

Application delivery unified.

Every Edge. Every Cloud. One Platform.

Run your applications securely and reliably across cloud, data center, and hybrid environments with one unified platform for DNS, load balancing, traffic management, application security, and networking. Seamlessly run single IP's across multiple clouds and networks.



Page of Contents

- 1** Why Total Uptime
- 2** How it all fits together
- 3** Cloud DNS Service
- 4** Application Delivery (ADC) — SaaS + On-Premise
- 5** Global Server Load Balancing — SaaS + On-Premise
- 6** Web Application Firewall — SaaS + On-Premise
- 7** Multicloud Networking
- 8** Multicloud Networking — how it works
- 9** BGP Over GRE / VPN
- 10** Protective DNS Service
- 11** EdgeDirector
- 12** Get in touch

Why **Total Uptime**

Total Uptime is the only application-delivery company that runs everywhere you do. Our SaaS cloud delivers DNS, ADC, GSLB, WAF, DDoS and networking as a fully-managed service on a 100% anycast global platform that never goes down, and our on-premise products (EdgeADC, EdgeGSLB and EdgeWAF) deliver the same engine inside your own perimeter.

One vendor, One view, Outstanding support, Total responsibility.

Pick the deployment that fits each application or mix and match across your portfolio. Eight cloud services plus three on-premise products, all under one roof, all designed to work together.

Real human support

24×7 phone and email support included from every tier — no enterprise gating.

100% uptime SLA

Backed by a multi-POP global anycast platform — refunds if we ever fall short of the SLA.

One workflow

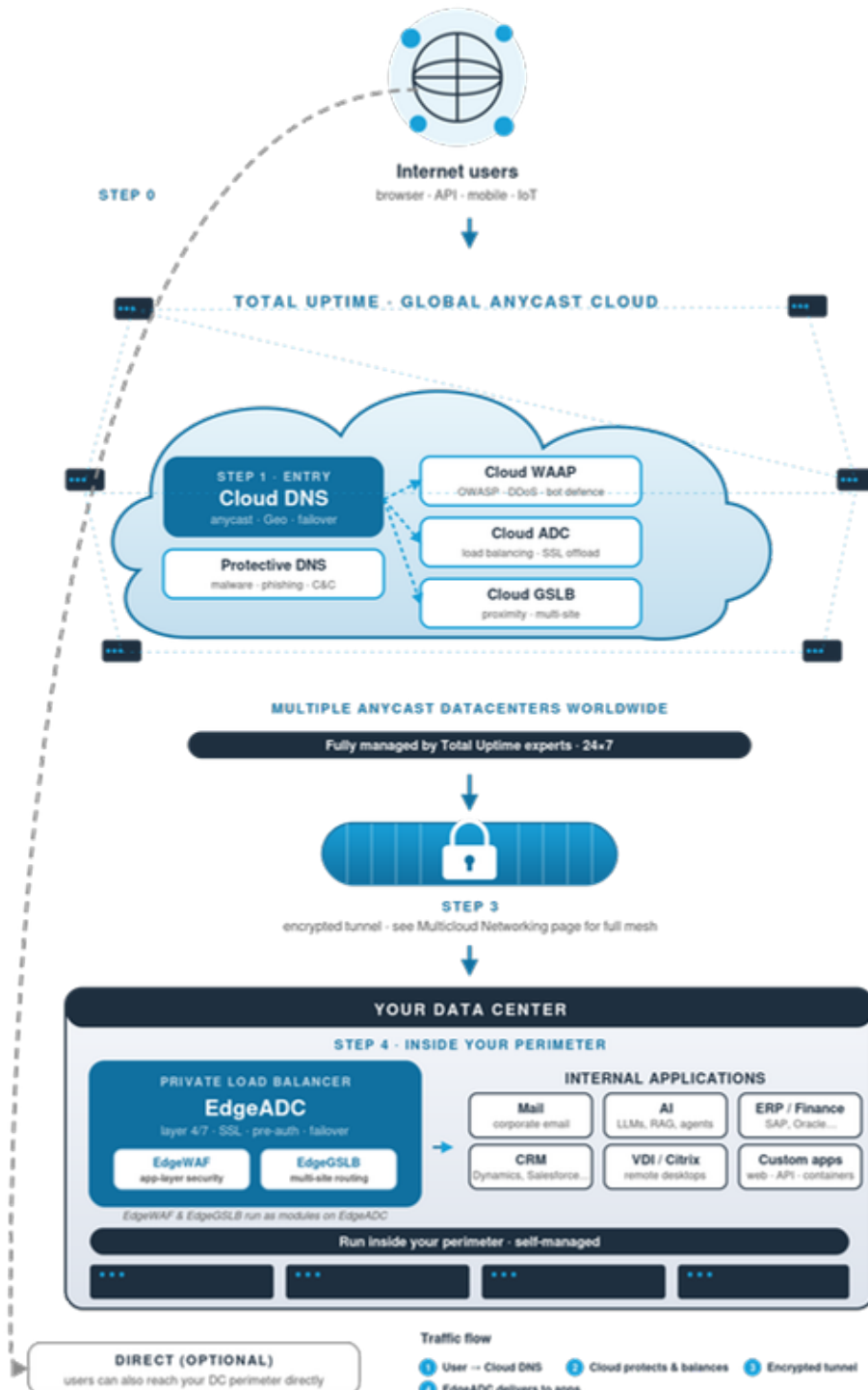
Manage on-premise EdgeADC, EdgeGSLB & EdgeWAF and SaaS load balancers from the same admin language and rule engine.

