Mend.io

From Reactive to Effective: Building Application Security that Works

In 2023, 71% of enterprises admitted their AppSec programs were in a constant state of reaction as they played catch-up to a never-ending list of vulnerability alerts.

That's not a good number—and context makes it even worse. Consider the following:

Nearly 70% of organizations have directly encountered at least one serious security incident from a software vulnerability over the last 12 months.[1]

Data breaches are at an all-time high, a **78% increase** from 2022.[2]

Those attacks have made application security a board-level priority for **85% of companies**.[3]

That adds up to increased business risk for a lot of companies and fuels an urgent need to improve application security strategies. To solve the problem, organizations must shift to a mature and proactive application security program that provides visibility and control.

The key is to give developers and AppSec teams exactly the tools they need to not only remediate effectively, but also reduce the number of issues introduced in the first place—all while helping them work together. Doing so will ultimately help companies stop chasing vulnerabilities and start managing the risk in applications.

[1] ESG Report: Optimizing Application Security Effectiveness

[2] ITRC Annual Data Breach Report

[3] ESG Report: Optimizing Application Security Effectiveness

How Did We Get Here?

Reactive application security is a big reason why only 52% of companies say they can effectively remediate a critical vulnerability, and even fewer application security practitioners (44%) agree with that assessment.[4]

The tendency for many AppSec teams to react rather than take charge stems from the early days of the practice, when many programs started as a regulatory compliance tool.

Those teams needed documentation more than anything else, so tools were built to scan and alert. The results yielded plenty of information, but it was not always easy to take action on the data.

Shift-left security testing is another factor. By embedding security as early as possible in the software development life cycle (SDLC), companies can detect issues earlier in the process, saving time, resources, and potential damage-control costs.

However, shifting left also resulted in a bifurcation of responsibilities, as AppSec moved from being a security-only duty to one shared by both developers and the security team. And while these teams share a common long-term goal, they have different ambitions, different processes, and different tools. Developers want to meet release deadlines and stay in the tools and environments they use the most. Security needs visibility, control, and tracking to make better-informed strategic decisions.

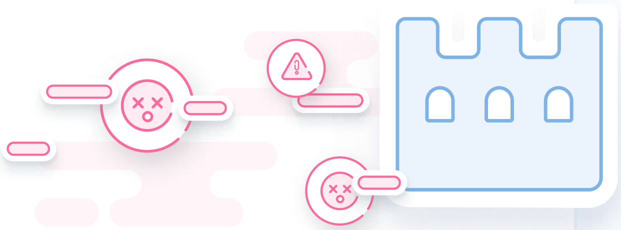
Characteristics of Reactive Teams

While understanding the historical context helps explain the reactive nature of application security, it's even more crucial to focus on the daily challenges faced by development and security teams. As the manifestations of reactive root causes, they provide clear targets for improvement.

Only 52%

of companies

can effectively remediate a critical vulnerability.



[4] ESG Report: Optimizing Application Security Effectiveness

Developers

Neglecting dependency updates

One recent study found that 89% of codebases contained open-source code more than four years out of date. That's classic reaction AppSec.[5]
Why? Ignoring dependency updates accumulates technical debt. And when declining software quality finally forces an upgrade, the fix will be far more painful.

Side effects of alert fatigue

According to 88% of CISOs, alert fatigue is causing developers not to remediate critical vulnerabilities.[6]
As a result, teams often don't know what to fix when a significant security incident hits, sending them into panic mode.

Security

Fragmented data, funcionality, and processes

For 65% of companies, fragmented security infrastructure impedes response effectiveness as security teams struggle to get a holistic view of all their vulnerabilities.[7]

It's crucial for application security teams to identify and prioritize vulnerabilities according to the risk they pose. However, many security teams have very limited information to effectively prioritize vulnerabilities' remediation.

Cannot 100% cover critical applications

Complex deployment of existing tools across data centers and cloud environments prevents teams from getting full coverage of applications. It also blocks crucial mass-deployment capabilities and usage for many enterprises.

[5] https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

[6] https://cycode.com/blog/introducing-the-state-of-aspm-2024-report/

[7] https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

88%

of CISOs

say developers aren't remediating critical vulnerabilities **due to alert fatigue**

89%

of codebases

contained open-source code more than **four years out of date**

The Solution

Building a strategy that truly manages application risk starts by addressing the primary pain points of reactive AppSec. As long-time proponents of proactive application security, Mend.io has helped customers build and manage a mature, proactive AppSec program—and the numbers back this up. We surveyed a representative sampling of Mend.io customers that use repo integration; respondents reported improved outcomes for both developers and security teams (see data below.)

So what do proactive application security programs look like? Let's start by solving the common pain points listed above.

Proactive State: Developers

Developers keep their dependencies up to date, while identifying and prioritizing the high-risk vulnerabilities most in need of remediation.

