Your Guide to Modern Application Security

Build with speed and confidence with Mend.io and AWS

In collaboration with

mend.io

Table of contents

70%

of all components used in applications today are open source

35%

of external attacks occur through a software vulnerability exploit

New software development approaches, new security challenges

Modern software development is based on cloud-native application architectures designed to take full advantage of the speed and scalability of the cloud. These applications are more often assembled than they are written, built from open source components strung together with a small amount of custom code. In fact, it's estimated that open source components make up at least 70 percent of all components used in applications today.

While this approach helps organizations deliver applications faster and more efficiently, it also makes application security (AppSec) more complex than ever before. And, at the same time AppSec has become more complex, it has also become more critical: research by Forrester found that 35 percent of external attacks occur through a software vulnerability exploit.

A modern approach to AppSec

What do security professionals, developers, and cloud engineers have in common? They're all looking for an integrated approach to AppSec that frees developers to deliver quality code faster and engineers to deploy with confidence—all without compromising security.

A mature, modern AppSec approach incorporates tools that address each stage of the software development lifecycle, from tools that help developers find and fix security issues to runtime protection tools that secure applications in production.

However, tools are only one piece of the puzzle. That's because most tools today focus on detection, which generates an exhausting list of alerts for security and development teams to deal with. While it's important to detect as many security issues in the application layer as possible, considering the pressures that developers are under to release applications quickly, it's unrealistic to attempt to fix them all.

That's why a modern AppSec approach includes strategies and technologies that help teams prioritize by giving them tools to zero-in on the security vulnerabilities that present the biggest risks. That way they can address them as quickly as possible.

After prioritization comes remediation—technologies that integrate seamlessly into the development cycle to help remediate issues when they are easier and cheaper to fix and that then update vulnerable versions automatically.

Bringing detection, prioritization, and remediation together makes it possible to increase the pace of development and delivery to meet critical business needs without compromising security. **And, as six out of ten of the largest software organizations know, that's where Mend.io delivers.**

Mend.io: Modern, integrated AppSec across industries

Mend.io is an application security company built to secure today's digital world. Mend.io's unique Application Security Platform goes beyond traditional detection-oriented solutions to reduce application risk without impacting development deadlines. Enterprises around the world trust Mend.io with their AppSec, including those in verticals that rely heavily on customer-facing apps and in-house development.

Financial services: It's obvious why cybercriminals are drawn to the financial services industry— that's where the money is. But it's not just banks. Financial services also include credit unions, investment and insurance companies, credit card companies, and mortgage lenders. All of these companies have websites and mobile apps that provide a huge attack surface for hackers. They're also highly regulated, which creates significant exposure when it comes to compliance.

Independent software vendors (ISVs) and technology firms: It's the business of ISVs and other tech companies to develop applications that are then sold or used as part of an online product. To save time, developers commonly leverage open source software. The first open source package they add to their codebase is always intentional, but once an open source package has been added, it can invite other open source packages to the party. The list of "transitive dependencies" can grow quite large. Increasingly, software buyers are demanding that ISVs provide a software bill of materials (SBOM) that lists all the contents of the applications they buy.

Retail: Retailers are leaders in the digital transformation space, deploying technologies online and in store that enhance the customer's buying experience and increase brand engagement. That transformation is driven almost entirely by software and cloud-native applications, either built internally or resourced from third parties, each one of which carries risk. Retailers also hold customer personal and financial information, making them a prime target for hackers and leaving them vulnerable to operational disruption and loss of revenue and reputation.

Meet Mend.io

Mend.io, formerly known as WhiteSource, effortlessly secures what developers create. An Amazon Web Services (AWS) Advanced Technology Partner, Mend.io 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.

Mend.io and AWS: Autopilot for AppSec

These days, application security must do more than check the compliance boxes. A truly modern program reduces risk and accelerates development by leveraging automated tools built into the technologies that software and security teams know and love. Think of it as autopilot for application security.

As an AWS Partner, Mend.io is uniquely positioned to help build a preventative approach when it comes to securing their applications running on AWS, the world's most comprehensive and broadly adopted cloud platform.

Mend.io integrates seamlessly with existing AWS DevOps environments and CI/CD pipelines. Mend.io also works with AWS Lambda, Amazon Elastic Kubernetes Service, Amazon Elastic Container Service, Amazon CodeCatalyst, AWS CodeCommit, and AWS CodeBuild. These integrations reduce complexity and increase developer velocity.

Mend.io helps enterprises meet their obligations as part of the AWS Shared Responsibility Model. Under that model, AWS is responsible for the security of the cloud, while customers are responsible for securing their apps in the cloud. Together, Mend.io and AWS provide an end-to-end application security solution.

