COSGrid NETWORKS

MicroZAccess

Granular and Adaptive Zero Trust Network Access delivered Seamlessly in Minutes

In recent years, the scale and scope of ransomware attacks and data breaches have increased exponentially, mainly due to the sophisticated nature of the attacks on the expanding attack surfaces such as work from anywhere, multi-Cloud, and IoT. The cost of data breaches has also been increasing year on year and is estimated to be **$4.35M (global average cost of a data breach) and it's $9.44M for US average cost), as per IBM**. As a response to this trend, industries and organizations globally have started moving to the **Zero Trust Security approach**

Challenges

Traditional network access technologies, including VPNs, pose huge risks in today's cybersecurity context. A few significant problems are listed below:

- **Vulnerable to Data Breaches** due to lack of fine-grained Access and micro-segmentation
- **Easily Susceptible to Phishing Attacks** despite Multi-Factor Authentication
- **Highly Error Prone in ever-changing VMs/Containers setup:** Dependencies on Manual and IP-based configurations
- **Ransomware attacks on workloads** due to Lateral Movements across networks
- **VPN gateway dependencies -** Constraints due to the need for High available service with adequate capacity
- **Poor User experience -**Higher Latencies due to VPN Gateway Traffic Hairpinning and Login fatigues.

Highlights

- **Stronger and Multi-fold Improved Security:** Hidden cloud services, prohibits lateral movements,least privilege access . A secure Access alternative to VPN
- **Seamless End-User Experience:** Peer-to-peer connectivity, supports relays/gateways, universal protocol support
- **Scalable, Highly Available, and manageable:** Enables scalability, high availability, and easy management with SSO using SAML2 Integration and OpenID Connect support, single pane visibility for reliability
- **One Comprehensive Zero Trust and SSE Platform:** Covers all perimeter traffic, micro-segmentation can be combined with SWG, FWaaS, and threat detection

By 2025, At least 70% of new remote access deployments will be served predominantly by ZTNA as opposed to VPN services, up from less than 10% at the end of 2021

Gartner

Problems -MicroZAccess Addressing

Authentication and Authorization Vulnerabilities

- Credential theft / Identity attacks / Brute force attacks
- Poor Access Control/ Authorization -Misconfiguration

Remote Code Execution (RCE), Software & OWASP related

Session Hijack Attacks & Lateral Movements esp. in VPNs

DNS Rebinding/DNS tunneling C2C Attacks

Distributed Denial-of-Service (DoS) Attacks

Integration Vulnerabilities - (SAML)

Protocol vulnerabilities/ Supply Chain risks

Social Engineering Attacks

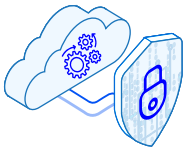
APT & Zero Day Attacks

MicroZAccess Overview

MicroZAccess enables least privileged access to resources through a mutually authenticated peer-to-peer encrypted Overlay network.

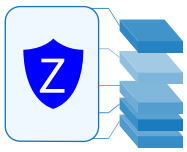
Verify User & Device

- Multi-Factor Authentication (MFA) with IdP
- Device Trust & Security Posture.



Verify Enhanced Identify & Context

- Security Policy evaluation including User Identity, Device Posture, Groups, Location, Time



Establish Micro-Tunnels

- Micro-segmentation target Apps
- Allowed Group Memberships

Least Privilege access to resources

- User to Service (North-South)
- Service to Service (East-West)

Use Cases

- Secure and granular Remote Access of Apps
- Zero Trust Access to Data in SaaS such as OneDrive, AWS S3 etc and Data Protection
- Secure Infrastructure Access, DevOps and Multi-Cloud through micro-segmentation
- Simple Cloud Workload protection
- Compliance Enablement - Auditable Access Logs and micro-segmentation for PCI DSS, HIPPA
- Third party / Contractor Access control

Outcomes

- Reduces the Risk of a Data Breach
- Streamlined security policy creation
- Improved end-user experience
- Flexibility when moving apps, data and services
- Improved Compliance (PCI DSS, NIST 800-207)
- Improved Visibility & Monitoring