On-prem AND SaaS

Run application delivery on your own hardware or let us run it for you. Same product family, your choice.

How it all fits together

From the internet user, through the Total Uptime cloud, into your data center, one architecture.



Cloud DNS Service

Comprehensive DNS Infrastructure — three products in one.

When DNS fails, everything fails.

Every application, login, API call, payment and email starts with a DNS query. Most providers only host records. Total Uptime protects your infrastructure with DNS + Monitoring + Failover + Traffic Routing in one managed platform, one SLA, one dashboard.

FOUR INTEGRATED LAYERS, ONE PLATFORM

1

Authoritative DNS

Global anycast hosting every TLD, DNSSEC, native IPv6, reverse DNS, custom TTLs from 60s to 1 year.

2

Traffic Management

Failover pools, round-robin, Geo DNS, traffic steering, multi-region and multi-cloud failover routing.

3

Integrated Monitoring

Built-in Ping, HTTP, HTTPS, DNS, content-match and custom app checks from multiple global regions.

4

Automated Failover

Health-driven DNS updates, manual override, auto-rejoin prevention and maintenance windows included.

INCLUDED ON EVERY PLAN — competitors charge extra (or enterprise-tier only)



DNS Failover Pools

Health-driven IP pools automatically add or remove devices from A-records.

Cloudflare requires Load Balancing add-on; Route 53 charges per health check.



Built-in Monitoring

Ping, HTTP, HTTPS, DNS, content-match and custom app checks from global regions.

Not in Cloudflare DNS; separately billed in Route 53; limited elsewhere.



Secondary / Backup DNS

Mirror zones from your existing DNS provider to our anycast network.

Cloudflare: Enterprise tier only (typically \$1,000+/mo minimum).



Geo DNS Routing

Zone-based and proximity routing — better page loads, better SEO.

Cloudflare: Load Balancing add-on; Route 53: routing-policy add-on.



Maintenance Windows

Suppress alerts and freeze failover during planned changes.

Not available from Cloudflare, Route 53, NS1 or Akamai.



24×7 Phone Support

Real humans on the phone, every plan — architecture advice included.

Cloudflare / NS1 / Akamai: Enterprise contracts only (\$1,000+/mo minimum).

SEE WHERE THE MATHS FLIPS — total cost at each level of capability

Real-world scenario	Total Uptime	Cloudflare	AWS Route 53
Basic DNS hosting (1 domain, no failover)	\$49 /mo	\$0 (Free)	~\$1 /mo
Multi-region with failover (50 domains, 10M queries)	\$125 /mo	~\$25-40 /mo + LB	~\$50-80 /mo + checks
Secondary DNS + failover + Geo (200 domains)	\$299 /mo	~\$1,000+ /mo Ent.	~\$200-400 + support
Full traffic management (500 domains, 100M queries)	\$625 /mo	~\$2,000+ /mo Ent.	~\$500+ /mo + support

As you add monitoring, failover, secondary DNS and real human support, Total Uptime becomes dramatically more cost-effective than competitors charging à la carte or gating capability behind Enterprise tiers.

