DATA SHEET

ETM® System

PRODUCT OVERVIEW

Enterprises need strong security against the growing tide of attacks and other threats against their business-critical voice network resources. The increase in such attacks has been well documented by the FBI and DHS over the past few years. These include Telephony Denial of Service (TDoS), financial fraud / social engineering, toll fraud, harassing calls, voice spam, and voice phishing (vishing), and other forms of threats and misuse / abuse, such as internal abuse of outbound toll services, unauthorized access to voice systems, and large-scale outsider theft of outbound toll services via compromised IP-PBXs or voice gateways.

- High-profile service outages (TDoS attacks)
- Loss of contact center uptime and impaired customer response times / satisfaction (TDoS attacks and negative-value calls)
- Financial fraud against the enterprise and / or its customers (social engineering and other fraud schemes)
- Financial exposure from theft and / or abuse of toll service (external and internal)
- Loss of safety and business productivity (harassing and malicious calls)

Protection against these types of voice security attacks requires the ability to dynamically identify abnormal or unusual patterns of calls based on the underlying metadata of each active call. Real-time analysis of this metadata, in turn, requires a mechanism to dynamically define voice security policies, in order to rapidly modify the metadata analysis and thereby adapt to new voice network attack strategies as they evolve.

Indeed, when an enterprise voice network is being attacked, the perpetrator will often modify his attack strategy while the attack is in progress to make it more difficult to protect against. The sophistication of malicious voice network attacks has grown dramatically in recent years as the perpetrators develop increasingly advanced tools to execute their voice network attacks. As such, voice security policies protecting the enterprise voice network against such attacks must be at least as sophisticated and dynamic to identify and adapt to changing patterns of malicious calls.

Traditional IP firewalls or Session Border Controllers (SBCs / eSBCs), on their own cannot adequately support such dynamic voice security policies, as they are statically configured to provide stability and reliability of the voice network session control and routing. At best, they provide static blacklists to block incoming calls. But, manually maintained, static blacklists are totally inadequate defense against the sophisticated voice network attacks that now commonly occur.

The SecureLogix ETM® System provides universal, real-time, adaptive voice policy-based security that integrates with existing telecom equipment, including all brands of SBCs, gateways, and IP-PBXs, to allow your enterprise to manage and mitigate the voice security threats that, if ignored, could cripple the voice network essential to the success of your business operations.

FEATURES & BENEFITS

Real-Time Policy-Based Call Control and Alerting

The policy-based ETM Voice Firewall examines each TDM or VoIP call on the voice network to determine which calls are allowed to pass through, which are denied access, and what alerting occurs when a call matches a policy rule. Each voice policy rule is defined to look for any combination of source, destination, call direction, type of call, DTMF digit pattern, call duration, and / or specific call times.

The policy-based ETM Voice Intrusion Prevention System (IPS) provides real-time detection, alerting, and prevention of threatening or abusive call patterns that can indicate international toll fraud, TDoS attacks, and other suspicious or anomalous traffic. Voice IPS policies allow you to establish thresholds for a variety of service types, such as outbound international calls, and for specified call count thresholds from known or unknown source numbers, accumulated call duration, accrued toll charges, and mid-call DTMF digit patterns.

Policy-Based Call Recording of Calls of Interest

The ETM Call Recorder provides policy-based recording of the audio of targeted calls of interest for security and quality assurance; no user intervention is needed to begin recording—recording begins automatically at the start of a call for the specified extension(s)s and call direction.

Enterprise-Wide Visibility

Enterprise-wide reporting provides visibility and actionable data. All call data, security tracking, and monitoring data for every call seen by the ETM System is stored in a secure, central relational database for enterprise-wide scheduled or ad-hoc reporting via the robust integrated ETM Report Tool or with thirrd-party reporting tools.

Configurable real-time alerting provides immediate visibility to security and monitoring policy rule firings and system events.

Easy-to-Use Graphical User Interface (GUI)

Distributed ETM Client applications provide an intuitive, easy-to-use GUI to define and install voice security and monitoring policies and manage all of the components in the system.

Scalable Distributed Client/Server Architecture

The ETM System Voice-Network Monitoring & Security applications are deployed via software or hardware on customer-premises voice networks. These applications monitor and control voice network traffic in real time based on user-defined policies to deliver real-time call-access control (CAC) and alerting for issues and calls of interest. They are controlled by a central ETM Management Server managed from distributed ETM Client applications that can manage multiple ETM Servers and hundreds of distributed Voice-Network Monitoring & Security applications.

Configurable real-time alerting provides immediate visibility to security and monitoring policy rule firings and system events.

TDM and VOIP Circuit Support

The ETM System supports both TDM and VoIP networks simultaneously. Deployment options include:

- **SIP Networks with Cisco Voice-Aware ISR/ASR**

  For environments with SIP trunking (or other VoIP protocols, except MGCP) or hybrid TDM / SIP networks using a Cisco voice-aware ISR / ASR, the ETM Unified Trunk Application (UTA) integrates with the router via an API that SecureLogix and Cisco co-developed to provide security-policy-based call control without the need for another device inline on the voice network. The router holds the call while it sends important call information to UTA for security policy decisions, and then UTA directs the router how to route the call based on the policy result—allow as dialed, redirect to an alternate destination, or terminate prior to call setup. Policy processing occurs in a matter of milliseconds and adds no latency to the call.
- **SIP Voice Infrastructure**

  For environments with SIP trunking that do not use a Cisco voice-aware ISR / ASR, the ETM Stateless SIP Proxy sits logically inline on the enterprise SIP trunk between the SBC and PBX. All inbound and outbound SIP traffic is proxied through the Stateless SIP Proxy in real time to enable security-policy-based call control and monitoring throughout the enterprise.

- **Traditional TDM Infrastructure**

  For traditional TDM voice networks, the ETM telecom-grade 99999-reliable purpose-built

FEATURES & BENEFITS *continued*

TDM appliances sit physically inline on your voice circuits to enforce your enterprise voice security policies in real time. They are built with a fail-safe design to ensure traffic on your voice network is not affected in the event of power failure or an OS or application issue. They can monitor T1, E1, PRI, and SS7 circuits.

800-817-4837
securelogix.com