MicroZAccess Components

MicroZAccess
App

- User Authentication
- Device Signature
- Device Security Posture
- Micro-Tunnel Origination / Termination
- PEP with Identity aware Host Firewall

MicroZAccess
TURN Mediator

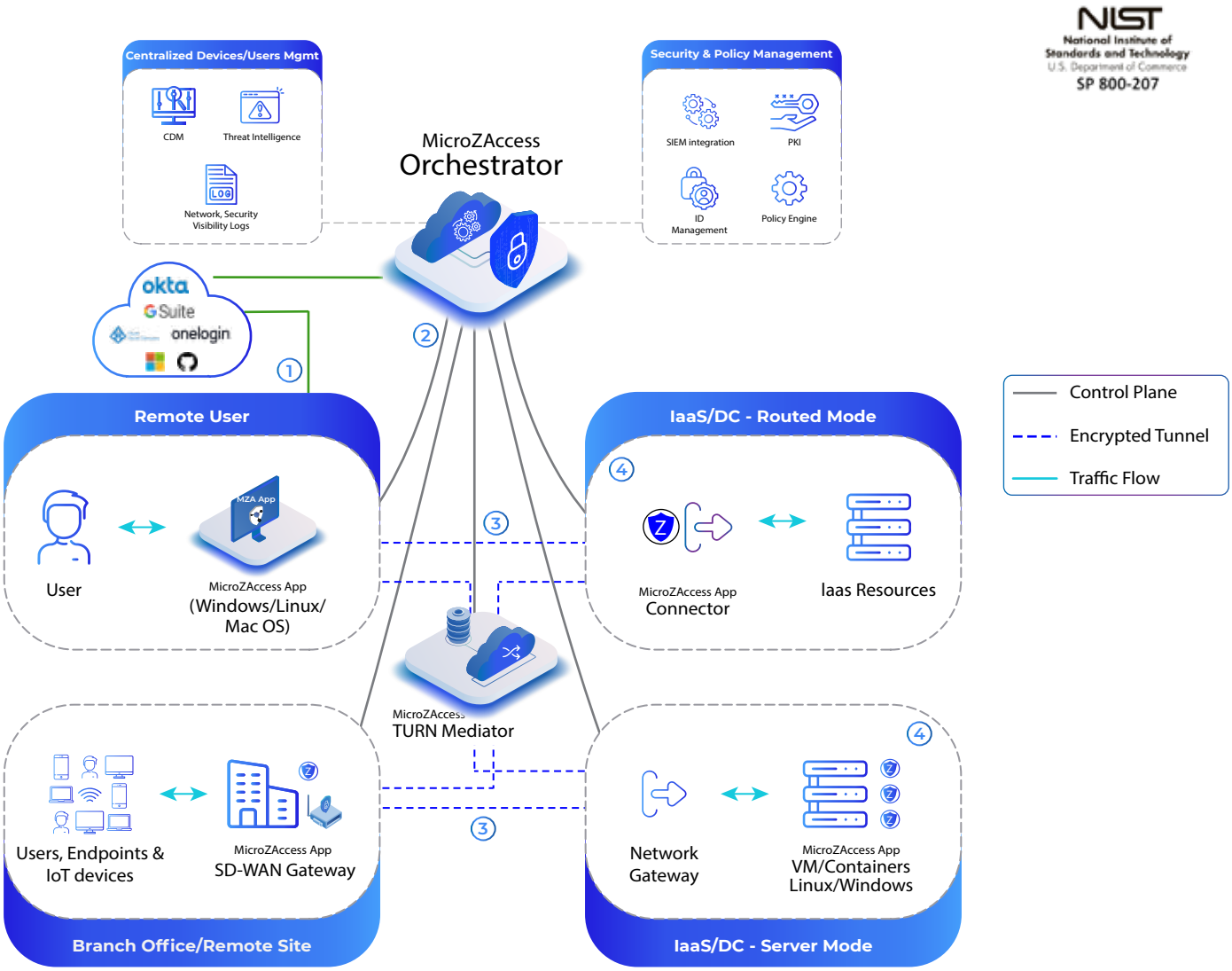
- Cloud based or On-Prem
- Performs Policy Admin
- Policy Enforcement Point
- Facilitates Micro-tunnels between End-points
- Can acts as forwarding Relay, on need basis

