ensono®

WHITE PAPER | CLOUD SECURITY

Ensono Secure Cloud

Layered-In Layer 4 DDoS Protect and Layer 7 Application Protect

Jane Bradshaw, Ensono Security Product Management
Ronnie LaMontagna, Ensono Senior Security Services Manager
Chandlor Mullins, Ensono Security Product Management

Continuous, always-on protection against volumetric, protocol, and application-layer attacks — engineered into the managed cloud platform, and mapped to the regulatory frameworks that matter most to financial services, insurance, public sector, healthcare, and enterprise IT.

AUDIENCE

Security and infrastructure leadership (CISO / CIO / CTO) and technical decision-makers (security architects, infrastructure, and platform teams)

VERTICALS

Financial Services & Insurance • Public Sector / SLED • Healthcare • Enterprise IT

This document is for informational purposes only. Product capabilities and service-level commitments are governed by the applicable Ensono service agreement.

Contents

Executive Summary

Cloud adoption improves speed and flexibility, but it also expands operational complexity and creates exposure points that many security programs do not fully address. Distributed denial-of-service (DDoS) and application-layer attacks have moved from episodic nuisances to a sustained, industrialized threat to availability, and the scale is escalating: in the fourth quarter of 2025, a single hyper-volumetric campaign peaked at 31.4 Tbps — a record at the time — while attacks exceeding 1 Tbps or one billion packets per second became a near-daily occurrence, and application-layer "Web DDoS Tsunami" floods now routinely exceed 50 million requests per second.[1]

Cloud environments rarely fail because of one missing control. They fail because infrastructure, application, API, and availability protections evolve at different speeds across hybrid estates, public cloud platforms, and legacy workloads. Five gaps recur most often across the organizations we work with:

1. Hybrid Complexity Creates Blind Spots. Organizations operating across private cloud, public cloud, colocation, and legacy platforms often continue to govern security as though the environment were centralized and uniform, producing inconsistent controls, fragmented visibility, and slower response when attacks move across environments.

2. Network-Layer Resilience Is Often Underbuilt. A cloud security posture can look strong on paper yet still fail under the volumetric and protocol-based floods — SYN, ICMP, and UDP floods among them — that target availability before traditional application controls have a chance to respond.

3. Application-Layer Attacks Bypass Infrastructure Controls. Even where perimeter and network defenses are solid, attackers increasingly target the application layer, closer to revenue-generating services, user sessions, and APIs, using HTTP/S floods, encrypted attack traffic, and low-and-slow web DDoS techniques designed to evade infrastructure-centric defenses.

4. APIs, Bots, and Modern App Traffic Are Under-Protected. Many programs still assume a web application firewall alone is sufficient, while modern attacks increasingly exploit API abuse, malicious automation, and client-side weaknesses that sit outside traditional rule-based inspection.

5. Security Tools Exist, But Operations Are Fragmented. Organizations often own capable tools yet still struggle with policy tuning, deployment consistency, alert triage, and keeping protection aligned with business change across a fast-moving cloud estate — the gap is as much operational as it is technical.

Ensono Secure Cloud closes these gaps by building protection into the platform rather than bolting it on. Two capabilities are native to the managed cloud environment:

- **Layer 4 DDoS Protect — always-on, behavioral, network- and transport-layer mitigation that absorbs volumetric and protocol floods upstream, before they reach customer workloads, closing the hybrid-complexity and network-resilience gaps above.**
- **Layer 7 Application Protect — machine-learning-based web application and API defense that inspects application traffic, stops the OWASP Top 10 and zero-day exploits, and mitigates encrypted application-layer DDoS, closing the application, API, and bot-traffic gaps above.**

Both capabilities are delivered through a global cloud security network of 65 scrubbing centers and 30 Tbps of mitigation capacity and operated for the customer under Ensono's managed services model — directly addressing the fragmented-operations gap by giving lean security teams enterprise-grade defense without new headcount. The result is defense that spans OSI Layers 3, 4, and 7 in a single, coordinated posture.[2]

Why it matters

Availability is a board-level and regulatory concern — not just an IT metric.

Native, always-on protection removes the reconfiguration delay that lets attacks cause damage.

Ensono operates the controls, so lean security teams gain enterprise-grade defense without new headcount.

