EMA Case Study: The SaaS Model Stands Out in Global Vulnerability Management

A Case Study from the 2010 EMA Research Report, *Security as a Service*

The complexity of IT in the world's largest enterprises can be one of the most daunting challenges in security management. For these organizations, automation is critical for processes such as vulnerability assessment—but automation by itself isn't enough. These organizations need worldwide scalability from their vulnerability assessment tools. At the same time, vulnerability assessment must go deep as well as broad, able to drill-down on specific issues in individual systems, no matter where found. Tools must also deliver practical analysis and reporting of assessment in order to support their primary purpose—the management of risk in IT.

Global enterprises can hardly afford to cut corners on security management, particularly in today's threat climate, but resources spent on security become unavailable for other priorities. How can enterprises best deal with issues such as vulnerability management on a worldwide scale, when they may have thousands (if not millions) of resources, each with its own security requirements, on nearly every continent?

Cisco claims as many as 30 million IP addresses subnetted into more than 56,000 networks—and a team of approximately 13 to oversee vulnerability assessment.

Defining a Global Challenge

This was the question facing a team responsible for securing one of the largest and best-known technology vendors in the world. Cisco Systems claims as many as 30 million IP addresses or more, subnetted into more than 56,000 networks—and a team of approximately 13 to oversee vulnerability assessment (VA) and coordinate vulnerability management with other groups worldwide.

This extreme disparity in scale between the assessment team and the challenge they faced required them to define their vulnerability assessment objectives clearly:

- Their most immediate priority—high-risk assets exposed in DMZs worldwide.
- Because of this global distribution of assessment targets, automation and performance would be critical. Ideally, they would seek to perform rapid scans for high-risk resources in three days or less, across the entire organization.
- At the same time, onsite and internal scans would be required for drill-down on specific issues, or to support local security efforts. This would require the ability to scan both outside and inside network boundaries, in a phased deployment that would expand vulnerability assessment throughout the organization.

©2010 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

In addition, the ability to provide usable analysis of assessment data—on a global scale, across tens of thousands of often highly changeable networks—was key:

- The identification of resource owners and support groups as well as unauthorized hosts and services in production DMZs would be key to containing risk exposures—particularly considering the high risk of unmanaged, poorly managed and "orphaned" systems in an enterprise of this size and reach.
- Incident response requirements meant that the preferred provider would need to quickly identify unauthorized functionality or network connections, differentiating legitimate links from unauthorized backdoors or other exposures.
- The support of regulatory compliance, globally, would be a significant goal.
- Output data would be required to integrate with other management tools, such as Security Information and Event Management (SIEM) worldwide.
- Metrics providing insight into the effectiveness of vulnerability management would be required, for tactical operational management as well as to inform strategy.

As one of the earliest entrants in the market of hosted security services, Qualys had built a reputation for scalability and performance, as well as for reliability and support.

The Qualys Advantage

Initially, Cisco vetted 10 vendors, but eliminated 3 early on because of their inability to support the scale of automation required. An additional 3 were eliminated, since they used highly similar technology as one of the final four selected for a "bake-off."

Among this final group was Qualys, which was chosen in part because of the following qualities:

- QualysGuard's hosted model provides on-demand scanning and assessment worldwide, from a central point of delivery as a service.
- Because the hosted model requires the provider to ensure scalability and performance, the model mapped well to this corporation's requirements.
- QualysGuard's SaaS delivery model is complemented by QualysGuard appliances, which can be placed behind network firewalls for local or in-depth scanning capability.
- As one of the earliest entrants in the market of hosted security services, Qualys had built a reputation for scalability and performance, as well as for reliability and support.

The final group of four candidate vendors was then subjected to rigorous testing in an environment containing known vulnerabilities to evaluate ease of deployment, ease of use, scan duration, false positives, false negatives, reporting, and other factors. "And," says Doug Dexter, Cisco's team lead for this effort, "we broke every vendor's product—including Qualys."

But it was that event that made Qualys begin to stand out for the evaluation team. "What I really admired about Qualys was that their CTO actually thanked us," says the team lead, "since he viewed this event as an opportunity to make the product better. His view was that, if it works here, it will work for any other Qualys customer." This rational commitment to customer support and service improvement earned high marks for Qualys and was a key factor leading to its final selection as this organization's ultimate choice.

