



“Five years on, we are still using the same solution but on a much broader geographic and functional scope. Herein lies the strength of the Software as a Service model : continuous and transparent integration of the evolution of our specific needs and those of the market in general.”



Abdellah Cherkaoui,
Chief Information Security Officer
Sodexo

SODEXO STRENGTHENS THE RELIABILITY OF ITS SUBSIDIARIES' INFORMATION SYSTEMS WITH QUALYS GUARD

Complementing on-site technical audits with permanent and automated monitoring and management of each subsidiary's IS vulnerabilities.

It was the ever-draining Danaides' barrel: relying upon on-site technical audits to help the teams of its thirty subsidiaries worldwide improve their IS security, Sodexo Service Vouchers & Cards' (SVC) group audit team could hardly repeat the exercise more than once every two years, at best. *“In the meantime, IS configurations changed at the rapid pace imposed by the constantly evolving needs of the business and of our customers. It was often necessary to re-start from scratch”*, explains Abdellah Cherkaoui, Chief Information Security Officer of the Group's SVC activity. On-site audits gave a detailed vision of the security level of each subsidiary's IS and provided lists of pinpointed recommendations to improve it but this method could not follow the activity's increased growth and the creation of new subsidiaries. Furthermore, it could not offer the head office an immediate picture of its risk exposure. *“We could not increase the frequency of our on-site audits nor did we want to set up local teams for fear of sacrificing their auditing independence”*, continues Abdellah Cherkaoui. Another solution had to be found.

The Group therefore set out to find a technical solution capable of complementing on-site audits, adding continuity to vulnerability management and allowing a permanent vision of its subsidiaries' exposure. This proved a tricky act to balance on a functional level: the solution had to meet both the needs and the constraints of the wide range of subsidiaries, from the largest which alone contributes a significant portion of the activity's business volume right down to the smallest. *“But a simple solution adequate for the latter would not necessarily be complete enough to meet the requirements of the former and vice versa”*, observes the security manager. Furthermore, the solution should also be simple to deploy and administer and allow a centralised view of the risk level and management of each subsidiary, without however requiring dedicated resources in the subsidiary. Finally, the solution should provide effective and continuously updated recommendations to allow local teams to discover and correct vulnerabilities as they appear.

“The market offered two opposing approaches: traditional software, requiring a dedicated infrastructure, and Software as a Service. But we had decided to begin by analysing our exposure from the outside and the SaaS model seemed the most appropriate for that. Not having anything to deploy internally or the necessity of setting up a specific infrastructure to support the solution argued strongly in favour of this model”, justifies Abdellah Cherkaoui.

Modelling the corporate organisation

The teams in charge of the project identified several solutions based on the SaaS model. *“Of all the solutions we studied, the Qualys solution was a step ahead on two counts: First thanks to its interface, which allowed a very flexible and adaptable classification, for instance by types of hardware or by levels of risk. This flexibility of the interface also allowed us to stick to our geographic organisation. Second, the Qualys service sets itself apart by the quality, completeness and granularity of its reporting capabilities as well as its precise recommendations for vulnerability remediation. The latter point was key for local teams with limited security skills. They can take the report as is and quickly know what they need to do and where to find additional information when necessary.”* continues the CISO.

Sodexo then requested an evaluation licence and tested the QualysGuard service in the field. *“We simply compared the results of analyses with the detailed reports provided by our auditing team”*. And the results were in line with the team's expectations in terms of quality of the analysis. Nevertheless one last stumbling block remained: the fear of having confidential data hosted externally. Should Qualys core databases ever be compromised, whatever the

Sodexo strengthens the reliability of its subsidiaries' Information Systems with QualysGuard.

reason, all Sodexo vulnerability data could potentially be accessible.

"We conducted a risk analysis and assessed the likelihood and impact of an exploit of Qualys' customers vulnerabilities in comparison with the benefits provided by the service. Let's be realistic: having an encrypted database of vulnerabilities hosted by a recognized provider whose core business relies on the security of such data is much less risky than keeping critical information systems with many open vulnerabilities as was once the case", admits Abdellah Cherkaoui. Moreover, Sodexo audited Qualys. *"We proceeded with on-site visits and obtained independent audit reports guarantying the effectiveness of the controls put in place and maintained by Qualys . We were reassured by the security setups and by the fact that all customer data can only be decrypted by the customer's own private keys. Noone at Qualys can read our reports",* explains the security manager.

