FIRSTWAVE
CLOUD SECURITY TECHNOLOGY

Cloud Web Security

A DNS and intelligent proxy security service to prevent threats at the Internet foundational level

With the dynamic security landscape increasing in complexity and severity, firewalls can no longer provide complete and effective protection for your business – especially as more users are roaming, using cloud-based apps and accessing the internet off the corporate network. FirstWave Cloud Web Security is your first – and only necessary – line of defence against online threats, providing complete visibility into internet activity across all locations (on and off the corporate network), devices and users – blocking threats before they reach your network or endpoints.

Using DNS-based and intelligent proxy technology, Cisco Talos intelligence, and Cisco Advanced Malware Protection (AMP), Cloud Web Security can determine the trustworthiness of web requests, URLs and files. Determining them as being 'safe', 'malicious' or 'risky', they are subsequently routed, blocked or sent for deeper inspection.

Key Highlights

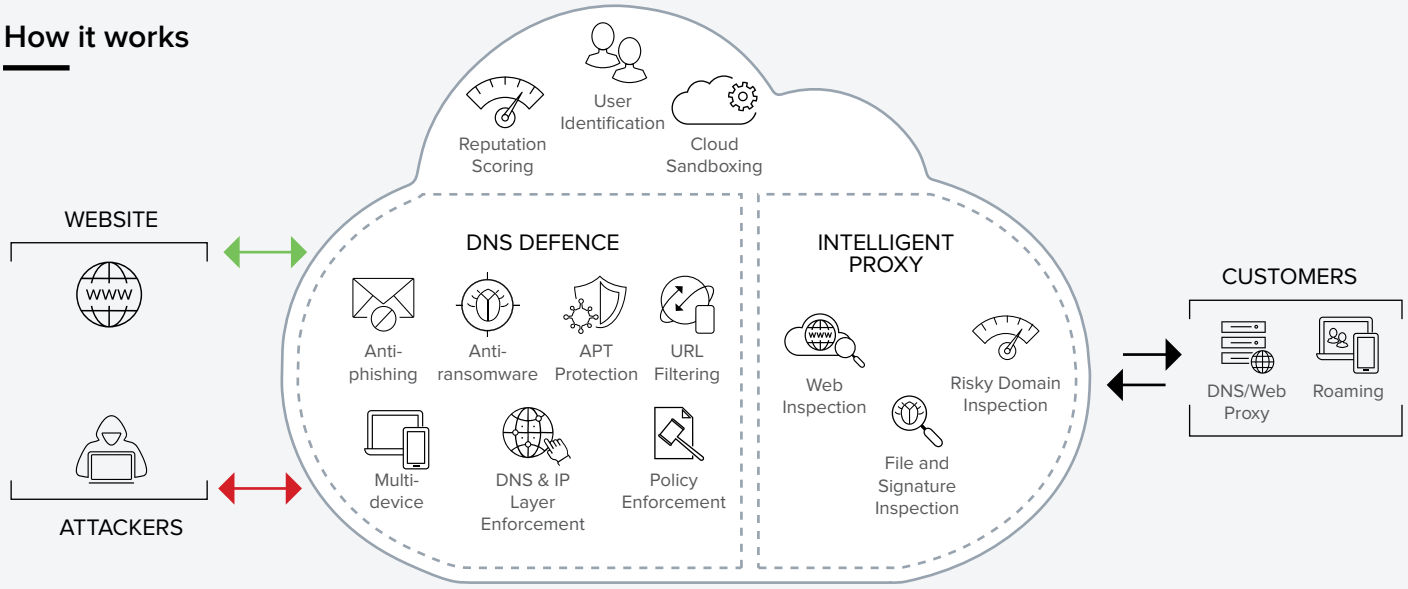
An all-inclusive, enterprise-grade web security solution for businesses of any size

Offers real-time protection and thorough enforcement of web usage policies

Provides complete visibility into internet activity across all devices, users and locations

75%
of organisations surveyed reported a security breach or infection in the past
12 months

How it works



Cloud Web Security

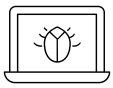
www.firstwavecloud.com

ISO 9001 CERTIFIED
ISO 27001 CERTIFIED

FIRSTWAVE
CLOUD SECURITY TECHNOLOGY

Why choose Cloud Web Security Service?

Advanced protection that adds a predictive security enforcement layer at the early stage



Fast identification of infected devices and prevention of data exfiltration

Fast and reliable without added latency

Rapid enforcement of security policies across 30 global data centres

Round-the-clock proactive monitoring and alerting capabilities for high availability

Problem management, and security operations by a premium support function consisiting of a team of highly experienced engineers

Full visibility across all network devices, locations and users via real-time activity logs

Enterprise-wide activity search, reporting and identification of targeted attacks to determine potential cloud and IoT risks

Quick and easy deployment of software

Powerful pre-configured ‘out of the box’ policies, essential testing and service verification, on-boarding and customer training

Easy design and integration of Virtual Appliance (VA) and Connector and Active Directory (AD) (POA)

Comprehensive Security Features
Cloud portal (single sign-on) with RBAC-based console
Cloud management portal
Command and control call-back blocking
IP layer enforcement
Intelligent proxy
Web filtering
Collective security intelligence
Portal reporting
Centralised policy management
File reputation
AnyConnect VPN client with Umbrella integration
Virtual appliance integration
Active directory integration service
Log extraction
Data retention (integrated with Amazon S3)
Category-based URL filtering