CyberOne

Zscaler Internet Access (ZIA) as a Service

G-Cloud 15

Service Description

Service Description
Zscaler ZIA as a Service

Target Audience Profile

This service is designed for organisations that want enterprise-grade internet and SaaS security without building and running a specialist Zscaler operational function in-house. Typical triggers include:

- A shift to hybrid work and increased reliance on SaaS, with rising "shadow IT" risk and policy complexity.
- A requirement to improve protection against phishing, malware and modern web-borne threats, especially those hidden in encrypted traffic.
- Performance issues caused by legacy proxy stacks, VPN-led internet access, or backhaul architectures.
- The need for repeatable deployment governance (change control, segmentation, regional variation) and a clear path from pilot to scale.

What CyberOne delivers

1. Deploy with Confidence (Design & Build)

CyberOne designs and implements a ZIA foundation that is secure, scalable, operationally ready, configured "right first time" and aligned with the organisation's security and risk posture.

Core activities typically include:

- Discovery workshops to confirm goals, constraints, user segmentation and rollout approach.
- Architecture and traffic forwarding design, selecting the most appropriate patterns for your environment.
- Identity and authentication integration design (commonly SAML-based), enabling policy enforcement and consistent access control.
- Policy framework design across web, SaaS and data controls, ensuring policies are enforceable, supportable and aligned to real operational workflows.
- CyberOne also brings "implementation realism": the decisions that most often create friction later SSL certificate pinning exceptions, privacy exclusions, bypass rules and logging strategy are defined early and documented clearly.

2. Run With Confidence (24×7 Operations)

Once live, CyberOne operates ZIA as an extension of your team, providing monitoring, operational support and ongoing policy management to keep protection consistent and user experience stable as your business changes.

Operational coverage includes:

- Third-line engineering support for advanced troubleshooting (authentication, forwarding, policy enforcement, inspection behaviour).
- Change support for policy updates and onboarding new requirements (new departments, new apps, new risk controls).
- Visibility enablement through dashboards, reporting and audit-ready logging patterns (including SIEM integration points where required).

3. Grow With Confidence (Optimisation & Governance)

ZIA is most effective when it avoids policy sprawl, noisy alerts and performance regressions. CyberOne drives ongoing optimisation and governance to ensure ZIA keeps pace with the threat landscape and with how your teams actually work.

This includes:

- Quarterly strategic reviews covering adoption, access trends, security outcomes and prioritised improvement actions.
- KPI-style reporting that demonstrates security impact and operational efficiency (e.g. reduction in risky SaaS usage, improved policy compliance, reduced incident volume).
- Continuous refinement of URL filtering, file controls, app governance, SSL inspection policy and exceptions management based on evidence and feedback.

In-Scope Components (Typical)

CyberOne ZIA as a Service commonly includes the following service components (final scope depends on your ZIA subscription and desired operating model):

- Secure Web Gateway controls (web access policies, URL filtering and threat protection).
- Encrypted traffic inspection approach (SSL/TLS inspection policy, privacy exclusions and pinning exceptions).
- Threat protection tuning, including sandboxing and DNS security patterns where available.
- Application control and cloud access policies to manage sanctioned/unsanctioned SaaS usage and reduce shadow IT risk.
- Traffic forwarding design and rollout support (Client Connector and/or site-based forwarding).
- Logging, reporting and SIEM integration planning to deliver operational visibility and compliance reporting.

- Integration guidance with Microsoft security tooling (e.g. Entra ID, Intune posture signals, Defender XDR / Sentinel ingestion) where required.

2. Run With Confidence (24×7 Operations)

Once live, CyberOne operates ZIA as an extension of your team, providing monitoring, operational support and ongoing policy management to keep protection consistent and user experience stable as your business changes.

Operational coverage includes:

- Third-line engineering support for advanced troubleshooting (authentication, forwarding, policy enforcement, inspection behaviour).
- Change support for policy updates and onboarding new requirements (new departments, new apps, new risk controls).
- Visibility enablement through dashboards, reporting and audit-ready logging patterns (including SIEM integration points where required).

3. Grow With Confidence (Optimisation & Governance)

ZIA is most effective when it avoids policy sprawl, noisy alerts and performance regressions. CyberOne drives ongoing optimisation and governance to ensure ZIA keeps pace with the threat landscape and with how your teams actually work.

This includes:

- Quarterly strategic reviews covering adoption, access trends, security outcomes and prioritised improvement actions.
- KPI-style reporting that demonstrates security impact and operational efficiency (e.g. reduction in risky SaaS usage, improved policy compliance, reduced incident volume).
- Continuous refinement of URL filtering, file controls, app governance, SSL inspection policy and exceptions management based on evidence and feedback.

