REPORT REPRINT

This Impact Report was published by 451 Research as part of our syndicated Market Insight subscription service and subsequently licensed for commercial use by Subex.

# Subex takes on IoT security challenges facing telcos, government and enterprises

BRIAN PARTRIDGE, PATRICK DALY

28 APR 2017

The provider leverages telecom fraud detection and security experience to target new types of customers that require IoT security monitoring. Subex claims it can deliver IoT security services at a competitive price among comparable offerings.

451 Research®

Subex has brought an IoT security product to market designed to monitor and alert to threats in near real-time Internet of Things (IoT) environments. The Subex security narrative focuses on the concept of holistic 'cyber resilience' from asset and incident discovery and monitoring through response and recovery. In addition to its specialized, agentless software for heterogeneous IoT environments to extract and analyze data from IoT edge sources and apply IDS and SIEM capabilities, it also can offer SLA-based 24/7 monitoring services via a global network of SOCs, honeypots and skilled security analysts. Subex uses an agent-based model for homogeneous deployments focused on remote attestation.

## THE 451 TAKE

Subex aims to provide 'cyber resilience' for IoT deployments. This message should resonate for potential customers because it can offer in-depth IoT defense as a managed service at a very low cost. Subex means to deliver threat detection on IoT devices that is akin to approaches taken in the industrial IoT security space; that is, signature, heuristics and anomaly-based detection that rely on near real-time traffic analysis. The company's coverage of traffic from multiple IoT sources rather than a single layer of the network means it is less likely to miss a breach but also implies more alerts, which threatens to strain its human resources and generate high costs. It is partly for this reason that we haven't seen much IoT-specific security monitoring plays outside the industrial sector. We believe if Subex is able to offer its product at the low costs it claims and effectively deal with the number of alerts generated within its system, it will be able to provide value to its customers and gain traction in the market.

## CONTEXT

Subex was founded in 1992 with headquarters in Bangalore, India. Its primary business is telecom software including B/OSS (Business and Operational Support Systems) for CSPs. The company has 39 of the world's top 50 CSPs as its customers. With IoT security, it sees an opportunity to serve its existing customer base and also branch out to sell directly to government and enterprise clients. The company, which is publicly traded on the National Stock Exchange of India, has more than 900 employees today, with a dedicated department of IoT security. Subex initially planned to cross-sell its IoT security offering to existing customers, although it says that today the product is generating new business.

## PRODUCTS

The Subex IoT security offering is a managed service that primarily consists of four distinct technologies, an intrusion detection system, a web access firewall, a SIEM and something the company calls 'IoT aware,' which is essentially a contextual anomaly detection system based on a monitored device's unique characteristics, including the protocol used and expected traffic patterns. In addition to monitoring services, Subex works with clients to develop customized incident response plans in the event of a breach. Through its partners, Subex also brings private VPN, encryption, authentication and secure key storage services to its clients. In the case of a customer that manages its devices via an IoT platform, most of these services would already be offered by the platform provider, but Subex leverages partnerships with point vendors to fill gaps.

The combination of Subex's native security capabilities results in threat detection based on signatures, heuristics and anomaly detection, allowing the company to identify both known and unknown threats. One criticism of alert-heavy detection technologies such as IDS or SIEMs is the labor-intensive nature of following up on the high volume of alerts generated. Subex takes the onus off its customers to deal with these alerts by employing a team of dedicated security analysts at shared SOCs in Bangalore, Denver and London. Subex also operates a network of IoT honeypots based on 200 architectures and 300 different devices that are deployed globally to detect IoT-specific threats. This has allowed the company to build a threat intelligence feed that is used to enhance the company's signature- and heuristic-based threat detection. Subex's offering currently scans for 41,000 different threats. About 30% of these detection elements are organically generated by Subex through its security research and it is focused on IoT and ICS.

The monitoring and detection engine is deployed as either a software VM or a separate hardware appliance; the software deployment is able to handle speed-specific traffic while the hardware option is designed for deployments that go beyond that. The offering plugs into a mirror port for traffic replication to passively analyze network traffic for threat signatures and behavioral anomalies. Traffic analyzed comes from a variety of sources across the IoT environment, including packet capture of data from edge gateways that sit on top of IoT endpoints, sensor and log data from IoT platforms, database activity, webserver logs and HTTP data and packet capture fed by the customer's network security products.

## GO TO MARKET

Subex has a variety of pricing options available to its customers, although the majority prefer to go through a subscription model where price can be based on either the number of devices monitored or the traffic generated by those devices. The company's larger enterprise customers, however, prefer the company's licensing model where they buy and install the product, which is then run as a managed service. Subex claims that because of its size and economies of scale, it is capable of selling IoT products at a competitive price. This could be a major differentiator for the company, especially in the early phase of IoT where proving ROI for IoT security is especially difficult and keeping costs low is a priority for many enterprise executives.

In addition to its capabilities in the telecom and consumer/enterprise IoT space, Subex recently built support for industrial control system security monitoring at the insistence of clients that are looking into security for smart city infrastructure projects. That offering includes cascading policy controls across different levels in the ICS environment, role-based access control, privilege control and audit trails. While the company does not want to compete with ICS security vendors that have already cornered the market, it viewed the development of these capabilities as necessary for tying its value proposition into the smart city vision of its potential clients. Subex sees the smart city as a key opportunity for its IoT security offering and thinks that it is well positioned to take advantage of that opportunity given its prior experience with telecom providers and partnerships throughout the Southeast Asian markets.

The company works with local partners to drive sales growth to governments and enterprises, especially in its primary market in Southeast Asia, and monitors millions of devices across its three enterprise customers. Although this number is a drop in the bucket compared with the number of connected devices globally, these customers will likely serve as important proofs of concept for future enterprise sales. The company only recently began increasing its go-to-market initiatives for the IoT security product and is targeting 150% revenue growth for the offering in 2017.

## COMPETITION

Subex will compete against managed security service providers that combine proprietary software for threat detection with security operations teams for incident response. This includes Symantec, which has several IoT security-related offerings, as well as IBM Security and SecureWorks, along with other providers in the space. In addition to the MSSPs, Subex will likely face competition from the same type of IoT platforms it partners with since they already have native security capabilities. Some, like ClearBlade, are beginning to market their native security capabilities as a differentiator from other platforms.

Subex needs to make sure it clearly differentiates its security capabilities to customers, such as its proprietary database of IoT threats and team of security analysts, to avoid being viewed as solely an added cost. Another vendor with monitoring capabilities is ZingBox, although the companies operate primarily in different markets.

## SWOT ANALYSIS

### STRENGTHS

Subex's experience providing monitoring services for the telecom industry will serve the company well as it continues to build its presence in the IoT security monitoring space.

### WEAKNESSES

Talented security analysts are increasingly difficult to come by, making it difficult to scale effectively when the number of alerts that the company can resolve depends on analyst bandwidth.

### OPPORTUNITIES

Subex could generate a new source of revenue by licensing the threat intelligence database gathered by its honeypots to its existing security customers. Subex should be more aggressive in developing its direct and indirect selling force into larger enterprise and government accounts.

### THREATS

Subex notes that providing security for smart city initiatives is the company's primary focus, but it will be several years before smart city deployments are in full swing. If Subex focuses too much on smart cities before there are implementations, the company will forgo potential growth from not focusing on other markets.