
Edgio
APPLICATIONS
BUNDLE SERVICE
DESCRIPTIONS

Features	Free	Professional	Enterprise	Premier
Platform Features		Platform Features		
Website Delivery & DDoS Protection Traffic	✓	✓	✓	✓
Developer Services - API, CLI, & EdgeJS	✓	✓	✓	✓
Role-based Access Control (RBAC)	✓	✓	✓	✓
Authoritative DNS	✓	✓	✓	✓
PCI DSS Level 1 Platform	✗	✓	✓	✓
100% Platform Uptime SLA	✗	✓	✓	✓
Single Sign-On (SSO) Support	✗	✗	✓	✓
Custom Contract Terms	✗	✗	✓	✓
Dedicated IP Support	✗	✗	✗	✓
Origin Shield (Regions)	✗	1	2	4
Dev Environments Per Configuration	1	3	10	100
TLS Certificates	Let's Encrypt	Let's Encrypt	DV/OV/EV Wildcard-SAN	DV/OV/EV Wildcard-SAN
Security Features		Feature to protect your website & application		
Layer 3, 4 & 7 DDoS Protection	✓	✓	✓	✓
Advanced Access Control List (ACL)	✓	✓	✓	✓
Managed Security Ruleset	✓	✓	✓	✓
Dual WAAP Mode	✗	✓	✓	✓
Security Audit Control	✗	✓	✓	✓
Custom Virtual Patching	✗	✗	✓	✓
High Capacity IP ACL	✗	✗	Up to 10,000	Up to 50,000
API Security	✗	✗	✓	✓
Client-Side Protection	✗	✗	✓	✓
TLS Fingerprinting	✗	✗	✗	✓
Mutual TLS (mTLS)	✗	✗	✗	✓
Custom Mitigation - Custom Challenge, Advanced Challenge CAPTCHA, Silent Drop	✗	✗	✗	✓
Rate Limiting	Standard	Standard	Standard	Advanced
Bot Manager	Standard	Standard	Advanced	Advanced

Features	Free	Professional	Enterprise	Premier
Attack Surface Management (ASM)	✗	✗	✗	100 Assets Under Management (AUM)
Performance Features	Features to drive performance of your properties			
Application Rules	✓	✓	✓	✓
CDN-as-code	✓	✓	✓	✓
Image Optimization	✓	✓	✓	✓
Instant Global Purge	✓	✓	✓	✓
Predictive Prefetching	✓	✓	✓	✓
Advanced Compression	✗	✗	✓	✓
Purge By Tag	✗	✗	✓	✓
WebSocket Protocol	✗	✗	✗	✓
Traffic & Feature Management	Features to test and experiment with variations of your website			
Canary Deployment	✓	✓	✓	✓
Feature Flags	✓	✓	✓	✓
A/B & Multivariate testing	✓	✓	✓	✓
Iterative Migration	✓	✓	✓	✓
DNS Load Balancing	✗	✗	✓	✓
# of Experiments	1	10	20	Unlimited
Edge Compute and Development Platform	Features to build or augment your websites, apps and APIs on the Edge and the Cloud			
Support for modern frontend frameworks	✓	✓	✓	✓
Edge Functions (# of invocations)	5 million	50 million	100 million	200 million
Cloud Functions (GB-Hours)	100	1,000	2,000	3,000
Branch Preview (# of deployments)	100	1,000	2,000	3,000
Observability Features	Observability Features			
Full Stack Debugging Tool	✓	✓	✓	✓
Real Time Log Streaming	✗	✓	✓	✓
Security Analytics API	✗	✗	✗	✓
Security Analytics Dashboard	7 Days	30 Days	60 Days	60 Days

