

Secure Internet Access with
Smart web filtering



Client Overview

- Client Name:** iGSSL
- Industry:** Banking and Financial Services
- Size:** 300+ Employees
- Location:** India
- Use Case:** Secure Web Access Control

Client Background

iGSSL is a leading financial services institution with multiple branches across India. As digital banking expanded and remote work grew, the organization faced rising concerns around internet misuse, phishing attempts, and web compliance. They sought a lightweight, policy-based security solution that could be quickly deployed on user devices with centralized control and reporting.

Security challenges faced

- **Uncontrolled Web Access:** iGSSL lacked the tools to restrict or manage employee access to non-work and unsafe websites.
- **Exposure to Malicious Sites:** Users could inadvertently access harmful or non-compliant domains, increasing security risks.
- **Phishing and Web Threats:** The organization faced frequent phishing attempts and lacked proactive web threat protection.
- **Regulatory Compliance Gaps:** Enforcing consistent internet usage policies across branches and remote users was challenging.
- **No Real-Time Visibility:** IT teams had limited insight into user web activity, delaying threat detection and reporting.

The Solution: COSGrid's MicroZ Access

To address these challenges, iGSSL deployed Secure Gateway- a lightweight, policy-driven solution built for modern enterprise environments. It empowered the IT team to centrally define and enforce category-based and application-specific web access policies, monitor real-time user activity, and generate compliance-ready reports. With minimal resource impact on endpoints, the solution delivered strong protection against web threats.

Web Filter Key Features

- Policy-based Web Access Control
- Protection Against Malicious and Inappropriate Web Content
- Category-based URL Filtering
- Custom Allow/Block List Management
- Real-time Web Activity Monitoring and Reporting
- Seamless Integration with COSGrid MZA Client

