verizon

SECURELOGIX +

1. GENERAL

1.1 **Service Definition.** SecureLogix provides security to the voice traffic of Customer sites through analysis, verification and authentication of call traffic. Depending on Customer's Order, SecureLogix may include software, managed services, cloud deployment and/or hosting through SecureLogix Call Defense™ or Orchestra One™ Call Authentication systems (individually a "Product" or a "Service" and collectively the "System") provided by SecureLogix through Verizon. Customer's SecureLogix solution will be documented by Verizon in a solution-specific Playbook as provided below.

1.2 **Standard Features.**

1.2.1 **Call Defense™ System.** The Call Defense System is deployed and positioned at the edge of the Customer's voice network to address robocalls and harassing callers. Components of the Call Defense System include a Voice Firewall, voice Intrusion Prevention System (IPS), a malicious callers database (Red List), and forensic reporting. Call Defense also helps secure Customer's voice infrastructure from more serious threats, such as telephony denial of service, toll fraud, and call pumping. It provides visibility and control of incoming and outgoing voice calls and includes an ability to implement and update voice security policies. Call Defense may be deployed as Enterprise Telephony Manager or PolicyGuru.

1.2.1.1 **Enterprise Telephony Manager.** Enterprise Telephony Manager (ETM) applications continuously patrol all signaling and bearer traffic, and use an expandable policy engine to examine calls and take actions based upon user defined rules. ETM supports a variety of hardware platforms, VoIP protocol and can be deployed in various configurations and hardware.

1.2.1.2 **PolicyGuru.** PolicyGuru (PG) monitors SIP signaling to provide visibility and call access control of activity across your enterprise voice/UC network. Centrally managed policy rules are distributed across the network to specify whether calls are allowed as dialed, terminated before call setup, or redirected to a different destination.

1.2.1.3 **Call Secure™ Managed Services.** Call Secure managed services provides the management of the Call Defense System, and works with Customer to optimize the Call Defense service.

1.2.2 **Orchestra One™ Call Authentication.** Orchestra One is a cloud-based subscription service that dynamically orchestrates the call authentication process using a variety of metadata services to assign a risk scoring matrix for incoming voice traffic from automated call authentication and spoofing detection through analysis of the incoming call invite. Orchestra One can be configured to interface with Call Defense or Conductor Virtual Appliance software to execute security policies based upon risk scores assigned to calls. The Conductor Virtual Appliance can also store and employ for policy execution customer-specific phone number blacklists.

1.2.2.1 **Standard Authentication.** Standard authentication is the base subscription for validation leveraging the Orchestra One Application Programming Interface (API).

- **Level 1.** With Level 1 authentication, low-cost metadata, industry, and proprietary data sources are leveraged to complete the SIP analysis.
- **Level 2.** In addition to the Level 1 data sources, Level 2 uses additional sources, including STIR/SHAKEN, and recent porting data.

1.2.2.2 **Advanced Authentication.** Advance authentication is additional incoming call authentication using wireless carrier APIs to confirm that (i) a number is registered to that carrier and (ii) that number is engaged in an outbound call to the destination number registered for Advanced Authentication.

1.2.2.3 **External Authentication.** External authentication allows for additional authentication data sets that can be incorporated to the overall risk score returned on selected inbound calls.

1.2.2.4 **Conductor Virtual Appliance.** The Conductor Virtual Appliance is an optional virtual appliance that Customer can select as the mechanism to query the Orchestra One API solution and execute security policies to reject and/or redirect calls based upon risk scores assigned by Orchestra One or customer-specific phone number blacklists.

1.2.2.5 **Managed Services for Conductor.** Managed Services for conductor provides management of The Conductor Virtual Appliance and is required with any purchase of the Conductor Virtual Appliance.

1.3 **Implementation.** Site survey and testing plans vary according to subscribed services.

1.3.1 **Site Survey.** Verizon will conduct a remote survey via conference calls or web meetings to capture necessary installation details (e.g., rack space, electrical power, network connectivity, and telco circuit technical details as applicable). Verizon will document these details in the Playbook and use them to identify all Customer Site preparation details prior to installation.

1.3.2 **Implementation and Configuration Services.** Verizon will remotely configure each virtual appliance to monitor voice traffic. This includes configuring Customer's ordered service for use and connecting to the SecureLogix platform to assure Verizon is able to remotely access system data. At the conclusion of the implementation services Verizon will provide documentation of Customer's solution via the Playbook.

1.3.3 **Testing.** Verizon will perform standard testing of Customer's System to validate that the Customer's system meets Verizon's implementation standards and is ready for use. After testing, Verizon will submit written notification of the testing and a summary of the test results to Customer (Test Completion Notice).

