



VERIZON DNS SAFEGUARD +

1. GENERAL
 - 1.1 Service Definition
 - 1.2 Basic Service Features
 - 1.3 Premium Service Features
 - 1.4 Service Activation and Implementation
2. SUPPLEMENTAL TERMS
 - 2.1 Services Agreement Flow Down Terms
 - 2.2 Customer Responsibilities
 - 2.3 Warranties
 - 2.4 Use of Data
3. SERVICE LEVEL AGREEMENT
 - 3.1 Service Level Description
 - 3.2 Credits
4. FINANCIAL TERMS
 - 4.1 General
 - 4.2 Early Termination Charges
5. DEFINITIONS

1. GENERAL

- 1.1 **Service Definition.** Verizon DNS Safeguard (DNS Safeguard or DNS Service) is a cloud-based security platform intended to provide a first line of defense against threats on the Internet by detecting and blocking inappropriate and malicious sites and content before the Internet Protocol (IP) connections are established. DNS Safeguard is powered by Cisco and enhanced with threat intelligence feeds from the Verizon Threat Research Advisory Center which, learning from internet activity patterns, automatically uncovers current and emerging threats to continually keep the network safe.

The DNS Safeguard platform operates as a DNS resolver that converts domain names to IP addresses which allows the platform to prevent IP connections to known malicious sites. When a legitimate domain is resolved, the DNS Service returns the actual IP address. When a malicious domain is resolved, the DNS Service returns a safe IP address that goes to a landing page that lets the user know the reason the site was blocked. Customers may also configure settings based on risk tolerance (high, medium or low) and categories. Internet data is routed to an Open DNS server based upon Border Gateway Protocol (BGP) routing decisions, which are dynamic, based on providing the most efficient route. If one data center is experiencing downtime or latency, the data will be routed to the next closest data center.

- 1.2 **Basic Service Features.** The following service features are included with DNS Safeguard Basic:
 - 1.2.1 **DNS Layer of Breach Protection.** DNS Safeguard is able to detect and block malicious sites and content before they reach the network as a DNS request is made before IP connections are established. Malware, ransomware, phishing, spyware, botnets, and command & control call-backs are blocked over any port or protocol before such threats can reach users and network.
 - 1.2.2 **Web Content Filtering.** To control internet usage, the DNS Safeguard web portal administration console enables set up, manage, and test of different acceptable use policies with selections from over 60 categories or blocking/allowing individual domains through the black/white list.
 - 1.2.3 **Off-Network Protection.** Off-Network Protection provides DNS Safeguard security and policy-based protection to be enforced on Customer end user computers for any network connection by using a lightweight DNS roaming client that runs on either Windows or Mac OSX. Enabling the Off-Network



Protection feature is done via installation of roaming client software directly on the connected Customer end user computer, installation of Cisco's Security Connector for iOS mobile devices, or by using Cisco's AnyConnect VPN client a module.

1.2.4 **Internet-Wide Visibility.** The DNS Safeguard web portal provides a log of all internet activity in real-time through dashboards and downloadable reports. Data is categorized by type of security threat, web content, or cloud service, and enables remediation action.

1.2.5 **Verizon's Threat Research Advisory Center.** DNS Safeguard includes the Verizon Threat Research Advisory Center's display of all threat analytics and intelligence gathered through proprietary and open source data and Verizon internal data for global threat landscape capabilities.

1.3 **Premium Service Features.** The following service features are included with DNS Safeguard Premium. DNS Safeguard Premium also includes the Basic Service features and functionality.

1.3.1 **Active Directory Integration.** Active Directory Integration enables Customer to define separate user groups and synchronize user-to-group, computer-to-group and group-to-group memberships, from which Customers may create and enforce group-based settings and to tailor different security policies for each defined group.

1.3.2 **Enhanced Intelligent Proxy.** Enhanced enforcement capabilities via the intelligent proxy provide the ability to customize blocked URLs list at the page level and file inspection adds the ability to scan files for malicious content hosted on suspicious domains.

1.3.3 **Intelligent Proxy.** With Intelligent Proxy, only web connections to partially malicious or suspicious domains are routed through the platform for deeper inspection, providing a more responsive network to the broad range of safe locations.

1.3.4. **Granular Reporting.** The Premium Service Features support web traffic audits and reporting which tieback to both specific network users and devices for both the Active Directory Integration and Off-Network Protection features. Such reporting provides Customer a means to determine the entry points of malicious content, as well as assisting in understanding the flow of such content throughout a network to identify downstream systems that may be compromised.

1.4 **Service Activation and Implementation**

1.4.1 **Service Activation.** The DNS Service Activation Date is 10 Business Days following the Order Confirmation Date.

1.4.2 **Implementation of Service.** Once DNS Service is activated, the Authorized Contact or Delegated Admin assigned a Full Admin Role is responsible for completing all required configuration and customizations directly within the DNS Service portal. For the Premium Service Features, there will be additional configuration steps that need to be completed outside of the DNS Service portal.

