Conversant

MaxiSafe Solution Brief

Protect What Powers Your Business
Web Apps, APIs, and Performance

Challenge: The edge has shifted, so have the threats

Your web applications no longer live in one place and neither do the attacks. Today, web apps continue to be the top attack vector and adversaries are leveraging AI and automation to exploit APIs, mimic users, and slip past defences at unprecedented scale.

These shifts have made web application security more complex, **complicating threat detection and their impact on performance**.

63% Cited 'complex and evolving threat landscape' as greatest challenge.

72% Organisations said that cyber risks increased.

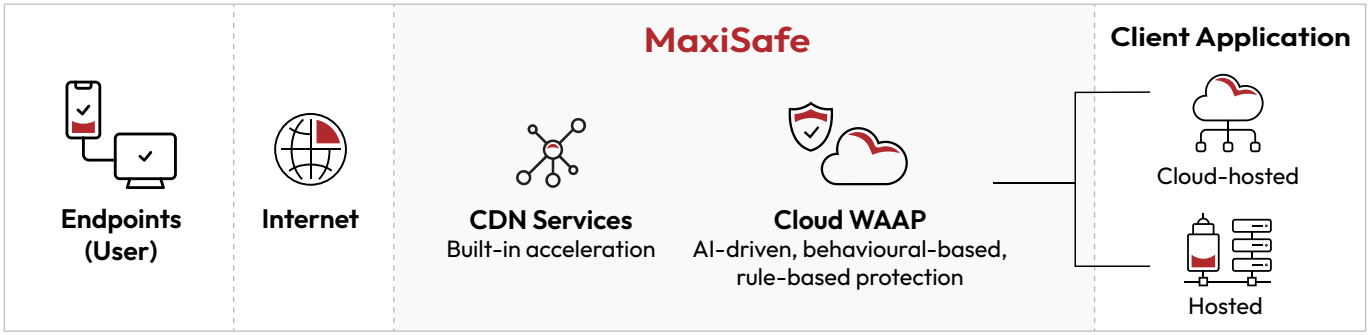
47% Ranked AI-powered threats as top concern.

Source: Global Cybersecurity Outlook 2025, World Economic Forum

Solution: Adaptive protection combined with performance efficiency

Protecting your business's digital presence today means defending both the web application experience and the data behind it. MaxiSafe unifies WAAP security with built-in CDN acceleration, deployed at the edge, so threats can be neutralised before they impact your apps, and users stay protected without performance trade-offs.

MaxiSafe unifies protection & delivery for fast & secure performance



Built on 3 Adaptive Protection Pillars for resilient, always-on protection

AI-Driven Awareness
Detects grey-area and logic-based threats using context and threat patterns.

Rule-Based
Applies signature-based, policy-based controls to stop known and emerging threats.

Behaviour-Based
Analyses user interactions to detect automated attacks and logic-based abuse.

Core Features	How It Works	What It Does	Defends Against
AI-WAF	Blocks sophisticated web threats in real time and reduce alert noise	AI detection, semantic analysis, rule engine, defacement protection	Injection attacks, brute force attempts, defacement, OWASP Top 10
API Protection	Analyses API activity to prevent misuse, unauthorised access, and data leaks	Schema validation, DLP, sequence enforcement, API discovery	API misuse, data exfiltration, business logic abuse
Bot Management	Stops scraping, automated fraud, and account takeover attempts	Fingerprinting, silent challenge, CAPTCHA, browser validation	Credential stuffing, scraping, fake signups, automation abuse
Business Threat Awareness	Detects emerging threats like impersonation and fraud using behavioural analytics	Threat intel, reputation scoring, behaviour tracking, fraud pattern detection	Impersonation, fraud campaigns, emerging threat patterns
Programmable Mitigation	Automates defence actions based on traffic behaviour and business logic	Custom rules, progressive challenge, flow control	Checkout abuse, logic abuse, transaction tampering
DDoS Mitigation	Maintains speed and uptime even during attacks	Rate limiting, behaviour-based filters, burst protection	Layer 7 DDoS, resource drain, volumetric bursts
Content Acceleration	Speeds up site performance globally, even during traffic spikes	Edge caching, CDN load balancing, automates SSL/TLS certifications, HTTP/2 & HTTP/3 support	Slow site speeds under load, content latency, congestion-related drop-off
Emergency Mitigation	Triggers instant response modes during critical attacks or live events	Kill switch, geo-blocking, static mode, read-only controls	Flash event abuse, targeted traffic spikes, active incident containment

With Maxisafe, you can

- Defend APIs, web apps, and business logics from real-time abuse.
- Block threats early without slowing users down.
- Detect anomalies that other security tools fail to detect.
- Stay fast, even under pressure with built-in CDN acceleration.

Start risk-free with no lock-in period.

Choose from ready-made plans with free trial or customise a package based on your threat profile and delivery needs.

Learn more: www.conversant.tv/maxisafe | **Contact us:** www.conversant.tv/contact-us

Conversant