digicert®
Ultra Products

Web Application Security

Now with bot management

The changing landscape of security threats – from networks to applications, from business disruption to data exfiltration, and from single-vector to multi-dimensional attacks – is driving an architectural shift in the security industry. Application-layer threats have become more damaging and are also much more difficult to detect as they provide little to no advance warning before they wreak havoc. This necessitates a security posture that is always-on but still provides the scale to respond to the largest network and application-layer threats that are prevalent today.

Security leaders are struggling to find ways to protect their customer-facing and mission-critical applications against ever evolving threats that target their online web resources. DigiCert UltraWAF™ is a cloud-based web application protection service that protects against threats that target the application layer. With UltraWAF, organizations can reduce their costs and consistently configure rules anywhere, without any provider restrictions or hardware requirements. UltraWAF also fights attacks by detecting and categorizing bots, applying appropriate countermeasures to neutralize malicious bots, all without impeding legitimate traffic.

Benefits

- Cloud deployment with no hardware or software required
- OWASP Top 10: Protects against known security risks
- Profiles traffic and makes recommendations based on traffic heuristics via Learning Mode
- Positive and negative security: Allows or blocks access efficiently
- Seamlessly detects and manages bot activity via a flexible framework
- 24/7 customer support from a team of dedicated security experts

Features

- Request & Protocol Validation
- Cross-Site Scripting Attacks
- SQL Injection Attacks
- Geo Blocking
- IP Block/Allow Lists
- HTTP/s Rule Sets
- SSL-Based Protection
- Virtual Patching
- Learning Mode
- Real Time Reporting & Monitoring
- Custom Signatures
- Bot Traps
- Device Fingerprinting

UltraWAF Key Benefits

Cloud, Hardware, and Environment Agnostic

UltraWAF fits anywhere that your applications are hosted, so you can reduce costs and configure consistent rules without any restrictions.

Layered Protection

UltraWAF defends critical applications even with the most complex workflows and prevents the most common threats that target the application layer, such as SQLi, XSS, and CSRF.

Positive & Negative Security Capabilities

Whether your security posture assumes that all traffic is allowed except that which includes an already identified threat or an attack (Negative Security) or you take the position that unless traffic is explicitly permitted it is denied (Positive Security), UltraWAF can help you catch zero-day threats, as well as attacks that feature malformed packets or non-RFC-compliant traffic. Additionally, automated learning through traffic heuristics can empower you to match a profile to the traffic to your online presence.

Learning Mode

Learning mode takes note of the traffic passing through UltraWAF and makes recommendations on what relaxation rule, if any, should be applied. This feature profiles traffic and can help you to delineate between true anomalous behavior, which you might want to block, and an application that features an unusual pattern but is still considered legitimate.

With UltraWAF, organizations can reduce their costs and consistently configure rules anywhere, without any provider restrictions or hardware requirements.

Customizable Signatures

The UltraWAF policy editor lets you create your own rules in a variety of formats and provides the option to continuously add new threats (signature protection for CVE and CWE, such as CMS vulnerabilities, etc.) captured by the DigiCert threat research team.

Seamless Administration

An easy-to-use online portal lets you seamlessly manage all of your web security needs from one place, regardless of where your applications are hosted. You can make configuration changes instantly, and reporting/logging capabilities allow you to analyze the effectiveness of your website and application security.

Secure Control

UltraWAF uses a Hardware Security Module (HSM) to provide secure key storage for your digital certificates, protecting your applications even when using encrypted payloads.

Standalone or Augment Your On-Prem WAF

UltraWAF fits anywhere that your applications are hosted. UltraWAF can also augment the effectiveness of your existing on-prem WAF investment by filtering out bad traffic from the public cloud before it reaches your network. This reduces the overall traffic load on your on-prem devices, which can then be focused more precisely.

Bot Management

Nearly a quarter of all internet traffic comes from malicious bots. UltraWAF is an enterprise-grade solution that can detect and defend against malicious bots ensuring you know who or what is interacting with your online presence.

Ready to fortify your defenses?

We're here to help you build a resilient protection strategy tailored to your organizational needs.

Call USA +1 (844) 929-0808
Call EMEA +44 808 175 1189
vercara.digicert.com

digicert®
Ultra Products

Securing the online experience.

SS-VER-UWAF-J93966-09.03.2025

©2025 DigiCert, Inc. All rights reserved. All logos, trademarks, servicemarks, registered trademarks, and/or registered servicemarks are owned by DigiCert, Inc. All other logos, trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.