Vormetric enters encryption gateway fray with latest extension to its platform strategy

Analyst: Garrett Bekker

13 Apr, 2015

In the past few years, Vormetric has been busy showing the world that it's no longer just your father's file and database encryption vendor. Since the launch of its Vormetric Data Security platform strategy in early 2014, the company has been hard at work extending the platform's capabilities with new features and functionality that address a growing variety of data-protection use cases across cloud and big-data environments. In 2013, Vormetric achieved certification for Cloudera and MongoDB, and in the past year it announced certification for Hortonworks and partnerships with most of the remaining big-data players such as Couchbase, DataStax and IBM (BigInsights); it also recently unveiled encryption and access control capabilities for Teradata.

In February, the company entered the tokenization and data-masking realm, in part to help organizations looking to reduce PCI scope by de-identifying sensitive data in app development and analytics scenarios. Its latest move is a new SaaS encryption gateway – aptly named Vormetric Cloud Encryption Gateway (VCEG) – that for now is designed to protect data in popular cloud file-sharing services such as Amazon Web Services' S3 and Box.

The 451 Take

As we noted in our 2015 Trends in Information Security preview, the market for cloud security has become quite fragmented, and for many organizations that are already dealing with a mélange of on-premises security tools, adding another layer of point services to gain control of their cloud and big-data resources is both undesirable and unsustainable. The intuition behind Vormetric's platform motivation is simple: follow its customers' data wherever it resides with products that, in combination, can deliver lower TCO than stand-alone offerings, with a single-pane-of-glass view for key management, policy creation, administration and

reporting.

To be sure, the vision is in place, but there is still work to be done, and for now, the company still lacks features that some of its more specialized peers offer, including format-preserving encryption (FPE), static data masking, stateless tokenization, and support for more complex SaaS apps such as salesforce.com, Office 365 or ServiceNow. Still, we suspect that the platform story will appeal to customers with heterogeneous environments that need protection for a variety of on-premises and cloud-based resources and are seeking economies of scale that point services can't offer.

Context

Vormetric was founded in 2001 and is based in San Jose. The company has historically been known for providing encryption for both structured and unstructured data, particularly database and file-level encryption. Current CEO Alan Kessler joined Vormetric in 2012 after executive management stints at HP, TippingPoint and 3Com, and has overseen an expansion of the company's product portfolio, international sales reach and partner program. Vormetric has raised a total of $20m in funding – including a $15m round led by Split Rock Partners and also involving existing investors JK&B Capital, QTV Capital and Sigma Partners – to support its aggressive growth strategy.

The company doesn't disclose specific financial data, but we estimate its revenue to be comfortably in the range of most recent information security IPOs (we listed Vormetric as one of the infosec vendors likely to pursue an IPO in the near future in our 2015 M&A Outlook). Its efforts appear to be paying off, with bookings growth accelerating in 2014 to more than 34%, up from roughly 20% in the previous year. Vormetric has also grown headcount to support its new initiatives, exiting 2014 with over 160 total employees. Its customer count grew to 1,500+, up from 1,300 at the end of 2013.

Products

Like Vormetric's Token Server, the cloud encryption gateway is a free download that can be run inside a VM or virtual appliance. Customers will also need to purchase a 'security blade' for each protected application; for example, a blade for Box, a blade for S3, etc. The stateless and virtualized gateway architecture allows for gateway software and blade upgrades without interruption. The company expects that most initial deployments will be run on-premises and have

all of the encryption and key management done before it leaves the enterprise. Customers will also have the option to run the gateway in the cloud; for example, in AWS's EC2 service.

In terms of architecture, like most encryption gateways VCEG is proxy-based, though in its current form it is a forward proxy. Many cloud security firms that are using proxies offer them as either forward or reverse proxies, and we anticipate that Vormetric will make VCEG available as a reverse proxy in the future (forward proxies are mostly for controlling network access, while reverse proxies are usually used to 'mimic' the destination application in order to terminate traffic before it reaches the service provider).

VCEG must be paired with Vormetric Data Security Manager (DSM) for encryption key and policy management. Both VCEG and DSM are available as virtual appliances, though the latter may also be deployed as a FIPS 140-2 Level 2- or Level 3-certified hardware appliance. By combining with DSM, the centralized key management leaves the keys in the customer's control, and removes the possibility of encryption key or data compromise at the cloud storage vendor. As a new extension of the Vormetric Data Security Platform, the gateway also shares encryption key policy, administration and management infrastructure with some of the company's other data security offerings such as transparent OS-level file and volume encryption, application encryption, tokenization and data masking, as well as data access monitoring and auditing.

For tokenization and data masking, the company's new offering is the Vormetric Token Server (VTS). VTS is a VM download that can be deployed as a virtual appliance. It provides application layer tokenization that uses APIs to allow communication between the application and the tokenization server. An example use case could be for protecting a credit card or driver's license number in an application running on a Web server. When the sensitive data is entered, the app will send the number to the tokenization server via a REST API. The token server creates a 'token' that replaces the original data, which is then encrypted and placed in a token vault to provide an additional layer of security. It is then delivered back to the app server in place of the original credit card number or driver's license. VTS also includes dynamic data masking, which can tie in with AD or LDAP directories and serve data as clear text or partial clear text based on the user's role.