By freeing developers from the burden of application security, Mend.io also helps expedite the development and deployment of apps on AWS. Mend.io makes it easy for companies to scale with confidence.

Close the gaps. Fix the apps.

Mend.io ensures that applications running on AWS are secured using a remediation-first approach. Mend.io makes it easy to:

Manage open source security with Mend SCA

Open source software requires a different type of application security than enterprises have traditionally used. The highly publicized vulnerabilities known as Log4j (December 2021) and Spring4Shell (March 2022) show the urgent need for open source application security, as have malicious software supply chain attacks coming from open source registries such as npm.

Mend.io is a market leader in software composition analysis (SCA), and securing open source software on AWS starts with Mend SCA. From identification of open source components (including transitive dependencies) to automated remediation to protection from malicious open source packages, Mend.io provides the most accurate and developer-friendly product on the market. Mend.io enables AWS customers to use open source freely and fearlessly without compromising on security or agility.

Mitigate open source supply chain risks with Mend Supply Chain Defender

Given the increasing number of software supply chain attacks, it is imperative to have a tool that prevents malicious software from entering the codebase at any point of the development process. Mend Supply Chain Defender detects and blocks malicious open source packages before developers can download them—and before they can pollute the codebase with malicious activity.

Manage custom code security with Mend SAST

While today's applications rely heavily on open source software, most still use about 20 percent custom code, which must be secure to secure the app as a whole. Mend.io offers Mend SAST, a next-generation static application security testing product that deploys with ease thanks to its unique hybrid architecture. Mend SAST seamlessly integrates with developers' existing workflows and development environments so they can easily trigger security tests when they need them most—when they're writing code. Mend SAST provides peace of mind and bridges the gaps between developer and security teams.

Automate dependency updates with Mend Renovate

The more up-to-date a dependency is, the lower the number of known vulnerabilities it will tend to have. Mend Renovate is the industry's first auto-dependency update solution that natively integrates with AWS CodeCommit and AWS CodeBuild. Renovate's robust configuration options enable users in almost any environment to get started within minutes. What's more, crowdsourced Merge Confidence data from tens of thousands of repositories enables developers to make easy update decisions.

The fast lane to bottom-line benefit

Whether you're managing open source risks, protecting the entire software supply chain from malicious attacks, or automatically updating dependencies, Mend.io empowers your developers to deliver with speed and confidence, driving business value.

Manage open source security with Mend SCA

Reduce your application security risk by as much as 90 percent. Organizations using Mend.io report greater visibility into risks in their codebase, faster mean time to remediation (MTTR), and far lower overall levels of application risk.

Stop malicious packages. Detect and eliminate malicious packages in your existing code base and block them from entering new applications with Mend.io's 360° Malicious Package Protection.

Reduce security alerts by approximately 80 percent. With Mend.io, your team can focus on what really matters by eliminating false positives and prioritizing vulnerabilities based on their impact.

Give developers back their time. With Mend.io, developers save up to 80 percent of the time they would have otherwise spent remediating AppSec issues. By freeing developers from security tasks, Mend.io eliminates the app development security vs. speed tradeoff and reduces friction between developer and security teams.

Mitigate the cybersecurity skills gap. Because Mend.io's automated remediation provides exact fixes for each line of code, even less experienced developers can easily deliver safe, risk-free code. Mend.io's easy-to-learn and easy-to-use platform empowers developers at all levels, minimizing the impact of the ongoing cybersecurity skills gap and boosting developer velocity and throughput across your team.

Mend.io in action: Global media and technology company chooses Mend.io to mitigate open source security risks

Situation

As a result of several high-profile security breaches, including Equifax's 2017 data breach, this global media company wanted to be more proactive about app security to reduce risk to its large customer base and its trusted brand.

Solution

Much of the media company's code is open source, so it needed a solution that put open source security first. Another goal was to shift app security left—earlier in the software development lifecycle (SDLC)—so it integrated Mend.io into developer workflows and CI/CD pipelines.

Results

Mend.io brought order and security to the media company's open source usage. The company says Mend.io is more reliable than competitors, easier to integrate, and less expensive on a per-developer basis. Ease of use is very important: if a security tool doesn't easily integrate with other tools, developers won't use it. By using Mend.io, the company is more efficient when it comes to identifying vulnerabilities, with fewer false positives.

Deploy confidently with Mend.io and AWS

Ready to secure your application development with the help of Mend.io and AWS? Deploying with confidence starts here:

Find Mend.io in the AWS Marketplace ›

Try Mend.io for free ›

Learn more about Mend.io and AWS ›

In collaboration with

mend.io

aws PARTNER

- DevOps Software Competency
- Security Software Competency