In-Scope Components (Typical)

CyberOne ZIA as a Service commonly includes the following service components (final scope depends on your ZIA subscription and desired operating model):

- Secure Web Gateway controls (web access policies, URL filtering and threat protection).
- Encrypted traffic inspection approach (SSL/TLS inspection policy, privacy exclusions and pinning exceptions).
- Threat protection tuning, including sandboxing and DNS security patterns where available.
- Application control and cloud access policies to manage sanctioned/unsanctioned SaaS usage and reduce shadow IT risk.

- Traffic forwarding design and rollout support (Client Connector and/or site-based forwarding).
- Logging, reporting and SIEM integration planning to deliver operational visibility and compliance reporting.
- Integration guidance with Microsoft security tooling (e.g. Entra ID, Intune posture signals, Defender XDR / Sentinel ingestion) where required.

Deliverables

Deliverables are designed to be usable by both security leadership and engineering teams and to support a controlled rollout from pilot to scale:

- ZIA design documentation: architecture decisions, forwarding model, identity integration approach, core policy framework and governance considerations.
- Policy and control artefacts: URL filtering design, file-type controls, app control/CASB-style governance approach, bandwidth/QoS policy intent, SSL inspection rules, and exception/bypass documentation.
- Rollout plan and playbook: pilot structuring, sequencing, communications guidance, escalation paths and rollback considerations (usable as a repeatable framework for broader rollout).
- Reporting pack: dashboards and summaries aligned to visibility, security outcomes and optimisation opportunities, including a quarterly review format.

Prerequisites & Access Requirements

To deliver efficiently, CyberOne typically requires:

- ZIA administrative access appropriate for design, configuration and operational management.
- Identity provider inputs for authentication/SSO and group mapping (commonly SAML), plus confirmation of user segmentation.
- Agreement on SSL inspection posture (what to inspect, what to exclude, privacy/compliance constraints) and certificate deployment approach.
- Technical inputs for forwarding methods (networks, egress patterns, device estate characteristics) and any required change windows.
- Logging and visibility requirements (retention expectations, SIEM integration goals, reporting audiences).

Assumption (explicit): Zscaler Internet Access (ZIA) licensing may be customer-provided or supplied through CyberOne. Where CyberOne provides licensing, Managed Licensing services, including licence administration and optimisation, can be included in scope.

Out of Scope (To Prevent Scope Drift)

Unless explicitly agreed as an extension, the following are out of scope:

- End-user device build/refresh, general endpoint management, or MDM implementation (beyond what is required for ZIA rollout).
- WAN redesign, LAN switching changes, or broad network transformation activities not directly required for ZIA, full enterprise-wide rollout programme management (where the engagement is scoped for pilot/initial deployment).
- Non-ZIA platforms and unrelated security tooling rationalisation (except where needed to integrate logging/visibility).
- Pricing, contractual terms, or specific SLA commitments (these are agreed separately).

Outcomes & Benefits

By adopting CyberOne ZIA as a Service, organisations typically achieve:

- Reduced web risk through consistent, identity-driven policy enforcement and stronger inspection of threats, including encrypted traffic where appropriate.
- Improved visibility and governance over internet and SaaS activity, helping control shadow IT and strengthen compliance reporting.
- Better user experience through direct-to-cloud access patterns that reduce latency and avoid legacy backhaul bottlenecks.
- Operational efficiency by consolidating web security controls into a single cloud-native platform, backed by a partner-led operating model.
- A repeatable deployment and optimisation framework that supports growth and continual improvement over time.

Why CyberOne

- **Cyber Security Since 2005** - 20 years of demonstrable cyber experience across regulated industries, aligned to organisational, operational and regulatory needs.
- **Microsoft Security Leadership** - Top 100 Global Microsoft Security Partner, MISA member, trusted by Microsoft to deliver advanced protection, productivity and ROI.
- **Global SOC. Microsoft Verified Managed XDR** - CREST-accredited 24x7 Global Security Operations Centre delivering measurable detection, response and resilience with defined SLAs and outcomes.
- **Escalate Fast With NCSC-Accredited Response** - NCSC Cyber Incident Response available by retainer or call-off SoW, delivered by the same team that monitors you for faster coordination and simpler management.
- **Audit-Ready Compliance** - Timelines, approvals and evidence captured automatically with control mappings that integrate directly into audits and board packs.
- **Complete Visibility. Total Control -** Your data remains sovereign within your Microsoft tenant, with no third-party data storage. We access only your Microsoft log ingestion, giving you full control.

