safous

Simple and Secure Zero Trust Access

Guiding Principles

- **One-Time Passwords**
  Ensure single-transaction authentication – every time.
- **Least Privileged Access**
  Ensure controlled access to business resources.
- **Minimized Attack Surface**
  All users are verified and validated.
- **Always-On Diagnostics**
  Catch threats before they become breaches.

Never Trust, Always Verify

Eliminate implicit trust and ensure security policies are fulfilled across critical business activities.

A Quick Start to Your Journey

The Safous onboarding process is simple and straightforward. ZNTA can be deployed to any network topology without budget adjustments or complex configuration changes.

Beyond Perimeter Defense

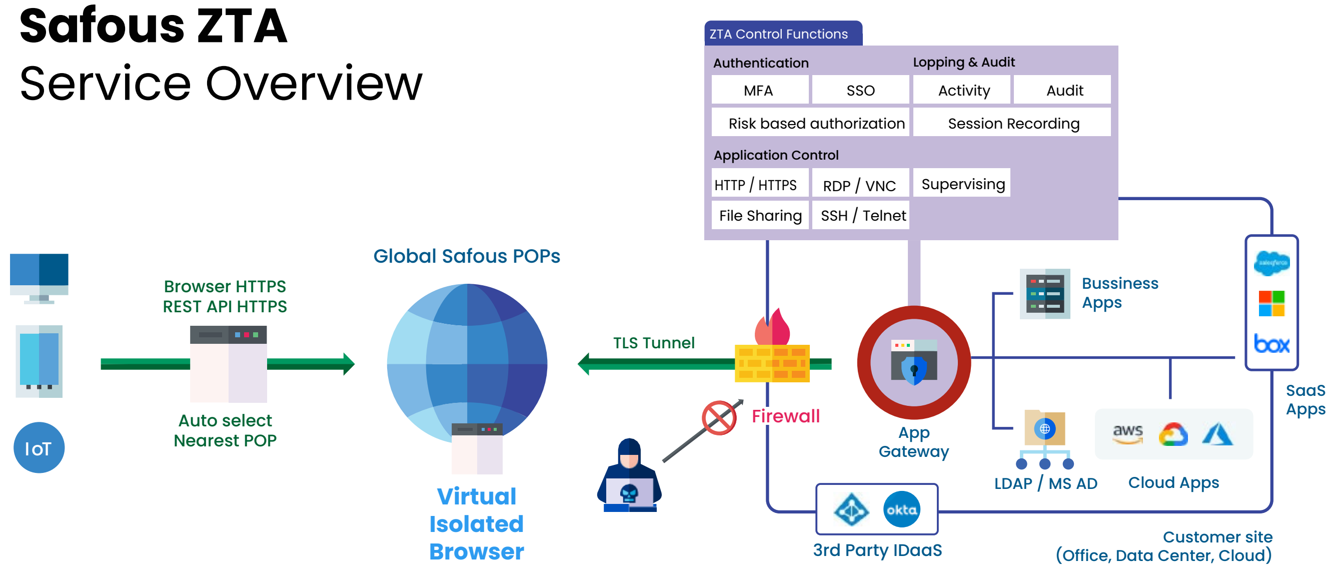
Traditional perimeter-oriented defense architectures are no longer viable in modern hybrid and remote work environments. ZNTA minimizes the attack surface.

Scan to find more

www.safous.com

info@safous.com

Safous ZTA
Service Overview



Securely
Publish Applications

Publish business applications without opening a firewall port. Block all ingress traffic while minimizing the attack surface.

High-Level
Auth & Control

Attach MFA & SSO to your business applications and connect to your IdPs for app-based access control.

Support for a
Variety of Devices

Agentless architectures support various web applications, RDP, SSH, and more.

Stay
Compliant

Safous allows you to choose your data storage location, ensuring you stay compliant with data security regulations for your industry.

Fully Managed
Service

We provide 24/7 remote monitoring – so you stay ahead of all potential 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 hour 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 hour urgent troubleshooting by ticket /phone / email (English and Japanese) Setting & configuration support by email during business hours for each region: 03:00-13:00 GMT
Device Support	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 user)
Storage	150GB *If the recording function is enabled, additional disk is required. This assumes data is 2MB/min/user.*
Network Bandwidth	32Kbps per user