Application Delivery (ADC)

Same capability. Your choice of deployment.

AS A SERVICE

ADC-as-a-Service

Enterprise application delivery, anywhere, without hardware.

Improves availability, security, performance and cloud integration for any application on-prem, colo, hybrid or multi-cloud — no hardware to buy. Provisioning, tuning, monitoring and 24×7 incident response are handled by our application-delivery experts; you focus on your apps.



Layer 4/7 Load Balancing

11 distribution methods, 7 persistence types and device-based weighting.



DDoS & WAF Protection

Blocks volumetric attacks and all 15 OWASP application vulnerability classes.



Anycast Global Backbone

Deployed across multiple POPs by default. No single region, no single point of failure.



100% Uptime SLA

Multi-POP redundancy with refunds if we ever fall short. Predictable monthly pricing.

ON PREMISE

EdgeADC

Application delivery, uncomplicated.

The on-premise ADC for organisations that need elegant load balancing inside their own perimeter. Hardware, VM, container or cloud. Same elegant control plane, no SaaS dependency, no per-server licensing.



Drag-and-drop GUI

Visual rule builder for traffic management, no coding required.



flightPATH Engine

Custom traffic rules: redirect, rewrite, geo-block, header logic.



Pre-Auth & SSO

Keep bad guys out before they hit your apps and let the right people in, fast.



Deploy Anywhere

Hardware, VM, container, AWS, Azure, GCP, your call, no per-server fees.

Global Server Load Balancing

Proximity routing and multi-site failover, your way.

AS A SERVICE

Cloud GSLB

One global anycast IP. Route users anywhere.

Proximity-based routing to any device behind a single anycast IP. Automated failover the moment health checks fail, no DNS waits, no propagation delays. Configuration, monitoring and 24×7 operations are run by our experts.



Anycast Global IP

Behind one VIP, never stuck in a single AWS region or AZ.



GEO IP Proximity Routing

Send visitors to the closest healthy site based on IP intelligence.



19 Health Monitors

Customisable checks from multiple regions trigger automatic action.



All Protocols & Ports

12 protocol types and unlimited TCP/UDP ports — not just HTTP.

ON PREMISE

EdgeGSLB

Global traffic steering, on your terms.

Brings proximity-based routing, multi-site failover and geographic distribution to your own infrastructure. Sits between your global users and your data centres, your DNS, your IPs, your rules.



DNS-Based Steering

Lightweight integration with any DNS provider you already use.



Per-Site Weighting

Granular per-site traffic weighting and affinity controls.



Multi-Site Health Checks

Monitor every site from multiple monitoring locations.



Self-Managed

Full control inside your perimeter, no SaaS dependency required.

Web Application Firewall

Block bad traffic at the edge of the internet or inside your perimeter.

AS A SERVICE

Web Application & API Protection (WAAP)

Block bad traffic before it reaches you.

Shields apps and APIs from DDoS and application-layer attacks at the edge of the internet. OWASP coverage, DDoS mitigation and origin stealth — long before threats reach your datacenter. Our security team runs rule tuning, signature updates, incident response and threat intel for you, 24×7.



OWASP Top 15 Coverage

Defends against 15 classes of web app vulnerabilities, from buffer overflow to SQLi.



Origin Stealth

Only the Total Uptime IP is exposed publicly, your origin stays hidden.



Zero-Day Protection

Positive-security model with deep content inspection blocks unknown attacks.



Anycast DDoS Defence

Stops volumetric, SYN flood and zombie attacks at the network edge.

ON PREMISE

EdgeWAF

Security that thinks ahead.

EdgeWAF is your first and last line of defence, built right into the ADC. AI-driven behaviour analysis learns, adapts and shields apps from known and unknown threats. Start with core EdgeWAF protection and scale to enterprise-grade security powered by Check Point — same control plane, no PhD required.



AI-Driven Threat Detection

Behaviour-based analysis spots attack patterns humans (and signature lists) miss.



Zero-Day Protection

Stops unknown exploits before they spread, no signatures, no late-night patching.



Check Point Power-Up

Enterprise tier adds global threat intelligence and automatic cloud-driven rule updates.



Deploy Anywhere, Easily

Cloud, hybrid or on-prem, with one-click rule updates and visual policy templates.