1.3.4 **Customer Acceptance Process.** Customer will have 5 business days after its receipt of the Test Completion Notice to indicate, in writing, whether any System implementation or Service defects have been found. If defects have been found, Verizon shall (i) investigate and respond in writing to Customer's concerns, and (ii) promptly remediate any material defect in its performance of the implementation. Customer Acceptance of the System shall occur upon the remediation of any material defect to the System or will be deemed to have occurred If Customer does not respond to a Test Completion Notice within 5 business days.

1.3.5 **Onboarding for Managed Services.** Upon Customer Acceptance, Verizon will assign an Onboarding Lead to coordinate and execute Managed Services onboarding. This includes the following:

- Schedule and lead a conference call with Customer to formally transition the project into the managed services and establish a schedule for Managed Services onboarding tasks;
- Perform Managed Services start-up tasks, including configuration and tuning of Customer's System to support the Managed Services, populating key data sets, and configuring the monitoring alarms and

alerts, as appropriate, to be delivered to Customer;
- Conduct a comprehensive analysis of baseline reports to determine Customer's normal traffic patterns and establish initial recommendations for alert thresholds, as appropriate, and security policies provided under the Managed Services;
- Conduct a presentation to Customer of findings and guided instruction on how to interpret the data elements in the Automated Monthly Report, as appropriate; and
- Hold regular conference calls during Onboarding to review project status.

1.3.6 **Other Services.** If necessary, a fixed number of hours may be required over and above the standard implementation cost shown in the SOF for Customer work or other work outside of the standard implementation parameters as shown in the site survey. Such services/hours will be agreed upon by both Parties.

2. SUPPLEMENTAL TERMS

2.1 Customer Responsibilities

2.1.1 **Implementation Support.** Customer must ensure that necessary technicians, configuration information, and responsible contacts are made available to access, support, operate and troubleshoot the implementation of the solution, as required. This may include, but is not limited to, any network and security infrastructure (routers, firewalls, etc.), voice infrastructure (PBX, SBC, etc.), and any servers or virtual machines that are required for the installation, management and use of the solution.

2.1.2 **Solution Lifecycle Maintenance.** Customer must ensure that any required access Verizon requires to systems to support the ongoing management is maintained and that the Customer provides necessary contacts to support the solution.

2.1.3 **Managed Services.** Customers must ensure that there is a primary point of contact (POC) that is available for regular communications including any alerts or policy updates and any regular status meetings. Such POC should have the ability to engage other Customer resources as necessary.

3. **SERVICE LEVEL AGREEMENT.** The Service Level Agreement (SLAs) for the Services is set forth at www.verizon.com/business/service_guide/reg/SecureLogix-SLA.pdf.

4. FINANCIAL TERMS

4.1 **Service Charges.** Customer will pay the charges for SecureLogix are set forth in the Agreement, or in the Customer's Service Order Form ("SOF"), as applicable and at the following URL: www.verizon.com/business/service_guide/reg/applicable_charges_toc.htm.

4.1.1 **Implementation.** The Implementation NRC is provided on the SOF.

4.1.2 **Activation Date.** The Activation Date is the date that Customer Acceptance has been provided for Orchestra One Implementation, Call Secure Managed Services, and/or related Call Defense System Implementation.

4.1.3 **Destination Management Fee.** The destination management fee is applied for the registration and maintenance of the set of destination telephone numbers.

4.1.4 **License Subscriptions.** Customer may order a 1, 2, or 3-year subscription term which will be billed on a monthly or annual basis, based on Customer's choice. The charge will be based on the term and the Service volume commitment.

4.1.4.1 **Overage Charges.** If the quantity of calls exceeds the volume commitment (overage), Verizon will true up the volume on a monthly or annual basis, following Customer's chosen billing term, and charge the Overage Rate set forth in the SOF.

5. **DEFINITIONS.** The following definitions apply to the SecureLogix service in addition to those identified in the Master Terms of your Agreement and the administrative charge at the following URL: www.verizon.com/business/service_guide/reg/definitions_toc_2017DEC01.htm.

Term	Definition
Intrusion prevention system or IPS	IPS is the group of policies that define thresholds for count or cumulative duration of suspect calling patterns, that systematically alert for investigation.
Playbook	The Playbook is the solution documentation used to conduct the initial Site Survey and provide configuration details post-implementation
Voice Firewall	Voice Firewall is the group of policies that include a white list (allow) and blacklists (log, alert, block, or redirect) depending on end user preferences.