Features	Free	Professional	Enterprise	Premier
Real Time Traffic Dashboard (Edge Insights)	✗	7 Days	30 Days	30 days
Real User Monitoring (RUM)	✓	✓	✓	✓
Managed Security Services (SOC) Features		Managed Security Services (SOC) Features		
Threat Intelligence	✗	✓	✓	✓
Managed WAF	✗	✓	✓	✓
24/7 Monitoring & Response	✗	✓	✓	✓
Custom Run Books	✗	✓	✓	✓
Incident Support	✗	✓	✓	✓
Assigned Security Architect • Advanced Reporting • Monthly Security Posture Review • Dedicated Threat Hunting • Custom Reporting • Rule & Policy Assessment • Dedicated Virtual Patch Support	✗	Add-on	Add-on	✓
General Support Features		General Support Features		
Client Support Email & Phone	Documentation	Email & Phone	Email & Phone	Email & Phone
Online Status Updates (status.edg.io)	✓	✓	✓	✓
Help Center/Self-Service Tool	✓	✓	✓	✓
Welcome Kit	✗	✓	✓	✓
Customer Portal/Ticketing Dashboard	✗	✓	✓	✓
Official Incident Report (OIR)	✗	✓	✓	✓
Root Cause Analysis (RCA)	✗	✓	✓	✓
Emergency Escalations	✗	✗	✓	✓
Custom Monitoring & Alerting	✗	✗	✓	✓
Crisis Bridge Support	✗	✗	✗	✓
Event Monitoring & Support	✗	✗	✗	✓
Initial incident response SLA	✗	≤ 30 minutes	≤ 15 minutes	≤ 10 minutes

Platform Features Descriptions

Website Delivery & DDoS Protection Traffic

Support unmetered delivery of all in-scope application traffic as well as unmetered DDoS protection of all application traffic through Edgio Application Platform.

Developer Services - API, CLI, EdgeJS & Terraform

Support managing application configuration using RESTful API, Command Line Interface (CLI), and Configuration as Code (Edge JS). Integrates management of services with a variety of developers and operation workflows.

Role-based Access Control (RBAC)

Support restricting system access based on predefined roles and permissions. Users are assigned roles, and each role has specific access rights to resources, ensuring they can only perform authorized actions.

Authoritative DNS

The authoritative DNS is the source of truth for a domain's DNS records and is the final holder of the domain's IP address and other DNS records like A, MX and CNAME records. The authoritative DNS is responsible for answering DNS queries with the most accurate data.

PCI DSS Level 1 Platform

Support access to Edgio's PCI DSS Level 1 compliant network footprints.

Platform Uptime SLA

To include a Platform Uptime Service Level Agreement (SLA) availability and operational continuity for the platform. More info about Platform Uptime SLA can be found in the Service Supplement in the service order form.

Single Sign-On (SSO) Support

Supports setting up SSO with identity provider using SAML to allow login using the credentials stored in customer's organization's SAML Identity Provider (IDP)

Dedicated IP Support

Support deploying TLS certificates and serving customer content from dedicated IP groups for customer applications. Note: While the IP groups are dedicated to a specific customer's content, the IP addresses are not intended to be static and are subject to change without notice.

Origin Shield (Regions)

Origin Shield establishes an additional layer of proxy servers in a tiered-distribution architecture to increase cache hit ratio and reduce the number of connections from proxy server to origin.

Dev Environments Per Configuration

Each property can have multiple environments which contain app configurations i.e. caching rules.

TLS Certificates

X.509 certificates that facilitate delivering content via Transport Layer Security (Protocol). It uses public key cryptography to encrypt communications between clients and servers.

Security Feature Descriptions

Layer 3, 4 & 7 DDoS Protection

Protection from Layer 3, 4 and 7 (network, transport and application/HTTP) distributed denial of service attacks.

Advanced Access Control List (ACL)

Ability to create access rules that identify valid or malicious requests via allowlists, accesslists, and blocklists.

Managed Security Ruleset

Protection from web application and API threats with rulesets automatically maintained and updated by Edgio's security team.

