SECURELOGIX +

1. GENERAL

1.1 **Service Definition.** SecureLogix can provide both inbound and outbound call security and assurance. The individual inbound or outbound elements are referred to herein as a "Service" and collectively, they are referred to as the "System."

1.1.1 **Inbound.** SecureLogix provides security to the inbound 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 provided by SecureLogix through Verizon. Customer's SecureLogix solution will be documented in a solution-specific Playbook as provided below.

1.1.2 **Outbound.** SecureLogix provides assurance to the outbound voice traffic of Customer through call branding capabilities, spoofing protection, and reputation management capabilities. Depending on Customer's Order, SecureLogix may include software, managed services, cloud deployment and/or hosting though SecureLogix Contact Call Branding^{TM}, TrueCall™ Spoofing Protection, and Reputation Defense™ Call Number Management systems provided by SecureLogix through Verizon.

1.2 **Standard Features.**

1.2.1 **Inbound**

1.2.1.1 **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.

- **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.

- **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.

- **Cloud Voice Security.** Cloud Voice Security is a fully cloud-based solution that includes our voice firewall and Intrusion Prevention System (IPS) application services to secure inbound call traffic.

1.2.1.2 **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**.**

1.2.1.3 **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 Customer-specific phone number lists for policy execution.

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

- **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. Certain wireless carriers require an additional agreement for access to their API. Verizon will help facilitate such agreement as required.

- **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 Outbound

1.2.2.1 **Contact Call Branding^{TM}.** Contact Call Branding is a subscription service that allows Customer to brand calls to be received by mobile phones of the wireless carriers shown on the Customer's Order by displaying an up-to-date name, as part of the CallerID, subject to the capabilities of the destination mobile phone.

1.2.2.2 **Managed Service Contact Call Branding Service**. SecureLogix will provide:

- The ongoing management of Customer's registered calling numbers with the branded calling providers.
- Continual updates to the branded calling providers based on Customer's request to add, delete, or change phone numbers to be branded.

- Standard, consolidated monthly reports. Verizon can provide ad-hoc reports, if available, upon request.

1.2.2.3 **TrueCall™ Spoofing Protection.** TrueCall Spoofing Protection is a subscription service that integrates with the wireless carriers shown on the Customer's Order and their call analytics vendors to label and/or block any spoofed calls using Customer calling numbers. It detects Customer's legitimate outbound calls and sends authentication to call the relevant analytics vendor while the call is being made. If a call has not been authenticated (i.e., a Customer calling number is being spoofed) the call can be labeled by the analytics vendor as possible fraud or blocked. TrueCall may be deployed with Conductor Virtual Appliance, Cloud Enablement, or Customer may integrate with their own RestFUL API client.

1.2.2.4 **Managed Service TrueCall Spoof Protection Service.** SecureLogix will provide registration and ongoing management of Customer's list of maximum calling numbers with spoof protection providers. SecureLogix will implement and manage caller profiles, calling policies, and notify each spoof protection provider when Customer is planning an outbound calling campaign to ensure calls are delivered and labeled properly. SecureLogix will continually monitor the calling numbers to provide that calls are processed appropriately. SecureLogix will provide consolidated reporting across all spoof protection providers.

1.2.2.5 **Reputation Defense™ Call Number Management.** Reputation Defense is a subscription service that actively monitors and redresses issues of Customer calling numbers that receive a negative reputation. The service works with the call analytics vendors of major wireless carriers to get updates to determine if a Customer's number gets into a negative state and works to clean and restore the reputation score.

1.2.3 **Inbound and Outbound Standard Features.**

1.2.3.1 **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.

- **Managed Services for Conductor.** Managed Services for Conductor provides management of the Conductor Virtual Appliance and is included with any purchase of the Conductor Virtual Appliance.

1.2.3.2 **Cloud Enablement.** The Cloud Enablement service enables routing and management of sessions to support other services such as TrueCall Spoofing Protection.

1.3 <u>Implementation and Configuration</u>.

1.3.1 PolicyGuru, ETM, and Conductor.

1.3.1.1 **Site Survey.** SecureLogix 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). SecureLogix will document these details in the Playbook and use them to identify all Customer Site preparation details prior to installation.

