Having a hard time hiring security engineers? There is another option!

Today we are going to take a look at what the “average” client at Data Defense, LLC (Cypress) looks like. We’ll call them “Fortune 1000 company”. Fortune 1000 company reached out to Cypress seeking security consulting as an alternative to hiring additional security engineers to run their secure development operations. They found it was hard to find application security engineers with experience at an affordable salary.

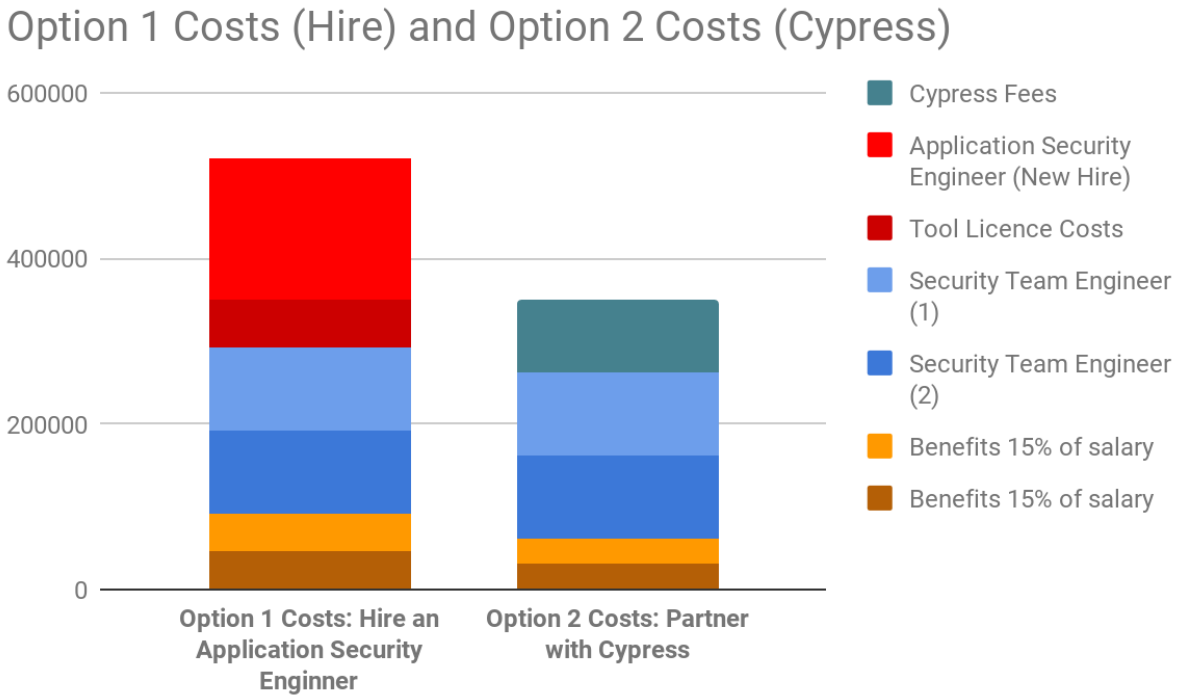
We are going to highlight how Cypress helps tech companies save significant amounts of money in their security budgets, while also helping development teams be more efficient, using the Cypress Application Security program (it is a service but we’re all getting a bit tired of “as a service”.)

Numbers to keep in mind

Fortune 1000 company has an IT department of 50 people. The industry average of security engineers is around five to ten percent of the IT department, and in this example, they would require a 5 person security team where 1-2 of them will be dedicated to application security. They already have a 3 person security team and need to add 2 more to manage their secure development operations.

The average security engineer’s salary in the US is **$109,932**, with an additional cash compensation of **$9,932** on average, according to GlassDoor. And this is for a lower-end application security engineer who won’t have the experience and expertise in automation and integration with the development pipeline.

The company has 3 engineers. In order to properly implement a secure dev-ops program, they will need two more security engineers, or **$109,932 x2 = $219,864** in additional costs if Fortune 1000 company wants to keep up with industry best practices (and we all know all Fortune 1000 company’s love to keep up with industry best practices). If we went the minimal route and just hired 1 additional engineer, we would be looking at **$109,932**. Oh yeah, that cost is without benefits, so tack another 15% - 30% on there for that.



The average cost of one commercial license for a Static Application Security Testing (SAST) or Dynamic Application Security Testing (DAST) tool is often upwards of **$60,000** to **$100,000 or more,** depending on how many applications are being scanned by the tool. If we add that to the cost of our engineer, we get **$109,932 + $60,000 = $169,932 minimum** in additional costs Fortune 1000 company is going to have to spend if they want to implement a secure dev-ops program.

The cost of contracting with Cypress Data Defense to implement their Secure SDLC solution: **less than $100,000, and there is nothing to manage!**

The look on their face when they realize how much time and money they saved = **priceless**

*Yeah I know I stole from a commercial. Shhh, don't tell.

What is the role of a security engineer team?

One of the main focuses of these security engineers other than security testing is to implement and manage the company's SAST and DAST tools. These tools scan for vulnerabilities to help the developers know when they write insecure code. Fortune 1000 company would also have to pay for the licensing, which, as mentioned, can be quite costly. Another critical responsibility to note is the security engineers also need to be available to the development team for regular

security audits and consulting during development. All of the above are the reasons that Fortune 1000 company is looking for solutions (like potentially hiring new team members) to take on the responsibility of running/implementing a secure dev-ops program.

You can see why application security engineer positions often require immense expertise, which is why their salaries can be very budget constraining!

After contracting with Cypress Data Defense, Cypress implemented and managed its own SAST and DAST tools directly into the development teams' issue tracking system for near-direct feedback so that the developers are aware of when they write vulnerable code. Cypress manages and executes regular security testing at the frequency that is best for Fortune 1000 company's development cycle to be sure they are doing everything they can to keep their code safe and secure. In addition to the above, Cypress is available to consult with the development team at the frequency best suited for the company.

After implementing the Cypress Data Defense Application Security solution, Fortune 1000 company no longer needs to hire additional team members, and their current security team can shift most of their focus to higher priority tasks like manual security testing, building security architecture, working early and frequently with the development teams for threat modeling, and helping mitigate other security threats that are more critical and don't have to worry about being bogged down by managing tools and consulting with the development team.

Major Take Away/What we learned/The Important stuff

Now that Fortune 1000 company can rely on Cypress Data Defense to provide the scanning tools, manage and implement the scans, perform audits, perform testing, and consult with the development team, they can get back to doing what they do best and can do it more efficiently.

The annual cost for this particular company to partner with Cypress with their Application Security program was under $100,000, which saved the Fortune 1000 company more than $200,000 in costs which they can now apply to different aspects of their budget.

OPTION 1	OPTION 2
Pros: ❏ An in house employee has more flexibility ❏ You get to spend more money! YAY!	Pros: ❏ No tool licensing fees ❏ Have near immediate access to industry-leading security experts with backgrounds in application development. ❏ Increase the efficiency of the current security team

Cons: ❏ Overall more expensive ❏ Potential employee turnover costs and headache	Cons: ❏ You don't get to spend as much money and annoy your CFO :)

Sometimes organizations must incur the hefty costs associated with hiring and managing a large in-house security team. But the folks at Cypress Data Defense are finding a lot of success with a different approach. Outsourced managed application security. Like they say if it's not what you do, outsource it!

So I leave you with this: Security is a necessity, but struggling with hiring and managing application security engineers and security tools is not.