Dual WAAP Mode

Offer the ability to analyze rule changes against production traffic without disabling production WAAP rules or affecting legitimate users. Dual WAAP enables faster, more accurate deployment of custom security rules.

Security Audit Control

Ability to log policy configuration changes and save version histories for policies across applications and domains.

Custom Virtual Patching

The ability to create custom rules matching on request metadata attributes including URL, request headers/body, cookies and more. This feature allows customers to quickly address any threat, including zero-days.

High Capacity IP ACL

Manage up to 50,000 IP addresses or IP blocks per access rule for access lists, allowlists, and blocklists (standard is up to 1,000 per access rule).

API Security

API Security provides protection for APIs, using machine learning (ML) to detect APIs while allowing you to manage multiple JSON schemas. API Security also allows you to enforce a positive security model, blocking all requests that do not adhere to the schema, and provides safeguards against sensitive data & code leaks, plus L7 (HTTP/S) DDoS attacks. The capability also supports JWT authentication on Edgio’s edge.

Client-Side Protection

The Client-Side Protection provides the ability to detect and prevent malicious scripts executed on an end user’s web browser, via using Content Security Policy. It protects against end-user data exfiltration i.e. Magecart credit card skimming attacks and allow customer to enforce a set of directives on resource loading.

TLS Fingerprinting

Additional client identification and tracking using information from the TLS protocol, to more accurately determine whether a request is legitimate or fraudulent.

Mutual TLS (mTLS)

mTLS establishes secure communication between clients and servers via bidirectional authentication and encryption protocols. Both clients and servers authenticate each other's requests by presenting TLS certificates, ensuring mutual trust and preventing unauthorized access. This two-way authentication mechanism protects the confidentiality and integrity of data transmitted over the network.

Custom Mitigation - Custom challenge, Advanced Challenge, CAPTCHA, Silent Drop, Progressive Browser Challenge

Flexible mitigation options for protection against automated threats with response options including CAPCHAs, silent drops, the ability to serve a Base64-encoded HTML page while Edgio evaluates whether a client request is legitimate, or the ability to customize the difficulty level of the browser challenge Edgio serves to the client

Rate Limiting

A rate rule restricts the traffic on Edgio's edge before forwarding to the origins, with the intention of diverting malicious DDoS traffic or preventing a customer origin server from being overloaded. Requests that exceed the rate limit may be dropped, redirected to another URL, or sent a custom response. The type of enforcement action that will take place is determined by the Security Application configuration that leverages it. Standard Rate Limiting allows the resources of Any, a unique combination of IP address and user agent while Advanced Rate Limiting allows additional sources including User Agent, ASN, Status Code, JA3, Cookie, ARGS and Header to be applied on the requests.

Bot Manager

Secure your web forms and APIs against programmatic attacks. With Bot Manager Standard, Edgio's high performance bot rules use browser validation to detect malicious automated traffic and prevent it from reaching your web application. Advanced Bot Management applies machine learning (ML) on top of signature and behavioral fingerprints to detect and mitigate malicious bots while allowing known "good" bots to do their job.

Attack Surface Management (ASM)

Attack Surface Management approaches threat detection and vulnerability management from the attacker's perspective. It provides continuous discovery, inventory, assessment, monitoring, risk prioritization score and mitigation of cybersecurity threat and potential attack vectors on Customer's web-based assets.

Managed Security Services (SOC) Feature Descriptions

Threat Intelligence

Edgio's Threat Intelligence team continuously monitors evolving security trends and attack techniques to tailor intelligence-driven rules and signature updates for our customers. Through analysis of traffic on Edgio's platform, combined with scanning of sources including forums, code repositories, and social media, Edgio identifies emerging threats and applies this intelligence within our managed ruleset across all customers, as well as specifically tailored rules for specific customers with unique needs.

