NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE = MAY 15, 2017

Security-as-a-Service supplier Alert Logic started with IDS and blossomed from there

CEO Gray Hall shares insights into what customers are using, where the industry is going

BY JOHN DIX, NETWORK WORLD

Gray Hall, CEO of Alert Logic, cut his teeth delivering enterprise-class services when he started VeriCenter, one of the earliest managed hosting companies. Hall eventually sold that company to SunGard Data Systems in 2007, and in 2009 joined Alert Logic where he has since driven revenue growth 12x. Network World Editor in Chief John Dix recently caught up with Hall to learn more about Alert Logic and the Security-as-a-Service movement.

Credit: Alert Logic

Let's start with a brief background on the company.

Alert Logic was founded in 2002 – the founders are still with us today in very key roles – and the original vision was to bring together Software-as-a-Service (SaaS) and managed security services, starting with Intrusion Detection Systems (IDS). Sourcefire had been around for a long time, they were the gorilla in the space (now owned by Cisco), but Sourcefire is a very advanced product and most of our customers would say it's expensive, complex, and you need a lot of expertise to make it work. It's only as good as the content you feed it and once you reconfigure your network, you have to do it all over again … tuning, configuration, etc.

So the vision was to deliver pain relief in the form of IDS as a service. We'll deploy the snort probe, we'll host centrally all the analytics that you need to escalate incidents. We'll escalate it to our own security operations center and we will tell the customer when there's a problem.

IDS as a service was the original concept and the company had grown to about $9 million in revenue, but in 2009 was having trouble getting to the next level. The growth rate was slowing and VCs came in and started making management changes. I was in the right place at the right time. There just aren't a lot of CEOs in the Houston market who have had success growing a tech company and delivering value to investors.

What I saw in Alert Logic was an opportunity to be way ahead of an important trend in the industry. This idea of IDS as a service could be broadened to apply to pretty much any proven detection or protection technique. By aggregating all the data centrally, there are things we can do that other people can't do. Today we have 4,000 customers and having all that data in one data store and being able to look for patterns and anomalies across all that data gives us a competitive edge compared to vendors that have single tenant solutions.

The other thing the company had figured out that really caught my attention was, they were the first security company to partner with a hosting company. Having run one of the first hosting companies, that hit me like a freight train. All the hosting providers struggle with security, and here was a company offering a security service that the hosting providers could simply add to their product catalog.

How do sales break down by category?

The company has always had direct sales, then it built partnerships with traditional security VARs, and finally started building the hosting channel in 2005. Then in 2012 we made the decision to invest in the technology required to extend the same offerings to cloud customers.

We were one of the first movers in AWS and Azure to deliver production security products. We built prototypes in 2012, released GA solutions in 2013, and so today our business is very distributed across cloud platform customers, hosting customers and what we call enterprise data center customers.

So, in terms of sales, it's pretty close to a third, a third and a third. It's all recurring revenue, very much like a hosting business. There are no perpetual licenses, no consulting. It's just monthly service provider fees, long-term contracts and pricing is based on the size of the environment the customers run.

Because it's all recurring, the bookings mix is going to be a leading indicator of the revenue mix. We're private so a lot of this is confidential, but I'm comfortable sharing that we're doing more than $100 million in revenue today, so the company has grown by a factor of 12 since 2009.

A quarter of that is customers of cloud platforms. The balance is split between hosting providers and customers who run in their own data centers. In terms of new business we're booking, 50% is customers of cloud platforms and again, the balanced split.

We're still growing through hosting providers, it's just not as dominant as it was at one point, and we're still growing with customers who run their own data centers, but what we're seeing is a massive trend to move – particularly net new applications – to the cloud. Customers may continue running their own data centers, but when they're talking about new capacity, new expansion, where the new apps are being targeted, it's mostly cloud.

