Coforge

Cyber Security

SecureAccess.360

June 2025

SecureAccess.360 – What it solves?

What is SecureAccess.360

SecureAccess.360 is a solution that provides seamless, secure access to the internet, SaaS & Private applications. It enhances productivity by inspecting traffic at scale, offering AI-powered threat protection, and performing full SSL inspection

IT OPS Challenges

- Managing multiple tools (SWG, CASB, VPN, Firewalls) are complex and expensive solutions.
- Traditional VPNs expose the entire network, increase breach risks, and slow performance
- Remote work has dissolved the boundaries and perimeter-based network segregation is no longer effective
- Increased Cloud adoption requires advanced strategies along with scalability to safeguard data and applications from cyber threats while handling increased data and user access

Use Cases

Threat Protection

- Get a holistic view of what's exposed to the internet, vulnerabilities, and TLS/SSL weaknesses
- Keep users, branches, and factories hidden behind the Zero Trust Exchange

Prevent compromise

- Block malicious sites with granular filtering
- Transform risky web content into a safe, dynamic stream of pixels

Remote Work Enablement

- Utilize AI-powered malware and zero-day protection
- Control user access to critical systems (SSH/RDP/VNC)

Eliminate lateral movement

- Enforce user-to-app and app-to-app segmentation
- Deploy decoys to detect and stop infected users from moving laterally

Zero Trust Networking

- Secure remote access to DC/cloud apps
- Extend secure private access to apps for third parties with superior agentless support for BYOD and unmanaged devices.

Cost Optimization

- Consolidates security tools (VPNs, firewalls, SWGs and CASBs)
- Reduce capex - No need for on-premise security appliances

Coforge – Our Managed Services

Services offerings

- SecureAccess.360
- SecureData.360
- SecureExperience.360

Value delivery stack

Technology Stack

SecureAccess.360	SecureData.360	SecureExperience.360
SWG	ZTNA	FWaaS	Data Protection
Threat Protection	User experience Monitoring	Application Monitoring

OUTCOME

- Minimal Business Disruption
- Real-time Unified visibility into exposure and risk
- Stronger cyber resilience
- Simplified & consistent security policies
- Simplified connectivity
- Improved user experience
- Reduced costs
- Reduced risk

ENABLERS

Native assessment tool	Configurator to choose right OEM	Policy auditing	Service SLA
Demo environment	Integrations-ITSM,SIEM,LAN	Policy convertor for smooth transition	QBR- Designated CSM
POC	Regular audit -policy optimisation	Golden templates for faster and precise provisioning	Fine tuned SOPs for faster response

Success Story: SecureEdge2Cloud Services for leading ISP

Client Background and Scope

- Implemented Zero Trust based solution for One of US leading broadband service provider

Volumetric and Geographical Coverage

- 7000 users across USA
- 800 applications

Challenges

- Customer was formed as a spin-off and needed urgent security protection
- Customer had multiple traditional point solutions which were managed in silos and created noise in daily operations
- Inconsistent monitoring for user experience and health checks
- Requirement for a robust solution for potential malicious data exfiltration risks and securing critical applications
- Need for a solution to extend secure access to apps for third parties

Coforge Solution

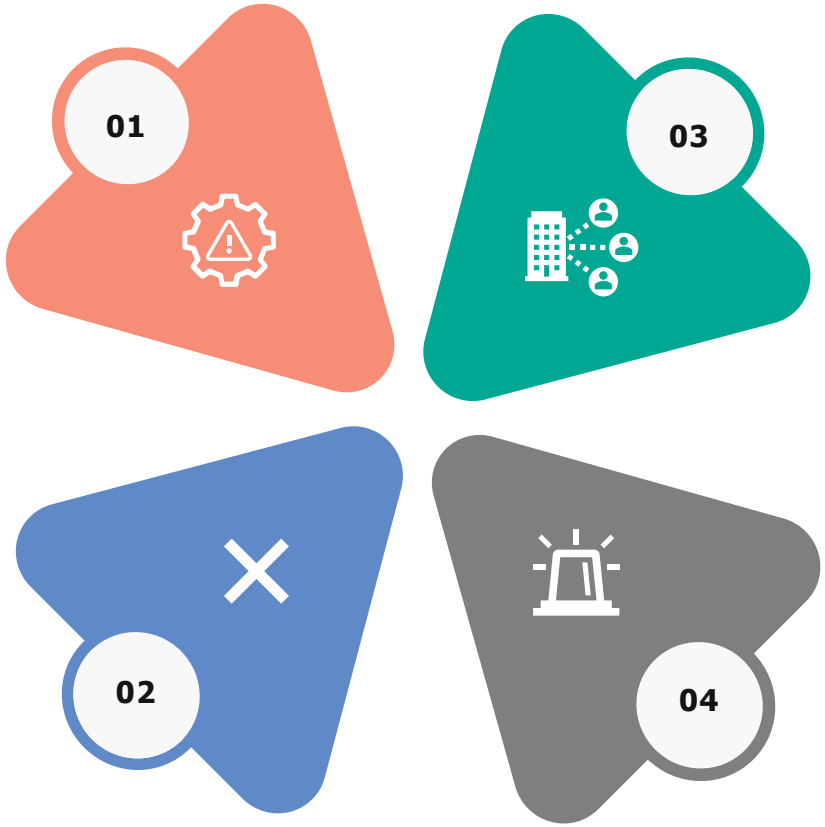
- Implemented **SecureEdge2Cloud solution** based on Zero Trust Network Access for all applications granting secured access control over cloud workloads.
- Provided a workplace security solution for **800 applications** and **7000 users** across multiple cloud environments
- Coforge solution enforced **browser isolation** and **blocked malicious sites**

Value Delivered

- Identified sophisticated threats hidden in encrypted traffic (Analysed encrypted traffic more than 100 TB while maintaining latency less than 10 milliseconds of proxy)
- Coforge solution provided real-time monitoring and improved user experience for client's 6 critical applications

Who needs this Solution

- **Legacy SWG/Proxy:** On-prem appliances or PAC files still in use
- **Limited SSL inspection:** Poor visibility into encrypted traffic
- **Shadow IT:** Unmonitored personal apps (e.g., Dropbox, WhatsApp Web)
- **SaaS-first:** M365, Google Workspace, Salesforce, Workday



- **VPN fatigue:** Performance issues, user friction, over-privileged access
- **Third-party access:** Challenges with M&A, contractors, temp users
- **BYOD access:** Need secure access without domain join
- **Remote access risk:** Implicit trust in network-based models

- **BYOD risk:** Uncontrolled access from personal devices/browsers
- **Sensitive data exposure:** IP/PII at risk without proper controls
- **No inline enforcement:** Reactive alerts, no real-time blocking

- **Helpdesk noise:** Frequent tickets on M365, Zoom, Teams slowness
- **No root cause visibility:** Hard to isolate user, ISP, or app issues
- **Distributed teams:** Users across varied geographies and networks
- **No real-time diagnostics:** Blind to full path from endpoint to app

Coforge

Thank You