Managed WAF

Edgio's Managed Web Application Firewall (WAF) service delivers 24/7/365 comprehensive monitoring and proactive management, tailored to your technology stack for optimal performance and security. Crucially, the ERS (Edgio Ruleset), central to our offering, is a dynamic framework ensuring cutting-edge protection against new threats while minimizing false positives for consistent site availability. Our team of experts adjusts the protection provided by ERS leveraging advanced AI enabled Threat Intelligence to develop and refine policies, signatures, and rules against risks like injection attacks, cross-site scripting, broken authentication and more as outlined in the OWASP Top 10. This comprehensive approach to ERS management ensures your web assets are robustly protected. Edgio also provides an assigned security architect (an addon service) to help develop a highly personalized security posture.

24/7 Monitoring & Response

Edgio’s 24/7 Monitoring and Response service provides continuous protection through our Security Operations Center (SOC), staffed by Security Analysts around the clock who are constantly analyzing events and anomalous activity identified across the Edgio platform. The SOC uses both manual and automated techniques to detect anomalous behavior, and leverage information provided by Edgio's Threat Intelligence service. When the SOC identifies a potential threat or incident, the team initiates a response based on predefined playbooks coupled with your custom preferences. The SOC can contain attacks through the Edgio platform by way of request rewrites and redirects, access control lists, rate limiting, bot management techniques, and more. The SOC will provide ongoing status and recommendations in response to detected attacks and the subsequent implementation of mitigation efforts to attacks.

Custom Run Books

The Security Operations Center (SOC) follows a set of custom run books that define the operating procedures for responding to a customer's threats. Run books are crafted to align seamlessly to each customer’s security needs. The runbook defines rules of engagement specifying customer points of contact, Edgio points of contact, threat severity identification, escalation procedures, and more. Defined run books allow the SOC to respond both efficiently and consistently, facilitating swift resolution during any engagement.

Incident Support

The Security Operations Center (SOC) is available 24/7/365 to respond to any customer inquiries or issues, regardless of how the incidents are created. Edgio’s commitment to customer success ensures inquiries are addressed promptly while maintaining the integrity of your security posture. Based on custom runbooks the SOC can suggest rule changes or process the changes with approval based on the request.

Assigned Security Architect

Premier level customers receive the added benefit of an assigned security architect to collaborate with in enhancing their web application / API security posture. The assigned Security Architect is a seasoned expert acting as an extension of the customer's IT team, committed to working hand in hand with stakeholders to fortify their web applications against potential threats. This partnership is designed to provide personalized insights, strategic guidance, and proactive measures tailored to specific security needs. This service is also available as an add-on service to customers that purchase the Professional or Enterprise bundle.

Advanced Reporting

Premier level customers can gain meaningful insights into their security posture with Advanced Reporting, which provides both an overview of the customer's overall level of security, as well as specific recommendations for addressing any deficiencies. Customers can choose to receive scheduled reports weekly or monthly for a consistent and comprehensive overview of their security posture. Customers can also request one-time ad-hoc reports for DDoS events, which will give them a comprehensive understanding of these critical occurrences and enable them to make informed decisions about how to optimize their security posture. This service is available with the Assigned Security Architect add-on service to customers that purchase the Professional or Enterprise bundle.

Monthly Security Posture Review

Edgio provides comprehensive services to constantly enhance a robust security posture, including a scheduled monthly review and strategy session led by an Assigned Security Architect. This session serves as a point-in-time analysis to assess the current state of affairs and strategic planning for the upcoming month based on expected events, projects, and specific customer needs. The monthly review can include: (1) an examination of potential security gaps based on the customer's current security configuration, including recommendations to address unprotected assets and strategies to prevent direct to origin attacks, 2) a holistic analysis of current security controls in place to ensure adequate Layer 7 DDoS protections are in place 3) a comprehensive review of active WAAP rulesets to ensure they are current and fine-tuned to optimal thresholds, minimizing false-positives while maximizing protection from threats, (4) an evaluation of audit policies with recommendations to enhance security posture, and (5) a report on attacks mitigated in the past 30 days, aiding customers in understanding and mitigating the threats they face. This service is available with the Assigned Security Architect add-on service to customers that purchase the Professional or Enterprise bundle.