A service offered to subsidiaries

Once the decision taken, the service was quickly implemented. After an initial purchase of about a hundred scannable IP addresses, the Sodexo team gradually modelled the group's organisation in the administration interface and launched analyses of all their external access points. Although the configuration of the tool is centralised, reporting on the other hand is targeted for the subsidiaries. *"It's a sale! We told the subsidiaries "this report is for you. We provide a local hassle-free tool, you do not pay. It will discover and explain how to correct your vulnerabilities. All updates, maintenance and support are included, you just have to identify your frontals. And we will continue to support you through technical on-site audits as usual",* explains Abdellah Cherkaoui. And the subsidiaries went along with it. They quickly took ownership of the tool, gradually increasing the frequency and scope of their vulnerability scanning and analysis, to such an extent that some even decided to hire the services of external consultants to help them correct their vulnerabilities more effectively.

Head office monitors trends from the central interface. *"The rule is that level 4 or 5 vulnerabilities (urgent or critical) should not remain uncorrected for more than a month. Furthermore, thanks to the improvements continuously made by Qualys, the tool becomes increasingly targeted and effective, as it can now correlate between vulnerabilities found on specific hosts and identify the effective risk associated with a given vulnerability: for instance a defect initially graded as critical but requiring the exploit of a vulnerability non-existent on that host in order to have any impact will be downgraded",* continues Abdellah Cherkaoui.

The emergence of new needs

As the usage level of the service increased, needs evolved and new ones appeared: Initially, vulnerability scanning was limited to external access points but the scope quickly broadened to encompass systems and equipments on internal networks. *"Demand came from the subsidiaries. At the time, Qualys offered an appliance deployable on internal LANs which we decided to test. Just in light of the number of default configurations and un-patched equipment easily discovered, we immediately saw the value of the appliance!"* recognises the CISO. Sodexo decided shortly after to deploy appliances in its subsidiaries, mandating their commitment to act upon the automated vulnerability reporting and obtaining a decrease in the levels of internal vulnerabilities of their IS.

More recently, the requirements of compliance with Sarbanes-Oxley and internal control rules triggered new usages for the QualysGuard service. *"We identified some fifteen or so key controls. We quickly saw that Qualys could help subsidiaries automate and make following-up certain controls simpler and more effective. An eloquent example is that of default configuration management. Thanks to Qualys, we were able to obtain report models specifically aimed at default configuration vulnerabilities, which we then immediately shared with all our subsidiaries",* explains Abdellah Cherkaoui, before concluding *"That is the strength of the SaaS model: we have always used the same product for the past five years but it has continuously evolved and adapted to our new needs".*

THE COMPANY

With 310,000 client companies and institutions, 20.2 million beneficiaries and more than 1 million affiliated partners in 30 countries, the Sodexo Group is the second leading Service Vouchers and Cards provider in the world.

THE SCOPE

Meeting both local needs and constraints, the Information Systems of Sodexo Service Vouchers & Cards' subsidiaries present much diversity: They are heterogeneous, often multi-vendor and multi-platform.

THE GOAL

The Group wanted to improve its knowledge and management of vulnerabilities for all its distributed Information Systems, located throughout the world in highly decentralised subsidiaries.

THE CHALLENGE

On-site technical audits conducted every two years on average proved insufficient for effective monitoring and remediation of vulnerabilities. Dedicating a local audit resource was difficult to consider as it would sacrifice the audit's independence from operations . Furthermore, local resources are focused on daily operational support and have little time or too weak the necessary skills to discover, analyse and correct IS vulnerabilities.

THE SOLUTION

QualysGuard Enterprise, the Qualys on demand solution delivered in a "Software as a Service" (SaaS) mode with a "plug and play" appliance to each subsidiary. Unlimited and on-demand analysis of all equipment on the network, from routers to databases, from servers to workstations, regardless of the vendor or the platform type.

WHY QUALYS?

- Quality, flexibility and wealth of the reporting
- Ability to model the Group's business organisation in the solution's interface
- Security of the platform at Qualys to insure data confidentiality
- Relevance of vulnerability analyses
- Direct source of knowledge for local resources of the Group's subsidiaries

WEB SITE

<http://www.sodexo.com>



USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
T: +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 München
T: +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
T: +33 (0) 1 41 97 35 70

