Callcredit adds HPE Security Fortify SCA into development lifecycle

UK consumer information management firm finds vulnerabilities early for secure code

Objective
Help ensure the security of applications developed in-house and by third parties as part of overall corporate policy aimed at protecting sensitive client data and reducing business risk

Approach
Deploy HPE Security Fortify Static Code Analyzer (SCA) and integrate it fully into the software development lifecycle, from developer desktop to build server to change control

IT Matters
- Installation of Fortify SCA on local workstations enables developers to scan their code before making major check-ins

- No disruption to the developer. Code check-in automatically triggers a Fortify SCA scan on the build server

- Including Fortify SCA in the change control process further enhances application security by helping to prevent release of code with critical or high vulnerabilities

- Broad language coverage of Fortify SCA enables Callcredit to scan all its different code bases

- Fortify SCA acts as a catalyst to remind developers to employ secure coding practices

Business Matters
- Reduces development costs. Finding and remediating vulnerabilities earlier in the lifecycle is much more cost-effective than doing it closer to release

- Ensures time to market without sacrificing security. Fortify SCA supports fast time to market by helping avoid security-related delays late in the development process

- PCI compliance posture improved. Callcredit's PCI compliance posture has improved significantly as Fortify SCA meets the requirement for 100% code review

- Security risk is mitigated through the creation of more secure code, both in-house and third-party

Callcredit Information Group's leading approach to deploying consumer information brings together experts across the fields of credit referencing, marketing services, interactive solutions and consultative analytics to provide clients with a range of innovative and effective products to discover new customers and to engage with current customers to optimize and increase profitability.

In a first for UK consumers, Callcredit launched Noddle (**noddle.co.uk**), a service that offers people free access to their personal monthly credit reports for life. Other products include award-winning fraud verification tools and database solutions to positively verify consumers, global operations to help expand businesses into new markets, digital solutions to improve the overall journey consumers make during interaction with a brand, and consumer marketing data and segmentation to improve understanding and targeting of customers and prospects.

Callcredit also offers products for its clients to assess a customer's credit risk and affordability, and its experts in collections and recoveries provide tailored debt recovery and tracing tools. Its market analysis and network planning function helps organizations develop profitable retail networks, and its tools in multi bureau, analytics, and metrics work to provide fully assessed bureau data.

Case study
Callcredit

Industry
Finance – Direct
Marketing and Credit
Solutions

Page 2

> "Some of our most recent applications have found zero vulnerabilities using Fortify SCA. The development teams have been able to essentially eradicate issues before they build them in."
>
> — Clement Pickering, Head of Testing, Design and Methodology

"Our bread-and-butter business originates from credit referencing and scoring, so we work with many financial institutions in that regard," explains Paul Morgan, Group Head of IT Procurement. "In addition, we are very active in information management in respect to taking data, cleansing that data, and then selling that data back. We are extremely careful when it comes to our clients' sensitive financial data, with a significant investment in firewalls, tracking devices, and other security measures to thwart hackers. HPE Security Fortify Static Code Analyzer (SCA) is a critical component of our security arsenal."

Where Fortify fits

Clement Pickering is head of testing, design and methodology. "As an organization we are an extremely large holder of data," he agrees. "We are an information business, and data really underpins everything we do. Also, the nature of our business potentially makes us a key target for 'hackers,' so it's very important that we have strong security measures in place to counteract any kind of threat that we might find ourselves under."

Callcredit first adopted HPE Fortify SCA in 2011. "My first exposure to Fortify, apart from the demonstration that HPE conducted, was when we engaged a third-party company to perform a security review of one of our main

applications," Pickering recalls. "We went to their premises to find out what they were doing so we could gain some knowledge ourselves, and they were using Fortify SCA as one of their tools. That showed us its true capability."

A proof of concept on two of Callcredit's Internet-facing financial services products— an anti money-laundering application, and a product to assess people against over-indebtedness—helped finalize the purchase decision. Says Pickering, "We were surprised that the scans immediately highlighted some critical vulnerabilities in the code. That testing certainly demonstrated the benefit of Fortify SCA straight away."

Agile development

Fortify is integrated into the entire development lifecycle at Callcredit. At the beginning of the process, developers write code on their local workstations. They have Fortify SCA installed on their workstations, usually through the Visual Studio plug-in or the Audit Workbench tool. The developers are encouraged to run scans on their local machines before making any major check-ins.

When code is checked in, it triggers a build on the build servers. "Certainly on a nightly basis we will run a Fortify scan over the

Case study
Callcredit

Industry
Finance – Direct
Marketing and Credit
Solutions

Page 3

entire code base, which of course includes the latest development changes that people have entered," says Pickering. The principal developers on the project then look at the results and immediately correct any vulnerabilities revealed by the scan. In a monthly review, Pickering and a member of the security team look at general long-term trends to see what projects are being scanned, how frequently scans are taking place, and what vulnerabilities have been uncovered.

Finally, Fortify is incorporated into the change control process. "Our acceptance into service or request for change process now essentially asks for the results of the successful Fortify scan," says Pickering. "We aim to make sure we don't release any applications that have critical or high vulnerabilities. Fortify SCA is absolutely part of our process now, and that's why it works so well—it's an automatic step that is triggered on build, not something you have to remember to do."

