LEGIT

CASE STUDY

Large financial services firm remediates 90% of secrets and governs AI use with Legit ASPM

After watching several peer enterprises struggle with debilitating ransomware attacks, a large financial services firm kicked off a detailed assessment of their security posture. They engaged an outside company to conduct an adversarial assessment and determine if they would also be susceptible to the same type of ransomware attacks plaguing their peers.

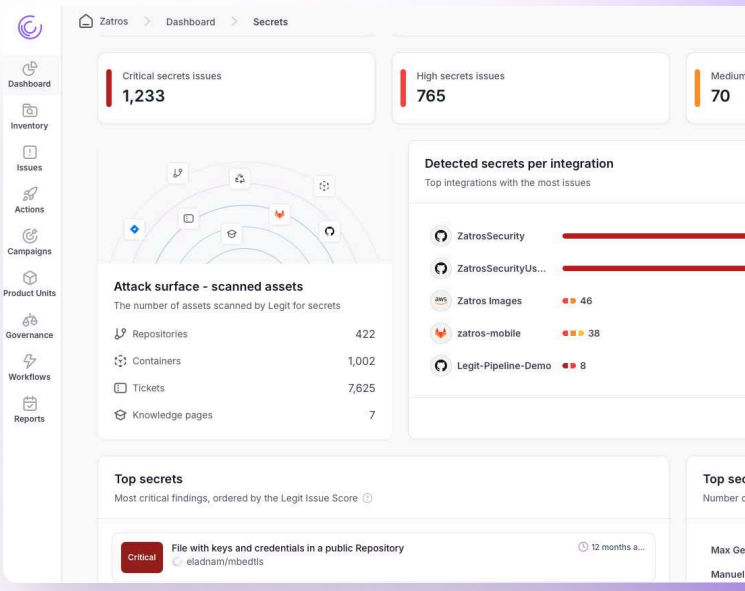
The hidden risk of exposed secrets

That assessment highlighted that the financial services firm had significant risk stemming from secrets stored across their development environment in places that were not adequately monitored or secured. Exposed secrets were identified in source code repositories, developer collaboration tools, systems used by the help desk, among other places. And they weren't just identified in shared repositories, they were also found in insecure files on developers' local machines. If a developer ended up with malware on their machine, the malware would have been able to identify and leverage those secrets.

Ultimately, these exposures increased the risk of attackers bypassing controls and accessing systems with valid credentials, without exploiting a vulnerability or performing any kind of brute force password guessing attack. This kind of breach would not trigger any security alerts, making it extremely difficult to identify.

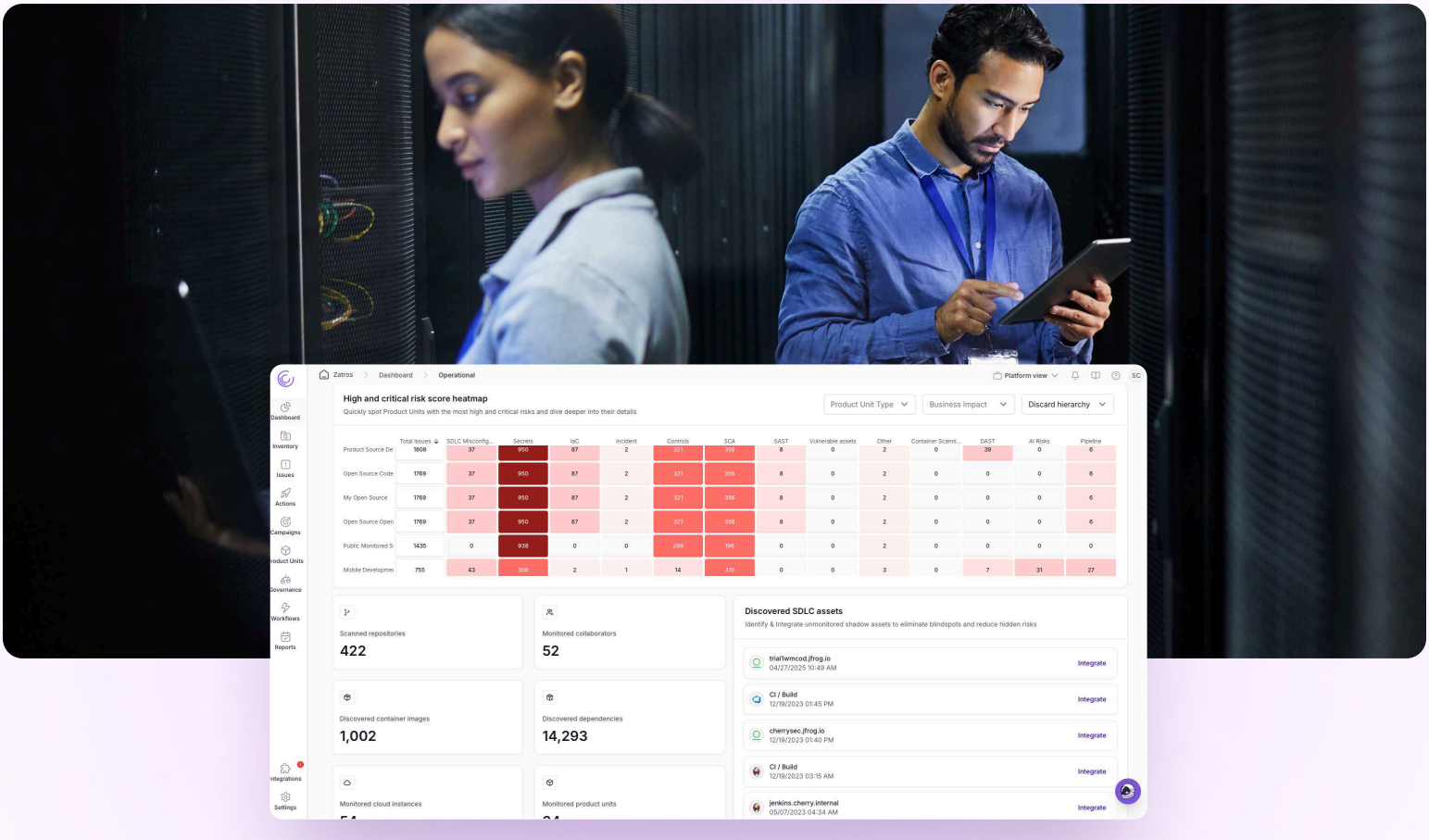
"To use a physical world example," says the head of cyber threat management at the financial services firm,

