Hewlett Packard Enterprise

Case Study

centrica British Gas

Centrica/British Gas picks HPE Fortify on Demand

Cloud-based managed security testing improves security and efficiency and reduces cost

Objective
Identify and remediate vulnerabilities in British Gas applications early in the software development lifecycle to reduce costs, improve efficiency, and enhance application security

Approach
Leverage cloud-based HPE Security Fortify on Demand managed service for static and dynamic scanning of code that is developed in-house and by third parties

IT Matters
- Enables static and dynamic scans of SAP-centric code base, along with coverage for other languages (e.g., Java and .NET)
- Supports "shift left" development culture by identifying and remediating vulnerabilities earlier in the lifecycle
- Involvement in concept phase of project planning helps minimize impact on project deadlines
- Senior management–supported developer awareness and training has significantly reduced code vulnerabilities

Business Matters
- Enhances application security for key digital channel and mobile applications
- Provides proactive approach to protecting sensitive customer data
- Improves compliance posture with industry regulations
- Meets budgetary and efficiency objectives of British Gas change plan
- Assures the security of third-party applications by Fortify on Demand's Vendor Management service applications

Centrica plc is a British multinational utility company headquartered in Windsor, Berkshire. It is the largest supplier of gas to domestic customers in the UK, and one of the largest suppliers of electricity, operating under the trading names Scottish Gas in Scotland and British Gas in the rest of the UK. British Gas serves around 12 million homes in the UK.

Paul Phillips is head of software assurance and integration at British Gas. His organization is responsible for application security and code assurance for all development activities that are delivered for the British Gas brand within the Centrica group. For the past three years, Phillips and his team have relied on HPE Security Fortify on Demand to help ensure the security of the software they develop.

British Gas previously used HPE Fortify Static Code Analyzer on site, in conjunction with HPE WebInspect. These products still support the company's operational needs, but Fortify on Demand is now the lead solution for application security.

"We need to understand and mitigate the risk, make sure the products we deliver fit the purpose and are secure, and protect the sensitive data of our customers. Fortify on Demand is key to actually doing all of that."

— Paul Phillips, Head of Software Assurance and Integration, British Gas

Changing landscape

A changing environment drove the decision to implement Fortify on Demand. "The area we work in is quality assurance and control," says Phillips. "We recognized the need to focus on secure code development, particularly in light of new technical developments. Our digital channel was growing in importance—in fact, more than 50% of our customer interactions now take place via this channel—and smartphones were starting to come to the fore. We needed to take a more proactive approach to protecting customer data, as well as complying with industry regulations."

Phillips researched the best way to establish a governance framework, and what sort of tooling would support that framework. Performance was key; cost was also a critical factor. "Within our industry there was a strong strategic direction toward utilizing service capability to drive cost containment and ensure that our headcount was being used efficiently," he says. "A service-based approach met those requirements. At the time, Fortify was one of the few solutions that were actually stretching their capabilities into the SAP space. This was particularly important for British Gas, as we are heavily SAP-centric."

British Gas has a long history of traditional information security, but the changing landscape called for a new approach. "Obviously the way you handle vulnerabilities in the emerging threat space, including social engineering, is totally different from traditional firewall protection," says Phillips. "It's a whole different mindset and a whole different approach."

Discover early, resolve early

The majority of development at Centrica/British Gas is in SAP ABAP, with other languages (including Java and .NET) making up the balance. The company has around 1500 developers—internal staff, as well as third parties that have been engaged on an outsourcing basis—who concentrate their efforts on approximately 50 business-critical systems and applications. These include www.britishgas.co.uk, the main digital channel for customers in the UK; the core SAP billing and CRM systems; and self-service customer applications. In addition to scanning code that is developed in-house, British Gas includes relevant wording in contracts to ensure that third-party code can also be audited using Fortify on Demand.

Says Phillips, "The approach we've taken is one of 'Discover early, resolve early.' We try to engage with projects right at the beginning of the lifecycle, in the concept phase, so we understand what the project is looking to deliver. Then we have a number of core service offerings, with static and dynamic scanning being two key aspects of that. We work out a plan and the appropriate funding that allows that project to deliver secure code. We're trying to make sure that project deadlines are not impacted by discovering a big lump of vulnerabilities right at the end of the development lifecycle."

Static scanning is actively engaged from unit test onwards; the dynamic piece comes to the fore when the code is more mature; and a dynamic scan at the project level helps ensure the code is clean before it goes into the overall release process. At this time approximately 90% to 95% of core business-critical systems are covered by Fortify on Demand, with new ones being added regularly. "We look to do at least one core scan per business-critical application every two years," says Phillips.

Education has been an important side benefit of the Fortify on Demand deployment. "We started from a low awareness point within our development community on how secure code could be developed," says Phillips. "We went through an initial education phase with all of our developers to explain why secure coding was important, and we created internal education packages. This developer awareness effort had the full support of senior management, and secure coding practices are now an integral part of company policy."

Business benefits

From a regulatory perspective, Phillips notes that Fortify on Demand has helped ensure the compliance of British Gas applications with industry regulations. "We have a defined framework and governance process in place that we share, and that seems to tick the boxes in terms of what we need to demonstrate from a compliance perspective," he says.

Application security manager Ramesh Nagaraj agrees. "HPE Security Fortify on Demand has increased our confidence in ensuring the quality and security of our critical applications, and it supports us very well in meeting our regulatory compliance requirements," he says. "As an integral part of our software lifecycle, it enhances productivity by enabling us to focus on critical things first."

British Gas has also realized benefits from a development perspective. Continues Phillips, "We've got a 'shift left' culture in terms of maturing the code more rapidly now: It's more maintainable and it has fewer vulnerabilities. I can see a definite downward trend in the volume and severity of vulnerabilities in our source code compared to when we started using Fortify on Demand." In the software development lifecycle of creating the code to ultimately deploying it, a "shift left" is anything that is done earlier, resulting in lower cost and greater efficiency for the business.

For Phillips, Fortify on Demand hits all points of the time–cost–quality triangle at British Gas. "We have quite a large-scale change plan—that's the name by which our budgeting mechanism is known—and a large

Case study
Centrica/British Gas

Industry
Energy

Customer at a glance

Solution
- HPE Security Fortify on Demand

estate in terms of lines of code," he says. "We needed to make sure we could provide a service that would help us understand and mitigate risk, but not compromise cost parameters and project schedules. We didn't want something that would add massive time to our delivery lifecycle or cost a fortune to implement. We use Fortify on Demand extensively now, and it is broadly accepted as a valuable part of our change plan."

The relationship with HPE is a strong one. "The actual Fortify on Demand guys have a strong and positive working relationship both with my application security team and also with the development community here at British Gas," says Phillips. "They can have sensible, pragmatic conversations around secure coding, and as a result we have gained a great deal of experience and understanding. This translates directly into continuous improvement in the security of British Gas applications."

Going forward, Phillips is keeping a close watch on the company's increased mobile footprint and exposure to social engineering as sources of new threat vectors; smart metering is likely to open up additional avenues of attack. "We are trying to make sure that we design securely at the very beginning—that we design out as many vulnerabilities as possible early in the process by understanding the architecture and potential approaches," says Phillips.

He's got the right solution for the job. "We need to understand and mitigate the risk, make sure the products we deliver fit the purpose and are secure, and protect the sensitive data of our customers," he concludes. "Fortify on Demand is key to actually doing all of that."

Learn more at
hpe.com/security

Sign up for updates

Hewlett Packard Enterprise

4AA5-3766ENW, November 2016, Rev. 1