safous | THINK YOUR ACCESS

Toray Industries, Inc. Case Study

Safous Secures Network Infrastructure for Leading Japanese Manufacturer

Toray Industries, Inc., one of Japan's leading basic materials manufacturers, was struggling to secure its geographically distributed and technologically diverse infrastructure. Safous offered a robust, easy-to-deploy solution.

The Challenge

Toray's complex IT ecosystem consolidated domestic and international group companies through a shared network, exposing remote access vulnerabilities.

Several international group companies experienced unauthorized access attempts targeting the manufacturer's management systems.

With so many servers to protect, Toray faced lengthy deployment times and high costs for a traditional privileged ID management system.

The Action

Toray implemented Safous to manage SSH and RDP access, block direct SSH and RDP communications to the group network, and provide gateway-based access control.

The manufacturing company was able to integrate Safout with Microsoft Entra ID – formerly Azure Active Directory – to ensure consistent security across its IT infrastructure.

Safous engineers worked side-by-side with Toray's IT team to resolve any implementation challenges along the way.

"Safous' success is demonstrated by the fact that, in the more than a year that we have been using it, we have not experienced a single unauthorized attack against servers using administrative communication."

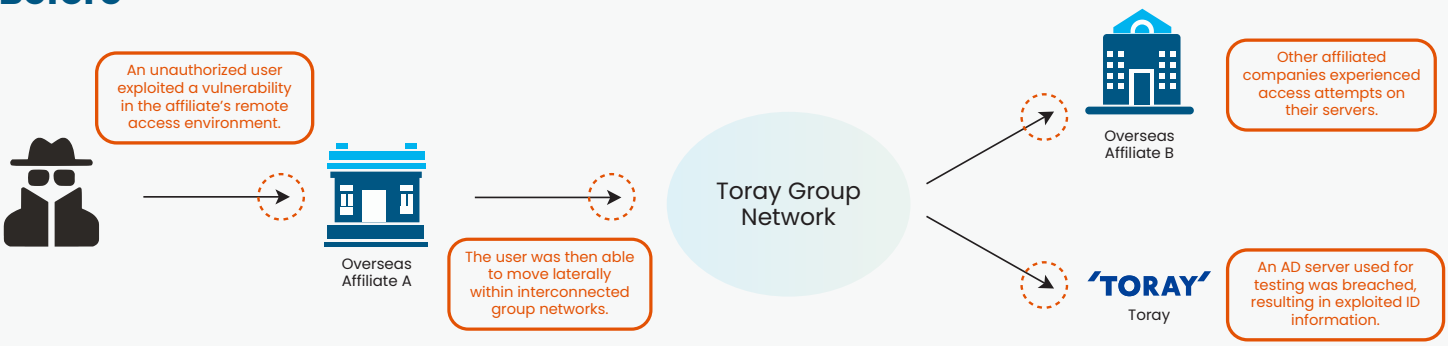
- Yasushi Oka, Toray Systems Center,

The Results

Implementing Safous transformed Toray Industries' network infrastructure, dramatically improving security and operational resilience across its global systems. The manufacturing company was able to establish a robust zero-trust access model for remote management to prevent potential attacks targeting group companies.

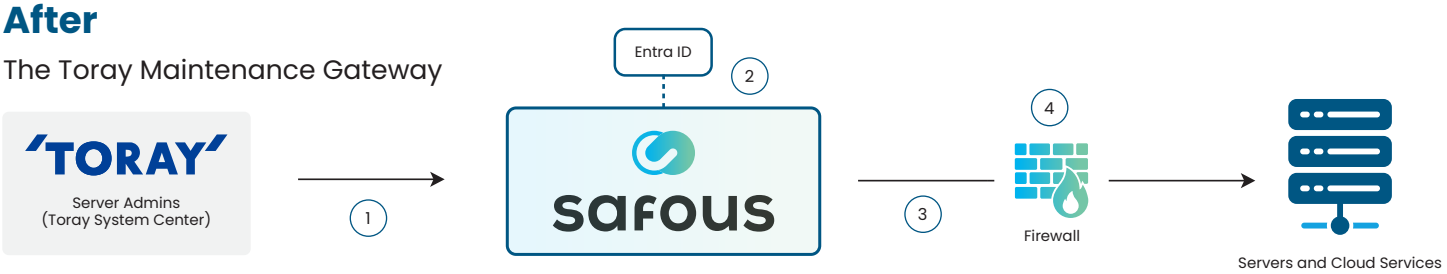
- Zero unauthorized access attempts on servers using administrative communication
- Eliminated direct server access risks
- Plans to expand Safous to digital data access control, OT access control, and cloud access management

Before

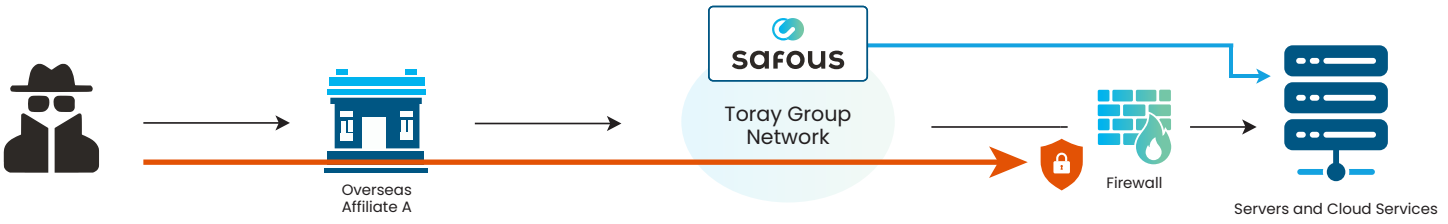


After

The Toray Maintenance Gateway



1. The server administrator signs into the web-based Safous portal.
2. Their identity is verified using multi-factor authentication with Entra ID.
3. The IIJ Omnibus service connects them to the Toray Group Network.
4. The firewall prevents any management-related communication, except required communication from Safous.



As a result, any unauthorized access attempts on the server (even via affiliate company networks) are blocked.