

eIQnetworks launches SecureVue 3.0, adding flow and GRC to its enterprise ESIM

Analyst: Nick Selby

Sector: Enterprise Software

When **eIQnetworks** released its enterprise-class SecureVue line in February, we noted that the Acton, Massachusetts-based vendor – best known for ultra-low-cost enterprise security information management (ESIM) products (the cheapest line, Enterprise Security Analyzer, or ESA, starts at about \$800) – was ambitiously moving to bring its new flagship into the world of integrated IT service management (ITSM), ESIM, vulnerability and asset and risk management. Six months later, it has released version 3.0 of SecureVue, and the vendor says it has about 15-20 customers, with average deal sizes of \$125,000-150,000. More important, it is reporting buy-in from multiple groups within organizations – security, networking, compliance – and not just from within security. This is key.

The 451 Take

There is much to like about SV3.0. After a partnership with network behavior anomaly detection vendor Mazu Networks, eIQ has launched its own flow-based NBAD. Combined with its converged view into enterprise IT, this could be a powerful tool in an organization that turns on all the features. That may not be happening yet, but these are early days. We like eIQ's business model, go-to-market strategy, lean approach and creativity in getting deals done in some pretty impressive end users. We suspect one upside of being self-funded is that eIQ can concentrate on developing features it feels are necessary, rather than be driven by the need to market. It has fiscal viability disproportionate to its funding and, indeed, to its revenue.

Context

When eIQ launched SecureVue earlier this year, it said it was targeting \$150,000 as an average deal size. As customer numbers have crept up – 10 in June, after about six months on the market; an estimated 15-20 now – so have deal sizes, increasing SecureVue's importance as a revenue source. Early SecureVue deals brought in 'around \$100,000,' but the company says over the last quarter average deals were \$125,000-150,000. We are heartened by the number of deals it has cut in the past six months. We suspect that the deal sizes have not been so much discounted as very creatively put together to span multiple budget cycles.

Overall customer numbers – including downstream customers of resellers – are now above 2,600, up from 2,300 in June. eIQ says OEM deals and channel partners each comprise 15-20% of deals.

Headcount remains at 85, with about 60 developers in Hyderabad, India. The company says it is both profitable and cash-flow positive on a US GAAP basis.

Strategy

The basic path being followed here is to make eIQ's product rise from the ESIM category into that of governance, risk and compliance (GRC). CEO Vijay Basani has bet much of the farm that this is the general direction of ESIM, going one further than our take that ESIM should move into ITSM – as outlined in our Enterprise Security Quarterly 1: Security information management report last winter. We think that Basani has a point and that he has the will and resources to move the product in that direction. We also think the company must invest in its image and the look and feel of the product itself.

The SecureVue customers we have spoken to expressed general happiness with the product. Both were customers whose pleasure carries weight: one is a large newspaper known to us to be extremely reticent in its purchasing habits; the other is a financial institution whose security is run by a man whose most recent experience was at a very large retailer. These end users describe two things we find notable: First, the stuff generally works as advertised. Though both customers noted that they had not been fully deployed because the product has only recently been released, the newspaper tells us that it recently expanded the deployment to cover substantially more territory and to help it comply with Payment Card Industry (PCI) rule sets. This is a substantial win for eIQ.

Second, eIQ shows creativity in going to the table. As we mentioned in our Enterprise Security Quarterly report, ESIM customers use a variety of tactics to get the price down. The most popular claim is 'We really need this stuff, but I simply cannot get my budget higher than x, so what can you do for me?' eIQ, with its unique funding story and Basani's drive, has shown an ability to work with that question in a manner we feel will bear fruit in the long run.

What's wrong? We believe that the company will not be taken as a serious competitor for enterprise-class GRC or, indeed, ESIM until it invests in more enterprise-friendly marketing, including a reworked user interface that expresses more elegantly the impressive functionality that just does not get shown off to advantage. To our knowledge, we've never before called for more eye candy. But in this case, a more intuitive, user-friendly and polished UI would make eIQ's product move up in the eyes of those approving budgets. It needs to look more expensive.

Technology

Users point network flow to eIQ's product; it does not use or offer external sensors. It claims to be able to handle **Cisco** NetFlow, plus S-Flow and J-Flow. eIQ tells us of one major equipment vendor (it has asked us not to name it) that is licensing this NBAD technology for products it sells in India. Its default self-training period is seven days, though this is user configurable. Data or conversations are dropped after 90 days, though customers may choose to archive flow. Its application understanding is port bound. For example, if it observes traffic on port 21, it will assume that this is FTP and treat it as such. This is also configurable for custom user applications.

With this and other features – e.g., its configuration database and endpoint intelligence that provides registry-level information about Windows hosts and detailed information about Linux and Mac hosts, and information on traffic – data is then split four ways to group by source:destination, source:destination-group, source-group:destination-IP and source-group:source-group. It says it can also profile all host logon activity. Administrators can, through a role-based panel, drill down into any given host or IP in the Workbench, which

allows views of questions like 'What does this host normally do?' and view all the applications the host serves, those it accesses, etc.

