

Managing Security Risks: Securing a Major Global Enterprise with Automated Vulnerability Management



www.sodexo.com

Thanks to QualysGuard Vulnerability Management, Sodexo has a higher level of visibility in regards to vulnerabilities across its network of global subsidiaries, covering approximately 13,000 IP addresses.

INDUSTRY: Consulting / Services

BUSINESS: On-site service solutions across corporate development, education, health care, facilities management and employee motivation.

SCOPE: HQ in France, worldwide

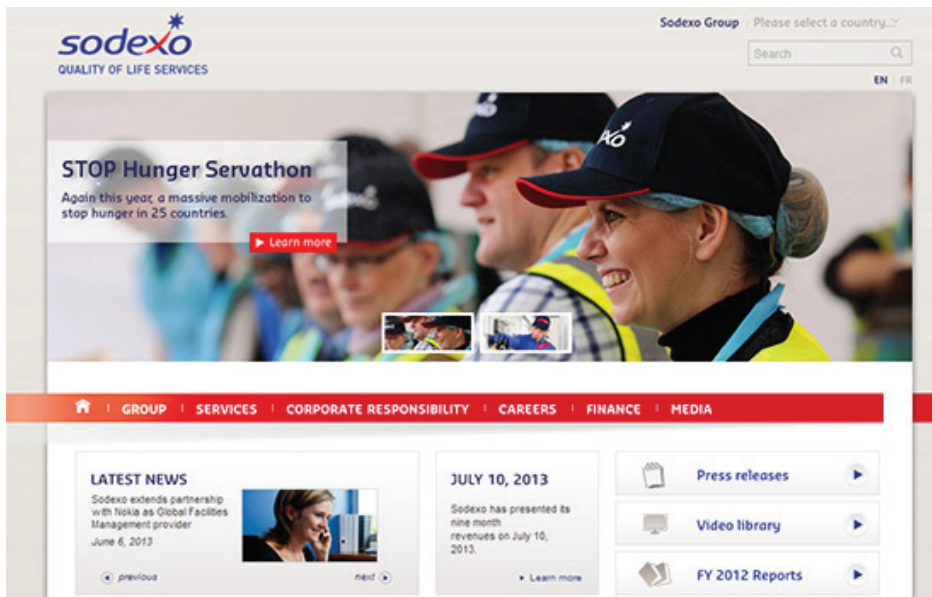
SIZE: 420,000 employees in 80 countries

BUSINESS CHALLENGE: Sodexo needed to improve the visibility of security vulnerabilities across its large and diverse Global infrastructure, covering approximately 13,000 IP addresses.

SOLUTION: Sodexo deployed QualysGuard Vulnerability Management (VM) as its strategic platform for maintaining visibility of threats to operational security.

WHY THEY CHOSE QUALYSGUARD:

- Flexibility: SaaS business model provides elasticity and removes the need for capital expenditure.
- Quality: The Qualys solution delivers accurate and timely assessments of security vulnerabilities, with actionable remediation plans.
- Comprehensiveness: The Qualys solution provides consolidated reporting at group, business unit and country levels, for a complete



As a leading and global company focused on delivering quality-of-life services, Sodexo offers a fully integrated set of innovative services in more than 100 categories across corporate development, education, health care, facilities management and employee motivation. With over 420,000 employees across more than 34,000 sites in 80 countries, Sodexo serves 75 million individuals daily and is the world's 20th largest employer.

To deliver its diverse set of services to the high standards its clients expect, Sodexo maintains a large set of IT resources across its different business units, subsidiaries and country operations. These now include new solutions based on private, public and hybrid cloud infrastructures. As the trend for digitization of services continues, and as Sodexo provides more web-based tools to staff and clients, the information-risk profile is constantly evolving – and the company must try to stay one step ahead of threats at all times.

To mitigate the IT risks represented by known and unknown

vulnerabilities, and to support a new global IT security governance framework, the Sodexo Global Technology Services team set out to deploy a standardized vulnerability management solution.

Full Lifecycle Auditing and Vulnerability Management

After evaluating several options, Sodexo selected QualysGuard Vulnerability Management (VM), leveraging the QualysGuard Cloud Platform, as its strategic solution for automating the lifecycle of network auditing and vulnerability management across its global enterprise. The QualysGuard solution provides a complete range of functionality, including network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking prioritized by business-risk profile.

