safous

Simple and Secure Access for Your Zero Trust Strategy

Decisive Principles

- **One Time Pass**
  AuthC & AuthZ at all time
- **Least Privileged Access**
  Just-Enough-Permission in time
- **Minimize the Blast Radius**
  Verify & validate by the gatekeeper
- **Always-on Diagnostics**
  Catch the signal of threats

Fully trusted Zero-Trust

Our Zero-Trust security platform's features can ensure that your corporate security policies are fulfilled across all critical business activities

A quick start to your journey

The onboarding process is simple and straightforward. It can be deployed to any network topology without the budget adjustments nor any complex configuration changes which are needed to start your journey.

Beyond the perimeter defense

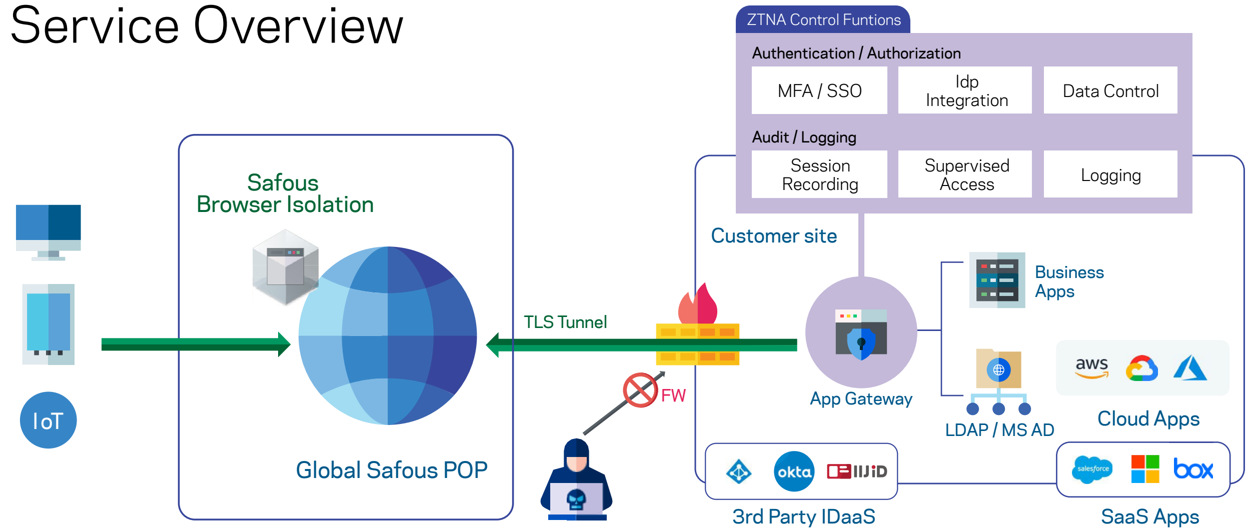
Traditional perimeter-oriented defense architectures are no longer viable. Due to the increase of new threats in the recent years, brand-new cutting-edge approach to minimize our fragile network surface is crucial.

Scan to
find more

www.safous.com

info@safous.com

Safous ZTA
Service Overview



Securely publish

Business applications publishing without opening any firewall port. Blocking all ingress traffic while minimizing the attack surface.

High level auth & control

Attach MFA & SSO to your business applications with connecting to your IDPs for App-based access control.

Flexibly fit to abundant devices

Even the agent-less architectures supports various web applications, RDP, SSH and more.

Perfect compliance

Complying with data security regulations, Safous allows you to choose the data store location fitting to the corporate security governance.

Fully Managed service

Our 24/7 remote monitoring and operation for any troubles and threats.

Service **Specifications**

Feature	Specification
Access Protocol	HTTPS
Agentless Support Application	Web browser-based: HTTP / HTTPS / RDP / VNC SSH / TELNET / SMB Native client-based: RDP / SSH
Agent Support Application	TCP (1-65535) / UDP (1-65535) / IP Network segment
Recording Session Support	Web browser-based: RDP / VNC / SSH / TELNET/ Native SSH
Monitoring	24 hours remote operation monitoring for App Gateway Service up / Service down
Browser Isolation	Control clipboard up/down, File download/upload, Audio connection
Alerting (Service down)	Send email to specific customer email address
Operation Support	24 hours: Urgent troubleshooting by Call / Email (English and Japanese) Business hour (03:00-13:00 GMT): Setting & configuration support by Email
Support Device	Agentless: Windows / Mac / Linux / Android / iOS / IoT (HTTP CALL) Agent: Windows / Mac / Linux

App Gateway **Requirements**

Function	Specification
Support OS	Ubuntu 20.04 /22.04, RHEL 8 (Server Base Environment)
Recording Session Support	4 cores + 1 core per 30,000 users
RAM	Min 7GB (6GB + 512KB per users)
Storage	150GB **if the recording function is enabled, additional disk is required. Assumption data is 2MB/min/user*
Network Bandwitdth	32Kbps per user