

CipherCloud looks to stay at the head of the cloud security class with \$50m funding

Analyst: Garrett Bekker

11 Dec, 2014

After starting out with a mission to secure data in popular SaaS applications like Salesforce and Gmail, CipherCloud has been working hard to broaden its horizons. The company has always had broader ambitions than just doing encryption for SaaS apps, and over the last year has added app discovery and monitoring capabilities to its arsenal, while the recent announcement of FIPS 140-2 compliance may help ease early concerns about the robustness of CipherCloud's encryption techniques. The cloud security market is still very immature, although with headcount more than doubling in 2014 to over 500, CipherCloud appears to be growing up faster than the rest of the kids. A recent \$50m series B round led by new investors Transamerica Ventures and Delta Partners, and joined by existing investors Andreessen Horowitz and T-Venture (the venture capital arm of Deutsche Telekom) should go a long way to helping CipherCloud keep its foot on the gas.

The 451 Take

Securing the 'cloud' is a daunting task, with a wide variety of architectures (IaaS, PaaS, SaaS) and deployment methods (public, private, hybrid) that each present their own unique security challenges. As discussed in our 2015 Information Security Preview, the nascent market for cloud security is highly fragmented, with a growing assortment of vendors tackling the problem from different angles and with different technical approaches. While many of these upstart vendors have emerged to address largely tactical needs, we expect to see both convergence and consolidation – and not all of them will 'cross the chasm.' With an additional \$50m in its bank account, a growing product arsenal and substantial business momentum, CipherCloud has positioned itself as one of the horses to beat in the race for cloud security supremacy. Still, as with most emergent cloud security players, there are gaps to be filled, and the recent raise should help CipherCloud address some of them, via either organic

development or acquisition – though current valuations for many cloud security players could pose a problem in the near term.

Context

CipherCloud is one of the more well-known brands in cloud security, in part the result of a fairly aggressive marketing and sales strategy. According to the December 2013 Information Security Study by The Info Pro (TIP), a service of 451 Research, CipherCloud ranked first among enterprises looking to deploy a cloud security approach within the next 6-18 months. The company was founded in 2010 (using the name Trustosphere) by current CEO Pravin Kothari, who also founded SIEM vendor ArcSight (acquired by HP in 2010 for \$1.65bn) and GRC vendor Agilience. The company came out of stealth in 2011 with a proxy gateway designed to encrypt data in SaaS applications – initially Salesforce. Subsequent additional functionality included tokenization, DLP and malware protection, and with the acquisition of stealth vendor CloudUp Networks early in 2014, extended its reach into what 451 Research refers to as the Cloud Application Control (CAC) market. Most recently, CipherCloud has added SaaS application discovery capabilities through a combination of internal development and the CloudUp acquisition.

In January, CipherCloud moved into new, larger headquarters in San Jose, and also opened an office in Sydney in August of 2013 to serve as a hub for its APAC operations and to complement existing offices across North America, Europe and India. Headcount now stands at over 500, a staggering growth rate of over 100% since the beginning of the year. The company claims revenue growth in excess of 200%, which 451 Research estimates is rapidly approaching the halfway mark toward the \$100m annual revenue milestone. CipherCloud claims it protects over three million users in over 25 countries and 11 different verticals, including regulated industries like financial services, government, healthcare and retail. The company has raised a total of \$80m to date, with past investors Andreessen Horowitz, Index Ventures and T-Venture (the investment arm of Deutsche Telekom) recently joined by Transamerica Ventures and Delta Partners in a \$50m series B round.

Products

Although the simple characterization of CipherCloud would be as a SaaS encryption gateway vendor, CipherCloud sees itself more broadly as a 'cloud visibility and data protection' vendor, and views the market for cloud security as involving three critical pieces: first, understanding which cloud applications are being used and the data that resides in them, and how the data interacts with policies and business rules; second, protecting that data using a variety of security controls

(encryption, tokenization, malware protection, DLP); and finally, monitoring cloud activity to look for suspicious behavior and detect anomalies.

CipherCloud offers several distinct products all tied together under the CipherCloud platform umbrella, including CipherCloud for Salesforce, CipherCloud for Box, CipherCloud for Gmail, CipherCloud for Office 365 (Exchange Online and Hosted Exchange), CipherCloud for Amazon Web Services (EC2, S3, Redshift, Simple DB), CipherCloud for ServiceNow, and the newest piece, the aptly named CipherCloud for Cloud Discovery.

CipherCloud for Salesforce is the company's first and flagship product, and is based on a reverse-proxy gateway architecture that can be deployed as a physical or virtual appliance in the DMZ, in a virtual private cloud such as AWS, or hosted with service providers like Rackspace or NTT. The gateway intercepts outbound enterprise data on its way to Salesforce, and applies encryption, tokenization, malware protection and CipherCloud's own DLP capabilities, although users can also integrate with existing DLP tools from Symantec or RSA. CipherCloud also has pre-built DLP templates for specific industries such as financial services and health care as well as templates for credit cards, personally identifiable information and health information. CipherCloud uses a similar architecture for Gmail, Office 365 and ServiceNow, and for employees not behind the corporate firewall, CipherCloud provides an API that can be used to direct traffic to the gateway appliance.

In terms of encryption, CipherCloud can perform format-preserving encryption of specific fields or even parts of fields within Salesforce that permit standard operations like search and sort on encrypted data, or what's become commonly known as 'encryption in use.' Encryption keys never have to leave the customer premises, and can be stored on the CipherCloud Platform or on a KMIP-compliant server.

