finezza

COSGrid NETWORKS

Customer Story - Case Study

Finezza Replaces Perimeter Access With COSGrid MicroZAccess (ZTNA) and Secure Web Access (SWA)

At a Glance

Customer	Finezza (Fintech / Digital Lending)	**Scope**	Multiple internal applications, multi-role access (QA, Dev, DevOps)
Region	India	**Replaced**	Public exposure, IP allow-listing, flat network access
Use Case	Secure access to DevOps & CI/CD + endpoint web protection	**Solution**	COSGrid MicroZAccess (ZTNA), Z3 SASE App Connector, Secure Web Access (SWA)

About Finezza

Finezza is a fintech company building lending infrastructure for banks and NBFCs. Operating in a regulated environment, the organization requires strict control over access to internal systems while ensuring engineering teams can work efficiently.

The Challenge

Finezza's QA, Developer, and DevOps team needed access to the same internal systems—but with clearly defined access boundaries. The existing model relied on:

- Public exposure of internal tools
- IP-based allow listing
- Cloud security groups

This led to:

Limited access control

Network-based access couldn't differentiate user roles

Increased attack surface

Limited exposure controls on internal systems

Operational complexity

Manual IP allow list management

Finezza required a solution that enables **identity-driven access, removes exposure, and strengthens endpoint security.**

Solution Overview

Finezza deployed

Secure Web Access

Secure Web Access (SWA)

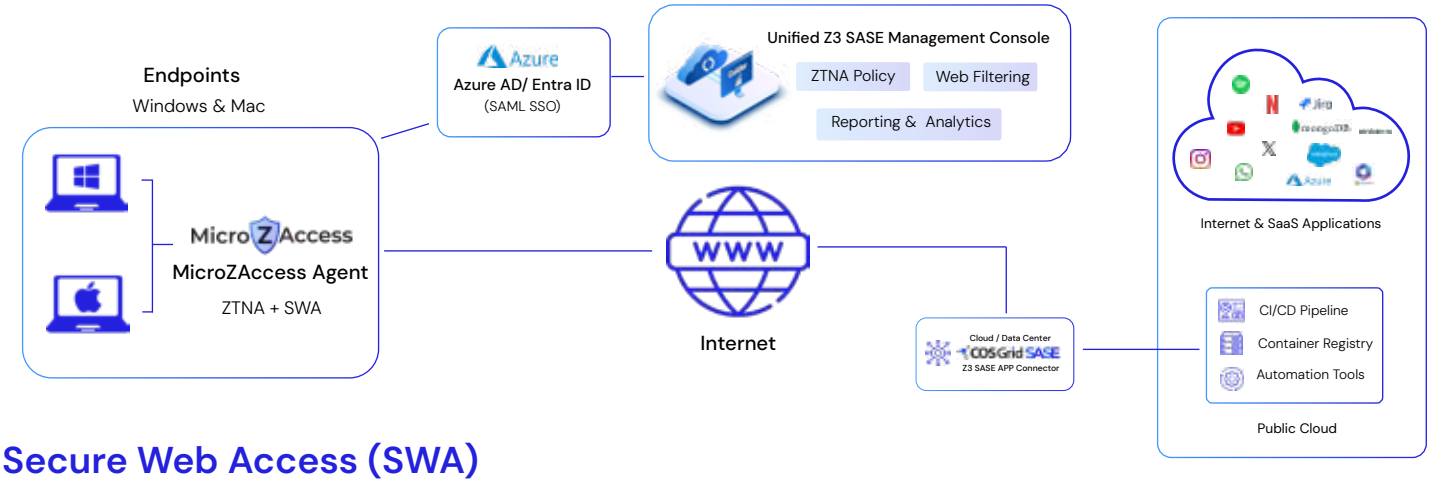
MicroZAccess

COSGrid MicroZAccess (ZTNA)

Key Capabilities

- Per-user, per-application access (RBAC)
- Support for multiple protocols (HTTPS, SSH)
- Direct, efficient connectivity without traffic redirection
- Private application access without public exposure
- Endpoint-level web filtering

Deployment Architecture



Secure Web Access (SWA)

Secure Web Access is enforced directly on endpoints:

- Blocks access to risky or non-business domains
- Protects against phishing, malware, and anonymizers
- Works across all networks (office, home, remote)
- Eliminates dependency on external proxy infrastructure

Results

Area	Before	After
Application Exposure	Publicly accessible	✓ Private via overlay
Access Control	Network-based	✓ Identity-based
Granularity	Broad access	✓ Role-based access
Onboarding	Manual updates	✓ Centralized policy
Endpoint Security	No filtering	✓ Risk-based web access control
Traffic Path	Indirect / variable	✓ Direct connectivity

Results Achieved

Rapid Deployment
Completed full rollout in under 2 hours

Granular Access Control
Precise role-based access without manual effort.

Scalable & High-Performance Access
Direct connectivity with scalable, consistent performance.

Reduced Attack Surface
Eliminated exposure and IP-based access risks

Operational Efficiency
Removed proxies and manual IP allow-listing.

Enhanced Endpoint Security
Real-time protection against phishing and malware.

Conclusion

Finezza successfully transitioned from a perimeter-based model to a modern Zero Trust architecture using COSGrid SASE.

By combining

Secure Web Access (SWA)

MicroZAccess

COSGrid MicroZAccess (ZTNA)

They achieved

- Stronger security posture
- Granular access control
- Reduced operational overhead

www.cosgrid.com
info@cosgrid.com
COSGrid Networks
India | US