

Vigilant launches Fulcrum, a config library to scale its ESIM deployment chops

Analyst: Nick Selby

When big organizations that deal with large and complex fraud and security issues related to their heterogeneous, geographically dispersed networks set up security operations, the task is daunting. **Vigilant** is one of a relatively new class of companies that specializes in 'standing up' and co-sourcing security operations centers. The task makes Vigilant part consultant, part vendor, part services provider. Vigilant's services include providing general security assessment, policy development and penetration-testing services, but it focuses on the monitoring and management of enterprise security information management (ESIM), with an eye to efficient management of security issues and specific expertise in understanding external and internal fraud.

Vigilant's new product, Fulcrum, is its library of configurations, comprising rules that in Vigilant's experience are sensible as mittens: industry-specific and government regulatory rule sets and the ISO 27002 (formerly 17799) security standard.

The 451 Take

From a technical standpoint, Vigilant is first rate, and the services and content it offers is highly useful to large-scale enterprise. From its deep understanding of a range of ESIM deployments, it is able to consult firms on the best classification of sources of events, then help the company use whatever ESIM platform it's adopted in a more efficient manner, authoring correlation rules that help the ESIM produce alerts that are most relevant (Vigilant also consults on which ESIM to buy, if the customer is not yet committed). It provides a range of services, from co-sourcing ESIM to penetration testing and other security services, as well as consulting on antifraud and money laundering. An area of concern Vigilant hopes to address with Fulcrum is just how it can scale.

Context

Vigilant was self-funded with less than \$100,000 and operates on very little overhead. It claims profitability since year one, which is not uncommon for what's essentially a pure consulting offering. It then reinvested profits to build out employee headcount to its current level of about 30. It has not ruled out a venture funding round, but doesn't plan one either. We have spoken with three customers, and while Vigilant won't allow us to print customer names it has shared under a nondisclosure agreement, we can say that its more than 50

customers are primarily in banking and finance, publishing, healthcare and pharmaceuticals – not surprising given the firm's ESIM and fraud focus.

Sales are 100% direct. Average deals range from about \$250,000 to \$500,000, and generally last from four to six months during deployment. There are often follow-on and continuing engagements. Typically, Vigilant does work at the assessment and design stages, then interviews groups within the customer organization to understand the requirements and propose an architecture. It then looks at the deltas between the architecture and what the customer actually has.

Products

At a high level, Vigilant consults with firms on the best ways to use their ESIM products by pointing out additional data sources like transaction and application logs, etc. It studies the business needs of its customers, puts forth a reference architecture and best practices guideline, then works to customize processes and rules and reports at the client premises. Finally, it turns over to the client the day-to-day operation, but provides 'co-sourced' monitoring, in that the customer is running the systems while Vigilant monitors them from its remote location. Vigilant likes to be as agnostic as possible, though it has the most experience with **ArcSight**, **Novell eSecurity**, **Intellitactics** and **RSA's EnVision**.

Technology

Fulcrum is Vigilant taking the ISO 27002 security guidelines and its own experience, and translating that into conceptual use cases it considers to be relevant to security monitoring. These have been further distilled into a library of ESIM content comprising ESIM content objects – essentially correlation rules. For example, Fulcrum will have high-level business objectives stated as clear business English goals. That is then broken into a conceptual use case and, finally, into content objects like rules and workflows related to a specific ESIM product like ArcSight. The content objects will identify the relevant data sources that support the rules and answer questions such as: 'What do we need to make this model work?' and 'How do we configure the various bits to get the events we need?'

In this manner, Vigilant (and competitors including **Decurity**) seek not merely to codify content objects but to proffer guidance about the source devices that must be in place to support the use cases and, by extension, the customer's compliance with regulatory rule sets themselves.

Competition

Part of the problem that Vigilant faces is that it competes on many levels with the ESIM vendors themselves, other firms like Vigilant, managed service providers and consultants. And a large issue in scaling out the business is that consultative, ad hoc and custom-made nature: There's a lot of knowledge Vigilant has that can scale, but a whole lot more that is absolutely peculiar to each customer. So as with consultancies, much time is spent just normalizing the requirements. Fulcrum seeks to combat this dynamic.

Direct competition comes from Decurity, a Tampa, Florida-based firm that was founded by a former senior ArcSight managed services leader and a former **Unisys** consultant (we will be writing on Decurity in the coming days). Competition comes from the professional services wings of ESIM vendors, especially ArcSight, **IBM**, RSA, Novell and **Symantec**, and from log management vendors including **Splunk Inc**, **LogLogic** and **Tenable Network Security**. On the managed services side, Vigilant comes up against large MSSP players including **AT&T**, **BT Counterpane**, **Verizon/Cybertrust** and **EDS**, as well as other large managed security services vendors. Competition from consultants comes from **Knowledge Consulting Group**, **Deloitte** and **PricewaterhouseCoopers**.

SWOT analysis

Strengths	Weaknesses
Vigilant has a solid technical and business team in place and good experience; it has A-list customers that speak highly of it.	Even with Fulcrum, a lot of the expertise required to scale this business is not quite repeatable, leading to long engagements and limited scalability.
Opportunities	Threats
Vigilant is one of a small handful of companies making headway in this emerging space, and it has sufficient specialization and differentiation to grow – if it can scale.	ArcSight may be approaching \$10m a quarter with its professional services arm, and we think it may expect to push that considerably harder. IBM is making inroads in this area as well.

Reproduced by permission of The 451 Group; copyright 2009. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to: www.the451group.com