FROST & SULLIVAN

QUALYS®

2017 Global Vulnerability Management Market Leadership Award

Contents

Meet the Analyst

Frost & Sullivan analysts specialize in particular markets and industries, tracking these spaces from year-to-year. They constantly engage and interact with market participants, technology and business partners, customers, and related companies within the value chain. Frost & Sullivan analysts also attend industry tradeshows and conferences throughout the year, interview with trade and industry media, and speak on panels and in keynotes, keeping them tuned in with the latest developments of their given industry.

Background and Company Performance

Industry Challenges

Vulnerability assessment (VA) is a network scan technology that runs a detection script of known vulnerabilities against an endpoint. Vulnerability management (VM) is the formal reporting and actionable intelligence that happens after the scan.

If vendors only offered vulnerability assessment, the service would be invaluable as the best incident detection strategy is to harden a security surface before a breach occurs. However, VM platforms also offer visibility and contextual awareness on what exists on the endpoint. During a VA scan, the VM platform creates a comprehensive inventory of the OS, protocols, applications/software, ports (network mapping), and services on the endpoints being assessed.

VM vendors compete against each other for clientele. An accurate scan technology is self-evidently a key buying criterion. However, customers seek VM vendors for other important reasons:

- **Vulnerability prioritization.** Finding vulnerabilities in a network is not difficult to do, but prioritizing vulnerabilities in terms of which can cause the most damage if exploited and doing this accounting for time, accessibility, and the value of the asset is the fruition of the craft in action.

- **Integration of VM with other network security technologies.** Multilayered network security is the most prevalent enterprise network approach. Many companies make investments in next generation firewalls (NGFW), security information and event management (SIEM), and intrusion detection and prevention (IDS/IPS) platforms. Information shared across platforms occurs bidirectionally through APIs. This shared information bolsters the efficacy of each platform as well as the efficacy of the collective.

- **Compliance auditing and compliance reporting.** An important aspect of VM is reports can be fashioned to prove National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS), or other vertical market compliance standards. Importantly, VM platforms can generate reports that show all of the scanned endpoints and infrastructure equipment that comply with dynamic inventory control, which is a key requisite of many compliance standards. (For example, the US federal government requires all of its agencies to provide a monthly comprehensive report of all endpoints and what OS and software has been uploaded to each endpoint device).

- **The ability to scan multiple environments.** VM scanning is now expanded to include public and private cloud environments, mobile devices, Internet of Things (IoT), as well as traditional on-premises networks.

In technology, the idea of "frenemies" remains true. While it is true that VM platforms can be joined with other network security technologies for better visibility of the enterprise network, it is also true that other cyber security technologies are trying to enhance the value of their own vendor relations. SIEM, NGFW, and network access control (NAC) providers provide variations of contextual awareness of the endpoint. VM vendors do not have a cozy niche in cyber security anymore.

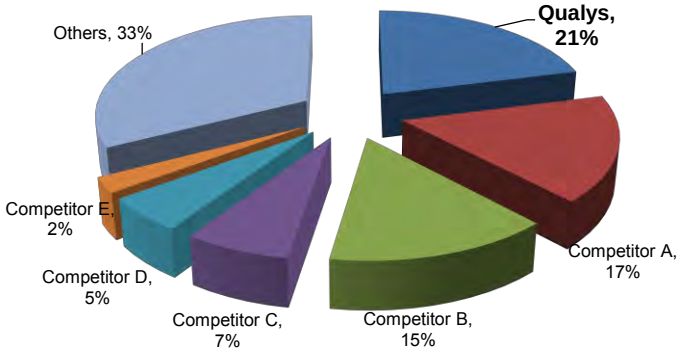
Market Leadership

Frost & Sullivan has monitored VM technology since 2009 and in all subsequent reports, Qualys has been identified as the market leader. This Best Practice award discusses what Qualys did to lead the pack in terms of global VM revenues. Worth noting is that not only did Qualys demonstrate market leadership in VM for another year, the company is evolving its product architecture and expanding its services in anticipation of competition from network endpoint detection and contextual awareness tools.

Growth Strategy Excellence

In 2011, Qualys competed with McAfee Foundstone, Rapid7, Tenable Network Security, and nCircle for supremacy in VM. At the 2011 RSA Security Conference, Qualys announced the Qualys IT security and compliance SaaS suite of applications in the cloud. At the time, the only other major VM solutions were VA scanners deployed as on-premises software, or as physical appliances. The Qualys decision to offer SaaS, and their procurement option both shaped cloud-based VM deployments and annual service subscriptions. Web-based and cloud-based deployment options allowed companies to forego CAPEX expenses for cyber security software to more palatable OPEX expenditures. Additionally, this change in procurement and delivery options also improved the attractiveness of Qualys VM solutions with midsized companies.

