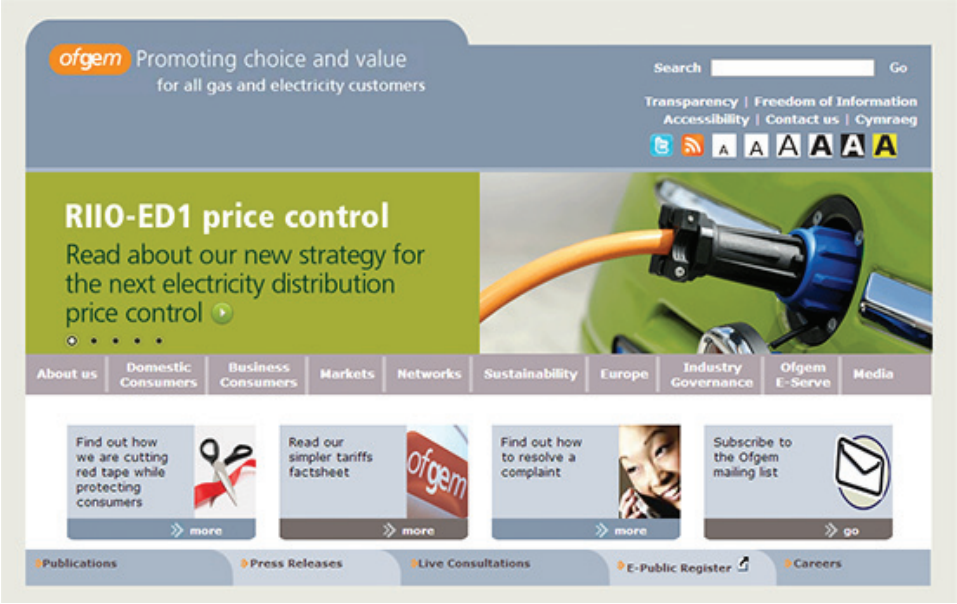
Deploying Comprehensive Security Measures and Enabling End-to-End Compliance in a Multi-Faceted Organisation

By deploying a suite of security solutions from Qualys, Ofgem has gained full visibility of and control over security and compliance issues across its infrastructure.



Ofgem – the Office of the Gas and Electricity Markets – is the body that protects UK consumers by regulating the monopoly companies which run the gas and electricity networks. Governed by the GEMA authority, Ofgem promotes competition between utility companies, monitors and promotes energy security, and contributes to the drive to curb climate change and reduce harmful greenhouse-gas emissions.

As part of its work in standing up for consumer rights, Ofgem has a duty to provide information and services for consumers, including a range of web-based tools. For example, members of the public can look up licensing information to check that a particular company is authorised to offer a particular service or government subsidy.

To improve the protection of sensitive data – both commercial and personal – across internal and external systems, Ofgem needed to increase its visibility and understanding of emerging security threats, and its ability to set and maintain effective security policies.

www.ofgem.gov.uk

INDUSTRY: Government

BUSINESS: Office of the Gas and Electricity Markets protects UK consumers by regulating the monopoly companies running gas and electricity networks.

SCOPE: UK

SIZE: 700 employees

BUSINESS CHALLENGE: Improve the visibility of security threats to its IT infrastructure. Existing approaches to vulnerability management were fragmented and one-dimensional.

SOLUTION:
QualysGuard
Vulnerability Management (VM)
QualysGuard Policy Compliance (PC)
QualysGuard
Web Application Scanning (WAS)

WHY THEY CHOSE QUALYSGUARD:

- Transparency: Qualys technologies provide a clear, timely view of vulnerabilities.
- Ease of use: Automated scans and reports save time and effort for IT personnel.
- Comprehensiveness: Qualys enables Ofgem to protect every element in the IT infrastructure.

Protecting a Multi-Faceted Organisation

With approximately 500 servers – mostly virtual – in its infrastructure, and a user base that extends beyond the 700 employees to encompass potentially the entire UK population, Ofgem has its work cut out when it comes to ensuring security. Web applications in particular are subject to a broad and growing range of vulnerabilities, from SQL injection and cross-site scripting to PHP injection, code execution and cross-site request forgeries.