Multicloud Networking

One mesh to connect everything, everywhere.

Multi-cloud doesn't have to mean multi-headache.

Most multi-cloud strategies fall apart at the network layer. Full-mesh IPSEC between sites means dozens of tunnels, complex routing, fragile DR and one wrong policy from chaos. Our anycast service mesh collapses that into one tunnel per site, one VIP per app and one policy engine, no SD-WAN appliances to ship, no per-cloud connectors to license.

WHAT YOU GET OUT OF THE BOX



Global Anycast VIP

A static VIP announced from VPN concentrators worldwide gives every site one resilient anchor.



Single-Tunnel Simplicity

Each site builds one IPSEC tunnel into the mesh — no more full-mesh sprawl.



Subnet-Level Policy

Define exactly which subnets at which sites are permitted to communicate.



ISP & Firewall Failover

Run dual ISPs active/active or active/passive with automatic failover.



Automated DR Failover

Cloud mesh reroutes VPN traffic to your DR site automatically when primary fails.



Real-Time Analytics

Live and historic traffic graphs by date, time and geography.

WHERE IT WORKS

1

Hybrid Cloud

Connect on-prem to AWS, Azure and GCP without per-cloud connector fees.

2

Multi-Site Estates

Replace dozens of site-to-site IPSEC tunnels with a single mesh anchor.

3

Disaster Recovery

Automatic reroute to your DR site, no manual reconfig at 2am.

4

ISP / FW Failover

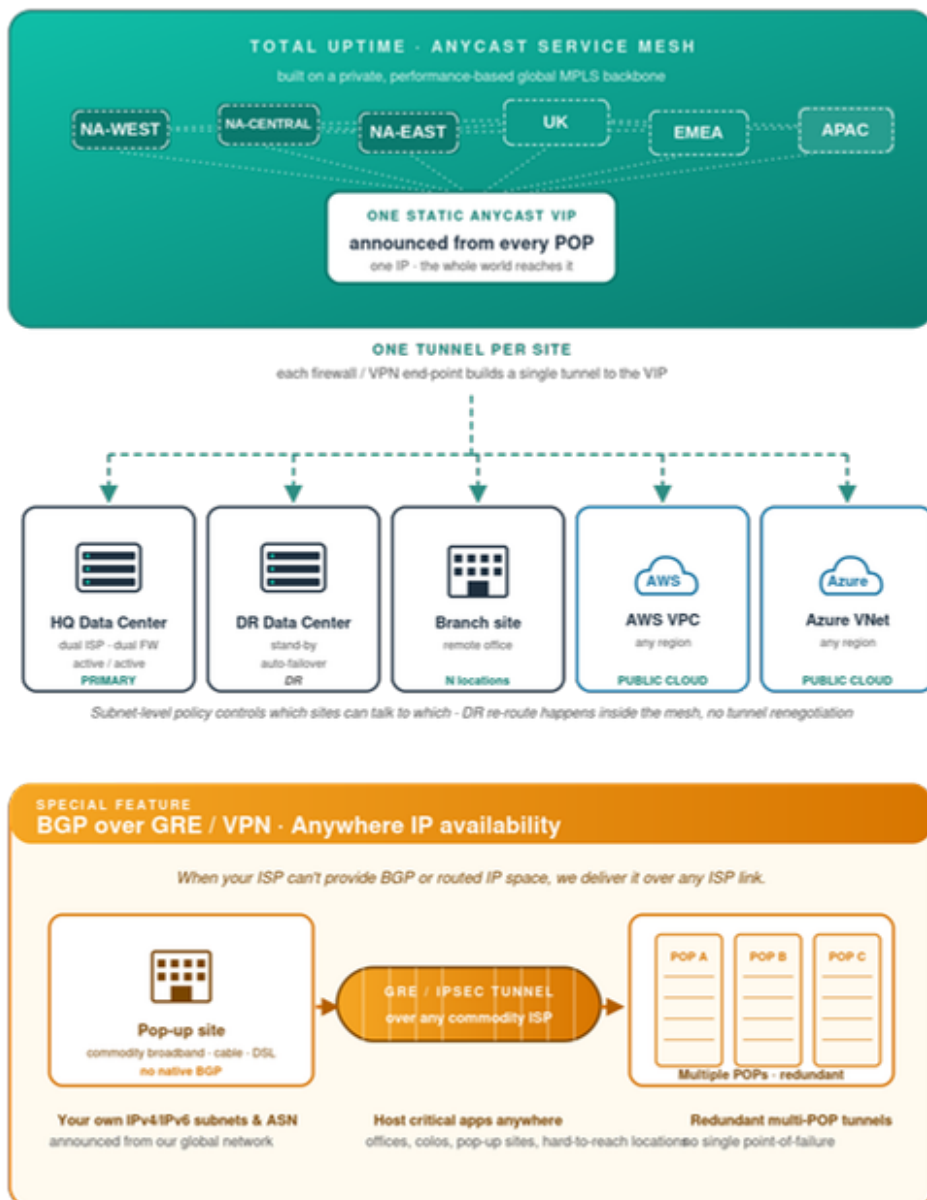
Dual ISPs or firewalls active/passive, with sub-minute switchover.