Implementation Highlights



Phase-I rollout on 300 systems



Policy controls successfully tested



Seamless integration with existing tools



Centralized cloud-based management



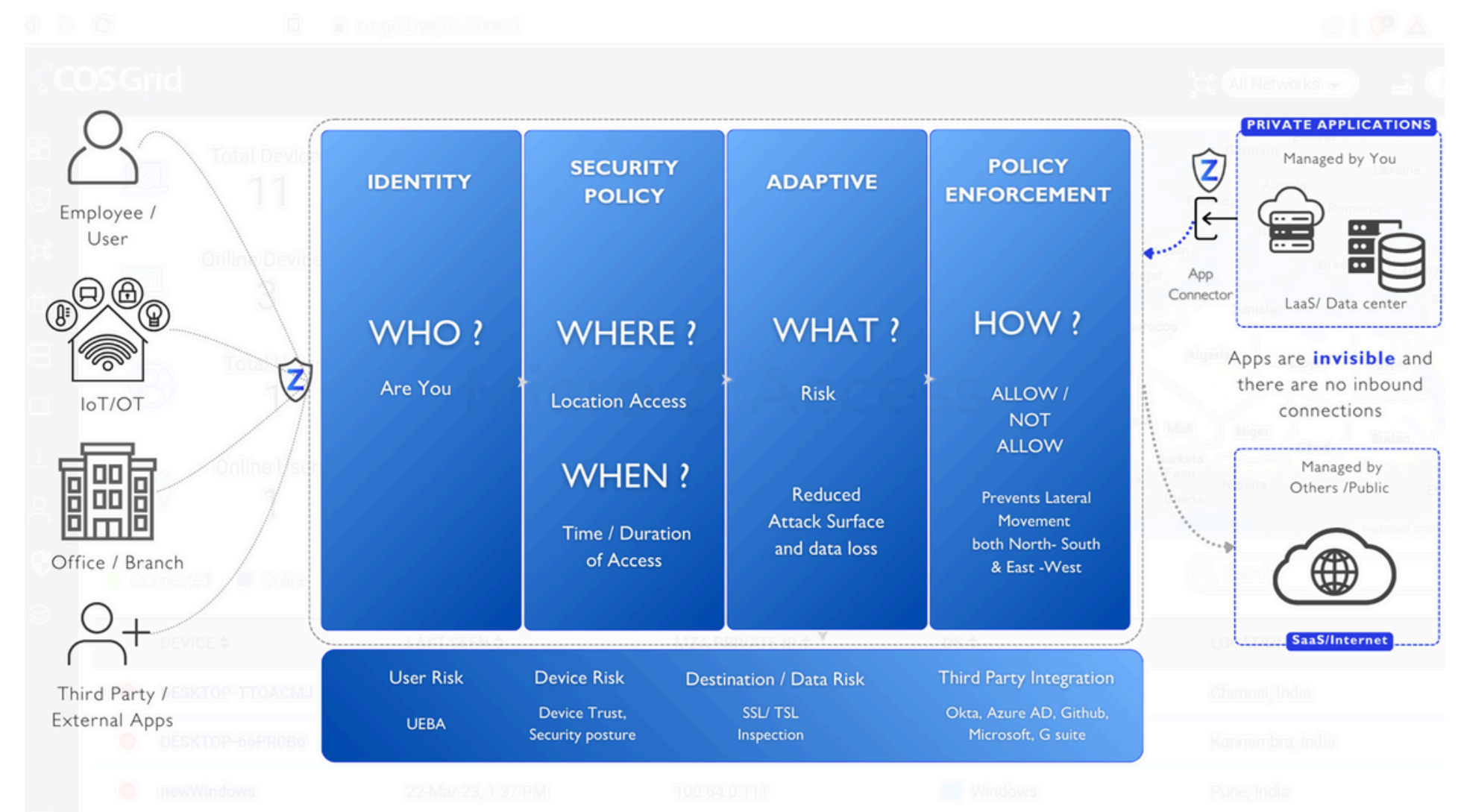
“COSGrid WebFilter gave us a reliable way to control employee internet usage while safeguarding our systems from online threats. The deployment was fast, well-supported by their team onsite, and it seamlessly integrated with our existing security infrastructure. It’s helped us stay secure and audit-compliant without adding complexity.”