Dedicated Threat Hunting

With Dedicated Threat Hunting, Premier customers will get ahead of the curve for protection from zero-day vulnerabilities through rapid deployment of mitigating rules, before those updates are available for GA. The Assigned Security Architect will: (1) Determine if the disclosed vulnerabilities are relevant to the customer's web properties. (2) Use the suite of WAF tools to mitigate vulnerabilities (custom rules, access rules, rate rules, and bot detection). (3) Identify encoding obfuscation attacks that are specific to the customer's properties and suggest custom rules to mitigate such attacks. This service is available with the Assigned Security Architect add-on service to customers that purchase the Professional or Enterprise bundle.

Custom Reporting

Custom Reporting refers to the ability to define the WAAP activity reports that cannot be generated with UI features or cannot be covered by readily available Advanced Reports. Custom reporting can include report that cover multiple properties (all, or specific subset of properties), specific WAAP actions (e.g. Alerts and 403 Block), most abusing clients (by IP, ASN, UA, JA3 hash, bot type, etc.), top attack methods, top targeted URLs, and more. Custom reports will be generated by the security architect assigned to the customer on a monthly basis and delivered via email with the option to meet with the customer to discuss the report in detail. This service is available with the Assigned Security Architect add-on service to customers that purchase the Professional or Enterprise bundle.

Rule & Policy Assessment

Edgio's Rule and Policy Assessment is an ad-hoc review conducted outside the regular monthly security posture review, initiated either at a customer's request or when our Security Operations Center (SOC) identifies anomalies. This service is particularly beneficial ahead of significant events or when abnormal behavior is detected in your Web Application Firewall (WAF) configurations. During the assessment, Edgio experts meticulously review WAF configurations, policies, and audit records to spot coverage gaps, outdated rules, and opportunities for performance tuning, ensuring alignment with best practices like the OWASP Core Rule Set. The team provides actionable recommendations, including rule revisions, updated allow/deny lists, and new policy sets, all aimed at ensuring consistent and enhanced security. This service is available with the Assigned Security Architect add-on service to customers that purchase the Professional or Enterprise bundle.

Dedicated Virtual Patch Support

Dedicated Virtual Patch Support includes custom written WAF signatures to protect application specific vulnerabilities not covered by current Edgio rulesets. This would apply for any zero-day protection outside of publicly disclosed CVEs. These are on-demand in nature and require iterative testing to ensure no false positives are included. This service is available with the Assigned Security Architect add-on service to customers that purchase the Professional or Enterprise bundle.

General Support Feature Descriptions

Client Support Email & Phone

Access to support via email tickets@edg.io or (877)334-3236.

Online Status Updates

Access to online network and platform service status updates at status.edg.io.

L3/L4 DDoS Protection

Protection against L3/L4 (network and transport layers of OSI model) distributed denial of service (DDoS) attacks.

Welcome Kit

Access to a welcome kit delivered by email, with information on support contact information, response times, and more.

Help Center/Self-Service Tool

Access to an online, self-service Help Center to find user guides, release notes, diagnostic tools, customer notification, setup and troubleshooting information, and more.

Customer Portal/Ticketing Dashboard

Access to an online ticketing portal for support requests.

Official Incident Report (OIR)

An Official Incident Report (OIR) will be delivered within 24 hours of the resolution of a service degrading incident.

Root Cause Analysis (RCA)

A Root Cause Analysis (RCA) will be delivered within 5 business days of a major service disruption.

Emergency Escalations

Access to the Support Management Team for critical events at escalations@edg.io.

Custom Monitoring & Alerting

Access to custom monitoring and alerting based on unique customer application and service thresholds.

Crisis Bridge Support

Access to a bridge support call that remains open (at the discretion of the support team?) until the resolution of any incident.