While the visualization and UI still look a little rough around the edges, the visualization tools offered are impressive. Forensic search capabilities allow administrators to visualize thousands of events and see them as mapped representations. Lines grow thicker and clusters grow larger based on traffic, and configuration changes and known vulnerabilities affect color. When clusters appear, administrators can drill down into specific groups of traffic and separate out individual hosts and split into clusters, using factors like compliance or risk scores, etc.

In the world of enterprise ESIM this is not earth-shattering stuff. We think that eIQ's advantage here is that it is performing these tasks, offering performance of quad-core processors and offering what is – to our knowledge – unusual if not unique endpoint configuration capabilities for a far lower price than the products of larger competitors.

For its audit functions, eIQ engaged a PCI auditor to help it develop rules for SOX, PCI, FISMA, GLBA, HIPAA, CA 1386, NIST, CoBIT, ISO 17799 and other rule sets that it says can provide its audit center the ability to make snapshots of, for example, PCI compliance status based on its fetched configuration database. We spoke with one customer that does this and is happy with the results.

Any data eIQ has – ESIM, vulnerability, asset, performance, configuration, etc. – comprises a set that is required to verify a control called for by a section of the PCI regulation. For example, since PCI 5.1 says antivirus software should be running, eIQ gathers information on whether it is as part of its application-collection process. This can also be drilled into: Click on a specific node and view the values. While looking to see if, for example, **McAfee's** anti-malware agent is installed, eIQ can peek into that host's registry settings as stored in its configuration database, see the presence or absence of keys and determine whether the agent is running. Charts map compliance over time.

Vulnerability data may be imported from Nessus, **ISS** and **Foundstone** scans but not yet from **Qualys**, **nCircle** or **Outpost24**.

Competition

While eIQ would like to go up against the **Archer Technologies** of the world, we believe its main competition is still with ESIM vendors seeking to move up from security to network operations management, such as **ArcSight**, **ExaProtect**, **RSA's** Envision (**Network Intelligence**), **IBM** Tivoli Security Operations Manager, **OpenService** and **Enterasys Networks'** NetSight Automated Security Manager (Enterasys licenses **Q1 Labs'** Radar for its ESIM). **TriGeo Network Security's** ESIM product offers increasing looks at network information, including intrusion detection, endpoint port and device control and configuration. We will report on some of its functionality enhancements shortly.

Change management vendors include **BMC Software**, **CA Inc (Cendura)**, **Opsware**, **HP** IT Management Software and **mValent**. Auto-discovery and mapping come from **Network Infrastructure Inventory Inc**, **Magnum Technologies**, **Voyence**, **EZManage** and **Infra Corp**. Security players like **Lumension Security** (née **PatchLink**), **ScriptLogic** and **Shavlik Technologies** discover infrastructure topology while scanning for vulnerabilities.

SWOT ANALYSIS	
Strengths	Weaknesses
EIQ is lean, aggressive and adequately funded. It has a laser focus on the issues it believes will take it through the next 24 months on a rapid and steadily growing trajectory. Its self-funding means it is beholden not to the whims of external funding sources but to those of its CEO.	There's a real perception issue: eIQ is known as the cheap stuff, and it is really only several months into its new offerings that are more expensive, enterprise-class offerings.
Opportunities	Threats
Even as the low-priced alternative, eIQ established relationships with managed security service providers by concentrating on role-based access and dashboards. As its product lines and features grow, it is leveraging those relationships to greatly expand its MSSP relationships – and then using them as reference customers to large enterprise leads.	ArcSight, EMC/RSA, Intellitactics and NetIQ, among others, are targeting the same very large enterprises. Along with LogLogic and LogRhythm, they are going after the enterprise-wide log-management-as-compliance-tool route. All have substantially better UIs and marketing head starts.

About The 451 Group

The 451 Group is a technology industry analyst company focused on the business of enterprise IT innovation. The company's analysts provide critical and timely emerging-technology insight to clients at vendor, investor, services and end-user organizations – insight that aids both strategic and tactical decision making for competitive advantage.

The company's services include the 451 Market Insight Service, which delivers daily insight into emerging enterprise IT markets; 451 TechDealmaker, a weekly analysis service focused on forward-looking M&A within the enterprise IT business; 451 Special Reports, which are produced on a periodic basis to analyze key emerging enterprise IT markets in greater depth; and 451 Strategic Counsel, the company's analyst-inquiry program, which provides clients with direct access to 451 analysts. The company also produces via 451 Events periodic industry summits and investor conferences that address opportunities and obstacles facing emerging enterprise IT markets.

The 451 Group is headquartered in New York, with offices in key locations, including San Francisco, London and Boston. The company also operates Tier 1 Research – an independent division of The 451 Group, headquartered in Minneapolis – which analyzes the financial and industry implications of developments impacting public and private companies within the IT, communications and Internet sectors.

For additional information on the company or to apply for trial access to its services, go to: www.the451group.com