The ability to scan a broad range of languages with Fortify is an important feature, according to Pickering. "We don't use one language exclusively," he explains. "We use .NET, including some VB .NET legacy but mainly C-sharp; we have T-SQL code; and we also have some C++, VB6, and PHP. It's critical that we can scan all of those different code bases with Fortify." Callcredit occasionally outsources development, but most applications are created and maintained by the in-house staff of approximately 80 developers. Third-party code is also scanned with Fortify SCA.

Catch it early

Callcredit had a strong application security policy prior to implementing Fortify, but the emphasis was on end-of-lifecycle activities—penetration testing, for example, or using a third-party security assessment company prior to release. "The penetration testing by itself wouldn't necessarily find all the problems," recalls Pickering. "If we paid a third party to do a more comprehensive security

assessment, it would potentially be more effective but also far more costly. And then, of course, it wasn't real-time—we couldn't react as quickly. The key difference with Fortify is that we've integrated it continuously throughout the lifecycle."

Pickering is a big believer in this approach. "Anything that you leave to the end generally increases risk," he says. "It also severely limits your ability to do anything about it, especially if you've committed to client timeframes. What's more, problems that you find later in the lifecycle will inevitably cost far more to fix, based on the time and effort it takes to correct them and the number of people that have to get involved. You also have to consider the potential impact of release delays on time to market. All of which adds up to additional cost, so finding vulnerabilities and fixing them early is more cost-effective."

This idea fits in with Callcredit's agile development model—not doing a "big bang" release at the end, but trying to do things in smaller batches throughout the entire course of the development lifecycle. "For any activity that's going to be risky or painful, we try to do it early and often rather than just at the end," says Pickering. "That very much applies to security and code review. It shouldn't be an end-of-lifecycle activity. It should be something that you do continuously through the process."

Business benefits

Beyond the obvious advantage of reducing security risk through more secure code, Pickering points to regulatory compliance as a major benefit of Callcredit's Fortify implementation. "That was one of the key reasons for buying the tool in the first place," he says. "Our use of Fortify SCA basically meets the requirement of doing 100% code review. There's no question it has helped us massively with PCI compliance." Pickering anticipates that Fortify will prove equally valuable to Callcredit as the UK's Financial Conduct Authority (FCA) regulations continue to evolve.

Case study
Callcredit

Industry
Finance – Direct
Marketing and Credit
Solutions

Customer at a glance

Solution
• HPE Security Fortify Static Code
  Analyzer (SCA)

HPE Services
• Implementation services

• Developer training

Fortify has also helped create a stronger focus on security within the development organization. "It certainly has heightened awareness of secure coding practice," Pickering continues. "I would say the tool has been a catalyst to get people to think more about it. Before integrating Fortify into our lifecycle, we ran a secure coding course for developers; but the tool almost acts as the thing that prompts people to not forget about it. I think it certainly has helped our developers become more skilled in this regard."

When Callcredit initially ran Fortify against its legacy code base several years ago, the scan results revealed a number of vulnerabilities. Today, that has changed. "What we have found with the greenfield projects we've done since then—basically, applications that we're developing from scratch—is that we have an extremely low number of vulnerabilities," says Pickering. "In fact, some of our most recent applications have found zero vulnerabilities using Fortify SCA. The development teams have been able to essentially eradicate issues before they build them in."

Support from HPE Services enhances the solution. "We've engaged with HPE in the Fortify area a number of times, and we have been very impressed with the consultants who have been onsite," says Pickering. "They are skilled and knowledgeable in a wider security context than just HPE, and that is helpful to us. We have found the services around Fortify to be very effective."

Looking forward, Pickering sees additional opportunities for Fortify as Callcredit investigates and adopts new technologies, particularly in the areas of database and middleware. "We are evaluating different things in terms of the best way to organize data, including Big Data products," he says. "If we look at new technology and have to write code against it, perhaps even adopting a new language that is more appropriate to that technology, then we would want Fortify to help ensure the security of that code."

Early and often

In summarizing the overriding benefit of Fortify SCA at Callcredit, Pickering returns to the notion of "early and often." "I think the key thing for us is it allows us to bring security early into the process and have it run continuously throughout," he says. "To me, that is the major advantage—having Fortify scans built in as an intrinsic part of the day-to-day development lifecycle, as opposed to something that's done by a separate team at the end." Minimizing security-related delays and lengthy feedback cycles allows Callcredit to remain responsive, while reducing the risk of exposure to incidents that could damage the business.

Of the many Fortify SCA features that Callcredit appreciates, Pickering points to automation as his personal favorite. "The fact that we can integrate Fortify via command line into our continuous build process is absolutely vital," he concludes. "If it relied on a manual interface, it would be a major problem for us. The automation is something I like very much: The scanning happens automatically, and the results get logged in the Fortify server automatically. Fortify SCA is an excellent fit in our agile development environment."

Learn more at
hpe.com/security

f 🐦 in ✉

Sign up for updates

Hewlett Packard Enterprise