Multicloud Networking how it works

Anycast service mesh + single-tunnel sites · plus BGP over GRE/VPN for anywhere IP availability.

Multicloud Networking + BGP over GRE / VPN

one anycast service mesh · one tunnel per site · any cloud, any location, any ISP



How it works

- 1 Build one tunnel from each site to the static anycast VIP
- 2 Declare which subnets at which sites can talk to which others
- 3 DR / dual-ISP failover happens inside the mesh — no tunnel renegotiation
- Need static IPs where ISPs won't peer BGP? BGP-over-GRE/VPN delivers your IP space anywhere

BGP Over GRE / VPN

Static IP space over any ISP link.

Your IPs. Anywhere internet reaches.

Dedicated BGP peering usually means expensive circuits, ISP contracts and weeks of provisioning — and only the locations carriers want to serve. We deliver routed IP space over standard GRE or IPSEC tunnels on any commodity internet connection, so pop-up offices, DR sites, hard-to-reach colos and remote branches all get the same corporate IPs as your HQ.

WHAT YOU GET OUT OF THE BOX



Anywhere IP Availability

Get a static IPv4 or IPv6 subnet at any location with normal commodity internet.



BGP Over GRE Tunnels

Deliver routed IP space and BGP sessions over standard GRE tunnels.



BGP Over VPN

Alternative IPSEC VPN delivery where GRE isn't an option.



Bring Your Own IP Space

Use your own ASN and prefixes, announced from our global network.



Multi-POP Redundancy

Build redundant GRE or VPN tunnels from multiple network POPs.



Bandwidth Analytics

Live and historic availability and utilisation via real-time graphs.

WHERE IT WORKS

1

Branch Offices

Bring corporate static IPs to commodity broadband or cable links.

2

DR Sites

Keep IP continuity on remote ISP links so failover is invisible to users.

3

Anywhere Hosting

Run customer-facing apps from locations carriers won't peer BGP at.

4

ISP Independence

Same IPs across multiple ISPs, true multi-homing without your own ASN deal.

Protective DNS Service

AI-powered DNS filtering at the gateway and at the endpoint.

Your IPs. Anywhere internet reaches.

Dedicated BGP peering usually means expensive circuits, ISP contracts and weeks of provisioning, and only the locations carriers want to serve. We deliver routed IP space over standard GRE or IPSEC tunnels on any commodity internet connection, so pop-up offices, DR sites, hard-to-reach colos and remote branches all get the same corporate IPs as your HQ.

WHAT YOU GET OUT OF THE BOX



AI-Powered Detection

ML algorithms analyse unknown domains on the fly, not static lists.



Malware & Ransomware

Stops users reaching hacked sites that deliver malware and C&C callbacks.



Phishing & Typosquat

Blocks phishing pages and misspelled-domain traps before credentials are entered.



Content Category Filters

Policies for adult, illegal, streaming and social, with enforced SafeSearch.



Off-Network Roaming Clients

Windows, Mac, iOS, Android and ChromeOS, filter every device anywhere.



Comprehensive Reporting

Activity, security threat and real-time query log visualisation.

COMPLIANCE & DEPLOYMENT

1

NSA / CISA PDNS

Meets all 11 capabilities of the US PDNS framework.

2

Roaming Clients

Windows, Mac, iOS, Android, ChromeOS, protection follows the user.

