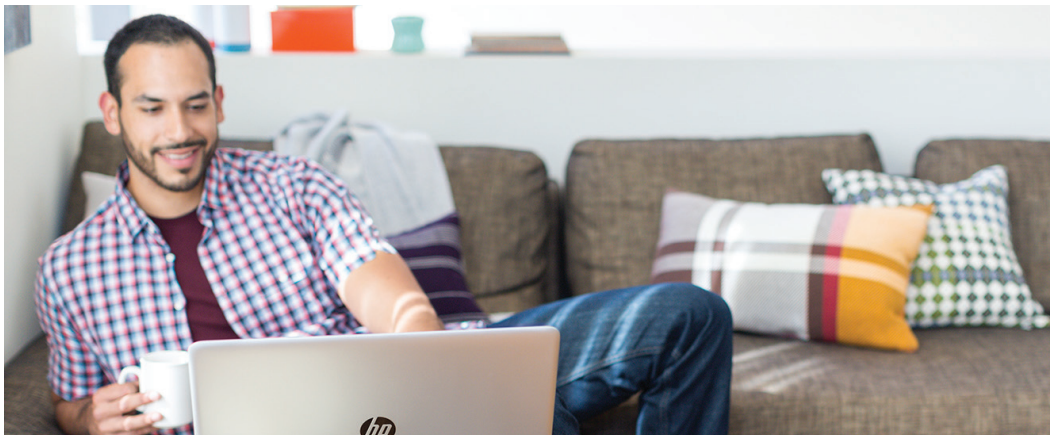
Hewlett Packard Enterprise

Case Study

Aaron's looks to achieve secure code excellence with HPE Fortify solutions

Specialty retailer reduces application risk by using HPE Fortify



Objective
Strengthen security within the software development lifecycle to reduce the number of application vulnerabilities, protect customer data, and meet industry best practices and standards

Approach
Deploy HPE Fortify on Demand for static application security testing and HPE WebInspect for dynamic application security testing (DAST)

IT Matters
- Reduced overall application security risk and decreased high-risk vulnerabilities
- Trimmed one to two weeks off the application development lifecycle
- Enabled continuous improvement of secure coding best practices through detailed defect tracking, trending, and reporting
- Streamlined the application development lifecycle by allowing concurrent static code scans

Business Matters
- Improved return on investment by accelerating application go-to-market timelines
- Saved time for developers and security testing staff to work on strategic projects to help the business grow
- Met the company's immediate needs while transforming security into a business enabler
- Achieved significant cost savings thanks to improved secure coding practices and declining application vulnerabilities

Specialty retailer Aaron's needed to meet industry standards for managing application vulnerabilities that could put data at risk. After an intensive evaluation, Aaron's deployed HPE Fortify on Demand and HPE WebInspect to identify and remediate security vulnerabilities at every stage of the application development lifecycle.

Aaron's, Inc. (Aaron's) is a specialty retailer serving consumers through the sale and lease ownership of furniture, consumer electronics, computers, home appliances, and accessories in over 2,100 company-operated and franchised stores in the United States and Canada. Headquartered in Atlanta, the company was founded in 1955 and has been publicly traded since 1982. Aaron's is the industry leader in serving the moderate-income consumer and offering affordable payment plans, quality merchandise, and superior service.

To optimize business efficiency and continually adapt to meet evolving customer needs, Aaron's runs an extensive in-house software development program. The company follows an agile methodology to

> "Through an SSDLC using Fortify on Demand and WebInspect, we've not only addressed our immediate needs but also set Aaron's on a path of secure code leadership in our industry.
>
> — Bhavin Patel, Senior Information Assurance Engineer, Aaron's

move applications through the software development lifecycle quickly, which is critical in the highly competitive retail marketplace. However, Aaron's well understands that speed cannot be at the expense of security.

Using WebInspect, Aaron's started with limited dynamic application security testing (DAST) to scan running applications before they went into production, but soon found that DAST alone was not sufficient.

Chris Bullock, Director of Information Assurance at Aaron's, explains, "We do regular penetration testing as part of our standard security best practices; however, we decided additional security testing was needed earlier in the process."