For online file sharing, CipherCloud has an integration with Box that allows all content to be scanned via the Box API before it hits Box's servers, and can then either block files, quarantine and replace files with marker files, prohibit sharing or protect with encryption.

The newest piece of the puzzle is CipherCloud for Cloud Discovery, which was introduced in April. The essential idea is that you can't protect what you don't know about, so the new offering analyzes network logs to discover thousands of SaaS applications in a wide variety of categories including CRM, HR, file sharing and collaboration. CipherCloud also uses crowdsourcing to allow users to add newly discovered SaaS apps to the CipherCloud CloudSource knowledge base. Once apps are discovered, CipherCloud generates a risk profile for each app based on a variety of factors such as the use of SSL encryption, validity of SSL certificates, the location of the cloud app's servers,

header analysis and the types of data being uploaded. In terms of remediation, CipherCloud has the ability to encrypt or block specific features of roughly 100 SaaS applications, and plans to add more integrations over time. For applications for which CipherCloud doesn't have integrations, admins can completely block applications that are deemed too risky.

Strategy

In terms of pricing, CipherCloud is generally sold and packaged similar to other SaaS offerings, on a per user/per month basis, typically under three- to five-year contracts. Since many SaaS apps are procured at the business unit level and not deployed enterprise-wide, CipherCloud often deals with a variety of internal constituents. CipherCloud claims sales engagements are typically driven by a line of business that has fast-tracked a new cloud project but wants to maintain control over their data to avoid compliance or data residency issues.

CipherCloud for Cloud Discovery assessment is available for free, and is likely intended to serve as a means of bringing in new customers and as an eventual upsell opportunity to other CipherCloud services.

In terms of strategic alliances, CipherCloud has relationships with: salesforce.com, Box, ServiceNow, SuccessFactors, NetSuite, Google Gmail and AWS, both at the partner and application level.

CipherCloud also has out-of-the-box integrations with Salesforce, Box, ServiceNow, Microsoft Office 365 and Gmail. Channel partners include global systems integrators such as Accenture, CapGemini and Cloud Sherpas, as well as regional resellers like Bluewolf and Sliced Tech.

Competition

Although cloud computing has become a fixture of modern life, the term 'cloud' is a bit misleading, as it implies a fairly homogeneous group of products and services. The reality is that what is broadly referred to as 'the cloud' really represents a variety of services – IaaS, PaaS, SaaS, public, private and hybrid cloud – each of which has a distinct architecture and addresses completely distinct use cases. Similarly, while the term 'cloud security' suggests a fairly uniform set of tools and techniques designed to keep cloud users and data safe, the market as currently constituted is a highly fragmented assortment of products that address fairly narrow use cases: SSO, encryption, data masking/tokenization, discovery and monitoring, typically for a single architecture (primarily SaaS with some IaaS mixed in), and in some cases for just a handful of service providers (Box, Dropbox, Office 365, salesforce.com, Workday). As we documented in our recent 2015 Information Security Preview, 451 Research believes the current state of cloud security is unsustainable, and

foresee several likely outcomes, two of the most likely being convergence and consolidation.

Given its roots as provider of encryption and tokenization for SaaS applications, CipherCloud's most direct competitors are fellow SaaS encryption gateway vendors PerspecSys and Vaultive, although CipherCloud appears to be putting some distance between its peers in terms of growth and customer adoption. PerspecSys has taken a slightly different route to market, with a greater focus on tokenization and data residency requirements as a primary use case. Vaultive has to date been focused primarily on Office 365 as its primary use case and go-to-market channel, and recently appointed a new CEO to help regain some market momentum.

With the acquisition of CloudUp and the subsequent addition of SaaS application discovery capabilities, CipherCloud will also face growing competition from the emerging CAC crowd, including companies like Adallom, Bitglass, Elastica, FireLayers, Netskope, Skyfence (Imperva) and Skyhigh Networks, many of which are adding their own encryption and DLP functionality to their existing app discovery and user-monitoring capabilities.

SWOT Analysis

Strengths

With headcount and revenues nearly doubling in 2014 and a recent \$50m added to its coffers, CipherCloud is certainly doing something right and has emerged as one of the early favorites for SaaS security leadership.

Opportunities

It's an understatement to say that adoption of SaaS apps is growing rapidly, and the opportunity to secure them all is still a land grab, with plenty of open space to roam.

Weaknesses

Like many cloud security vendors, CipherCloud relies heavily on a proxy-gateway architecture, which has both benefits and drawbacks. While CipherCloud provides out-of-the-box integrations with Salesforce, Box, Gmail, Office 365 and ServiceNow, there is still a lot of ground to cover. Although adding discovery and risk scoring of SaaS apps is a logical first step, CipherCloud will need to expand its remediation capabilities beyond the 100 or so apps it is currently integrated with.

Threats

CipherCloud has had a fairly open runway to date, although some CAC vendors are adding encryption to their SaaS discovery and monitoring capabilities, and could take some wind out of CipherCloud's sails. Trend Micro recently added SaaS security capabilities for Office 365, and other large incumbents could follow suit.

Reproduced by permission of The 451 Group; © 2014. This report was originally published within 451 Research's Market Insight Service. For additional information on 451 Research or to apply for trial access, go to: www.451research.com