opentext™ | Cybersecurity

EQUIFAX®

Position Paper

Equifax—Transforming the Organization with Fortify on Demand

Learn how Equifax adopted a shift-left culture and secure DevOps practices utilizing Fortify on Demand when transforming development to the cloud.

Equifax is going through a transformation. As a global data, analytics, and technology company, they believe that knowledge drives progress. It's this shared belief that drives Rajan Gupta, Vice-President of Product Security, to transform the company's applications and infrastructure to modern platforms securely.

The software development organization at Equifax develops applications that help people understand their financial scores and risk. Security is paramount as these applications typically manage Personally Identifiable Information (PII). "Security is always top of mind with everybody at Equifax," said Gupta. "We are partnering with Micro Focus (now part of OpenText™) to drive AppSec modernization with Fortify on Demand by OpenText™ to deliver actionable, data-driven results."

> "Together, we are fundamentally transforming how AppSec meets the needs of our developers with Fortify on Demand."
>
> **Rajan Gupta**
> VP of Product Security
> Equifax

Transforming Centralized Security to Decentralized with Responsible Security

Operating in over 24 countries, Equifax has 6,000+ developers worldwide and, just like in other organizations, a far smaller application security team. Gupta believes that for an organization to scale and deliver business value at DevOps speed, security should be everyone's responsibility and not just the application security team's responsibility.

Instead of performing security scans and audits, AppSec specialists at Equifax act as security coaches for the developers. Gupta has moved Application Security from being a centralized function, where developers were relying on security specialists to tell them if their code is secure, to a decentralized function where developers are responsible for making sure that their own code is secure. Gupta and his team enable them to take that responsibility by integrating Fortify by OpenText™ into their daily process and development tools, allowing developers to continue their process and not slowing them down. "At the end of the day, organizational transformation is about the people and the process," says Gupta. "We are transforming from a centralized security organization to a decentralized team with responsible security."

> Instead of performing security scans and audits, AppSec specialists at Equifax act as security coaches for the developers.

Didn't work

- ✗ Consultants to write Secure SDLC
- ✗ On-premise AppSec Tools
- ✗ Siloed SAST, DAST & SCA

Worked

- ✓ Engineering handbook
- ✓ Train FTE and CTE
- ✓ Baking AppSec Tools in parallel pipeline
- ✓ Integrated Security Gate in Change Management
- ✓ Metrics to measure success

To Do

- ○ Reduce suppression queue
- ○ Shift suppression to Dev
- ○ Governance and oversight that stand in the way

Developer to Developer Coaching

It was not an overnight process. In order to transform the development team to apply security during the coding process, Gupta had to train them. He started offering iEngineer sessions twice a day for 6 months. These sessions would start with a little bit of Fortify training followed by a different security-related topic every week. At Equifax, developers were already thinking about security and Gupta pointed out that Fortify is a great and proven tool that has consistently been rated at the top of the leaders' quadrant by Gartner. It helped that Gupta himself had 20+ years of experience building applications for Fortune 100 companies. The developers viewed him as one of their own, and he was able to talk their language and understand their needs and challenges.

At Equifax, developers were already thinking about security and Gupta pointed out that Fortify is a great and proven tool that has consistently been rated at the top of the leaders' quadrant by Gartner.

All developers went through one or more iEngineer sessions. Whether their team was already executing in a mature DevOps process or were still using a Waterfall or Agile software development lifecycle (SDLC) model, application security became an integrated part of the developer's day. "I'm less concerned about what methodology is being used and more interested in integrating application security into the process," said Gupta. "I didn't want to force all developers to use the same methodology. It wouldn't have worked."