The Evolving Threat Landscape

From Volumetric Floods To Application-Aware Campaigns

Early DDoS attacks were blunt instruments: overwhelm a network link with raw traffic and force it offline. Those volumetric attacks have not disappeared — they have grown larger — but they are now accompanied by more surgical techniques that target the transport and application layers where filtering by volume alone is ineffective.

Modern campaigns blend three attack surfaces:

- Volumetric (Layer 3/4): UDP reflection/amplification, carpet-bombing across entire IP ranges, and terabit-scale floods intended to saturate bandwidth and exhaust infrastructure.
- Protocol (Layer 4): SYN, ACK, and state-exhaustion floods and high packets-per-second attacks that consume the connection tables and CPU of firewalls, load balancers, and network gear.

- Application (Layer 7): HTTP/S floods, low-and-slow assaults, and encrypted "Web DDoS Tsunami" attacks that mimic legitimate users and can only be identified by inspecting decrypted application content.

Why Traditional Defenses Fall Short

Network-based defenses cannot accurately mitigate application-layer DDoS because doing so requires decrypting traffic and inspecting Layer 7 headers and payloads – something perimeter volumetric scrubbing is not designed to do. Conversely, an application firewall alone cannot absorb a multi-terabit flood. Effective defense requires coordinated protection at every layer, which is precisely why Ensono Secure Cloud pairs Layer 4 and Layer 7 protection as built-in, complementary controls.

Attack Class	Example Techniques	Primary Defense In Ensono Secure Cloud
Volumetric (L3/L4)	UDP/DNS amplification, carpet bombing, terabit floods	Layer 4 DDoS Protect – upstream scrubbing
Protocol (L4)	SYN/ACK floods, state exhaustion, high-PPS attacks	Layer 4 DDoS Protect – behavioral mitigation
Encrypted app-layer (L7)	HTTPS floods, Web DDoS Tsunami (>50M RPS)	Layer 7 Application Protect – keyless L7 defense
Web exploitation (L7)	OWASP Top 10, injection, zero-day, bad bots	Layer 7 Application Protect – adaptive WAF + bot mgmt

Ensono Secure Cloud: Protection Built In, Not Bolted On

Ensono Secure Cloud is a managed cloud platform in which resilience is a design property, not an add-on purchase. Layer 4 DDoS Protect and Layer 7 Application Protect are provisioned as part of the environment, tuned by Ensono's operations teams, and kept current as the threat landscape shifts. Customers consume protection as an outcome – sustained availability – rather than as a set of appliances they must integrate and staff.

The Three Principles Behind The Design

- Always-On, Not On-Demand. Because mitigation is native to the platform, there is no diversion delay or manual reconfiguration when an attack begins. Protection is continuously in path, so the damaging first minutes of an attack are covered.
- Layered By Default. Layer 4 handles volume and protocol abuse upstream; Layer 7 inspects application and API traffic. Together they close the gaps that single-layer solutions leave open.
- Operated, Not Just Licensed. Ensono configures, monitors, and mitigates on the customer's behalf under a managed services model – extending scarce internal security capacity.

The Radware Foundation

Both capabilities are powered by Radware's cloud security technology and its DefensePro X mitigation backbone.

Global network: 65 cloud security / scrubbing centers with 30 Tbps of aggregate mitigation capacity, doubled from 15 Tbps in early 2026.

Full-mesh Anycast routing mitigates attacks closest to their point of origin, absorbing even the largest volumetric campaigns.

Layer 4 DDoS Protect — Network and Transport Defense

Layer 4 DDoS Protect defends the network (L3) and transport (L4) layers: the bandwidth, connection state, and packet-processing capacity that every application depends on. Its job is to ensure that volumetric and protocol attacks are absorbed and filtered upstream, so that only clean traffic reaches customer workloads.

How It Works

- Behavioral, AI-Driven Detection. Rather than relying solely on static thresholds or signature blocklists, the service learns normal traffic baselines and identifies anomalies in real time, distinguishing legitimate users from attack traffic and generating protective signatures automatically — including for zero-day floods.
- Upstream Scrubbing At Scale. Suspicious traffic is diverted to Radware's globally distributed scrubbing centers, cleansed, and the legitimate remainder forwarded to the origin. Anycast routing draws attack traffic to the nearest center, reducing latency and containing the blast radius.
- High-Rate Protocol Mitigation. The DefensePro X mitigation engine blocks high packets-per-second and state-exhaustion attacks that would otherwise overwhelm firewalls and load balancers, mitigating attack traffic while preserving quality of experience for real users.
- Flexible Deployment Posture. The underlying service supports always-on, on-demand, hybrid, and hybrid always-on modes. Within Ensono Secure Cloud it is delivered always-on so protection never has to be switched into place mid-attack.

