Skyhigh looks down to see competition heating up in cloud-app control market

Analyst: Adrian Sanabria
10 Dec, 2013

The market for cloud-application control is poised to explode. Skyhigh Networks was once the only player in this space to cover the entire spectrum of cloud-app control: discovering third-party cloud services, analyzing/auditing use and providing fine-grained tools to control access.

New contenders Netskope and Adallom have left the cover of stealth to challenge the early bird for the worm. On the heels of both of these startups, several more remain in the shadows, with plans to emerge in the next month or two with some new tricks. Although Skyhigh has the head start and was the first to write the rules, it remains to be seen whether it will become the Palo Alto Networks or FireEye in this market, or be overshadowed by one of several cloud-app control startups emerging in the coming months.

The 451 Take

Skyhigh has a solid product and already a substantial customer base. There is no question that this market has a lot of room to grow. In fact, many enterprises aren't yet aware the market exists. The question is whether Skyhigh can hold its place as the market begins to fill with competition. It won't take long, since by the time the 2013 AWS re:Invent and 2014 RSA US conferences have come and gone, this market likely will have grown to six or more players. As with any cloud-based SaaS product that can be tested and compared with minimal effort, bakeoffs will occur, and the best product will win. Skyhigh could have the advantage here, with the valuable benefit of time to have worked out most of the bugs. We see the competition catching up quickly, as well as bringing new features and functionality to the table.

Copyright 2013 - The 451 Group
Context

Founded in late 2011 and based in Cupertino, California, Skyhigh was one of the first companies with a product that covers what we have chosen to term the cloud-application control market. Coming out of stealth without a period of private testing under NDA, as is the norm for similar startups, Skyhigh went directly from stealth to general availability with its product, and that confident approach appears to have worked in its favor.

Companies are typically shy about announcing which security products they use in-house, perhaps worried the knowledge could give attackers an advantage. Surprisingly for a company yet to celebrate its first year out of stealth, Skyhigh’s website is flush with customer testimonials from the likes of Cisco, Diebold, SAP and Farmers Insurance Group, representing a wide range of vertical markets.

Founded by a trio of ex-Cisco employees and led by founder Rajiv Gupta, the company is experienced in growing startups. Two of the three founders, Gupta and Sekhar Sarukkai, joined Cisco via acquisition of Securent – a company also founded by Gupta and Sarukkai. Skyhigh received an initial round of $6.5m from Greylock Partners and private equity funding. Series B funding totaled $20m, in a round led by Sequoia Capital with continued participation from Greylock Partners. Staff of about 95 are currently employed. The company claims to do very well when challenged to a bakeoff with competitors, and prides itself in its ability to execute effective proofs of concept quickly.

Products

There are three distinct feature categories that define products in the cloud-app control market: discovery, analysis and control. Discovery is essentially a feature directly supporting the second category, analysis. The purpose of discovery is to show the depth that ‘shadow IT’ has penetrated into the enterprise. Analysis then allows an enterprise to quantify the damage, and use this data to answer questions like, ‘What cloud apps are the finance group using, and how are they using them?’ The third is the true seller – control. Control allows the enterprise not to simply block access to unauthorized services, but in theory, to encourage IT to allow use of some cloud-based applications with the caveat that use now be tightly controlled and monitored.

The discovery piece is enabled by forwarding logs to Skyhigh – any kind of logs from any kind of device that captures SaaS activity from users in a parsable format. The analytics abilities are
extensive and support many use cases. For the control piece to work, however, customers must enable applications to be 'managed' by Skyhigh. This means configuring services to redirect through Skyhigh's services.

One way to achieve this is to leverage the SaaS vendor's SAML configuration. For example, although a user might log into salesforce.com, that company's SAML configuration will be tweaked to redirect the user to something like crm.customerx.com, which forwards to customerx.salesforce.skyhigh.com instead. Other cloud-app control vendors use this same method, though Netskope takes a different approach, requiring installation of a browser plugin to redirect policy-enforced apps through its proxy.

The advantage of the SAML approach in this example is that no modification of mobile or enterprise devices is necessary to achieve control over access. All this is done in Skyhigh's SaaS console. But for customers that choose not to use the cloud due to discomfort, mistrust or policy, Skyhigh also offers an on-premises version of its cloud-based proxy that can apply security policies to cloud-application use.

Cloud-app risk scoring has so far been a ubiquitous feature in the cloud-app control market, associated with the analytics function. Partially sourced and inspired by the cloud SSO/IAM market, Skyhigh has applied risk scores to each cloud application based on detailed in-house analysis of security-related features and breach risks. More than a simple risk ranking based on feature sets listed on a SaaS vendor's website, Skyhigh conducts a detailed assessment of each vendor – going as far, for example, to consider certifications obtained by the datacenter physically holding the vendor's data.