IT Head, iGSSL

Application



Architecture



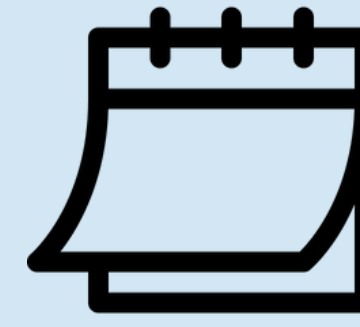
Deployment Snapshot



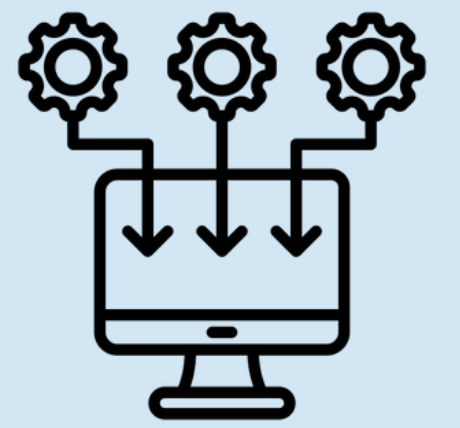
Deployment Time: 3 hours



Only 1 Engineer and 1 IT Admin Involved

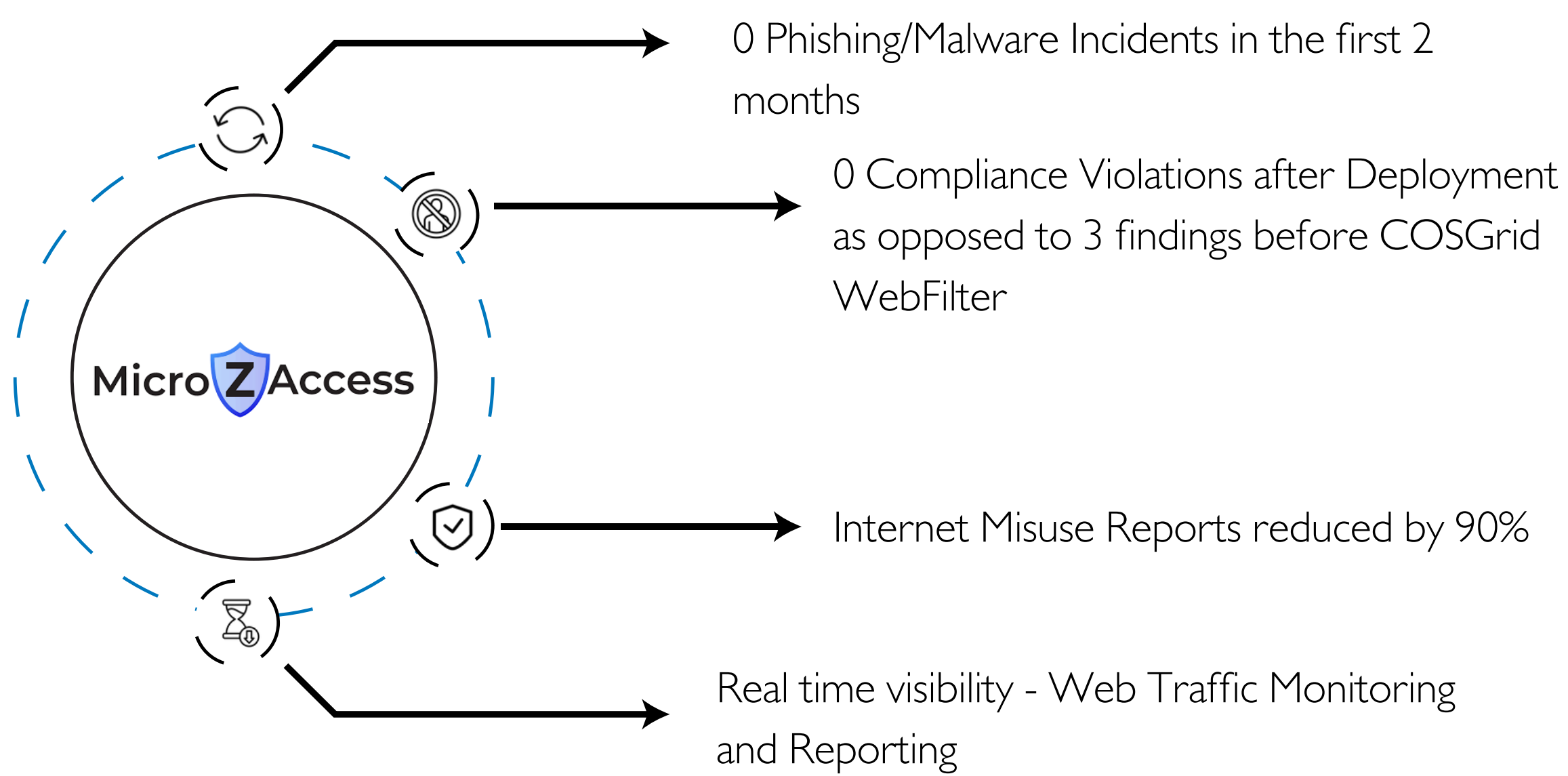


Go Live the same day

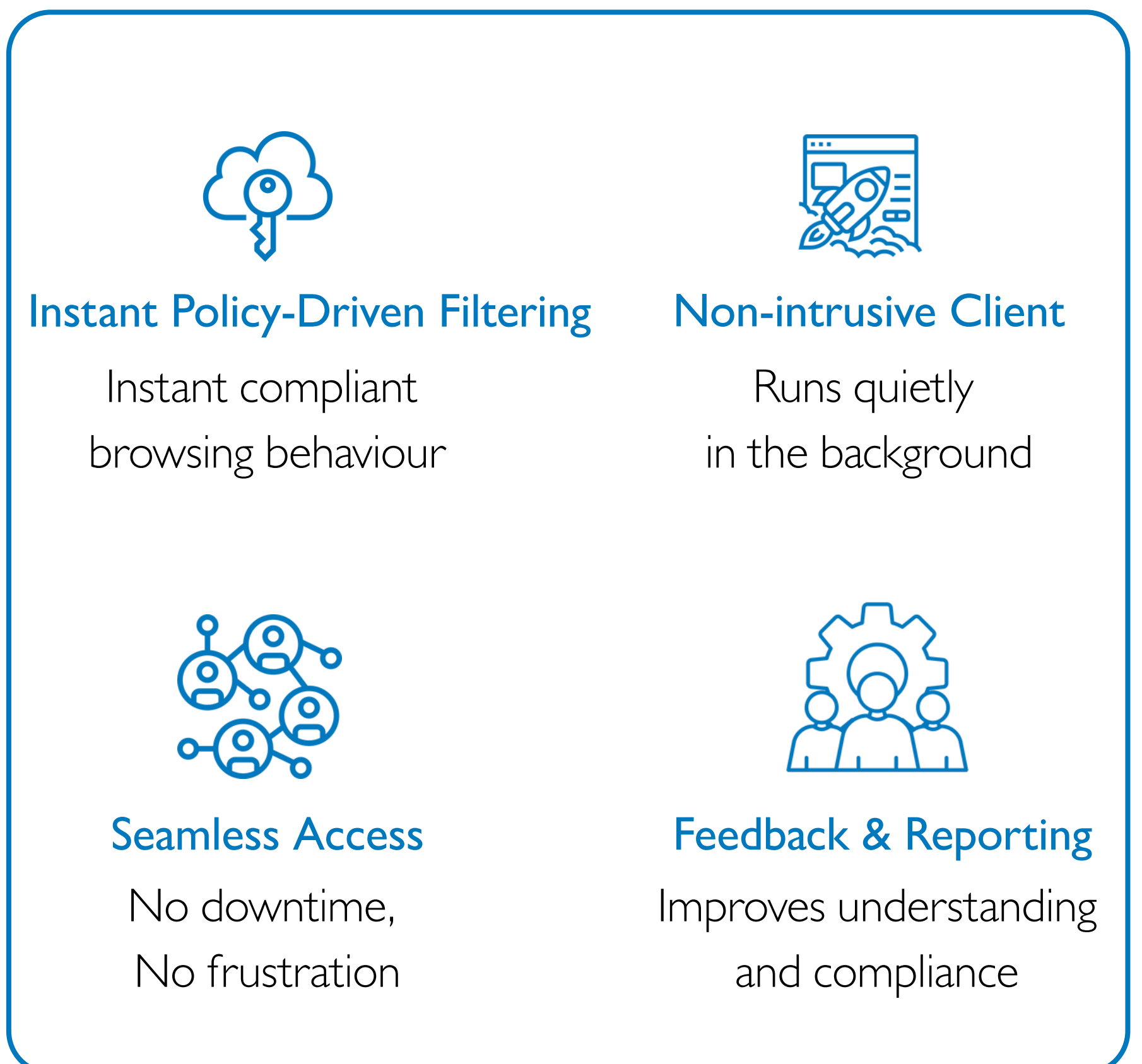


Centralized Cloud Console

Results Achieved



User Experience



ABOUT COSGRID

COSGrid Networks is a leading networking and cybersecurity products company that delivers secure access and protection to users data, applications, and workloads across clouds, remote sites and users anywhere. One of the few unified SASE companies globally that enables 'Cyber-resilience Simplified' for organizations with advanced threat detection, zero trust architecture, and patented adaptive SD-WAN-based steering to deliver seamless connectivity across WAN links, including 4G/5G.

Cyber Resiliency Simplified with Smart SASE NetSecOps

info@cosgrid.com www.cosgrid.com