Capability	What It Delivers
Global scrubbing network	65 centers, 30 Tbps aggregate mitigation capacity, full-mesh Anycast
Layers covered	OSI Layers 3 and 4 (network and transport)
Detection method	AI / behavioral analysis with real-time automated signatures
Zero-day floods	Behavioral detection mitigates novel attacks without prior signatures
Service posture	Always-on within Ensono Secure Cloud (no diversion delay)
SLA commitments	Granular commitments for time to detect, alert, divert, and mitigate

Layer 7 Application Protect – Web and API Defense

Layer 7 Application Protect defends the application layer, where attacks look increasingly like legitimate traffic. It combines an adaptive web application firewall, bot management, API protection, and application-layer DDoS mitigation into a single, coordinated control set.

Adaptive Web Application Firewall

The WAF pairs a negative security model (thousands of signatures for known vulnerabilities) with a positive security model that automatically learns the patterns of legitimate application behavior, builds a tailored policy, and blocks anything that deviates. This combination delivers out-of-the-box coverage of the OWASP Top 10 and catches zero-day exploits that signature-only WAFs miss. Machine learning continuously reviews traffic logs and refines policy as the application changes, reducing false positives without manual tuning.

Bot Management And API Protection

More than half of internet traffic is automated. Behavioral bot management fingerprints browsers, devices, and machines and applies Intent-Based Deep Behavior Analysis across hundreds of parameters to separate humans and good bots from malicious automation – addressing the OWASP Automated Threats. Dedicated API protection automatically discovers the API attack surface (including undocumented endpoints), validates schemas and tokens, and blocks injection, parameter tampering, and API-focused DoS.

Encrypted Application-Layer DDoS – Without Sharing Keys

Web DDoS Tsunami attacks operate over HTTPS and can only be stopped by inspecting decrypted content. Layer 7 Application Protect applies machine-learning behavioral detection to identify and block these floods – including campaigns exceeding tens of millions of requests per second – while generating real-time signatures for zero-day variants. Radware's architecture can inspect and mitigate without requiring customers to share SSL private keys, preserving privacy and simplifying certificate governance.

Threat	Layer 7 Protection
OWASP Top 10 & zero-day exploits	Adaptive WAF: combined positive + negative security models
Injection, XSS, data leakage	Signature filters, input normalization, sensitive-data masking
Malicious bots & account abuse	Behavioral bot management, device fingerprinting, IDBA
API attacks	Automated API discovery, schema/token validation, API DoS defense
Encrypted L7 DDoS (Tsunami)	ML behavioral detection, real-time signatures, keyless inspection

Coordinated Layers: One Posture, Every Vector

The strategic value of Ensono Secure Cloud is the coordination between the two layers. Layer 4 DDoS Protect ensures the pipes and infrastructure stay clear under volumetric and protocol assault; Layer 7 Application Protect ensures the applications and APIs behind them stay available and uncompromised under sophisticated, encrypted, application-aware attacks. Neither layer alone is sufficient against a modern blended campaign — together, and operated by Ensono, they provide continuous L3–L7 defense.

Dimension	Layer 4 DDoS Protect	Layer 7 Application Protect
OSI layers	Network & transport (L3/L4)	Application (L7)
Primary threats	Volumetric & protocol floods	Web/API exploits, bots, L7 DDoS
Core method	Upstream behavioral scrubbing	Adaptive WAF + ML behavioral analysis
Encrypted traffic	Packet/flow-level filtering	Keyless content inspection
Outcome	Bandwidth & infra stay available	Apps & data stay available and safe

Vertical Relevance and Compliance Alignment

Availability is not only an operational goal — in regulated industries it is a compliance obligation. Confidentiality, integrity, and availability (the "CIA triad") sit at the center of every major control framework, and DDoS resilience maps directly to the availability requirements those frameworks impose.

Financial Services And Insurance

For banks, insurers, and payment providers, downtime is measured in lost transactions, SLA penalties, and reputational damage — and DDoS is a frequent cover for fraud. Continuous L3–L7 protection supports PCI DSS requirements to protect cardholder-data environments and maintain availability, and aligns with operational-resilience expectations from financial regulators. Bot management additionally curbs credential stuffing and automated fraud against customer-facing portals.