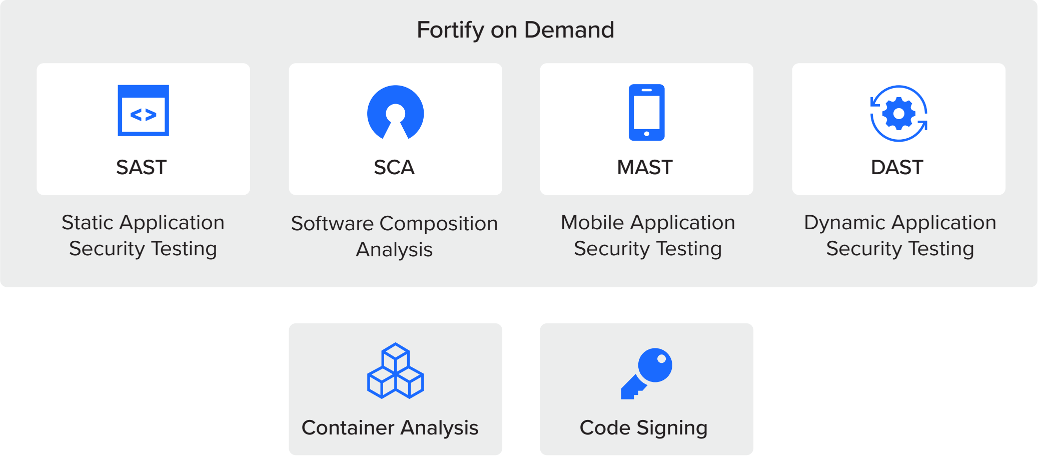
Now, instead of going to a security team as the application is about to launch and getting a security scan as a checkbox task, developers get security vulnerability reports from Fortify and manage security issues in the same way they manage functional defects.

Developer Adoption through Integration

Integrating Fortify into the development processes at Equifax meant integrating it with their existing development tools. "Developers are still most interested in delivering code on time," said Gupta. "So, while they are invested in applying security to their development process, it can't hinder them." This meant thatFortify by OpenText™ had to work with a number of different tools and programming languages developers were already using.

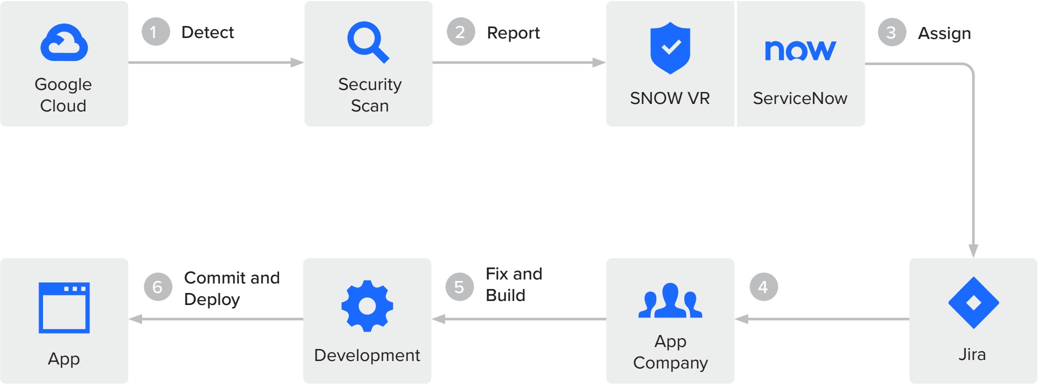
Integrating Fortify into the development processes at Equifax meant integrating it with their existing development tools.

Gupta worked with Fortify to integrate open source analysis using Sonatype's NexusIQ into Fortify so that scans are done once and developers can see SAST and SCA results in a single view. This changed the way developers viewed open source as from being a third-party library vs. a library they selected to use and hence having a higher responsibility towards the choices they made. It started to bring attention to open source and led to faster remediation of open source. Gupta says, SAST+SCA are better together.


Fortify on Demand
SAST
Static Application Security Testing
SCA
Software Composition Analysis
MAST
Mobile Application Security Testing
DAST
Dynamic Application Security Testing
Container Analysis
Code Signing

Gupta worked with Fortify to integrate open source analysis using Sonatype's NexusIQ into Fortify so that scans are done once and developers can see SAST and SCA results in a single view.

"Of all the Fortify integrations we use, the most important one is the closed-loop integration with Jira," said Gupta. With this integration, security vulnerabilities found by Fortify are entered as a Jira ticket and managed in the same way as a functionality defect. Developers review their assigned tickets and once the security vulnerability has been fixed, it is marked as ready for build. In the next Fortify scan, the integration updates the ticket status to closed if the vulnerability is no longer found.