- **One Portal. Total Clarity. Performance-Led** - Live incidents, prioritised insights and board-ready reporting in Jerico - with measurable outcomes. No chasing. No guesswork.
- **Immediate Value. Long-Term Protection** - DevOps-driven onboarding applies baselines, detections, controls and playbooks fast. SOC maturity in 7 days or less for immediate protection.
- **Maximise Microsoft Investments** - Get ROI from your Microsoft licences, we raise utilisation today and rapidly adopt new capabilities to widen coverage and reduce effort.
- **Focus on Growth. Unlock Innovation** - Remove the operational security burden, enabling you to focus on innovation, transformation and measurable business impact.

ZIA as a Service

Secure, Fast Access To The Internet & SaaS.
Reduce Risk. Simplify Operations.

Powered by Zscaler Internet Access (ZIA). Realised by CyberOne.

CyberOne delivers a Managed Secure Service Edge Service that inspects all outbound traffic, including encrypted, to block threats and prevent data loss while keeping the user experience high.

We design, deploy and operate ZIA, integrate with your identity, device and SIEM stack, then report outcomes the board cares about. Part of CyberOne's Managed Services suite that scale with your needs.

What is Zscaler Internet Access?

Zscaler Internet Access (ZIA) is a cloud service that secures internet access and software-as-a-service (SaaS) applications. It applies Zero Trust checks to every connection, at the nearest Zscaler location, so security stays close to users and does not slow them down.

One platform covers Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), sandboxing, Domain Name System (DNS) security and cloud firewall.

Zscaler Internet Access is your secure on-ramp to the internet. Office traffic takes the most direct route to the cloud. People working remotely use a lightweight app or simple browser settings. Security checks are performed at the nearest Zscaler location to ensure speed.

Key Features of CyberOne's ZIA as a Service

Move from stacked point products to a managed, cloud-first control plane. CyberOne designs, deploys and runs ZIA in your environment, integrating with your chosen identity provider, endpoint management and SIEM.

Deploy With Confidence

- Readiness, architecture and traffic-forwarding design for groups and users.
- Best-practice policies across SWG, CASB, DLP, sandbox and cloud firewall.
- Phased rollout model with pilot groups, change control and communications.

Run With Confidence

- 24x7 monitoring, incident response and SLA-aligned support from our Global SOC.
- Continuous tuning of SSL inspection, URL controls and data policies.
- Real-time visibility and dashboards for threats, usage and data movement.

Grow With Confidence

- Monthly and quarterly service reviews with KPIs and actions assigned.
- Rapid onboarding of new sites, users and SaaS apps without new hardware.
- Optional digital experience monitoring to cut Mean Time to Respond and ticket volume.

Unlock Business Value: Outcomes You Can Expect From CyberOne

- **Prevent Cyberthreats & Data Loss:** AI-powered inline inspection, including encrypted traffic.
- **Better User Experience:** Direct-to-internet via the nearest service edge for faster, safer access.
- **Reduce Cost & Complexity:** Retire appliances and consolidate controls in the cloud to cut cost and complexity.
- **Unified Visibility & Control:** One policy for web, SaaS and data protection across users and locations.
- **Faster Time To Value:** SaaS delivery with capabilities added without new hardware, deployed in hours
- **Strengthen Compliance:** Detailed logs and reporting to support audits and regulators with clear, exportable evidence.

Why Choose CyberOne's ZIA as a Service?

Guaranteed Outcomes
SLAs focused on threat prevention, experience and policy coverage.

Zscaler Expertise You Can Trust
A certified Zscaler Delivery Partner, we have delivered successful deployments for some of the world's most admired brands and organisations.

Modernise Without Disruption:
Structured migration from legacy proxies and web gateways.

Ongoing Monitoring & Reporting
Board-ready insights, KPIs and continuous improvement cadence.

Microsoft Experts
Microsoft Intelligence Security Association Members with Verified Managed XDR solutions, ensuring we maximise existing Microsoft investments.

Quick Start: From Pilot To Scale

1 Plan:
Confirm traffic-forwarding, target sites and user groups, identity provider (e.g. Microsoft Entra ID), device posture (e.g. Intune) and SIEM (e.g. Sentinel) and set KPIs.

2 Build Foundations:
Set up Zscaler, route office and remote traffic to it, enable SSO and device compliance checks, send logs to your security platform and prepare security operations centre runbooks.

3 Pilot:
Enable a small cohort and a few sites, validate policies and SSL decryption, monitor with dashboards while CyberOne SOC reviews alerts and user impact.

4 Migrate
Move locations and users in waves, replace proxy stacks and web gateways, tighten DLP and CASB controls, update service desk workflows

5 Run
24x7 Monitoring and Response, monthly reviews, KPI reporting in your SIEM, continuous optimisation and onboarding for new apps and locations.

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.

CyberOne

hello@cyberone.security

+44 (0) 3452 757575

cyberone.security