Equally, the company must ensure that workable security policies and standards are applied to servers, routers, switches, firewalls, desktops, laptops, printers and other end-points on the internal network. Finally, Ofgem undertakes numerous internal IT projects and software development projects, and must ensure appropriate security measures and security-aware coding throughout the full project and application development lifecycles.

> "Our approach to security was very one-dimensional in the past; with the QualysGuard suite, it's much richer and broader, and rather than having a scattergun approach, we can target our resources."
>
> **Bob Mann**,
> Chief Security Officer at Ofgem

First, Gain a Clear View

The old adage 'if you can't measure it, you can't manage it' was a fitting one for Ofgem. Without an enterprise-class toolset for monitoring and managing security vulnerabilities, the organisation lacked a clear view of the threats it was facing, let alone a structured way in which to address them.

Bob Mann, Chief Security Officer at Ofgem, explains: "Against a backdrop of corporate obligations and government regulations, we have to make sure that we keep abreast of emerging security threats while remaining agile enough to deliver what the business needs. Those threats change on a daily basis; the best practice is to monitor what's going on, and respond accordingly."

When Bob Mann took up his role at Ofgem, there was limited visibility of security threats, and limited ability to enforce clear security policies. To address these shortcomings, the organisation deployed a suite of security solutions from Qualys.

"IT departments and development teams are under constant pressure to deliver more complex solutions faster and at lower cost," says Mann. "In that kind of environment, there's always a temptation to cut corners on non-functional aspects such as security. I knew from past experience that the Qualys solutions would allow me to make IT security transparent and auditable without alienating IT personnel or introducing significant administrative overhead."

Understanding the Risks

Ofgem began its deployment by using QualysGuard Vulnerability Management (VM) to discover and group all assets on its IT infrastructure. “As the first step, we wanted to get a good picture of what was in each class of IT assets so that we could understand the risks,” comments Mann. “Later, we will use the asset discovery features to look into the software infrastructure and improve our management of software licences.”

Asset tagging allows Ofgem to flag each IT component involved in the end-to-end delivery of a particular business service, and then determine an overall risk rating. This helps the business units understand dependencies in their services, and enables better prioritisation of fixes and patches.

Based on the initial reports, Bob Mann’s InfoSec team is now working with IT to fix vulnerabilities. A weekly report goes out to IT covering four key areas in a single slide: servers, end-points, virtualized and network-attached devices. The report gives a top-level overview of security status, showing trends and upcoming fixes. Mann also reports on a monthly basis to the IT Director and the Chief Risk Officer, and twice annually to the Ofgem board. Reports also go to the internal audit, fraud and risk teams.

“With QualysGuard VM, we can provide updates on where we stand on a whole range of vulnerabilities, and show what we’re doing to address them,” says Mann.

A Stitch in Time Saves Nine

In addition to ensuring that the IT infrastructure is secure, Ofgem is addressing security throughout the full lifecycles of project management and application development. The organisation is using QualysGuard Policy Compliance (PC) to enforce security standards for servers, and QualysGuard Web Application Scanning (WAS) to check for vulnerabilities both before and after deployment.

“We are often dependent on last-minute decisions from government and from the regulators, and hackers know that we often have to make late changes to applications,” comments Mann. “The iterative process we’re introducing should minimise the chance of having to stop applications from going live for security reasons. During the project lifecycle, we’ll use QualysGuard WAS to run checks on the application, so that few or no vulnerabilities remain when we get to the final penetration-testing stages.”

Faster, More Transparent, More Secure

While it is still early days for Ofgem in terms of using Qualys technology, the organisation has already achieved a number of important benefits. The first is the complete visibility of vulnerabilities and related fixes in the IT infrastructure.

“We can now openly and transparently show the board what vulnerabilities there are and how we’re dealing with them – there’s no longer anywhere to hide!” says Mann. “We’ve also eliminated a lot of the drudgery involved in creating reports through automation, saving significant amounts of time for IT personnel.”

With a clearer and timelier view of vulnerabilities, Ofgem has improved its ability to prioritise vulnerabilities and increased the overall speed of remediation. This has had the effect of decreasing the total number of vulnerabilities present in the infrastructure at any given time.

“Our approach to security was very one-dimensional in the past; with the QualysGuard suite, it’s much richer and broader, and rather than having a scattergun approach, we can target our resources,” comments Mann. “Qualys provides the toolbox I need to make sure we deliver projects, including software, much more securely.”