2016 VM Global Revenue Market Share



Source: Frost & Sullivan

While Qualys enjoys the market leadership in global VM revenues, the company is not stopping at VM market share leadership alone. Qualys has designs on becoming the preeminent network cyber security solutions provider. Toward this goal, Frost & Sullivan identified five Qualys strategies consistent with the products Qualys has developed and with its vision stated in its November 2016 Qualys Investors' Day.

1. Create security products that are aligned with the network architectures and digital transformation business use cases of its customers.

2. Immediately and properly identify and tag on-premises, public or private cloud-based assets and endpoints as they enter the network.

3. Provide customers the ability to continuously scan their network environment via network scanners or self-updating cloud agents.

4. Offer continuous threat monitoring services for static systems/endpoints and Web applications.

5. Assist clients in consolidating the number of tools they need to effectively protect their networks as those networks expand into elastic clouds and with digital transformation.

The objectives are lofty. Viewed in concert though, the mix of technologies makes sense.

The enterprise network encompasses mobile, IoT, private, and public cloud environments. To meet the new requirements for comprehensive network visibility, Qualys expanded from on-premises scanning into decentralized scan capabilities utilizing multiple form-factors—Web-based, virtual appliances, cloud-based, and on-premises scanning appliances. Asset collection and discovery is a compliance requisite and an assurance that all possible attack vectors are at the least accounted for. Lastly, right-minded cyber security vendors will try to help their clients integrate existing tools with new platforms, or provide more comprehensive platforms that encapsulate aspects of different technologies that would otherwise be purchased separately. All of these are products and technologies that Qualys already offers.

Product Quality

The availability of different products and strength of reporting platforms has pushed Qualys to the top of global VM market share. However, the accuracy of VA scans is the long card for VM vendors, and Qualys owns a strong VM scan technology.

The depth of Qualys' scan capabilities is significant. Qualys is able to fingerprint all of the assets in a network. When a device enters a network, Qualys scanners can fingerprint the device and catalog the device's IP address, its OS, where it is mapped to, determine if there are SSL certificates, and provide a rating on the device's security/compliance posture.

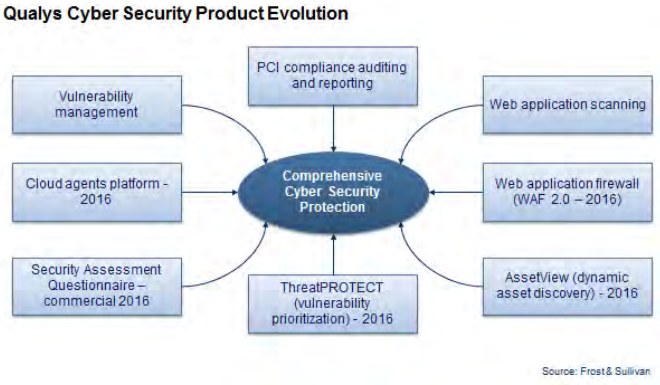
The Qualys core scan technology creates an inventory of the OS, protocols, ports, and services on the device being tested. This inventory is then used to seed a Qualys-developed vulnerability expert system, which chooses the appropriate set of vulnerabilities to test from hundreds of modules. Essentially this creates a customized scan for each endpoint/target. As a result, Qualys tracks all defects in its scanning solution and reports a six sigma accuracy rate of less than six defects per million scans.

The fingerprint also helps to establish a known good state, an individualized "golden image" of the device. The golden image is useful for several reasons. The golden image becomes the baseline for compliance. A network security team can establish scan and compliance parameters based upon the golden image—if a device shows different characteristics from its golden image, this can trigger an alert.

Golden image technology also bridges the transition between scans. In practice, a VA scan runs scripts of known vulnerabilities against endpoints. However, new malware strains, new OS, or uploaded applications can change the vulnerabilities that a device can be exposed to. To address this issue, Qualys developed Prediction engine Z-Analyzer. If a vulnerability is discovered between scans, the Prediction engine triggers the scan engine to scan endpoints most likely to be infected based upon changes against the golden image of one device.

Technology Leverage

On the surface, contextual awareness is the collection of endpoint information including: infrastructure equipment the endpoint belongs to, the OS, and applications associated with the endpoint; and which asset groups the endpoint belongs to. A proper assessment of contextual awareness provides both historical baselines and proof of compliance, and generates a predicative value. As contextual awareness becomes the cornerstone of any threat detection and mitigation planning, comprehensive, current, and reliable endpoint contextual knowledge is essential and extremely valuable.



