mend.io

Mend.io Helps Reveal

Maintain Ultra-High Standards for Mitigating Application Risk

About The Company

Reveal provides world-class document review technology, underpinned by leading processing, visual analytics, and artificial intelligence, all seamlessly integrated into a single platform for eDiscovery and investigations
They help organizations including legal service providers, law firms, and corporations uncover more useful information faster.

The Challenge

Every organization is different and every organization has a different tolerance for risk. As a legal discovery and document review software provider, Reveal has a tolerance that nears zero.
"The legal industry is one of the most risk averse industries known to man for obvious reasons. We're highly regulated but not necessarily by regulators, but by the industry itself. Everyone is looking and they expect us to be down to nearly zero vulnerabilities," said Reveal's Chief Technology Officer (CTO), Matthew Brothers-McGrew. "We weren't paying attention to it as much before and we were getting constant pings from our clients saying 'Hey, what about these vulnerabilities?' It was embarrassing when they found a vulnerability and it had been there for three years. How do you tell a client you haven't paid attention to it in three years?"

Brothers-McGrew looked at Reveal's leadership team and asked, "What do we not want to be talking about tomorrow or in six months? This is something we don't want to be talking about. And we don't want to look like we don't have a handle on it."

Key Solution Requirements

Repo integrations: As Reveal acquires companies with differing pipelines and maturity, they need a solution that integrates with various repositories, standardizing their security processes across all of their holdings and giving them quick insight.

License compliance: As a company financed by private equity, it is critical for Reveal to maintain license compliance in order to protect intellectual property.

Transparent pricing: Some providers offer pricing structures with hosting fees that can spiral out of control. Reveal needs per-developer pricing so the cost of adding new developers when acquiring new companies is simple and predictable.

The Mend.io Solution

Now employing about 600 people, it was around the 120 mark that Reveal matured their organizations and processes and brought in Mend. Several Reveal teams integrated Mend SCA into their various repos, including GitHub, and additionally integrated with JIRA so every new ticket goes to each teams' board. They set out with an initial goal to prioritize and address critical vulnerabilities first, before the next sprint.

"When we first put Mend SCA in place in our ecosystem, the vulnerability numbers were sky high. We're using over 8000 libraries and a lot were vulnerable!" said Brothers-McGrew. "I looked at our teams and said 'Look, I'm not going to beat anyone up. Let's prioritize and figure out how to bring the number down in a reasonable time. Then we don't have to talk about it ever again."

Brothers-McGrew didn't encounter much pushback from developers. Instead, it was the product team that needed to be convinced. "They drive features and client value. Anything I take away from that causes them some heartburn, but everyone understood this was something that we needed to do. We were very pragmatic when it came to security and rollouts. I'm not a believer in just checking a box. There has to be a reason," said Brothers-McGrew.

Reveal got their number of vulnerabilities down to just a handful of libraries within three months. "Once you get to the plateau and you have things under control, you just need to play whack-a-mole every month or two when new vulnerabilities come out. And that's already part of your process," said Brothers-McGrew.
Down to the final few vulnerabilities, Reveal's CTO made a decision to favor a perfect score over his usual pragmatic outlook. "When you get very close to the baseline, there's stuff in there that doesn't really matter because it isn't

