REPORT REPRINT

Dome9 sails into new cloud-security waters with Magellan

FERNANDO MONTENEGRO, JEREMY KORN

27 APR 2018

The company is exploring a new frontier for its cloud infrastructure security functionality with its Magellan Enrichment Engine. Magellan is a data-augmentation feature that integrates disparate information sources to enable more intelligent search, alerting and visualization for cloud security.

451 Research®

 | WWW.451RESEARCH.COM

According to 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics survey from 2017, almost 50% of respondents with hosted cloud architecture said their organization lacked the internal security skillsets required to properly secure this infrastructure. Despite this demand, cloud infrastructure security vendors face a key challenge – not only must they keep pace with new threat vectors, but they also have to cater to the needs of their customers as IT infrastructure undergoes radical readjustment. Dome9 is looking to stay on top of these waves of change. The company is now augmenting its vendor-agnostic cloud security platform with supplemental data streams to add intrusion-detection functionality, in addition to its compliance capabilities.

THE 451 TAKE

The widespread adoption of cloud-based workloads continues unabated – increasingly so for workloads deemed high-risk or mission-critical. Coupled with the increased demands on staff in terms of skillset and work volume, this points to increased interest in options to secure cloud workloads. Dome9 is looking to provide specialized functionality that focuses on cloud-specific workloads. Departing from a protection and compliance feature set, the new Magellan offering represents some of the evolution that is being required from cloud security vendors. Magellan is a welcome addition that should help the company provide additional functionality as monitoring running systems becomes more relevant. Still, the recent acquisition of rival Evident.io by Palo Alto Networks highlights not only the increased interest in the sector – leading to increased odds of Dome9 as an acquisition target itself – but also the highly competitive nature of the sector.

CONTEXT

Dome9 was founded in 2011 and came out of stealth in 2013. The company currently has 80 employees – up from 40 in 2016 – distributed across its headquarters in Mountain View, California; R&D outpost in Tel Aviv; and field teams in North America and EMEA. The company is led by cofounders Zohar Alon (CEO) and Roy Feintuch (CTO). Alon has experience as CEO and in venture capital, and had roles at Check Point. Feintuch led technology at monitoring vendor DVTel.

The company most recently raised $16.5m in series C funding from Softbank in April 2017, bringing its total funding to $29m. Dome9 says it has over 300 customers, including more than 100 Global 2000 customers, primarily in the financial services, technology and manufacturing sectors. Eighty percent (80%) of the company's revenue comes from the North American market, and 85% comes from enterprise customers. Dome9 claims to have year-over-year revenue growth of 150%. 451 Research estimates the company's revenue to be $10m-15m.

STRATEGY

Since releasing its products in 2013, Dome9 has made a transition from agent-based to agentless architecture. This reflects the company's strategy of focusing on securing workloads hosted at public cloud providers in lieu of also incorporating legacy datacenter architectures.

Initially focused on AWS only, the company transitioned to add Azure and Google Cloud support in early 2017, which was well received by customers. It has also made its offerings available on both AWS and Azure marketplaces. The company is quite clear that the focus for its offering is large enterprises. According to Dome9, these are the customers that have the highest awareness of the need for cloud security, that can benefit from the 'guard rails' that the company can provide to cloud operations, and that appreciate the challenges of cloud security at scale.

The company looks to support the needs of enterprises with different maturity levels of cloud security management. Some enterprises centralize security policy and operations, while others have more distributed operations while centralizing policy decisions.

PRODUCTS

Dome9 has evolved its Arc security platform to leverage the strong API capabilities offered by the public cloud providers, on top of which Dome9 offers its own security functionality. The platform is more closely aligned with cloud services as provided by AWS, but Dome9 has had a strong presence in Azure for over a year, and has increased its presence in Google Cloud as well.

Verifying the state of security groups, firewall rules and other cloud infrastructure security is the original functionality that Dome9 provided. It remains a key part of the Arc platform, and Dome9 is able to both collect information and present visualizations that can aid in identifying and preventing misconfigurations and possible vulnerabilities.