John Bruylant, Group CTO at Sodexo, states the following: "The QualysGuard solution was superior to the solutions we considered. The software-as-a-service business model eliminates the need to make capital investments in dedicated infrastructure, and the quality, completeness and granularity of the reporting make it easier for us to understand the IT risks for our business. QualysGuard VM not only highlights and ranks the vulnerabilities, but also makes precise recommendations for how to remediate them. This is a critical advantage for teams in smaller business units that may have limited IT security resources. These teams can now quickly understand what they need to do and where to find additional information if necessary."

Building on Initial Success

A key factor in Sodexo's selection of QualysGuard VM as its global standard for vulnerability management was the successful track record of the solution within the company's Benefits and Rewards Services (BRS), previously called the Service Vouchers & Cards (SVC) Group. In 2004, the BRS business unit deployed QualysGuard VM to improve security for its 30 worldwide subsidiaries.

Previously, the BRS business unit had been struggling to manage on-site technical audits across its rapidly evolving infrastructure. Although these audits provided a clear and detailed view of the security level and risk profile for each subsidiary, with recommendations for improvement, it was not feasible to run them more frequently than once every two years.

The BRS business unit chose QualysGuard VM to complement its on-site audits, adding continuity to vulnerability management and providing a constantly updated view of the risk profile of its subsidiaries. The Qualys solution was chosen for its simplicity of deployment and administration, for its ability to meet the needs of subsidiaries of all sizes, and for its effectiveness in highlighting emerging vulnerabilities.

"QualysGuard VM not only highlights and ranks the vulnerabilities, but also makes precise recommendations for how best to remediate them – a critical advantage for teams in smaller business units that may have limited IT security resources."

John Bruylant,
Group CTO, Sodexo



Global Deployment for Comprehensive Security

IT security is never just about tools: equally important are the corporate structures and policies that embed a culture of security. Within the Global Technology Services department, Sodexo set up a Security Operational Services (SOS) team dedicated to improve the Information Systems security across the organization. "Our mission is to enforce IT operational governance and excellence, but without impeding the agility and effectiveness of the business units," explains Bruylant. "We have deployed QualysGuard appliances in our subsidiaries, and made it a group standard to act on the automated vulnerability reporting, so as to reduce the number of internal vulnerabilities."



Within the Sodexo vulnerability management program, the QualysGuard solution is offered to business units as an internal IT service. The VM leaders for each unit produce consolidated reports that measure the effectiveness of the program for their portion of the infrastructure.

Growing Standardization on QualysGuard

Today, Sodexo uses QualysGuard VM on a daily basis across its Global organization to scan for vulnerabilities in information systems. Scanning frequency depends on the criticality of assets and on specific events such as business mergers and acquisitions, major IT security incidents and so on. The internal audit department also uses the QualysGuard platform to conduct periodic assessments.

The solution ranks vulnerabilities according to the business risk they represent – determined in part using Sodexo's own rules for risk evaluation – enabling the company to focus on the most critical fixes and helping it to adopt industry best practices for remediation.

"The rule is that level 4 or 5 vulnerabilities – those that are urgent or critical – must be resolved with the highest priority according to the country's patch policy," comments Bruylant. "Thanks to the continuous improvements made by Qualys, the solution is becoming increasingly targeted and effective. QualysGuard VM can now correlate between vulnerabilities found on specific servers and identify the effective risk associated with a given vulnerability. For example, the solution will downgrade a defect initially graded as critical if it requires the exploitation of a vulnerability that does not exist on that particular server."

The scope of the Qualys solution at Sodexo continues to grow as the company's needs evolve. Initially, vulnerability scanning was limited to external access points, but it now also encompasses systems and equipment on internal networks.

Extending Security to the Cloud and to Payments

As it looks to address new business requirements in a cost-effective approach and to make new services available to clients, Sodexo is adopting massively agile cloud-based solutions.

To ensure security, the company plans to integrate the QualysGuard solution into the development lifecycle for new applications in the cloud. Equally, Sodexo is taking advantage of the QualysGuard functionality to maintain PCI-DSS compliance for payment services where appropriate.

“Thanks to the vision and ongoing evolution of our strategic partner Qualys, we are confident that the QualysGuard platform will continue to deliver risk intelligence analysis and predictions as our infrastructure grows and changes,” concludes John Bruylant. “The Qualys solution enables us to maintain a clear understanding of the operational security risks at the Group, Region and Country levels, and to make better decisions about the remediation of vulnerabilities.”