

## Dome9 comes out of stealth with firewall management for cloud systems

**Analyst: Andrew Hay**

Tel Aviv-based **Dome9** has released a cloud-centric firewall management platform for hosted **Microsoft** Windows and Linux operating system native firewalls. Targeted at enterprise users and hosting providers, Dome9 aims to make security policy control for cloud, virtual and physical servers, in addition to **Amazon's** EC2 Security Groups, easier to agnostically manage across all major operating systems and service providers.

### The 451 Take

The ability to maintain command and control, even when IP addresses change, should be of great interest to IT administrators struggling with heterogeneous endpoint rule administration. An interface with a common look and feel should help administrators who may be unfamiliar with either Windows- or Linux-based firewall configuration to manage both rule sets with a single point-and-click interface while providing on-demand access to systems as required by the business and its users. Another interesting aspect of Dome9's product is its pricing. You are billed using either the \$20-per-month-per-server pricing model or at a rate of \$0.28 per hour, whichever model costs less at the end of the monthly billing cycle. This pricing model would likely be very attractive to development shops leveraging micro instances of Amazon's cloud infrastructure for development, testing and troubleshooting exercises.

### Context

Dome9 is led by CEO and cofounder Zohar Alon. Alon started his career by establishing the Internet division for **Calanit Group**, an Israeli software distributor. In December 1996, Alon joined **Check Point Software** as a technical marketing manager, where he established the technical marketing department in 1996 and led the group for over two years. In 1999, Alon moved into a product manager role and began work on Check Point's service-provider product offering, which later became known as Provider-1, and Check Point's GPRS/3G firewall product, Firewall-1 GX. When Alon left Check Point in January 2004, he acted as an independent adviser for several Israeli VC firms to evaluate software-based startup companies. As a result of this experience, Alon became a venture partner at **Evolution Venture Capital** while founding (and leading) fantasy sports betting platform **BetUknow**.

Roy Feintuch, the company's other cofounder and current CTO, began his career developing software for companies like **Telly Advanced Systems**, **Solid Capital** and **SeaPass**. Prior to

founding Dome9, Feintuch was a development team lead and systems architect for **DVTel's** IP-based physical security products. At DVTel, Feintuch served as the chief software architect, leading the architecture team and several R&D processes, and was in charge of special projects for the company.

Although primarily based in Tel Aviv, the company has started to expand its reach with the hiring of San Diego-based Dave Meizlik, formally of **Websense**, who serves as the company's VP of marketing and is in charge of Dome9's business development initiatives. Dome9 is currently in the process of opening a San Francisco-based office to house its sales and marketing personnel, which the company plans to fill in relatively short order.

## Products

Dome9 bills itself as cloud security management-as-a-service, but perhaps the best way to describe its product is system firewall management with a SaaS management interface. The installable agents, available for Microsoft Windows, **Red Hat** Enterprise Linux (RHEL), CentOS, Ubuntu and Debian Linux, allow Dome9 to centrally manage the firewall rules on deployed systems. The agent reaches out to Dome9 Central, the company's SaaS management interface, using a secure polling mechanism that checks to see if any new rules need to be pushed down. This polling method is quite useful when an endpoint's IP address changes, enabling Dome9 Central to maintain management even if the system is moved to a different cloud infrastructure or is leveraging a dynamic IP address that has the potential for random IP assignment. If you are using Amazon's Elastic Compute Cloud (Amazon EC2) and simply want to manage the Amazon Web Services (AWS) EC2 security groups, the installation of the Dome9 agent isn't required. All security policy management actions are performed through the AWS EC2 API interface, and all that is needed is the generation of an AWS API key and some simple configuration on Dome9 Central.

The product is managed from Dome9 Central, which provides management of distributed firewall agents and serves as the configuration point for all firewall rules and administrative functions. Within Dome9 Central, a user is presented with three tabs. The 'Manage' tab allows the administrator to add new servers where the agent is already installed, define AWS security groups and administer users. Specific services can be opened or closed for the system, and existing rules can be added, modified or deleted entirely.

The 'Audit' tab provides access to activity auditing primarily for compliance purposes. A full inventory of changes in policy is recorded, including rule changes, access lease requests, user login, and service lease acquisition and termination. Dome9 states that it is currently working on sending its audit log via syslog or another more consumable log transport method for better integration with ESIM and GRC products.