Our ability to be hybrid is a real differentiator for us because we can offer a single pane of glass for all of that. If they have some applications in a traditional data center environment and others in the cloud, they can use our interface to apply the same security policies and controls to all those applications, plus they get the managed service benefit that our people are watching and alerting and notifying them when something is wrong.

I presume you've added other services as you've grown.

We've expanded well beyond IDS. Let's go through the product catalog. Everything we do is part of what we call our Cloud Defender suite. Within Cloud Defender there are multiple products and services. Customers can subscribe to any one, any combination, or the whole suite.

If you go back to the original concept of IDS as a service, that's embodied in Threat Manager. Another component is Cloud Insight, a cloud-native vulnerability management solution. We are a PCI-approved scanning vendor and for non-cloud customers, our vulnerability management solution is included in Threat Manager. The reason those two capabilities are bundled is because that's what customers want, but also because the ability to match a snort event with a potentially related vulnerability gives us the ability to prioritize incidents more effectively.

Log Manager is our second oldest product and that's similar to a SaaS version of Splunk, the biggest difference being it's specific to security use cases. Splunk obviously is an IT operations platform that also gets applied to security. Log Manger is not a general log platform; it's very specific to security, escalating incidents based on what we're detecting, and we have an analytics engine coupled with that that gives us the ability to look for anomalies.

Web Security Manager is the last product in the Cloud Defender suite, and that's a web app firewall (WAF). If you're familiar with Imperva, Imperva being an on-premises, locally deployed, single tenant WAF, we are basically a SaaS competitor to Imperva. It provides both inline blocking and out-of-band detection based on traditional lab techniques.

All of these products ride on a common platform.

As an AWS customer, if you have an auto-scaling application that leverages the auto-scaling functions that are native in AWS and you are a Web Security Manager customer, the WAF will scale up and down with your app and provide inline blocking. That is a very popular offering in AWS because most AWS customers are more concerned with application security than network security.

That's one of the big differences between cloud and on-prem. In on-prem environments, there's still a pretty heavy focus on network security. In cloud environments like AWS, people feel like the foundational layers are very secure and there are a lot of things customers can do through AWS Virtual Private Clouds (VPCs) and security groups and the way they build a DMZ around their applications, where you don't need network firewalls.

In other words, the attacks tend to be at the application layer and that's where AWS tells customers, "Look, it's a shared security model and we're going to secure the foundational services but you as a customer need to secure your app." That's the problem we solve in AWS, so we felt it was crucial to have that web app firewall capability in addition to our IDS.

Those are the four technologies. Again, WAF, log, IDS and vulnerability management gives us what we call full stack visibility around the application stack.

All the data we collect at the network, system and application layers comes into our back-end systems. We have today one of the largest stores of security data in the industry and it's one integrated platform that allows us to run our analytics engine to detect threats and escalate incidents based on our proprietary analytics.

All of our event signatures, rules, anomaly detection, data science, machine learning, runs through this analytics engine. The analytics engine escalates incidents to software that we have in our security operations center that automates the workflow of the security analyst who is doing the human investigation.

Our security operations center, and the people we employ in that center would be analogous to what a Managed Security Service Provider does, but the difference is 100% of what we're doing is managing our own technology, and from there it's very much like an MSSP, where you're notifying the customer and telling them when they have a problem.

Our service level agreement says to the customer two things: one is, that all this technology I've described will be up and running 24/7 (we have a 99.9 SLA on the technology); and we have another SLA that says, within 15 minutes of us detecting malicious activity, we will notify you. That's the essence of the promise to the customer: full stack security, experts included. We'll tell you when there's a problem and we'll share this incident with you.

If you get back to what's in Cloud Defender, there's Web Security Manager, Log Manager, Threat Manager, and then ActiveWatch is a service that supports any one of those products. If you don't buy the whole suite you can buy Threat Manager with ActiveWatch. You can buy Log Manager with ActiveWatch. You can buy Web Security Manager with ActiveWatch or any combination of that. That's the product catalog today.

How much competition is there in SaaS security services at this point?