©2010 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

SaaS + Automation = A Worldwide Deployment Made Practical

Cisco has now been a Qualys customer for over five years, in a phased deployment that has continued to expand over that time, even though the initial phase of adoption was virtually instantaneous. "Because of the SaaS model, we were able to begin using QualysGuard immediately, from day one," says the vulnerability assessment team lead. The external scanning capability of the QualysGuard service kept this customer from having to purchase and deploy external scanning systems. No infrastructure setup was required, nor was there any need to provision connectivity between internal and external networks just to enable external vulnerability scanning.

In the second phase, the Cisco team deployed seven QualysGuard appliances at locations worldwide, initially to scan data center resources. The third phase of deployment extended this capability more widely throughout the organization, with a combination of hosted external scanning and internal scans originating from the seven QualysGuard appliances.

With fundamental assessment capability in place, the fourth phase of deployment marked the point at which QualysGuard capabilities for large-scale automation of assessment, analysis and reporting would become critical to the success of this global vulnerability management program. This would also require integration with equally large-scale network management.

Because Cisco's extensive networks change daily, vulnerability assessment tools must effectively create a new map of the entire network in the vulnerability assessment system on at least a monthly basis. QualysGuard's ability to deliver performance at scale through its hosted model made it practical for this global customer. Scan and reporting groups are also created monthly through the QualysGuard API, with "scan asset" groups based on scanner location, "reporting asset" groups based on the group providing support, and excluded networks determined for IP telephony subnets, extranets, and other networks not included in scans. "Tens of thousands of these groups are created and deleted each month, all via the QualysGuard API," reports the VA team lead. This ability to respond to the company's actual network, scanning and reporting changes makes the Qualys approach a realistic solution for their large-scale demands.

Although this third deployment phase has taken approximately 1-2 years to complete, the results have been highly satisfactory to the Cisco team. They estimate their costs of incident response at $250,000 per incident ("as a ballpark figure at least," as Dexter puts it). At a minimum, QualysGuard enables them to find, on average, four open proxy and six open telnet servers in their lab DMZs each year. By eliminating these incidents alone, the company estimates a minimum savings of over $2 million per year in incident response.

QualysGuard also enables them to centralize global vulnerability reporting into a consolidated view which can be queried as needed to yield data based on any number of parameters, such as vulnerability severity, asset or scan group, or network location. This allows them to identify their highest priority vulnerabilities for remediation. Says Dexter, "the ability to group and prioritize vulnerabilities reduces data to metrics that become a conversation about how much risk our constituents are willing to tolerate in their data centers as a function of how much they have, or need, to spend on vulnerability management. Now they can know what assets are affected, the severity of vulnerabilities detected, groups affected, and so on. We didn't have the ability to collect and analyze assessment data in this way before, and certainly not on this scale."

©2010 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

QualysGuard's on-demand scanning capability continues to yield benefits of high value to this truly global organization—but the SaaS model offers other benefits as well. The transparence of technology maintenance enabled by the SaaS model has high appeal. Says Dexter, "We began with Qualys at version 3 of their service. Today, we're at version 7, and we didn't have to do a thing. Oh, and by the way, we also got PCI capability added to this service without having to lift a finger—it just showed up. You can't imagine how happy we are."

As a company, Qualys continues to earn the loyalty of this customer, in part through its ongoing dedication to service improvement and support. What began with a recognition of the opportunity presented by this organization's unique challenges has continued throughout its Qualys customer relationship. "Ever since our initial evaluation of their capability, Qualys has been very proactive in keeping their service competitive. They recognize that when they improve things for us, *all* their customers benefit." This ability to extend service improvement for one customer to all those served is a hallmark of the SaaS model that continues to build traction for Security SaaS, and for Qualys as an early visionary that has played a major role in defining its market—but it is Qualys' commitment to customer support that helps it maintain its edge in the dynamic and growing field of Security as a Service.

> "Qualys has been very proactive in keeping their service competitive. They recognize that when they improve things for us, all their customers benefit."

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter (http://twitter.com/ema_research).

2101-QualysCS.061610

©2010 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com