- Change DNS server setting to point to Verizon DNS Safeguard platform;
- Login to the DNS Safeguard portal and perform the following configurations:
 - Add Customer network onto the portal and input public IP Address(es);
 - Configure security setting and turn on any additional security measures; and,
 - Configure category setting and select level of content filtering for your users (optional).
- If applicable, set up of Premium Service Features
 - Active Directory Integration
 - Roaming/Off-Network

2. SUPPLEMENTAL TERMS



2.1 Services Agreement Flow Down Terms

2.1.1 **Acceptance of Terms.** From time to time, Verizon may update the functionality and User Interface of the DNS Services, add new features to the DNS Service, and/or change the access configuration for the DNS Services. In such event, these terms shall also apply to any upgrades or updates subsequently provided by Verizon for the DNS Services.

2.1.2 **Use of the DNS Services.** Customer accepts the non-assignable, non-transferable, non-sublicensable, and non-exclusive right to access and use the DNS Service only as authorized in this Agreement and related documentation for the duration of the Service Commitment and for the number of licenses purchased by and allocated to Customer.

2.2 Customer Responsibilities

2.2.1 **Internet Access.** Customer must have internet access in place to use DNS Safeguard.

2.2.2 **User Interface.** In connection with the provision of DNS Service, Verizon may provide Customer with one or more user Logins to access a User Interface. Customer will at all times keep its Login strictly confidential and will take all reasonable precautions to prevent unauthorized use, misuse or compromise of its Login. Customer agrees to notify Verizon promptly upon learning of any actual or threatened unauthorized use, misuse, or compromise of its Login. Verizon is entitled to rely on Customer's Login as conclusive evidence of identity and authority. Customer will be liable for all activities and charges incurred through the use of Customer's Login, and will indemnify, defend and hold Verizon harmless from all liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) incurred by Verizon to the extent resulting from the use and/or compromise of Customer's Login, unless the unauthorized use, misuse or compromise of Customer's Login is solely attributable to Verizon's gross negligence or willful misconduct.

2.2.3 **Prohibited Use.** Customer will not: (i) use the Services for any unlawful, unauthorized, fraudulent or malicious purpose, (ii) modify, adapt, sublicense, translate, sell, reverse engineer, decompile or disassemble any portion of the Services (except to the limited extent applicable laws specifically prohibit such restriction); (iii) bypass any measures Verizon may use to prevent or restrict access to the Services or otherwise interfere with any other party's use and enjoyment of the Services; or (iv) use Customer's account or the Services to infringe any intellectual property or other right of any other third party. Verizon may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Subject to Verizon's Privacy Policy, Verizon reserves the right at all times to disclose any information as Verizon deems necessary to satisfy any applicable law, regulation, legal process or governmental request, or to edit, refuse to post or to remove any information or materials, in whole or in part, in Verizon's sole discretion.

2.3 Warranties

2.3.1 **Verizon's Disclaimer of Warranties.** Verizon does not warrant that any network, computer systems, or any portions thereof, are secure. Verizon does not warrant that use of DNS Service will be uninterrupted or error-free or that any defect in DNS Service will be correctable or that incidents will be fully contained. Customer acknowledges that impenetrable security cannot be attained in real-world environments and that Verizon does not guarantee protection against breaches of security, or the finding or successful prosecution of individuals obtaining unauthorized access. Verizon does not warrant the accuracy of information provided to Customer hereunder.

CUSTOMER'S USE OF THE DNS SERVICES IS AT CUSTOMER'S SOLE RISK. ALL DNS SERVICES ARE PROVIDED ON AN AS IS OR AS AVAILABLE BASIS, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERIZON EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT



LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND SATISFACTORY QUALITY. VERIZON, ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, OR SUPPLIERS MAKE NO WARRANTY THAT THE SERVICES ARE ACCURATE, TIMELY, UNINTERRUPTED, VIRUS-FREE OR ERROR-FREE, OR THAT ANY PROBLEMS ENCOUNTERED WILL BE CORRECTED. THE WARRANTIES AND REMEDIES SET FORTH IN THIS SERVICE ATTACHMENT ARE VERIZON'S EXCLUSIVE WARRANTIES AND CUSTOMER'S SOLE REMEDIES FOR BREACH OF WARRANTY, IF ANY, BY VERIZON.

2.3.2 Customer Warranty. Customer represents and warrants that Customer (a) has and will continue to have all rights, power, permissions and authority necessary to have Verizon provide DNS Service services including, without limitation, consent of all authorized network end users located in the European Union (EU) or other countries and where applicable (i) consulting all European Works Councils with respect to the operation of the DNS Service for EU based end users, and (ii) complying with all Data Protection regulators notifications and/or registration obligations with respect to the operation of the DNS Service for all end users; (b) will use the DNS Safeguard services, including all reporting, deliverables, documentation, and other information provided in connection with DNS Service solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use or access to its information, systems and applications including public internet service provided by Verizon and Customer will not market, sell, distribute, lease, license or use any such deliverables, documentation or information for any other purposes; and (c) will comply with all applicable laws and regulations. Customer will indemnify and hold harmless Verizon from any end user or other third party claims related to these Customer warranties.