"if there were a thief trying to get into my house, imagine that instead of trying to pick the lock, or trying a hundred different keys, they simply looked under the mat and found the key there. That would get them in the house a lot quicker."



In fact, the company conducting the assessment was able to use the exposed secrets it found to move laterally throughout the firm.

The financial services firm was, therefore, looking for a solution that would not only identify exposed secrets and remediate them, but also prevent developers from storing this kind of information in an insecure way.



Application security that works with a large, complex development environment

This financial services firm is a large, long-standing global company with dispersed application teams developing software in different ways with different languages and development environments – including both legacy and newer technology. Any security solution needed to be able to work across this whole landscape and support a diverse set of solutions.

Another key criterion was a centrally accessed and managed solution that a security vendor would help maintain and deliver. The firm is moving a lot of workloads to the cloud and works with a lot of SaaS vendors, so an on-prem solution would be a disadvantage.

Selecting Legit ASPM

The team selected the Legit ASPM platform to address their secrets exposure problem and shore up other areas of their SDLC because of its robust secrets scanning capabilities, plus its ability to easily scale to accommodate its large, complex development environment. The head of cyber threat management notes that Legit's size played a role.

"Especially in information security, where you're trying to keep pace with the innovation that the attackers have, and you're also trying to keep pace with the innovation of the technology industry, you get better results if you're dealing with a smaller, more nimble, engineering-driven company. I've always found that the sweet spot is dealing with vendors like Legit that are innovative and can adapt and respond to roadmap requests, integration requests, and feature requests at a pace that somebody in security needs."

"I've been in this industry for several decades now, and I would say Legit is in the top 5 vendor experiences that I've had."

– Head of cyber threat management at a large financial services firm

The financial services firm's results with Legit ASPM

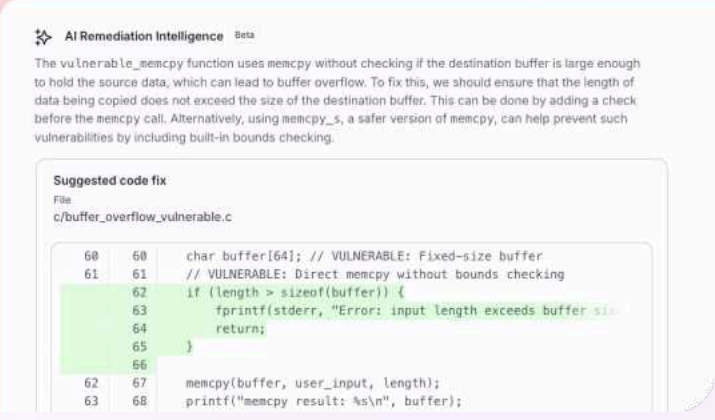
The financial services firm is now consistently remediating over 90% of exposed secrets.

They were especially pleased with Legit's capabilities beyond simply finding secrets exposure to supporting a full remediation lifecycle and closing issues.

Part of that impressive remediation rate stems from Legit's ability to adapt to the enterprise's internal process and lifecycle. Another part stems from the fact that the Legit ASPM platform produces information that a variety of people can read, understand, and take action on.

"That is not something that I see in a lot of the security products that are out there," says the head of cyber threat management. "You tend to have products that excel at finding things, but they are not helpful in actually getting the issues addressed, or addressed in an intelligent, risk-based way."

– Head of cyber threat management



Legit adds value beyond secrets scanning

AI is playing an increasingly large role in this financial services enterprise's development organizations. In turn, they are finding value in using Legit to help govern AI – to identify where AI is in use in their development environments, and whether it's being used within the standards the enterprise has established.

Legit is also helping their developers write good, compliant code right from the start, rather than waiting to address security issues in fully baked code.

> "Legit has been adding value since the first day we turned the product on"
>
> – Head of cyber threat management

People first

Ultimately, the head of cyber threat defense finds that the benefits of working with Legit go beyond the technology. "It's the soft skills," he says. "The interpersonal skills, the reach out, the proactive communication. All these things make a huge difference."

Learn more

Get more details on how Legit customers are super charging their AppSec programs with the Legit ASPM platform.

LEGIT