DATA SHEET

Force Field™

Call Security Managed Service for the PolicyGuru® Platform

PRODUCT OVERVIEW

The SecureLogix® PolicyGuru® Meta-Policy Controller provides policy-based call-access control security and monitoring for large enterprise SIP deployments, including centralized SIP, without the need for another device inline on the voice network. While the solution can be deployed on any size of SIP network, it scales for very high-volume environments.

The PolicyGuru System interfaces with SBCs that support the ENUM protocol with the Kaplan extension. The solution is not inline, but rather receives the important call data (source, destination, and direction) from the ENUM request and then returns the security policy decision for routing the call to the SBC—allow as dialed, redirect to an alternate destination, or terminate prior to call setup.

The PolicyGuru System is typically deployed with the SecureLogix® Force Field™ Call Security Managed Service, which provides many additional features and benefits in addition to those described below. If a customer chooses not to use the managed service, the following features and benefits are available.

FEATURES & BENEFITS

Voice Intrusion Prevention System (IPS) Policy Management

Unique calling patterns can indicate TDoS attacks, international toll fraud, misuse / abuse, and other issues of concern. IPS Policy defines thresholds for count or cumulative duration of suspect calling patterns. When a threshold is exceeded, alerts are automatically generated to initiate investigation and mitigation of the threat.

As part of the managed service, SecureLogix voice security experts develop, implement, and manage an IPS Policy to address aspects of voice network security such as TDoS and toll fraud mitigation. SecureLogix security professionals continuously monitor Voice IPS alerts and notify the customer when threats are identified.

In the event of an ongoing threat, SecureLogix security experts provide incident response to deploy additional policies to mitigate threats in real time as they evolve.

Voice Firewall Policy Management

Firewall Policy enforces real-time voice security policy for individual telephone calls across the enterprise. SecureLogix security experts develop, implement, and manage a Firewall Policy, including the management of white lists (allow) and blacklists (log, alert, block, redirect). As part of the service, SecureLogix creates a policy rule to enforce the SecureLogix proprietary blacklist of nuisance robocallers and source numbers associated with fraudulent activities, which is updated at least monthly. The service also includes a Voice Firewall Policy rule to enforce a customer-specific harassing/unwanted callers rule. And since many organizations have concerns about calls to or from specific countries, the PolicyGuru Solution managed service can support an organization's compliance program by monitoring, alerting, blocking, or redirecting calls to or from specific countries of interest.

Features & Benefits continued on next page

FEATURES & BENEFITS *continued*

Call Traffic Anomaly Analysis

Voice security threats are constantly evolving and adapting to countermeasures. Ongoing call traffic analysis by voice security experts is an important part of an organization's risk management and compliance policies. SecureLogix has developed proprietary automated analysis methods and will continue to evolve those tools. The managed service includes:

- Weekly automated traffic analysis searching for anomalous call traffic
- Events that appears to be security or fraud threats and other noteworthy situations are brought to the customer's attention so they can be addressed.

Enterprise-Wide Reporting with Actionable Analytics

A monthly summary report provides detailed, actionable analytics including call pattern trends for several key toll fraud and security elements, along with a percentage change from last month, top callers, and top call detail records. Customers can also request additional ad-hoc or scheduled reports for areas of specific interest to them. Up to 13 months of call and policy enforcement data is stored in the relational database for reporting and analysis.

Continuous System Health and Status Monitoring

The PolicyGuru System is an important part of your security and compliance infrastructure, so system availability is critical. Expert SecureLogix technical support and security professionals continuously monitor all the deployed production PolicyGuru System elements at the host level, as well as monitoring the PolicyGuru services and applications and providing proactive Technical Support in the event that faults are detected.

PolicyGuru® System Management and Administration

SecureLogix personnel provide management and administration of the production PolicyGuru System, including the PolicyGuru Mediation Server and associated SecureLogix product operation, administration, and management, remote installation of PolicyGuru software upgrades, and maintenance of key data sources such as lists and dialing plans.

KEY USE CASES

TDoS Mitigation

TDoS is a flood of inbound calls that consumes telephony resources to the point where business operations are adversely affected. In the case of a large-scale event, TDoS can affect the organization's entire trunk resources. Conversely, a small-scale yet highly focused attack could disable a critical business function. TDoS events can result in the inability of legitimate callers to reach the organization due to the consumption of limited trunk resources, or the attackers can tie up a limited number of customer representatives, causing legitimate callers to sit on hold for an excessive length of time. SecureLogix continuously monitors inbound call volume, receives notification of potential TDoS events, conducts forensic analysis to determine whether a TDoS event is underway, and if so, provides incident response to mitigate the attack in progress.

Harassing Caller Mitigation

Every organization receives unwanted calls from harassing, malicious, or abusive callers. While company executives are often the primary target, harassing calls can be a significant problem for many other employees in the organization. SecureLogix creates and maintains a customer-provided blacklist of harassing callers and adds numbers to the list upon customer request. This list is used in Firewall Rule to block inbound calls from numbers in the list.

Nuisance Call Mitigation

Inbound robocalls can simply be a nuisance that results in a minor productivity issue. However, in extreme cases, the volume of robocalls can reach the point where there is some financial impact and adverse consumption of trunk resources. SecureLogix maintains a proprietary list of common nuisance callers collected across all our managed service customers and other sources and implements a Firewall Policy Rule to monitor for these calls, periodically reports the top offenders, and places those numbers in a customer-specific nuisance callers blacklist in a Firewall Rule to be blocked.

Key Use Cases continued on next page

KEY USE CASES *continued*

Toll Fraud Mitigation

Excessive counts of outbound international calls can indicate toll fraud. SecureLogix monitors aggregate outbound international call volume, receives notification of possible toll fraud events, conducts forensic analysis to determine whether a toll fraud event is underway, and if so, provides incident response to mitigate the event.

Countries of Interest Management

A monthly summary report provides detailed, actionable analytics including call pattern trends for several key toll fraud and security elements, along with a percentage change from last month, top callers, and top call detail records. Customers can also request additional ad-hoc or scheduled reports for areas of specific interest to them. Up to 13 months of call and policy enforcement data is stored in the relational database for reporting and analysis.

800-817-4837
securelogix.com