Web Security +

1. GENERAL

1.1 **Service Definition.** Verizon Web Security helps to protect Customer's web sites, applications and origin servers. Web Security inspects inbound HTTP/HTTPS traffic against reactive and proactive security policies and blocks malicious activity in-band, and on a near real-time basis. Web Security further helps restricts malicious traffic (such as SQL injections, cross-site-scripting and application layer attacks), Distributed Denial of Service (DDoS) traffic, and helps prevent a Customer origin server from being overloaded (Rate Limiting). In addition, Web Security delivers traffic from a Customer's website to Users quickly by securing and delivering content from an origin point to Users (Web Acceleration). Web Security provides Customers with global domain lookup and translation services (Authoritative DNS) and an artificial intelligence screening functionality (Bot Management).

1.2 **Service Implementation and Configuration.** Verizon will assign a product implementation manager to Customer who will activate Web Security on Customer's account. Standard Web Security implementation includes on boarding of up to five applications. Customers requiring on boarding of more than five applications may contract separately for Professional Services. Web Security is configured by Customer in the Portal where Customer may define Rules and create a Security Application Manager configuration that enforces these Rules.

1.3 **Service Features**

1.3.1 **Web Application Firewall (WAF).** The Web Application Firewall feature of Web Security leverages Rules configured via the Security Application Manager to determine whether site traffic is legitimate or a threat. Customer will combine Rules through the Security Application Manager to set the appropriate application security policy.

1.3.2 **Threat Analysis.** Verizon will provide a dashboard where Customer may view a historical analysis of recent threats and Rate Limited requests for the prior seven days. Customer may make configuration changes and updates based upon this analysis in the Security Application Manager.

1.3.3 **Web Acceleration.** Web Security accelerates website traffic by using Verizon's Content Delivery Network (CDN). CDN provides two specialized delivery platforms through which data may be efficiently transferred to Customer's Users: (i) the Application Delivery Network (ADN), a platform optimized to deliver user-specific and database driven dynamic content such as login credentials and account information; and, (ii) HTTP Large, a platform optimized to cache and deliver static content such as HTML, CSS, JavaScript, ISO, multimedia and software downloads. Platforms are infrastructures of dedicated servers and devices distributed across the network of PoPs to secure and deliver content from an origin point to Users.

1.3.4 **Authoritative Domain Name System.** Verizon's Authoritative DNS provides global domain lookup and translation services through the creation and management of zones. A zone defines a data set through which authoritative name servers can provide a response to DNS queries. Customer may define primary and secondary DNS zones that define how traffic will be distributed to Customer servers.

1.3.5 **Bot Management.** Bot Management uses Artificial Intelligence (AI) to determine if an application request is from a fraudulent source and will route legitimate requests and mitigate fraudulent requests. Bot Management can be deployed to protect web and mobile applications, as well as HTTP APIs. Bot Management is provided by Verizon's supplier, Shape Security Inc. an affiliate of F5 Networks Inc. (Shape Security), according to terms supplied at this URL (www.f5.com/pdf/customer-support/eusa.pdf) (Shape Software). Bot Management includes either Shape Enterprise Defense, Shape Defense or Shape Blackfish.

1.3.5.1 **Shape Enterprise Defense.** Shape Enterprise Defense provides real-time, AI-based prevention of fraud that is caused by both automated (bot-based) and manual (human) attacks on web and mobile applications. It is delivered and operated 24x7x365 by Shape SOC and data scientists as a fully-managed, self-contained service, where the mitigation of threats is customized for each large enterprise.

1.3.5.2 **Shape Defense.** Shape Defense leverages the same real-time AI and accumulated machine learning as Shape Enterprise Defense, but with standardized (rather than customized) mitigation of threats, leveraging Shape's network-based intelligence. It is delivered and operated 24x7x365 by Shape employees as a fully-managed, self-contained service.

1.3.5.3 **Shape Blackfish.** Shape Blackfish is a real-time credential integrity checking service protects a login system. Shape Blackfish analyzes threat data, credentials (usernames and passwords) and provides notification of the use of compromised credentials used to gain site access.

2. SUPPLEMENTAL TERMS

2.1 **Transaction Volumes and Event Logs.** Verizon will measure Customer site traffic for Web Acceleration in Gigabytes (GB) and for invoicing purposes, delivered objects smaller than one GB shall be rounded up to one. Traffic measurements shall include transferred FTP and rsync data. Event logs provide details of Rate Limit enforcement.

2.1.1 **Transaction Volume Overage and Charges**. If at least five percent of Customer's transactions are erroneous (e.g., HTTP 1.1 standard errors that include HTTP status codes 403, 404, 500, 502 or 504), Verizon reserves the right to invoice Customer additional charges, up to $0.01 per 1,000 transactions. If Customer has enabled event logging functionality and is generating more than 5,000,000,000 log records per month, Verizon reserves the right to invoice Customer additional charges, up to $0.01 per 1,000 log records processed.

2.1.2 **Content Storage Services**. Customer may choose to store content for using CDN origin servers. For content storage services, each month Customer is responsible for paying the greater of (1) Customer's MRC for such storage Services or (2) the highest per-GB usage level for storage Services during that month (i.e., high-water mark) multiplied by the per-GB storage Services.

2.2 **Customer Data Processing.** Web Security is provided pursuant to the Data Processing terms at the following URL: http://www.verizon.com/business/service_guide/reg/web-security-data-processing-addendum.pdf.

2.3 **Warranties**

2.3.1 **Verizon Warranties**. Verizon warrants to Customer that it will perform its obligations in a good and workmanlike manner. Verizon does not guarantee Web Security will mitigate all possible attacks nor that all defects will be discovered through its use.

2.3.2 **Third Party Warranties**. For any third party products and/or services incorporated as part of the Service, Customer will receive only the warranties offered by such third party either directly to Customer or to the extent Verizon may pass through such warranties to Customer.

3. **SERVICE LEVEL AGREEMENT**. The Service Level Agreement (SLA) can be found at: http://www.verizon.com/business/service_guide/reg/web-security-sla.pdf.

4. **FINANCIAL TERMS.** Customer will pay the non-recurring charges (NRCs) and monthly recurring charges (MRCs) as set forth in the applicable Agreement. Unless expressly indicated otherwise, all NRCs will be invoiced upon Commencement Date and the initial MRCs will be invoiced upon Service Activation Date.

5. **DEFINITIONS.** The following definitions apply to Web Security, in addition to those identified in the Master Terms of your Agreement.

Term	Definition
Domain Name System (DNS)	A hierarchical and distributed naming system for any resource connected to the Internet. This system includes the capability to translate hostnames into IP addresses.
Point-of-Presence (PoP)	A location on the Verizon network through which Users can request and receive assets or content.
Portal	Customer portal and user interface where Customers will configure various Web Security settings.
Rule(s)	Modular rules through which Customers define security policies for inbound HTTP/HTTPS traffic and which identify legitimate traffic or threats via threat detection policies, access controls and/or rate limits.
Security Application Manager	A configuration which identifies the set of policies or Rules to enforce for WAF.
Super PoP	PoPs with high bandwidth capacity and large computing power.
User	A subscriber, member or other visitor of an online site or service owned and/or operated by Customer who uses, benefits from or accesses the Services.