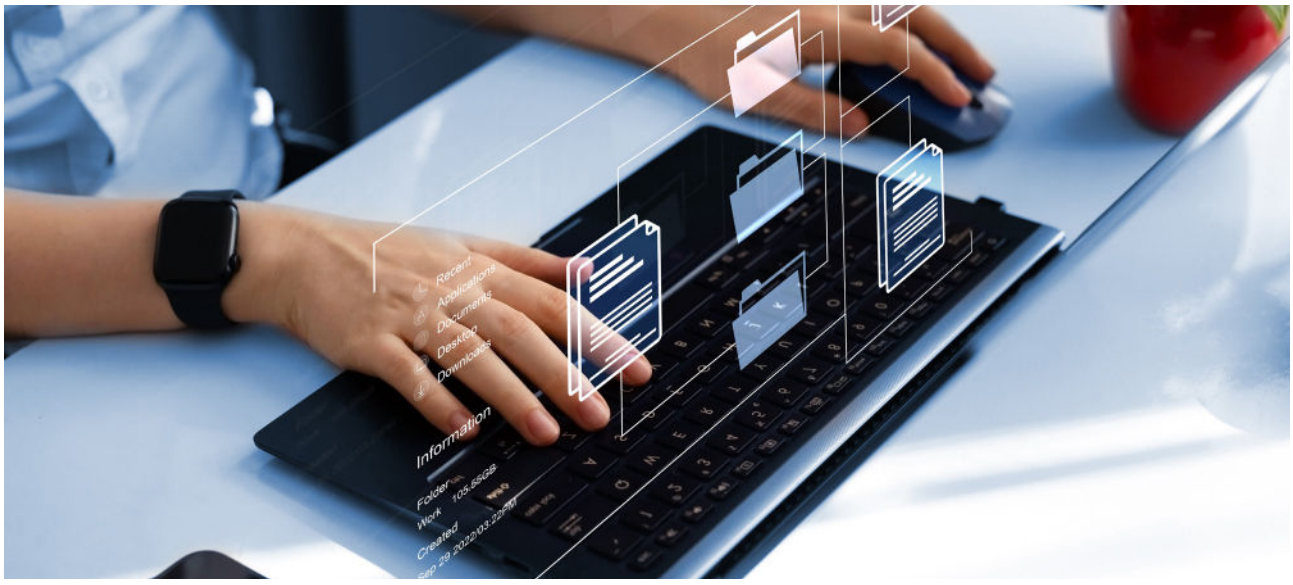
exploitable. At the same time, I knew big clients were doing their own scans and would come back about small things that had zero bearing, but I would have to spend so much time explaining it. If I try to get into nuance their eyes glaze over. I need a clean report," said Brothers-McGrew.

Solution Value & Benefits

For Reveal, one of the biggest benefits of using Mend has been faster due diligence processes. "I sit through a lot of these in my position and the more chinks they find in your armor, the harder they look. Their job is to find your skeletons. Now I can confidently say we have it all under control. It takes the wind out of their sails. We have less problems with each due diligence process," said Brothers-McGrew.

Reveal has found additional benefit in license monitoring. "It's been hugely helpful. When you sell a company, the only question anyone cares about is whether there's a product there that can actually be sold and that comes down to licensing. Using Mend SCA makes it easier for us to go through due diligence processes in the future when we sell or buy companies. We have a handle on vulnerabilities and licensing from day one so I can look at the legal team and say we have this under control, the licenses are free and clear, vulnerabilities are in check," said Brothers-McGrew.

Even with Reveal's security debt now all paid up, Mend SCA continues to be a useful tool, not just for continued scanning on every new code commit, but so they can repeat the process of bringing vulnerabilities down for each new company Reveal acquires. For Brothers-McGrew, he's been here before and knows what to do: "We add Mend SCA as soon as possible so we can get a good benchmark and know where we stand. I look at the new company and say 'Prepare yourself for big numbers. It's okay. Don't freak out about this. We'll get through this together. Let's start with the most critical..."'



About mend.io

Mend.io, formerly known as WhiteSource, effortlessly secures what developers create. Mend.io uniquely removes the burden of application security, allowing development teams to deliver quality, secure code, faster. With a proven track record of successfully meeting complex and large-scale application security needs, the world's most demanding software developers rely on Mend.io. The company has more than 1,000 customers, including 25 percent of the Fortune 100, and manages Renovate, the open- source automated dependency update project.

For more information, visit www.mend.io, the Mend.io blog, and Mend.io on LinkedIn and Twitter.