1.3.1.2 **Implementation.** SecureLogix 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 SecureLogix is able to remotely access system data. At the conclusion of the implementation services SecureLogix will provide documentation of Customer's solution via the Playbook.

1.3.2 **Cloud Voice Security (CVS).** Verizon will coordinate meetings for the following onboarding services between Customer and SecureLogix, who will provide the cloud SIP trunk connection:

- Planning call to gather telephony and networking requirements and to fill out the implementation questionnaire.
- Design of implementation (including routing, SIP and telephony-related parameters, security considerations, etc.).
- Develop test plan and configuration and test of the connection.

SecureLogix shall manage configuration and testing of CVS, including initial configuration of CVS, to include minimal requirements to accomplish the installation and testing.

1.3.3 **Orchestra One Call Authentication.** SecureLogix will provide administrative services and recommendations for the integration related to Orchestra One Call Authentication based on Customer's requirements. SecureLogix tasks shall include the following:

- **Conductor Orchestra One Authentication Routing.** SecureLogix will create new or edit existing Orchestra One authentication score routes based on the requirements specified in the Customer's request(s). Import or edit destination and strategy lists based on the requirements specified in the Customer's request(s).
- **Negative Value Callers List (NVCL) Management.** SecureLogix will install and update the NVCL as required.
- **Advanced Orchestra One Carrier Call Authentication.** SecureLogix will register Customer's destination numbers with the major wireless carriers as ordered.

1.3.4 **Contact Call Branding, TrueCall Spoofing Protection, and Reputation Defense** - SecureLogix will register Customer calling numbers with call analytics vendors.

- **Contact Call Branding** - SecureLogix will also work with Customer and the call analytics vendors on labeling policies.
- **TrueCall Spoofing Protection -** SecureLogix will confirm the architecture based upon the Customer's environment. Once an architecture design is finalized, the system is implemented based on the approved design. Initial testing will include testing the authentication of calls with the data analytics vendor(s). During this initial testing, Customer will place an outbound call and confirm that the call is authenticated through Orchestra One and the API for the appropriate data analytics vendor.

1.3.5 **Cloud Enablement**. SecureLogix will onboard Customer with analytics vendors, project manage implementation, and validate call processing.

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

- **Contact Call Branding, TrueCall Spoofing Protection, and Reputation Defense.** SecureLogix will work with Customer and call analytics vendors to ensure call labeling is correct.

1.5 **<u>Customer Acceptance Process</u>.** 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 and reported, SecureLogix 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.

1.6 **Onboarding for Managed Services.** Upon Customer Acceptance, SecureLogix 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 monthly reports, as appropriate; and
- Hold regular conference calls during Onboarding to review project status.

1.7 **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 **<u>Customer Responsibilities</u>.**

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 SecureLogix 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 https://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.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm.

4.1.1 **Implementation.** The Implementation Non-Recurring Charge (NRC) is provided on the SOF.

4.1.2 **Activation Date.** For SecureLogix services, the Activation Date is the date of Customer Acceptance.

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 as a Monthly Recurring Charge (MRC) or an Annually Recurring Charge (ARC). The charge will be based on the term and the Service volume commitment. Outbound service must be reordered at the end of the subscription term or the service will be discontinued.

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, as applicable, and charge the Overage Rate set forth in the SOF. When the annual prepay model is selected for services with a monthly volume commitment, overages will not be charged for an overage in an individual month, but will only be incurred when 12 times the monthly volume commitment has been exceeded within the subscription term.

4.1.5 **Auto-Renewal.** The Service Commitment period for inbound services will auto-renew for 1 year periods at the end of the then current Service Commitment period unless Customer provides written notice of non-renewal at least 60 days prior to the end of then then Service Commitment period at which point the Agreement will terminate at the end of the current Service Agreement. Outbound services to not auto-renew and must be reordered.

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.verizonenterprise.com/external/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.
Managed Services	Managed Services are applicable to Call Secure, Contact Call Branding Service, TrueCall Spoof Protection Service, and Conductor.
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.

© 2022, 2024 Verizon. All Rights Reserved.