The level of monitoring granularity with Skyhigh and most other cloud-app control vendors is more than just 'next-generation firewall, plus one.' It is possible to see, for example, that 'Jim from accounting uploaded EmpSal.xlsx, which contained social security numbers, to Dropbox from his corporate-owned laptop this morning at 8:54AM EST.' Skyhigh's analytics will also compare customers anonymously with peers, giving each an idea of how they stack up against others in terms of cloud-app risk and usage levels. It is an increasing trend for SaaS-based SIEM and threat management vendors to leverage hosted data for customers to compare themselves with the Joneses.

Once Skyhigh is managing a SaaS service, policies can be enforced based on a variety of attributes, including device type, time of day or week, user ID, user role or group membership, or even the type and version of browser being used. DLP, encryption, anomaly detection, detailed auditing and
SSO integration are also common features in the cloud-app control market, sometimes developed in-house, and sometimes provided through partnerships. Combining encryption and DLP, Skyhigh can either encrypt all corporate data as it is fed into the cloud, or encrypt based on DLP matches for sensitive data. Currently, encryption is supported for about 20 applications, but unsupported apps can be added for free in about two weeks.

**Strategy**

The cloud-app control market is being approached the same way next-generation firewalls (NGFW) are commonly sold – vendors offer to show potential customers the visibility they're missing with current tools. Rather than ship an appliance on-site like a NGFW vendor would, a potential customer only needs to upload some firewall or proxy logs to see what they've allegedly been missing. Since visibility is so important for security, this is an effective approach.

Although the discovery and analysis tools this market has to offer will attract initial attention to the products, the NGFW market can already show similar information. The cloud-app control market isn't a NGFW replacement or competitor – rather, its true purpose is access control and data protection for data that leaves the premises, destined for the cloud. These products allow companies to monitor and control data that has already left the corporate network, or originates from off-premises devices (e.g., mobile devices, remote office, home office, etc.).

For the discovery portion of cloud-app control to work, the product must somehow gain visibility into user activity. Skyhigh requires customers to upload log data to Skyhigh's service – one of several approaches used by cloud-app control vendors to discover what applications and services employees are using. This is potentially a sign that partnerships, acquisitions or new competition in the cloud-app control space could come from companies that already have in-line network devices in the enterprise. In a few years' time, it will likely be commonplace for NGFW, and perhaps even the offspring of MDM, to dissect and report on exactly what users are doing in the cloud.

**Competition**

The competition in the cloud-app control market differs depending on the features the customer is after. Netskope and Adallom are currently the only competitors that come close to competing feature-for-feature. Due to Skyhigh's head start in the market, the newcomers currently lack the breadth of features, especially in the area of application control. Both have plans to close these gaps in the near future.

At least three other direct competitors are set to come out of stealth in the near future. In-line
devices in other markets have overlapping features, and may become full competitors in the near future. Examples include other cloud-based services, on-premises solutions and hybrids. Bitglass doesn't do app control, but aims to protect and control data as it leaves the corporate network. Although SaaSID focuses mainly on its namesake, it also offers visibility and some control over access to cloud services. Zscaler now has a variety of services including cloud application control. Stonesoft is an example of a NGFW that has taken the next step beyond offering binary choices (block/allow) for cloud applications, and is now allowing users to control access to specific features within each cloud application (e.g., upload/download, read/write, IM, no IM, etc.).

Portions of this market also stand to be highly commodified, and will depend heavily on partnerships for non-core services. In fact, the discovery feature that makes up one-third of the cloud-app control vendor profile is being given away for free by Adallom. Data encryption, SSO, DLP, cloud-application reputation services and even vulnerabilities/breaches affecting cloud applications (and therefore users) will be refined and made available through partnerships or sold through subscriptions. The entry of NGFW into this market seems inevitable. It will be interesting to see how the firewall market enters – it could build the capabilities internally, enter the market through acquisition or enter through partnership.

There are already battles being fought over customers in this market, with only three directly competing players. Things will heat up more by first quarter 2014, when we are likely to see a total of four or five. We predict nearly 10 directly competing cloud-app control vendors by mid-2014, with competition growing from vendors with products already well positioned to jump into the fray (SSO, NGFW, UTM, etc.).

**SWOT Analysis**

**Strengths**

The Skyhigh offering doesn't require a browser plugin like Netskope, making implementation simpler and cleaner. The deep dive into determining the risk reputation of thousands of cloud applications will be valuable to customers, and valuable as a feed to potential partners. Lead time in the market is still an advantage.

**Opportunities**

If Skyhigh remains an innovator, it may be able to stay a step ahead of the competition. Efforts to maintain the proprietary risk reputation service could be a valuable source of revenue as a commodified feed for other vendors to use in products.

**Weaknesses**

The ability to reach more customers is limited on a startup budget. It is unlikely the bulk of Skyhigh's target market is even aware that this technology exists and is available.

**Threats**

What Skyhigh doesn't know could hurt it. With multiple competitors launching out of stealth soon, it will have to assess, adjust and act quickly to maintain a lead.