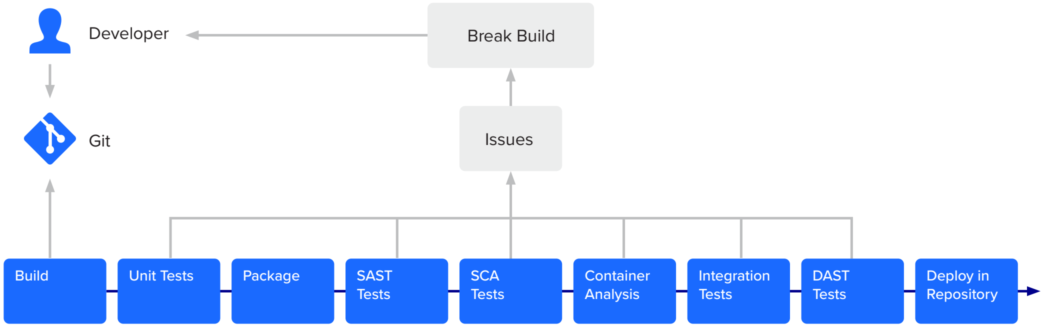


Equifax's development team also use Jenkins as their build server. For these teams, a security scan with Fortify is an automated part of the pipeline. While some teams use the available Fortify-Jenkins integration, others choose to write a shell script using FoD Uploader or kick off the Fortify scans manually. Gupta is focusing on automation as a top agenda as part of a standard pipeline architecture rollout, but some teams may not have a pipeline. "It didn't matter to me if a developer was using the available integration to automate or writing shell scripts or executing the scans manually," said Gupta. "It's an evolutionarily process, and I'm more interested that they were applying security to their process by scanning more regularly."

Fortify reporting serves as a transformational aid where an organization can gauge their security and automation maturity and build KPI against them. Gupta says that one of the KPI is automation maturity which tells which business unit is performing automated Fortify scans vs uploading via browser. Equifax has established an automation KPI which is reported monthly to management to report a business unit automation maturity.

Equifax developers also use IntelliJ, Eclipse, and Microsoft Visual Studio as their Integrated Development Environment (IDE). The Fortify integration with IDEs and increased automation are the top priorities going forward for Gupta and for Equifax. "We need to continue to shift security left," said Gupta. "I want to see us develop the right code the first time." The Fortify IDE integration available today alerts developers of potential security vulnerabilities as they write their code.

> **"This is a partnership to drive AppSec modernization with Fortify on Demand to delivery actionable, data driven results."**
>
> **Rajan Gupta**
> VP of Product Security
> Equifax



Data-Driven Decisions and Transformation

Today, Fortify is being used to scan applications being developed at Equifax. This includes both current and legacy applications. One of the factors for Fortify's success in Equifax is the information that it provides to Gupta and his development teams. "Fortify is finding nuggets and that makes it easier for developer adoptions," said Gupta. "Fortify is successful because we know it's finding legitimate issues."

Software as a Service model was one of the key success factors of Fortify global adoption. Fortify on Demand takes away the hassle of upgrading to new versions, patching and global availability of a security tool. Gupta says that Equifax is in the business of optimizing data nd enabling people to live their financial best and not in the business of maintaining tools. Fortify on Demand aligns with Equifax vision of moving to the cloud securely and responsibly.

Before implementing Fortify on Demand, developers at Equifax had limited line of sight on how many static and open source security vulnerabilities were in their code. Fortify now provides a measured baseline. “Every step is data-driven,” said Gupta. “Fortify provides visibility and the data to make the next step in our decisions.” For example, Equifax uses a naming convention that helps isolate where security issues are being introduced. Whether it may be a new business unit or a team that has gone through a lot of change, Fortify provides the data to identify where security vulnerabilities are being introduced.

> “Fortify provides visibility and the data to make the next step in our decisions.”
>
> **Rajan Gupta**
> VP of Product Security
> Equifax

Gupta’s goal is to make Fortify and application security part of the Equifax culture so that security is not impacted by growth and new developers joining or by employee turnover. “Application security with Fortify is part of the Equifax development culture,” said Gupta. “Fortify is really a transformation tool and not simply a security tool as it has the ability to transform your development environment and culture.”

- ✓ Develop empathy

- ✓ Hire experienced software architects in App Security

- ✓ Decentralize scans

- ✓ Integrated SaaS AppSec Tools
- ✓ Support decentralization
- ✓ Support transformation metrics e.g. automated scans vs. manual scans

- ✓ Integrate Security Gate in Change Management

- ✓ Code Change vs. Configuration Change

Gupta continues to work with the Fortify team to help bring to market new capabilities that provide immediate results. “This goes well beyond tools and is really about AppSec transformation,” said Gupta.

Learn more at
www.microfocus.com/en-us/cyberres/application-security

Connect with Us

www.opentext.com

opentext™ | Cybersecurity