The SaaS phenomenon didn't find its way into

security until very recently. If you look at all the categories of enterprise software, security is the last one to get on the SaaS train. Qualys is SaaS and Proofpoint is SaaS.

Which is the other thing I got excited about back in 2009; I was part of an early hosting deal and now here's an opportunity to be early in bringing SaaS to security. I'm eight years into it now and I almost still feel like we're early in bringing SaaS to security. We're early in the marriage of managed security services with SaaS to deliver an integrated solution, and we're early in the penetration of security solutions into the cloud market.

I mentioned our tremendous growth in cloud. Three years ago zero percent of our customers were cloud and we were, let's say, a $50 million company. Now we're more than $100 million in revenue with more than a quarter of our customers in the cloud. Just explosive growth, but I think we've only barely scratched the surface in terms of cloud customers that we can deliver our solution to.

I think our solution is even more appealing to a cloud customer than it has been to a hosting customer or a traditional data center customer because, if you think about it, when a customer moves to cloud they've made the decision to let the cloud service provider run the IT infrastructure for this app, so it's much more natural for them to think security as a service is the way to do security.

Is part of your pitch that customers will see a reduction in the number of false positives?

It entirely depends on the customer's situation. I think of it in terms of a signal-to-noise ratio. As long as I've been in the IT industry, the biggest complaint about security products has been they produce a lot of noise. I spent all this money, all it's doing is giving me more things to investigate, so it's creating more work but is it really helping?

Part of our value is to reduce the noise and increase the signal. If you think of the security maturity model, you may encounter a customer that is sort of early in that journey and only has in place basics like a network firewall, antivirus, some basic security techniques. In that case, the fact that we're alerting on snort events, log events, WAF events, we're delivering signal even though there may be some noise in there too that they've never received.

On the other hand, you may have a customer who has implemented a WAF but couldn't really get it working right, implemented an IDS, couldn't really get it working right. Maybe they even have a SIEM. As you know, many SIEM investments failed because they got tangled up in the integration. The value for these customers might be helping to find the signal in the noise.

We do strive hard to eliminate false positives and a lot of that is done through our system, but that's where the human layer really adds value. Having the security analyst will let us close out incidents and say, "No, I understand why it fired, but that's not a legitimate threat."

With ActiveWatch being common to the other products, do you grow by adding other offerings?

That's the question we're asking ourselves today, if you think of Threat Manager, Log Manager and Web Security Manager as the pillars and ActiveWatch being where it all comes together.

There are two ways we could evolve from here. One is to continue to add more legs to the stool, so to speak, or we could bolster what we have. If you think in terms of network system and application layers, why burden the customer with a tyranny of too many products? I think that's one of the problems in the security industry today. There are just all these categories and customers look at it and say, "How many do I need?"

We like simplicity and we like the idea of, if you need application security and you think you have the other bases covered, buy Web Security Manager. If you need network security or if you want the full stack, buy Cloud Defender. We like the simplicity of that approach, which means add more depth and breadth into the existing products. The best way to do that is through deeper and richer analytics which is why we're making the investments in data science, why we're making the investment in our analytics engine.

Is there a sweet spot in terms of customer size for you folks?

Obviously, as a $100-plus million company with more than 4,000 customers, there's a lot of mid-market customers, companies with $50 million up to $2-$3 billion in revenue, but we also have 150 of the Fortune 500 as customers. We don't really think size of the company is what dictates the sweet spot. What we've found is the sweet spot tends to be defined more by the type of application the customer is running.

What we found is there are three types of applications that are most common in our customer base and where the value prop is most distinct. The first is any type of Software-as-a-Service app. We find customers in all kinds of industries and of all shapes and sizes have more and more SaaS solutions. The second is E-commerce, and the E-commerce applications we secure are across dozens of industries and companies from super large down to startups. The third is digital media, digital marketing, corporate websites. Those are very common and tend not to be specific to any industry.