MicroZAccess
Orchestrator

- Controller for Devices, Users and Apps
- Policy Engine & Data Access Policy
- PKI & Identity Provider Integration
- Continous Diagonsis and Monitoring
- Threat Intelligence
- Real-time status, Network Activity visibility and Logs

MicroZAccess Architechture

MicroZAccess ensures secure connectivity for users/devices (employees/contractors) trying to access internal applications through **MicroZAccess App**, a lightweight agent installed on the user's devices or servers that works with **MicroZAccess Orchestrator & MicroZAccess TURN Mediator**



1. **Management Plane:** **Orchestrator** (Multi-tenant SaaS)

2. **Control Plane:** **TURN Mediator** (Shared or Customer Dedicated)

3. **Data Plane:** **App** (Components Options below)

i. Endpoint Agent (Windows / macOS /Linux) - User + Device Authenticated

ii. Server/ IoT Edge Agent (Windows / Linux) - Device Authenticated

iii. App Connector Mode (Linux) - Device Authenticated

iv. SD-WAN Agent - Device Authenticated

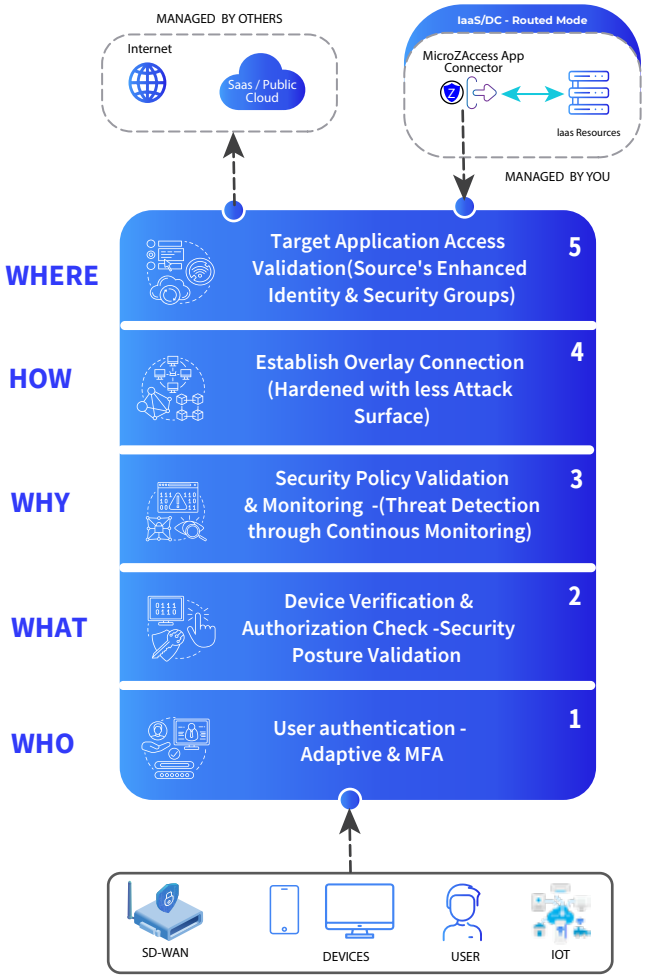
v. Container Side - Device Authenticated

The endpoints (Data plane components listed above) create **direct peer-to-peer tunnels** with others based on Zero trust tunnels based on Device trust and enhanced identities. No tunnels terminated in the middleboxes. Our architecture is primarily **Zero Trust Overlay Network** (ZTON) + **Software Defined Perimeter** (SDP). In our architecture, East-West traffic works well and without traffic traversing over MicroZAccess TURN Mediator (Relays).