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

2.4 Use of Data. As part of Customer's use of the Services, Customer will be providing certain (i) Network Data, (ii) User Data and/or Feedback. Some Network Data is necessary for the essential use and functionality of the Services. Network Data is also used to provide associated services such as technical support and to continually improve the operation, security, efficacy and functionality of the Services.

2.4.1 User Data. Customer grants Verizon a worldwide, royalty-free, sublicensable license to use, modify, reproduce, publicly display, publicly perform, and distribute the User Data only as reasonably required to provide the Service.

2.4.2 Network Data. Customer hereby grants to Verizon a non-exclusive, irrevocable, worldwide, perpetual, royalty-free and fully paid-up license to use (i) the Network Data that is aggregated and de-identified so that it does not identify Customer for the purpose of enhancement of the Services, and (ii) any information that Verizon learns in evaluating Network Data to create the Statistical Data for the purpose of enhancing, developing, and/or promoting the Services.

2.4.3 Feedback. De-identified Feedback may be incorporated into the Services, and Customer hereby grants Verizon a non-exclusive, irrevocable, worldwide, perpetual, royalty-free and fully paid-up license to use de-identified Feedback for any purpose whatsoever, including, without limitation, for purposes of enhancing, developing and/or promoting products and services, including the Services.

2.5 Term and Termination

2.5.1 Service Commitment. The Service Commitment is for a one-year term, two-year term, three-year term, or five-year term.



2.5.2 **Order Cancellation.** If Customer requests cancellation of Service, or Verizon cancels Service as a result of Customer’s failure to provide the necessary information or reasonable assistance required by Verizon to provision such Service, Customer will pay any set-up fees and other amounts accrued for such Service through the date of such termination, plus an amount equal to any applicable annual third party license fee, which Customer acknowledges are liquidated damages reflecting a reasonable measure of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.5.3 **Service Termination.** Customer accepts and agrees that, in the event (i) Customer terminates any order for convenience or (ii) Verizon terminates any order for Cause prior to the end of the Service Commitment, then Customer will pay Verizon Early Termination Charges and any applicable annual third party license fee, which Customer acknowledges are liquidated damages reflecting a reasonable measure of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

3. SERVICE LEVEL AGREEMENT

3.1 **Service Level Description.** The following Service Level Agreement (SLA) applies to the DNS Service:

Service Level Description	SLA
Global DNS Safeguard availability	99.999%

3.2 **Credits.** Customer will receive a credit for the pro-rated charges for one day of the monthly recurring charge for the service with respect to which availability SLA has not been met. Customer must request the calculation of DNS Safeguard Unavailability and request the credit.

4. FINANCIAL TERMS

4.1 **General.** Customer will pay the applicable monthly recurring charge (MRC) for the Service Tier ordered, as shown in the Agreement and other applicable charges at the following URL: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm.

4.2 **Early Termination Charges.** Customer will pay the applicable Early Termination Charges specified in the Agreement.

5. **DEFINITIONS.** The following definitions apply to DNS Service, in addition to those identified in the Master Terms and the administrative charge definitions at the following URL: www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm

Term	Definition
Authorized Contacts	Customer personnel authorized by Customer to access the product portal and to interact with Verizon for the DNS Service.
Delegated Admin	Customer personnel authorized by Customer to access the product portal and assigned a role. Roles can be assigned to any Customer account to grant limited access to sections of the DNS Safeguard portal.
Feedback	Any suggested changes, clarifications, additions, modifications or recommended product improvements to the Services that Customer provides as part of technical support or otherwise by direct entry into a product user interface, phone conversation, email or otherwise.
Full Admin Role	DNS Safeguard portal role which permits a Delegated Admin to access everything in the DNS Safeguard Customer portal.
Login	IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.



Network Data	Any technical data and related information about Customer's computer network generated as part of Customer's usage of the Services, including, but not limited to the operating system type and version; network host data; origin and nature of malware, endpoint GUID's (globally unique identifiers); IP addresses; MAC addresses; log files; network configurations; network security policies; information related to the usage, origin of use, traffic patterns, and behavior of the users on a network; and any aggregate, demographic or network traffic data.
Order Confirmation Date	Verizon will confirm Customer's order via email and the date of this email is the Order Confirmation Date. The Order Confirmation will confirm the DNS Service service(s) requested.
Service Tier	The number of users within an organization.
Statistical Data	Any information or data that is created from the Network Data, provided that such information or data is aggregated and de-identified or otherwise cannot be used to identify Customer's network.
User Data	All information and materials, including personal information, that Customer provides in connection with Customer's use of the Services, but does not include Network Data.
User Interface	A web-based portal, dashboard, or other electronic means to share information and reports with Customers that pertains to Security Incidents that are identified and escalated to Customer.