With an earned reputation established in VM, Qualys has expanded its cyber security product lines.

The first products that leveraged Qualys scan technology were related to PCI compliance reporting and auditing. The Qualys Cloud Suite for PCI is sold as an annual subscription that includes unlimited scanning. Qualys has offered Web Application Scanning since 2012, meaning Qualys has offered preventative scan technology for the network security surface and for Web applications for the better part of five years.

Qualys introduced five significant products in 2016; a brief description of each new product follows:

- **ThreatPROTECT.** ThreatPROTECT is designed to help companies understand which vulnerabilities should be acted upon first accounting for exploitability, threat expansion, and the asset's business value.

- **Security Assessment Questionnaire (SAQ).** An example of how the Qualys SAQ is used is in healthcare. A large healthcare provider might use subcontractors (Cigna might send work to an x-ray operator for example). In some cases, the healthcare provider may assume some indemnities. The SAQ can be used to ensure that subcontractors remain compliant. Additionally, SAQ can be used centrally by an organization to ensure individual departments meet internal compliance requirements.

- **Cloud Agent Platform.** In 2016, Qualys introduced agents deployed onto devices. The agents can be installed as lightweight (3 MB) virtual or software agents that are remotely deployable, centrally managed, and self-updating. Cloud Agents can be installed on endpoints, on-premise systems or within cloud environments for real-time vulnerability management and compliance monitoring. Qualys is also working on expanding its agent technology to provide file integrity monitoring and indication of compromise detection capabilities.

- **AssetView.** Used in concert with Cloud Agents, AssetView provides dynamic asset inventory, reporting, and fast search across millions of devices on a company's hybrid-network.

- **Private Cloud Platform Appliance.** A compact, private cloud solution for medium-sized companies, PCPA reduces the same robust private cloud security and compliance services found in the Private Cloud Platform into a purpose-built 1U appliance form-factor.

The cumulative effect of the new 2016 technology innovations is to give network security teams improved visibility of devices regardless of form (physical or virtual), transiency (static or mobile), and location (cloud or on-premises).

Customer Ownership Experience

In an ideal scenario, network security platform providers would have their own security platforms deployed in the enterprise's network. For VM platform providers, this is rarely the case. In 2016, some of the most significant announcements made by Qualys were about partnerships and integrations with IT/security tools. The following integrations were announced in 2016.

- Qualys Cloud Platform and Cloud Agents are both natively integrated with Microsoft Azure Security Center to automatically detect Azure virtual machines (VMs), streamline bulk Cloud Agent deployment, plus quickly identify vulnerable VMs from within the Azure Security Center.

- An integration with Infoblox' DNS, DHCP and IP Address Management (DDI) solution to provide notification to Qualys Cloud Platform when new physical, virtual, or cloud infrastructure elements join the network and when malicious events are detected.

- Qualys Cloud Platform is integrated with Cisco's threat-centric NAC technology to help change role based end user network access contingent upon the vulnerabilities detected.

- An integration with ServiceNow ticketing software allows IT teams to address alerts and security issues in the context of IT workflows.

- An integration with Lumeta was formed to add bidirectional contextual awareness of both platforms.

- Toward remediation, Qualys Cloud platform can be integrated with HEAT Software PatchLink technology.

- Qualys Cloud Platform can be integrated with Splunk to power VM and Web Application Scanning (WAS) data analytics.

Customers are making extended use of cloud architectures to host services and push applications. Qualys has completed native integrations with major public cloud platforms, including Microsoft Azure, Amazon Web Services and Google Cloud Platform. Qualys also offers Private Cloud Platform solutions (including a Qualys private cloud operated by Deutsche Telekom in Europe) for large and medium-sized enterprises that have geographic data restrictions. To that end, Qualys recently opened new Secure Operations Centers in the Netherlands and India to help further address customer data sovereignty needs. Worth noting, the Qualys Cloud Platform performs approximately three billion scans per year.

Qualys also made efforts in 2016 to increase its ability to support U.S. Government agencies adopting cloud-based security technologies, announcing that Qualys Cloud Platform had been granted an Authority to Operate (ATO) by the U.S. Department of Health and Human Services under the Federal Risk and Authorization Management Program (FedRAMP).

Other architectural changes are also worth mentioning if only because the network security surface continues to expand, and platform integrations can become wieldy. In 2016, Qualys went to Elastic search. By committing to Elastic search, Qualys can give customers visibility of every endpoint in a robust enterprise network in roughly two seconds, and continuously scans millions of assets per day. In terms of code, Qualys uses the same code base for all of its products. Consequently, repurposing modules to support customizable APIs is an intuitive process for customers.