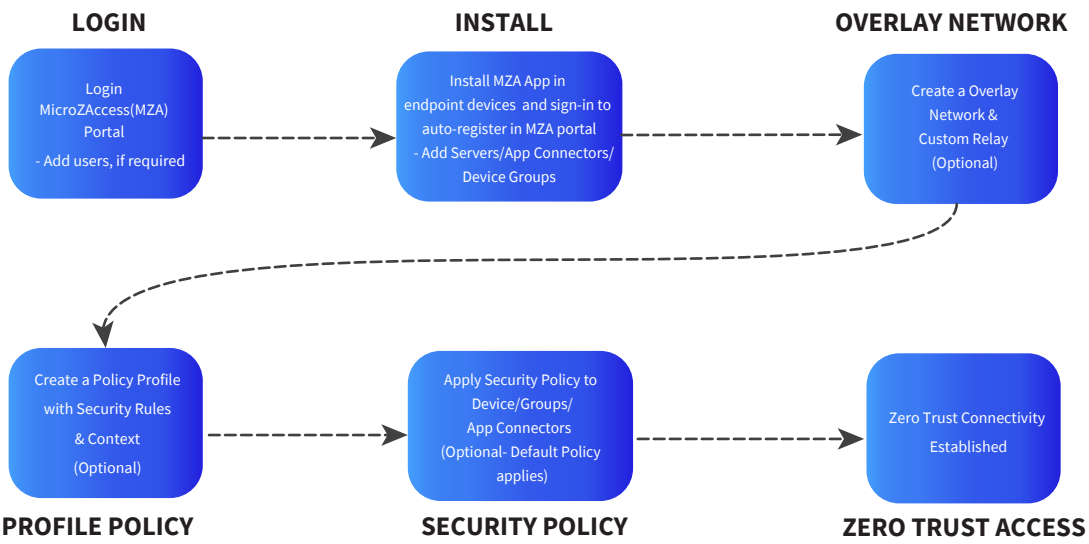
Working flow of MicroZAccess

1. **Authentication and Authorization**
    - **Authentication of Users:** with their existing SAML SSO or OpenID Connect via IDP or using Hosted Identity with COSGrid (**User/Client Mode**)
    - **Authentication of Servers and Gateways/Devices:** by MZA App using Extended Device Signature (**Server Mode**)
2. **Device Trust and Security Context**
    - In addition, MZA App can verify device trust and security posture as confiugured policy and updates **MicroZAccess Orchestrator to gain initial access.** For improved security, an extended security posture verification via third-party major EPP/EDR providers like Crowd strike, Microsoft Defender etc can be configured
3. **Secure Encrypted Micro-tunnel Establishment**
    - Upon successful verification and validation of user/device, the MZA agent can connect and forward traffic to the destination endpoints in two ways:
    - **Direct Peer to Peer Connectivity:** MZA App shares the destination device's IP address and port from the broker that has done UDP pin holing using the STUN method. Devices can establish direct peer-to-peer connectivity and exchange traffic
    - **For Dedicated Broker cum Relay:** For enhanced security, visibility, and control, the traffic can be set to flow through **MicroZAccess TURN Mediator** in situations where complicated NAT makes direct peer-to-peer connectivity difficult or when improved traffic control between devices is necessary.
4. **Policy Enforcement**
    - After the traffic reaches the destination endpoint through the micro tunnel, it undergoes enhanced identity checks of the packet source, including group memberships and allowed ports/apps, to enforce appropriate permission policies at each agent level