> *When the product you sell is an application you develop, your teams need to be fast, secure and compliant. These three factors often work in opposite directions. Mend provides the opportunity to align these often competing factors, providing Vonage with an advantage in a very competitive marketplace.*
>
> **Chris Wallace, Senior Security Architect, Vonage**

Effective Dependency Updates

Open source code has nearly always been updated by the time a vulnerability has been updated, so keeping up with dependencies is one of the most effective methods available for eradicating vulnerabilities. In fact, companies with effective AppSec programs are significantly more likely to apply dependency management for open source components[8]. By one estimate, teams that consistently update new versions within 48 hours of publication can reduce vulnerabilities by 83%.

When evaluating dependency update tools, ask the following questions.

- Does this tool scan repos to detect dependencies and check for updates?
- Does this tool submit automated pull requests delivered in the repo?
- Does this tool provide Merge Confidence scores to alerts on problematic updates?
- Does this tool automatically group and merge high-confidence dependency updates?
- Does this tool support private libraries/packages?

Mend Renovate

Mend Renovate is among **the top 1% of repositories on GitHub**, and is a key element in lifting the burden of security from your developers.

1.3 B downloads

↓83%

Teams that consistently update new versions within 48 hours of publication can **reduce vulnerabilities by 83%.**

[8] ESG Report: Optimizing Application Security Effectiveness

Spotlight Experience

To rapidly identify and mitigate high-risk vulnerabilities, developers must quickly narrow down what matters most—which means time is crucial. One important element of that is to provide developers an embedded experience that highlights what's critical.

Doing so makes it easy for developers to routinely apply AppSec processes. This translates roughly into a three times reduction of risk, while time to remediation is cut by 75 percent.[9]

Spotlight Experience	Before Mend.io	After Mend.io
Percentage of developers using AppSec tools regularly	5%	90%
Average time spent per remediation (hours)	5	1

Source: Mend.io customer survey

Some key features to consider when providing a spotlight experience include the following:

- ✓ Seamless integration into repo environment, gives developers everything they need within their workflow
- ✓ Prioritized vulnerabilities in the repo, including reachability analysis.
- ✓ Remediation suggestions or training guidance on how to fix.
- ✓ Real-time feedback to developers on commit
- ✓ Differential results—that is, vulnerabilities that were introduced since the last scan

> *One of our most indicative KPIs is the amount of time for us to remediate vulnerabilities and the amount of time it takes us to fix vulnerabilities, which has reduced significantly. We're talking about at least 80% reduction in time.*
>
> **Willis Towers Watson (WTW), Insurance Services**

[9] Mend.io Open Source Risk Report

Proactive State: Security Teams

When security looks like a puzzle, developers are forced to make decisions based on partial information—and that means they are only coming up with partial solutions. There are two important factors to get security teams out of reactive mode.

Full Visibility And Control

To get the big picture, security teams need all the pertinent information in one place. A unified view of all vulnerabilities, combined with the ability to identify the highest-risk security issue or dependency, means that teams have the information, control, and oversight to make smart decisions and deploy security policies at scale.

Some key features to consider when providing a spotlight experience include the following:

- ✓ Holistic view on platform
- ✓ Centralized scan configuration
- ✓ Easy integration with third-party tools via REST APIs
- ✓ Prioritization capabilities based on reachability analyses in the application layer and container layer; exploitability; and CVSS 4.0 scoring

Security KPIs	Before Mend.io	After Mend.io
Real-time application visibility	10%	90%
Application deployment stoppages per month due to security flaws	8	2
Days required to identify locations of zero-day exposures	10	5
Days required to remediate zero-day exposures	14	1

Source: Mend.io customer survey

Flexibility And Scalability

The ability to centrally deploy and mass-manage tens of thousands of repositories is another manifestation of holistic application security programs. This means cutting through the complex sprawl of existing tools, both on premises and in the cloud, to centralize and scale deployment and help security teams easily implement security policies. Building that scalability requires the following:

- ✓ Cloud-first elastic architecture with no limits on daily scans, applications, or projects
- ✓ Global repo configuration that gives teams central management and the ability to apply parameters to multiple repositories
- ✓ Mass-deployable to tens of thousands of repositories with minimal effort
- ✓ On-premises scanning scalability with no limits

Remediation KPIs	Before Mend.io	After Mend.io
Percent remediated	10%	90%
Average number of days to remediate a vulnerability	271	71

Source: Mend.io Open Source Risk Report

> *It is hard to assign a value to an incident you prevented from happening. You need to understand and manage your risks. Your company and customers demand it. You can not put a price on trust, and Mend helps us maintain the trust we have with our customers.*
>
> **Nick Banta, Vice President of Global Cybersecurity, Trimble**

Conclusion

As a foundational element of the digital world, applications have become an integral part of the way the world works—and consequently, one of the top targets for threat actors worldwide. However, many application security strategies have not kept up with the constantly evolving threat landscape. Built more for regulatory compliance than robust defense, such outdated programs often prove ineffective against modern threats. To adapt and defend against the threat landscape of today's digital world, organizations need to stop reacting and take charge with a modern and proactive AppSec strategy. Such an approach allows organizations to prevent, detect, remediate, and recover from the wide range of threats affecting applications—a vital strategy for supporting today's increasingly digital business ecosystem.

Mend.io

Contact an expert to learn more about proactive application security

Schedule a demo