available
- Proactive management identifies security issues before any damage is done
- Password automation increases protection without impacting productivity

Solutions

- One Identity Safeguard

3DS OUTSCALE had no way of managing and monitoring privileged access sessions proactively with administrators sharing passwords to avoid lengthy password requests and reset processes. In addition, one member of the company's IT staff was entirely occupied in investigating privileged access incidents.

By deploying One Identity Safeguard, 3DS OUTSCALE increased the efficiency of controlling and monitoring privileged access. And, by automating the password processes, the company tightened security without impacting productivity.

Cloud service provider 3DS OUTSCALE specialises in protecting not only customer data, but also internal access to its systems. Edouard Camoin, chief information security officer at 3DS OUTSCALE, says, "Customer data is our most important asset. It must be protected at all times. However, internal access control can't be overlooked. Security needs to be watertight from top to bottom."

Tightening up privileged access

3DS OUTSCALE looked to improve monitoring of administrators with privileged access. Administrators at 3DS OUTSCALE are labelled level one, two or three. Level-one administrators, often contractors, have restricted access to internal systems and follow well-defined support procedures. Level-two and -three administrators, on the other hand, have varying privileged access to business-critical internal systems that support the core 3DS OUTSCALE cloud.

Level-two and -three administrators gain access to the core infrastructure via a bastion host. Monitoring and reporting of each administrator session via the host were largely manual. A member of staff worked full-time on investigating potential security incidents and generating auditing reports. Edouard Camoin comments, "Our goal was to control and record privileged access, so we had data on every session readily available. We aimed to be much more proactive, so if a security breach looked like it was occurring, we could address it before any damage was done."

"The way we monitor privileged sessions is far more efficient with Safeguard. Session data is at our fingertips, so we can trace anything that raises an alarm."

Edouard Camoin,
Chief Information Security Officer, 3DS OUTSCALE

Edouard Camoin also wanted to take the risk out of managing passwords for privileged access, as the system that was used traditionally held some security risks—for example, through generic passwords. "It was a process whose risk I wanted to decrease through automation," says Edouard Camoin.

An easy-to-deploy solution

To reduce the access risk, 3DS OUTSCALE implemented Safeguard from One Identity. According to Edouard Camoin, the solutions were simple to deploy and manage. 3DS OUTSCALE chose Safeguard's Instant On mode of operation, which meant there were no changes to user workflows. As a result, administrators could continue to use their familiar client applications to access servers and systems without disrupting their routines. "The fact we didn't have to change administrators' habits too much was a big advantage of Safeguard because it made adoption easy," comments Edouard Camoin.

Saves the workload of one employee

3DS OUTSCALE no longer needs a member of staff working full-time investigating potential security incidents, because Safeguard records all privileged access sessions. These sessions are also indexed, making them easy to search. "The way we monitor privileged sessions is far more efficient with Safeguard," says Edouard Camoin. "Session data is at our fingertips, so we can trace anything that raises an alarm. Plus, all the evidence is there for auditing and compliance requirements."

Human error is eliminated, bolstering security

By taking the human element out of privileged access monitoring, 3DS OUTSCALE has eliminated human error. "Many of the monitoring tasks are simple and repetitive, so mistakes can be made. This was a big concern for us from a security and compliance perspective," says Edouard Camoin. "We can't afford errors."

3DS OUTSCALE is also using the recorded privileged sessions to help raise security awareness among administrators. Edouard Camoin comments, "We replay sessions to help administrators understand that we need to stay focused on security. It works well as a training tool."

Allows proactive management

Crucially for Edouard Camoin, 3DS OUTSCALE can be proactive in how it manages privileged access. Because Safeguard monitors sessions in real time, it can instantly raise an alert if it spots anything that looks out of the ordinary, such as a risky command or suspicious window title in a graphical connection. "I no longer feel as though we can't do anything until incidents occur," says Edouard Camoin. "With Safeguard, we can act straightaway before any damage is done."

Automation increases efficiency

Security around passwords is much tighter without any increase in management overheads. Thanks to Safeguard, administrator password requests and resets are automated for maximum efficiency. 3DS OUTSCALE has also tailored the approval process in line with company guidelines. "We no longer use shared passwords," says Edouard Camoin. "The whole process for allocation and resetting is pretty slick with Safeguard, helping us avoid any delays."

> **"I no longer feel as though we can't do anything until incidents occur. With Safeguard, we can act straightaway before any damage is done."**
>
> **Edouard Camoin,**
> **Chief Information Security Officer, 3DS OUTSCALE**

About One Identity

The One Identity family of identity and access management (IAM) solutions offers IAM for the real world including business-centric modular and integrated, and future-ready solutions for identity governance, access management and privileged management.

View all One Identity case studies at OneIdentity.com/casestudies