The right tools for the secure coding job

Bullock and his team evaluated several vendors for static application security testing (SAST) solutions. After an intensive proof of concept (POC), Aaron's chose Hewlett Packard Enterprise's (HPE) Fortify on Demand. While HPE offers on-premises and on-demand security testing solutions for both DAST and SAST, Fortify on Demand best matched the agile development methodology at Aaron's while leveraging the company's existing in-house expertise with WebInspect.

Bhavin Patel, Senior Information Assurance Engineer, states, "In the POC, we were concerned with false positives and how much time they would take to investigate. Fortify on Demand consistently produced reliable results and highlighted exactly where issues were in the source code making it easy for our developers to take corrective action. Plus our developers found the user interface to be very intuitive, which was really key since they were the ones integrating SAST into the development process. At the end of our decision process, we chose to go with HPE."

Bullock adds, "Any time you're putting your code out into a cloud environment, like Fortify on Demand, you have to be confident it's secure. We did a vendor risk assessment and found HPE to be the best product for us, and we are very comfortable with our decision."

Fortify on Demand now plays a central role in the SSDLC process by identifying and tracking vulnerabilities, as well as remediating them throughout the development and quality assurance processes. Aaron's continues to rely on WebInspect for both pre- and post-production dynamic security testing scans to uncover residual or newly discovered vulnerabilities.

Accelerates application go-to-market

Aaron's is scanning many applications concurrently using Fortify on Demand, including additional scans for each release of an application. With a busy information assurance team, Patel notes the value of having a flexible, on-demand cloud security testing solution for SAST.

"Number one, Fortify on Demand eliminates the up-front cost of us deploying a solution in-house," he says. "Being able to upload an application and have HPE do the analysis through a cloud appliance is hugely beneficial. It frees up time for both our developers and security staff to work on different projects, scale up to get more applications into production, and help the business grow."

Because Fortify on Demand scans for vulnerabilities while applications are still in development, it also eliminates the time required to remediate security findings after the fact, streamlining the application development lifecycle. Bullock estimates this will shave one to two weeks off the development lifecycle. "Fortify on Demand helped shorten the development lifecycle and accelerate our go-to-market timeline substantially," he remarks.

Security as business enabler

"HPE provides the tools that let me track vital security statistics and report back to executive leadership," says Bullock. "It raises awareness of how security can be a business enabler rather than just a technical solution."

Patel provides a pertinent example: "We found some applications that were causing resource problems like memory leaks that ended up degrading performance of our website. We turned that problem around with the insights provided by Fortify on Demand. It helps us manage resource allocation more efficiently and improve computational power so we can scale more users on our web servers. We now get better, more consistent performance of our website, which is important for customer satisfaction."

Case study
Aaron's

Industry
Retail

Customer at a glance

HPE Security Solution
- HPE Fortify on Demand
- HPE WebInspect

Code insights improve security best practices

Aaron's uses valuable insights from Fortify on Demand to improve its ongoing security posture. Fortify on Demand not only helped identify application vulnerabilities, it also provided useful information that the company used to enhance its development coding guidelines.

Patel points out, "Fortify on Demand establishes a baseline of our code development posture and then tracks remediation of defects over time. This allows us to continually improve code quality and security."

Bullock adds that these improvements will ultimately lead to financial benefits. "Fortify on Demand greatly reduces the number of agile iterations for our developers, because in each subsequent scan we're seeing fewer and fewer vulnerabilities," he notes. "The combination of better secure coding practices and declining application vulnerabilities will definitely translate to cost savings for Aaron's."

Meets industry standards

Extensive reporting from Fortify on Demand helps Aaron's demonstrate compliance with industry standards. Static code security testing scan reports provide a benchmark for comparing how an application measures up to standards at specific stages of development.

"We've mapped a large portion of our security plan to ISO 27002 standards for information security," Bullock declares. "Without question Fortify on Demand and WebInspect have helped us meet industry standards."

Patel concludes, "The net benefit is that by eliminating vulnerabilities in our application code we are helping to keep information more secure. And with e-commerce being a rapidly growing portion of our business, it's critical that customers feel confident doing business with Aaron's online. Through an SSDLC using Fortify on Demand and WebInspect, we've not only addressed our immediate needs, but also set Aaron's on a path of secure code leadership in our industry."

Learn more at
hp.com/go/esp

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0496ENW, March 2016, Rev. 2