

Alert Logic, in new Houston digs, launches on-demand grid-hosted log management

Analyst: Nick Selby

Sector: Enterprise Software

With the Payment Card Industry (PCI) standards providing the icing on the cake of the compliance-based feeding frenzy that has fueled the worlds of enterprise security information management (ESIM), security event management (SEM) and log management for the past several years, the pressure on companies to log increasing volumes of their activities is intensifying.

The ability to scale to the point that extremely large heterogeneous environments are compliant has been the domain, really, of firms like **LogLogic**, **SenSage** and **RSA** (through its acquisition in 2006 of **Network Intelligence**), and lately, **ArcSight** has been making aggressive overtures. On the midmarket side, companies like **LogRhythm**, **eIQnetworks** and, with its new Splunk integration, **TriGeo Network Security**, have been making impressive progress in the past year – LogRhythm and eIQnetworks in midsized enterprises and in managed security services providers outside the US. After hearing it out, **Symantec's** new hosted log management offering was not something we chose to report on.

Now a third way emerges: With its grid-based architecture, **Alert Logic** has the potential – if reality keeps up with its claims – to be a disruptive force in the log management world at both mid- and large-sized enterprises.

The 451 Take

Compliance with governmental regulations began the first wave that pushed log management into the 'gotta have' category; the PCI security standards have now emphasized the importance of log management in increasingly smaller businesses. Simultaneously, a dramatic increase in enterprise acceptance of managed security services and hosted applications has led, perhaps inevitably, to drives to provided hosted, on-demand log management services. The appeal to midsized regulated industries is clear; however, we think Alert Logic's grid-based architecture will scale to meet the needs of very large enterprises as well, putting pressure on software-based log experts like LogLogic, SenSage, RSA and, increasingly, ArcSight.

Context

Alert Logic was founded in 2002 with less than \$1m in angel money, it says. In September 2005, it took \$2.3m in series A funding from **DFJ Mercury**, **OCA Ventures** and **Access Venture Partners**. This was followed by a \$5m series B round in July 2006 with all investors from the first three rounds plus **Hunt Ventures**. The company currently has 60 employees, 374 customers and mainly targets midmarket businesses with its two product lines; its traditional managed intrusion detection system (IDS) and vulnerability management, and its new grid-based on-demand hosted log management product. Its Network Operations Center (NOC) has just successfully completed a SAS 70 type 2 audit (it is sharing the details with us,

and we will confirm this in our next report on the company) and uses data hosting centers that also have that level of physical security.

Strategy

AL says that 50% of its business comes to it through partners in the hosting or colocation space, such as **Rackspace, DataPipe, Data Return, GSI Commerce, Hostway, Internap** and others, including **CyrusOne**. It claims revenue of less than \$10m and fast growth. Average deal sizes are between \$2,000 and \$3,000 per month; its lowest price point is \$500 per month, and its prices go up to about \$10,000 per month. Its strategy is to offer tick-the-box upsells through its hosting providers and application service providers, such as GSI Commerce, which provides e-commerce and IT infrastructure for bricks-and-mortar players, including **Dick's Sporting Goods** and **Toys "R" Us**. Other publicly mentionable customers include **Amarillo National Bank, Concentra, Dyrand Systems, Guaranty Bond Bank, Harris County Hospital District, MHI Partnership/McGuyer Homebuilders, Moore County Hospital District, Paymetric, Philharmonic Center for the Arts, Stratos Global, Swift Energy** and **WebCE**. Building on that, it will target directly mid- to large-sized organizations to pitch the outsourced log story.

We have spoken quite a bit about the changing nature of the premises network, and would argue that at this point in most very large enterprises, the LAN is already in transition from the big red circle (in which everything outside is bad and everything inside is good) to that of many smaller circles, eventually arriving at the point at which the endpoint is the firewall. If that is the case, surely enterprises which even two years ago would not have considered sending crucial data 'outside the firewall' must now concede that the very idea behind that mind-set is increasingly quaint. We don't predict an easy ride, but we do predict that Alert Logic's ride gets easier.

Products

Log customers point syslog and Windows (WMI) sources toward the Customer Premises Equipment (CPE) box, which aggregates and can provide prioritization of logs by various methods. Log data is aggregated, compressed and encrypted and then sent to the primary datacenter. The primary datacenter immediately sends an encrypted copy to a secondary datacenter, and then both datacenters begin to process the logs in parallel (see Technology). CPE is a 1U pizza box; most interaction by the customer with the box is via a polished, Ajax-based Web-GUI. Reports, including a slew of out-of-the-box compliance reporting tools, are run through the Web interface and are as pretty as one would expect of an enterprise offering.