Strategy

As noted, the new gateway encryption, tokenization and data-masking offerings are just additional pieces of the puzzle for Vormetric's platform strategy. The essential idea is that for existing customers who have already purchased DSM, each additional module will only represent an incremental increase in the TCO of the overall package. That said, customers looking for just an

individual component piece that don't have the need for multiple offerings may be better served with a point product. As such, in the near term, demand for the new products will likely come from existing Vormetric customers who have already deployed DSM and are looking to address new use cases.

In terms of pricing, the tokenization, data-masking and gateway offerings will each be offered as a virtual appliance that is free to download. For existing DSM customers, tokenization pricing will be similar to Vormetric Transparent Encryption: that is, based on the number of servers or VMs protected. For example, five apps that live on a single VM would require only one license, while a single app distributed across five VMs would require five licenses. With a single license available for roughly $3,500, Vormetric claims that the total cost of adding tokenization for existing DSM customers would be a fraction of the cost of a stand-alone tokenization server deployment.

For the encryption gateway, as noted, the gateway is a VM that is free to download. Customers will be required to purchase a blade for each protected app, though pricing has not yet been finalized. We believe the company may look to price the offering in a similar manner to the services it is protecting; i.e., user-based pricing for cloud storage offerings like Box, while for S3 the cost will be based on storage or resources consumed.

Partnerships are an increasingly important part of Vormetric's overall go-to-market strategy, and in the past year the company has devoted substantial resources to building out its partner network. It has partnered with SIEM vendors such as Splunk, HP (ArcSight), IBM (QRadar), LogRhythm and Intel (Nitro) to be able to ingest Vormetric data to provide data security analytics such as predefined reporting and alerting. On the big-data side, Vormetric has relationships with the likes of SAP HANA, Cloudera, MongoDB, DataStax, Couchbase, Teradata and Hortonworks.

It has also established partnerships with most of the large cloud service providers in North America, some of which have embedded Vormetric's Transparent Encryption into their infrastructure and offerings as an additional service. Current cloud partners include Rackspace, FireHost, CenturyLink, Pegasystems, IBM (SoftLayer), Google (Cloud Platform), AWS, Virtustream and QTS. Vormetric notes that its cloud-related business is growing rapidly and generating a more material portion of its overall revenue: Q1 2015 cloud bookings grew more than 400% over the prior year.

Competition

As Vormetric has expanded its data-protection arsenal, its field of potential competitors has expanded pari passu. With the breadth of its current product portfolio now spanning database-, file-,

and field-level application encryption, key management, data masking and tokenization, big-data protection and now a SaaS gateway, the company's most frequent competitor is likely to be archrival and market leader SafeNet, which was recently acquired by Netherlands-based authentication giant Gemalto for $890m.

With the expansion of its big-data capabilities and the launch of data masking, tokenization and gateway encryption, Vormetric will also now vie with a growing range of less broadly constituted vendors in its various product categories. In the big-data-protection arena, for example, the company is most likely to encounter firms such as Dataguise and Voltage Security (recently purchased by HP). Vormetric also faces completion from big-data distributors themselves, some of which now offer their own native encryption after acquisitions last year – Cloudera's pickup of Gazzang, and Hortonworks' reach for XA Secure. While the latter may have skimmed off some low-hanging big-data fruit, we believe that Vormetric still has an ample pipeline of big-data opportunities with customers seeking more than a simple 'check the box' compliance purchase.

In the data-masking and tokenization space, Vormetric is most likely to face HP's Voltage, as well as Gemalto's SafeNet, Protegrity, Informatica and also potentially more specialized vendors such as Privacy Analytics. While Vormetric and Voltage overlap in some areas, there are differences: Vormetric may have an advantage in areas such as encryption for unstructured data and now gateway encryption, though it currently lacks email encryption and FPE. Both Voltage and Protegrity offer 'stateless tokenization,' which in simple terms removes the need for a separate token database and lookups that can impact performance. Vormetric does not currently offer stateless tokenization, though its product is designed so that lookups can be load-balanced between several servers to prevent a single server from becoming a performance bottleneck.

We have written extensively about the primary vendors in the SaaS encryption market such as CipherCloud, Perspecsys and Vaultive. Players specifically focused on providing encryption and key management for cloud-based file sharing and storage include Covata, nCrypted Cloud, Ohanae, Sookasa and SafeNet with its SafeMonk offering.

SWOT Analysis

Strengths	Weaknesses
With its platform strategy, Vormetric has quietly assembled one of the broadest data-protection portfolios on the market, and now can address most use cases across on-premises, cloud and big-data environments.	Though its platform strategy has come a long way in the past year, the company's portfolio still lacks some advanced features such as FPE, encryption for more complex SaaS apps, stateless tokenization, and static data masking, some of which we expect it to address in future releases.

Opportunities

As cloud and big data make further inroads into the enterprise, the need to protect data wherever it lives will increase accordingly. We view Vormetric as being the most competitive with mid- to large-sized enterprises with heterogeneous environments that need to protect data across a wide variety of architectures and use cases.

Threats

One of the biggest threats faced by all providers of third-party data protection may come from cloud and big-data vendors that have or may elect to provide their own native encryption and key management. While native offerings may be a useful starting point for customers beginning their cloud journey, we believe that organizations with heterogeneous infrastructure will be better served over the long term by third parties that can provide centralized management of encryption keys and security policy administration.