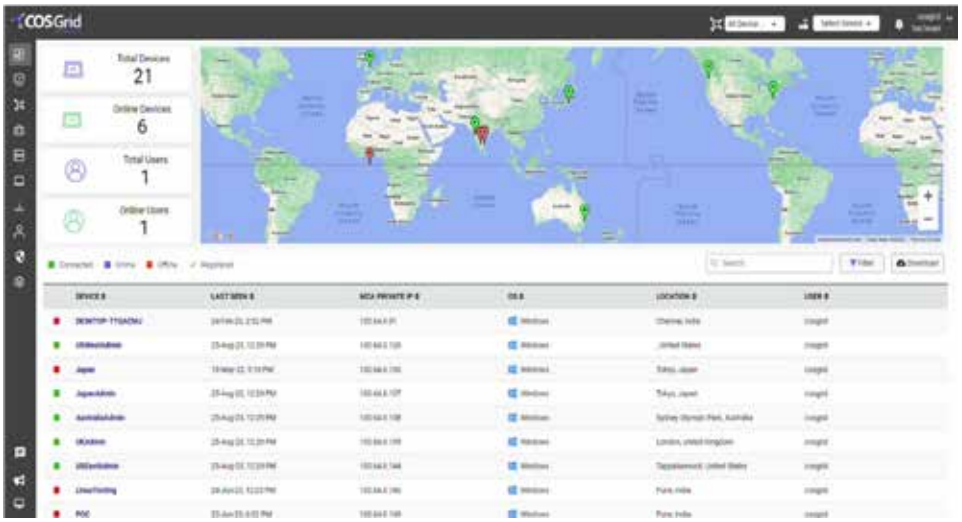
The above ensures a drastic reduction in the attack surface of systems up to 93%



Flow of events



MicroZAccess Dashboard Overview



MicroZAccess Client App Overview

Why COSGrid MicroZAccess ?

- Unparalleled Defense-in-Depth - 3X more Security
- Best in this Technology with upgraded ZTNA 2.0
- Faster connections & enhanced User Experience
- Scalable, Highly Available and Manageable with Customized Workflows & Automation
- Quick setup time and seamless Management .
- Reduces IT Costs

~80% ↓
Attack Surface Reduction
(Critical Application Access)

15 mins ↓
Set-Up time

70% ↓
Lower OPEX
(Management and Employee Support Costs)

Technical Specifications

Zero-Trust Security Capabilities	
Dedicated Certificate Authority (CA) and Enhanced Identity	Private CA per tenant and Enhanced Identities Certificates per device per connectivity profiles
End-to-End Least Privileges Connectivity	Host Agent enabled AES-256 encrypted Micro-tunnels using Noise Protocol Framework that's faster with smaller attack surface
Simple Cloud Workload Protection	Invisible applications only accessible after user and device have been authenticated and authorized
Device Trust	Device Identity and Device Posture Check(DPC) verification before a user or device can initiate access

Adaptive Authentication	
SSO Single Sign-On	SAML 2.0 integration IdP such as Okta, Azure AD, G Suite
Multi-Factor Authentication	MFA using SMS, E-mail, and Google Authenticator

Deployment	
Platforms support	Windows , Linux , MacOs
Deployment Options	MZA App: Host Agent mode or Gateway mode MZA TURN Mediator: Dedicated Hosted, Self Hosting in Public Cloud or DC

Secure Access Orchestration	
Software-defined Micro-segmentation	Finer segmentation of traffic based extended identity of users, devices, networks, groups and applications
ZTA (Zero Trust Access)	Host firewall per devices with a highly flexible Policy based
Flexible and Layered Protection Approach	Define and re-use Security Groups and Enhanced Group Membership across Multi-cloud and with a custom TURN Mediator

User Experience	
Data Privacy and improved User Experience	Traffic between Endpoints sent over Direct, encrypted Peer-to-Peer using NAT traversal / UDP port punching enabled by Central orchestrator

Monitoring, Management and API Integrations	
Centralized Management and Visibility	Single Pane-of-Glass Holistic visibility across. Activity audits & reports on logins, gateway deployments, device and app connections
API Integrations and all round Support	API available for integrations. Fully managed solution with 24*7 support

+91 90227 64534 cosgrid-networks @cosgridnetworks2141 @CosgridNetworks

Contact us for a free trial today!

Ph: +91 90227 64534, +91 86101 44212 | **E-mail:** info@cosgrid.com
Address HQ: COSGrid Systems Private Limited - Velachery, Chennai - 600042
Address 2: COSGrid Networks Inc - New Castle, US, 19808