Conclusion

Several years ago, Qualys set into motion two well-placed bets regarding cyber technology. The first bet was in cloud-based cyber security. While cloud-based services are now en vogue, at the time Qualys faced resistance because "the cloud" was not thought to be as secure as on-premises deployments, and cloud (Web) delivery mechanisms would be plagued by unacceptable performance fluctuations. Over time, as demonstrated with the rapid adoption of cloud services, these reservations have significantly diminished.

The second idea Qualys leveraged was endpoint scan technology as a gateway to additional network security services. Perimeter and prevention cyber security technologies are giving way to detect and respond technologies. Contextual analysis and analytics applied to endpoint behavior are fundamental to detect and respond, and Qualys continues to build platforms based upon these fundamentals.

Because of its strong overall performance, Qualys, Inc., has achieved a leadership position in Vulnerability Management, with a market share of 21% in 2016, and thus Frost & Sullivan recognized Qualys with the 2017 Market Leadership Award.

Significance of Market Leadership

Ultimately, growth in any organization depends upon customers purchasing from a company, and then making the decision to return time and again. Loyal customers become brand advocates; brand advocates recruit new customers; the company grows; and then it attains market leadership. To achieve and maintain market leadership, an organization must strive to be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition. This three-fold approach to delivering market leadership is explored further below.

Understanding Market Leadership

As discussed on the previous page, driving demand, strengthening the brand, and differentiating from the competition all play a critical role in a company's path to market leadership. This three-fold focus, however, is only the beginning of the journey and must be complemented by an equally rigorous focus on the customer experience. Best-practice organizations, therefore, commit to the customer at each stage of the buying cycle and continue to nurture the relationship once the customer has made a purchase. In this way, they build a loyal, ever-growing customer base and methodically add to their market share over time.

Key Performance Criteria

For the Market Leadership Award, we focused on specific criteria to determine the areas of performance excellence that led to the company's leadership position. The criteria we considered include (although not limited to) the following:

Criterion	Requirement
Growth Strategy Excellence	Demonstrated ability to consistently identify, prioritize, and pursue emerging growth opportunities
Implementation Excellence	Processes support the efficient and consistent implementation of tactics designed to support the strategy
Brand Strength	The possession of a brand that is respected, recognized, and remembered
Product Quality	The product or service receives high marks for performance, functionality, and reliability at every stage of the life cycle
Product Differentiation	The product or service has carved out a market niche, whether based on price, quality, or uniqueness of offering (or some combination of the three) that another company cannot easily duplicate
Technology Leverage	Demonstrated commitment to incorporating leading-edge technologies into product offerings, for greater product performance and value
Price/Performance Value	Products or services offer the best value for the price, compared to similar offerings in the market
Customer Purchase Experience	Customers feel they are buying the most optimal solution that addresses both their unique needs and their unique constraints
Customer Ownership Experience	Customers are proud to own the company's product or service, and have a positive experience throughout the life of the product or service
Customer Service Experience	Customer service is accessible, fast, stress-free, and of high quality

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Our analyst team strives to follow a 10-step process (illustrated below) to evaluate Award candidates and assess their fit with our best practice criteria. The reputation and integrity of our Awards are based on close adherence to this process.

STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	• Interview thought leaders and industry practitioners • Assess candidates' fit with best-practice criteria • Rank all candidates	Matrix positioning of all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	• Confirm best-practice criteria • Examine eligibility of all candidates • Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	• Brainstorm ranking options • Invite multiple perspectives on candidates' performance • Update candidate profiles	Final prioritization of all eligible candidates and companion best-practice positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	• Share findings • Strengthen cases for candidate eligibility • Prioritize candidates	Refined list of prioritized Award candidates
6	**Conduct global industry review**	Build consensus on Award candidates' eligibility	• Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates	Final list of eligible Award candidates, representing success stories worldwide
7	**Perform quality check**	Develop official Award consideration materials	• Perform final performance benchmarking activities • Write nominations • Perform quality review	High-quality, accurate, and creative presentation of nominees' successes
8	**Reconnect with panel of industry experts**	Finalize the selection of the best-practice Award recipient	• Review analysis with panel • Build consensus • Select recipient	Decision on which company performs best against all best-practice criteria
9	**Communicate recognition**	Inform Award recipient of Award recognition	• Present Award to the CEO • Inspire the organization for continued success • Celebrate the recipient's performance	Announcement of Award and plan for how recipient can use the Award to enhance the brand
10	**Take strategic action**	Upon licensing, company is able to share Award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess Award's role in future strategic planning	Widespread awareness of recipient's Award status among investors, media personnel, and employees

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.