Emergency Escalations

Access to the Support Management Team for escalations during critical events.

Event Monitoring & Support

Access to monitoring and support during pre-planned events. Customers should contact support before the event.

Response Times

Support response time based on severity levels. A bridge will be opened for troubleshooting with customers on Professional and higher tiers for P1 outages.

Performance Features Description

Application Rules

Application Rules determine how requests for a specific environment will be processed.

CDN-as-code

CDN-as-code allows you to configure CDN behavior using EdgeJS within a file.

Image Optimization

Image Optimization dynamically transforms your images to tailor them to your site and optimize their size.

Instant Global Purge

Purge cached content to force the CDN to request a new version of that content from an origin server or Cloud Functions.

Purge by Tag

Purge cached content by surrogate key (aka cache tag). A surrogate key is a label that you may apply to cached responses. Purging by surrogate key allows you to purge related content across your entire site.

Predictive Prefetching

Edgio allows you to speed up the user's browsing experience by prefetching pages and API calls that they are likely to need.

Brotli Compression

Edge server compression occurs when an edge server compresses cached content and provides this compressed response to the client.

WebSocket Protocol

WebSocket is a bidirectional communication protocol that can send the data from the client to the server or from the server to the client by reusing the established connection channel.

Traffic & Feature Management Description

Canary Deployment

Progressive rollout of an application that splits traffic between an already-deployed version and a new version, rolling it out to a subset of users before rolling out fully.

Feature Flags

Allows site administrators to enable or disable a feature without modifying the source code or requiring a redeploy.

A/B & Multivariate testing

Experiment where two or more variants of a page (or multiple pages) are shown to users at random to determine which variation performs better for a given conversion goal.

Iterative Migration

Incrementally migrate from a website a page or section at a time for the purpose of redesigning or replatforming a site.

DNS Load Balancing

Configuring a domain in the Domain Name System (DNS) such that client requests to the domain are distributed across a group of servers.

Experiments

Edgio Experimentation rules (Experiments) enable the distribution of site traffic among alternative origins or site variations for purposes that include iterative site migrations, canary deploys, and A/B testing with options to maintain caching and user session consistency.

Edge Computer and Development Platform Features Description

Full-stack application platform for high-performance websites, apps, and APIs with an integrated CDN (Edgio Performance) and a state-of-the-art web security suite.

Support for modern frontend frameworks

Pre-built integrations for frontend frameworks.

Edge Functions (# of invocations)

Edge Functions enable you to execute a small piece of JavaScript code software on our edge servers. They run on our globally distributed WebAssembly edge computing software stack. Edge Functions enable customers to build low-latency API services and to augment Edgio CDN behavior or their own web and API services among other use cases.

Cloud Functions (GB-Hours)

Develop, test, and deploy JavaScript-based software to one of many available regions around the world (with an automatic backup deployment in a different region for redundancy). These Cloud Functions can be used to power API services and web applications. Their usage is measured in “GB-Hours” which is a combined metric of amount memory available to your Cloud Functions and how long they ran during all their invocations.

Branch Preview (# of deployments)

Deployments to Edgio applications platform are versioned. Each deployment is assigned a unique version number. When deployed through “GitOps”, each deployment can receive an automatically generated URL. This allows you to preview or quickly roll back to any change

Observability Features Description

Real Time Logs Streaming

Real-Time Log Delivery (RTLD) delivers log data in near real-time to a variety of destinations.

Security Analytic API

Delivers Security log data via API calls.

Security Analytic Dashboard

Near real-time and comprehensive reporting for security events.

Real Time Traffic Dashboard (Edge Insights)

Use Edge Insights to gain historical and near real-time insights into threat profiles, performance, and CDN usage.

Real User Monitoring (RUM)

Our real user monitoring (RUM) library allows real-time tracking of your website’s Core Web Vitals for Chromium-based browsers and Firefox.