Dome9 enhanced its compliance and governance capabilities in mid-2016. This included ready-made support for well-known industry targets, such as PCI-DSS, HIPAA, NIST 800-53 and others. Customers are also able to create their own standards using a simplified specifications language. Compliance differences can be simply reported on or automatically remediated depending on policy. Dome9 looks to provide identity protection via the IAM Safety offering, which layers on top of the existing IAM controls on the cloud provider for more granular control over roles. IAM Safety preemptively locks down access to high-risk credentials or roles, and then provides a method for out-of-band just-in-time authentication.

Up to this point, the basic functionality on the Arc platform security has been centered on interpreting current cloud configurations against a model of where a customer wants cloud security to be. The company recently announced new functionality – named Magellan – that seeks to incorporate more real-time information into the security models it creates.

At present, Magellan consumes AWS VPC flow logs. Dome9 indicates that it will include other log sources – AWS CloudTrail, service-specific logs (S3 as an example) and (later) AWS Guard Duty data, as well.

One of the key differences in cloud environments is the ephemeral nature of elements. As workloads and instances of virtual machines, containers or serverless functions execute, information that used to be considered static, such as IP addresses, can no longer be relied upon. A key functionality for Magellan is to enrich information such as VPC Flow Logs with additional details about the workloads that the logs refer to. By doing this, it provides a more detailed view of events at runtime, allowing for a more precise understanding of the environment and enforcement of security rules. Enriched data is made available via JSON and can optionally be consumed as SNS messages.

Dome9 envisions four major use cases for Magellan: visualization of current and actual security state via its Clarity engine, as an intrusion-detection system for cloud infrastructure, as a near-real-time alerting system for noncompliance for automatic remediation, and as a data source for streaming enriched data to other analytics platforms (such as enterprise SIEM). Moving forward, the company looks to improve its event-detection capabilities and support for additional threat-intelligence integration.

COMPETITION

The cloud infrastructure security market has grown quickly over recent years, commensurate with adoption of cloud infrastructure and increased concerns about network security. Competition stems from multiple sources.

The large public cloud providers all have compliance and security offerings that were created through some combination of native development or acquisition. For example, AWS launched GuardDuty, a threat-detection service, at the end of 2017. In early 2018, AWS acquired Sqrrl, a security analytics company, to augment its offerings. Azure and Google also have significant offerings aimed at providing compliance and monitoring information for customer workloads.

Public cloud customers also have their choice of third-party security vendors, including CloudPassage, Evident.io (which will soon be acquired Palo Alto Networks), Alert Logic, Threat Stack, Cavirin, Saviynt, RedLock, Lacework, CloudCheckr and Cloudvisory, among others. These vendors provide varying options of configuration control and compliance management.

Lastly, a number of incumbent enterprise vendors also contest the cloud infrastructure security market, including Cisco with its Tetration offering, Trend Micro, McAfee, Symantec and others. Dome9's approach of layering services on a common platform is similar to that of Qualys, which also supports some level of API access to cloud providers.

SWOT ANALYSIS

STRENGTHS

Dome9 has evolved its cloud security offering to incorporate lessons it has learned, and seems to cover most of the critical use cases for cloud security. The IAM Safety feature provides further protection for sensitive accounts.

WEAKNESSES

Magellan represents a new avenue for providing functionality, but it must quickly evolve to include additional data sources beyond VPC Flow Logs and expand beyond AWS, particularly to differentiate from services such as Guard Duty.

OPPORTUNITIES

The broad acceptance of cloud services has tilted to the point of it being the preferred destination for many new workloads. This brings significant attention to how to provide adequate security oversight in this environment.

THREATS

The increased importance of cloud delivery also brings massive interest from competitors, ranging from specialized vendors to strategic IT providers and the cloud platforms themselves. Furthermore, vendors must navigate changes in buying patterns favoring different functionality.