Public Sector / SLED

State, local, education, and federal agencies deliver citizen-facing services that must remain reachable and are attractive targets for hacktivist and nation-state DDoS. Availability controls support NIST SP 800-53 (notably the SC and SI control families) and FISMA/FedRAMP requirements, while application and bot defenses help protect systems subject to CJIS security policy. Data-sovereignty needs are supported by Anycast mitigation that filters attacks close to their origin.

Healthcare

Patient portals, telehealth, and clinical systems are safety-critical: an outage can delay care. The HIPAA Security Rule requires safeguards for the availability of electronic protected health information (ePHI), and contingency-planning provisions expect resilience against disruptions. Layer 4 and Layer 7 protection keep patient-facing and integration services online, while WAF and API controls guard the interfaces through which ePHI flows.

Enterprise IT

For broad enterprise environments, the value is availability of revenue-generating and productivity applications, protection of hybrid and multi-cloud estates, and reduced operational burden. The controls support NIST Cybersecurity Framework outcomes and the availability objectives within NIST SP 800-53 and ISO 27001, giving security leaders defensible, framework-aligned evidence of resilience.

Vertical	Key Frameworks	How Ensono Secure Cloud Helps
Financial & Insurance	PCI DSS, operational resilience	Availability + fraud/bot defense for payment and customer systems
Public Sector / SLED	NIST 800-53, FISMA, FedRAMP, CJIS	L3–L7 availability controls for citizen-facing services
Healthcare	HIPAA Security Rule	Availability of ePHI systems; WAF/API protection of interfaces
Enterprise IT	NIST CSF, NIST 800-53, ISO 27001	Framework-aligned resilience across hybrid/multi-cloud

Compliance Note

These frameworks address availability alongside confidentiality and integrity; DDoS and application resilience are contributing controls, not stand-alone certifications.

Ensono provides the operated controls and supporting evidence; formal attestation remains the customer's program responsibility.

The Ensono Managed Advantage

Technology alone does not stop attacks – operating it well does. Ensono pairs the Radware-powered controls with a managed services model so that detection, tuning, and mitigation are handled continuously by specialists.

- Operated For You. Ensono configures policies, monitors traffic, and mitigates attacks on the customer's behalf – extending lean security teams without new hiring.
- Always-On By Design. Protection is provisioned into the platform, eliminating the reconfiguration delay that lets attacks cause damage before defenses engage.
- Backed By SLAs. The underlying service carries granular service-level commitments for time to detect, alert, divert, and mitigate.

- Aligned To Your Estate. Protection spans hybrid and multi-cloud environments, consistent with Ensono's heritage across mainframe, cloud, and security services.

Conclusion

DDoS and application-layer attacks have become larger, faster, and more sophisticated — and availability has become a board-level and regulatory concern. Point solutions and on-demand mitigation leave gaps in the critical opening minutes of an attack and in the encrypted application layer where modern campaigns now concentrate.

Ensono Secure Cloud closes those gaps by building Layer 4 DDoS Protect and Layer 7 Application Protect into the platform, powering them with Radware's global scrubbing network and adaptive, machine-learning defenses, and operating them under a managed services model. For financial services, insurance, public sector, healthcare, and enterprise IT organizations alike, the outcome is the same: applications that stay available, data that stays protected, and a resilience posture that maps cleanly to the frameworks the business must answer to.

Next Step

Engage Ensono for a resilience review to map your current availability controls to your regulatory frameworks and model the impact of built-in L3–L7 protection on your environment.

Ensono Secure Cloud, Layer 4 DDoS Protect, and Layer 7 Application Protect capabilities described here are based on Radware technology. Specific features, capacities, and service-level commitments are subject to the applicable Ensono service agreement and may change as the underlying platform evolves. Radware, DefensePro, and related marks are the property of Radware Ltd. This white paper is provided for informational purposes only and does not constitute legal or compliance advice.

Sources

1. Cloudflare, DDoS Threat Report 2025 Q4, blog.cloudflare.com/ddos-threat-report-2025-q4; Radware Web DDoS Tsunami (>50M RPS), Radware Pulse capacity update.

2. Radware Cloud DDoS Protection Service and network capacity (65 centers, 30 Tbps, DefensePro X), securitybrief.com.au; Radware Cloud Application Protection technical white paper, radware.com/solutions/ddos-protection.