The 'Access' tab, the place where administrators will spend the majority of their time, allows administrators to provide access to locked-down services for those systems that have been defined within the 'Manage' section of Dome9 Central. Invitations can be sent to users, informing them of access, for specific systems or all systems managed by Dome9. Access time limits can also be defined (e.g., one hour, one day or one week) and automatically closed after the predefined amount of time has expired – something a traditional endpoint

firewall is unable to do on its own. The tab also displays active access leases pertaining to specific system ports, expiration time, system scope and assigned users. Administrators also have the ability to terminate access to an actively assigned lease by simply clicking the 'Terminate Access' link for the associated rule.

Although Dome9 is targeting cloud-deployed systems, we can see several use cases where the company could also extend its management. For example, organizations are still struggling to push security controls down to 'road warrior' employees with laptops that infrequently connect back to the head office for firewall policy and configuration updates. Mobile devices are another concern. Organizations are allowing end users to bring their own devices into the office, and many are allowing those devices on the network – some even allow certain to be used for work purposes, which could lead to all kinds of privacy and personally identifiable information data-loss possibilities. Dome9 could leverage its centralized management capabilities to manage road-warrior systems with nothing more than some changes to its marketing literature, since the technology is already in place to deploy and manage firewall rules. The company would, however, have to develop mobile-device support – an easy task for the Linux-based Android operating system, but a much more involved R&D effort for **Apple's** iOS-based devices.

## Strategy

The company is offering its product in two flavors. The first is a personal free version that is available for noncommercial use and supports the installation on one server with one administrator, and does not include auditing or Dome9 API Connect. The second edition is a pay-as-you-go model that comes in at \$20 per month per server (or \$0.28 per hour, whichever results in less at the end of the monthly billing cycles) after an initial 14-day trial window expires. As more servers are added to an account, the total price decreases. The pay-as-you-go edition also includes secure access leases, multiple admins and auditing capabilities. Although the company is primarily based in Israel, Dome9 is aggressively targeting the North American market through a mixture of direct sales and service-provider relationships. Dome9 already has a partnership with **GoGrid**, and is talking to a number of others about partnering. The company also feels that MSSPs would do well to add Dome9 to their services portfolio, bundling the management and monitoring of customer cloud systems into existing security services. Dome9 has stated that the product can easily be OEMed or white-labeled for a service provider, given its SaaS-based management interface.

## Financial

Receiving somewhere north of \$2m for its first funding round through **Opus Capital**, Dome9 claims that Opus was the first company that it spoke with outside of Israel, and that their priorities lined up for the future growth of the business. Prior to receiving funding, the company operated in a primarily bootstrapped model, but, even then, was fairly confident of its sustainability for the next 2.5 years – even if the headcount were to double. We suspect that the company will likely field more investment calls with the opening of its San Francisco office, and might even rival the interest received by **CloudPassage**.

## Competition

Dome9's primary competition is likeminded firm CloudPassage – at least from a firewall management perspective. CloudPassage differs in that it also has a vulnerability and FIM angle that pits the company against a greater swath of entrenched vendors. Even though the management of firewall rules is limited to Microsoft Windows Firewall and the open source IPTables firewall for Linux-based systems, the firewall will compete with every single endpoint-protection vendor on the market, including, but not limited to, **McAfee**, **Symantec**, Check Point, **Sophos**, **AVG Technologies**, **Novell**, **Trustwave** and **IBM (BigFix)** – of course, the list becomes longer every day. Should customers without budget for costly endpoint-protection products find themselves specifically searching for something to manage their Windows and Linux host firewall rule set, however, Dome9 may be able to block the traditional players at the cloud horizon.

## SWOT analysis

Strengths	Weaknesses
The portability of Dome9 will likely be a key selling feature for IT systems and operations folks wondering how to extend traditional firewall protection to cloud instances. Users will enjoy not having to worry about updating rules to accommodate IP changes – something that plagues manual rule management on endpoints.	Dome9 needs to quickly establish itself in the Americas to drive profitability and sustainability – not to mention awareness of what it is capable of. The company would do well to hire a US-based thought leader with close ties to the operational security and IT community to serve as its pitchman.
Opportunities	Threats
We'd like to see Dome9 embrace Apple's OS X operating system in addition to some of the more popular mobile device platforms, such as Google's Android and Apple's iOS. If the company could boast firewall management for cloud, virtualized, server, laptop and mobile platforms, we feel that the company could make itself of more consequence to prospects.	Like CloudPassage, Dome9 must become sticky – and quickly. There is a real threat of cloud providers like Amazon, Microsoft and Citrix building a competing application that would block both companies at the door, although portability across disparate cloud architectures would likely not be of paramount importance like it is to Dome9.

Reproduced by permission of The 451 Group; copyright 2011-12. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to: [www.the451group.com](http://www.the451group.com)