As an IDS and vulnerability scanning box, it runs Snort, Nessus and, optionally, Unicornscan (see Technology), all of which is tuned by AL at no additional cost as part of the monthly subscription fee.

Technology

The CPE boxes are Linux-based appliances with limited shell access that does not permit sudo, su or root access.

As a dedicated log manager, AL claims rates of 3,000 to 4,000 sustained events per second (EPS), collected from all syslog sources, OPSEC devices and agentless log collection from Windows devices. The logs are prioritized (by a range of customer-controllable settings set

from a Web interface, such as type of device, time of day, etc.). The default setting compresses using Gzip with a modified library and end-to-end encryption with several cipher options. Batches of data, which AL refers internally to as Queue-Packets, are then sent back to the primary datacenter, which mirrors and then begins processing in parallel with the secondary datacenter (the default Queue-Packet comprises 500KB or 30 seconds worth of logs).

Within the datacenter, AL's grid comprises 1U quad-core Linux servers and a central management system; servers process jobs, and, when complete, requeue new jobs from the management server. In this fashion, adding new servers to the grid is simplified. All logs are indexed; logs that can be parsed are parsed, and those that cannot be are indexed. Short-term storage is on a relational (MySQL) database. For long-term storage, sharding spreads the jobs across the grid in 400GB database chunks to aid recoverability and separates the chunks by log or data or device type. The idea is to act as a giant search engine: AL uses indices produced by the C implementation of **Lucene**. The architecture allows it to use of the shelf hardware for its storage area network. It also keeps the signed, hashed Queue-Packets for immutability, and is able to replay the Queue-Packets for whatever reason – for storage recovery or (and this has not happened) to produce for evidence in a trial.

For its bundled security product, AL is using Snort and Nessus; IDS signature sets are compiled by AL based on signatures released by the Snort VRT, bleeding Snort and the AL team's own signatures, which they then make available to the Snort community through a relationship with **Sourcefire** and Snort. Standard vulnerability scanning comes from the 2.0 version of Nessus running the freely provided signature set by default, but customers can upgrade to the fully licensed Nessus build and feed from Tenable. AL also offers the option of network scanning via the blistering fast (and sometimes overkill) Unicornscan.

Competition

For log management, AL competes with LogLogic, ArcSight, eIQnetworks' SecureVue, SenSage, **EMC's** RSA, LogRhythm (which AL says it has been seeing increasingly in the past year). **Splunk Inc** is another obvious competitor for log management – we would like to think that Splunk's offerings are more toward the network trouble detection than security or compliance side – but it's been awhile since we spoke with it, and we hope to do so soon. **TriGeo Network Security** recently announced an integration with Splunk, in addition to its extant integration with Snort. This tuning truly makes TriGeo competitive at the lower end of the midsized market, and AL says it does see TriGeo in deals in the \$35,000 to \$40,000 range. **Q1 Labs'** QRadar recently launched a logging-only version of its product, upgradable to the full Q1 Radar integrated ESIM and NBAD with a software license key.

On the scanning side, vulnerability scanners as a service vendors that compete in the PCI world would be topped by a short list – **Qualys**, **nCircle** and **Outpost24** – the latter, interestingly, having acquired **Dyad Security**, whose founder co-authored Unicornscan. Managed security services and IDS/firewall management come from a slew of players, notably including **AT&T**, **BT (Counterpane)**, **EDS**, **Verizon** and many more.

Strengths	Weaknesses
We believe that this architecture and the particular implementations that Alert Logic is discussing have legs, the ability to scale, a true on-demand offering and the potential to be disruptive in the world of log management.	With little reputation outside the hosting community (where it is well thought-of), Alert Logic has some branding issues and marketing cut out for it – that and convincing people that, no, seriously, it's cool to outsource your log data.
Opportunities	Threats
There are partnership possibilities galore with this offering, and we could see several larger vendors getting interested in partnering – starting with ESIM, SEM and log management vendors looking to increase their viability in the ever-hotter services world. Symantec's new, overpriced managed log offering should raise awareness of the space, too.	AL is standing between battling big guys here, with log management offerings or claims from vendors like IBM, ArcSight, HP, EMC/RSA, Symantec, LogLogic and SenSage, and then smaller players including eIQ, LogRhythm, Intellitactics and many others.

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