3

Existing DNS

Sits in front of or alongside your corporate resolvers, no rip-and-replace.

4

Real-Time Reporting

Per-user, per-device and per-category dashboards for security and audit.

Edgedirector - NEW (Pre-release)

AI-powered System to manage across your entire Application Delivery estate

EdgeDirector is Total Uptime's AI-powered control and observability platform. It governs every service—DNS, ADC, GSLB, WAF, Multicloud Networking, and EdgeADC—providing AI-driven troubleshooting, policy-based automation, and audit traceability from a single console.

KEY FEATURES:

AI Troubleshooting:

Identify root causes in seconds, not hours.

Policy Automation:

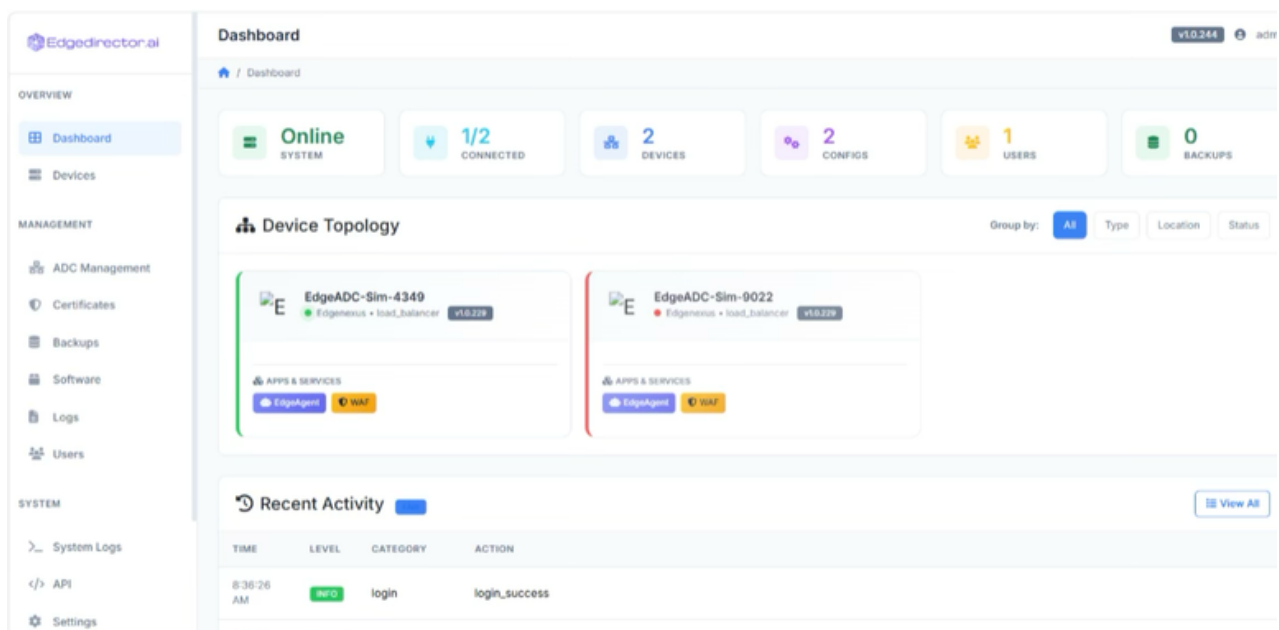
Apply configuration policies once and deploy them everywhere.

Full Traceability:

Every change and failover is logged for complete auditability.

Cloud + On-premise Governance:

Manage your entire infrastructure through one pane of glass.



Prevent your next outage

Eleven products. One company. On-prem or SaaS. 100% uptime SLA. Real humans on the phone, 24×7. Try it free or talk to an engineer about your stack.

Book a Demo

totaluptime.com · +1 800.584.1514 · +44 (0) 330.808.0228
· hello@totaluptime.com

CONTACT

USA & Canada: **+1 800.584.1514 / +1 828.490.4290**

UK & EMEA: **+44 (0) 330.808.0228**

Email: **hello@totaluptime.com**

Web: **totaluptime.com**

© Total Uptime Technologies. Total Uptime® and the Total Uptime logo are registered trademarks. EdgeADC, EdgeGSLB and EdgeWAF are product names of Total Uptime. All other trademarks belong to their respective owners.