APPSEC PHOENIX

APPSEC PHOENIX

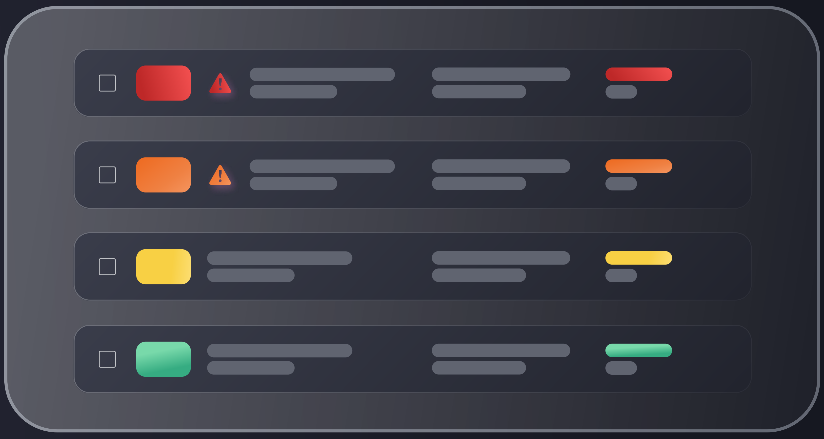
Fix today the vulnerabilities that will be exploited tomorrow

AppSec Phoenix gives developers the tools to build modern applications that are secure. Instantly turn your DevOps pipeline into a DevSecOps pipeline through the automated risk-based vulnerability management capabilities.

Security vulnerabilities are everywhere. Identifying the impact and severity of the vulnerabilities allows you to:

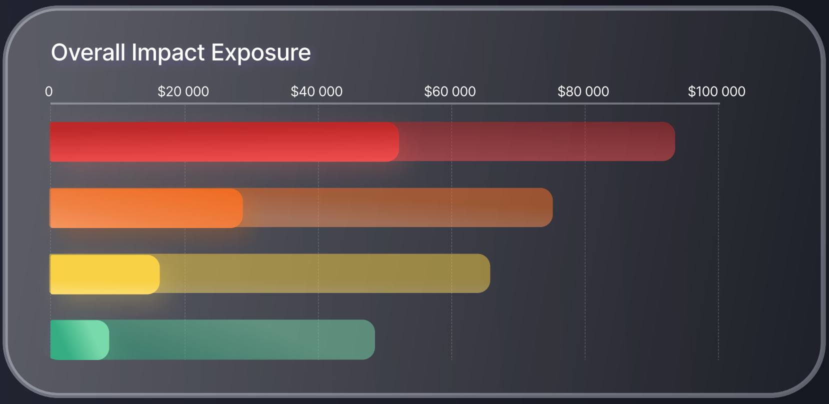
01 Prioritize

the most potentially damaging risks your applications face



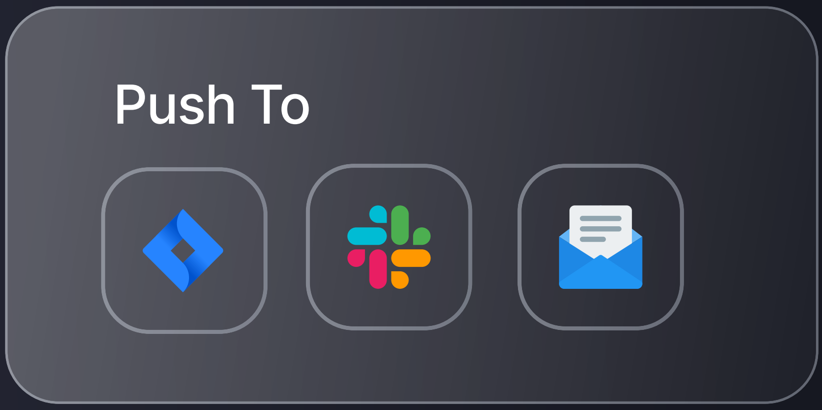
02 Quantify

the risk to help non-security professionals understand



03 Create

reports quickly and easily to share with C-level executives



04 Analyze

the risk using AppSec Phoenix's risk formula - threat x vulnerability x consequence

Medium
Exploit available Yes
Exploitability by Severity Medium
EPSS Low
External visibility by attackers Yes

And all of this comes from a single window - clarity in the sea of noise.

AppSec Phoenix is not just a dashboard.

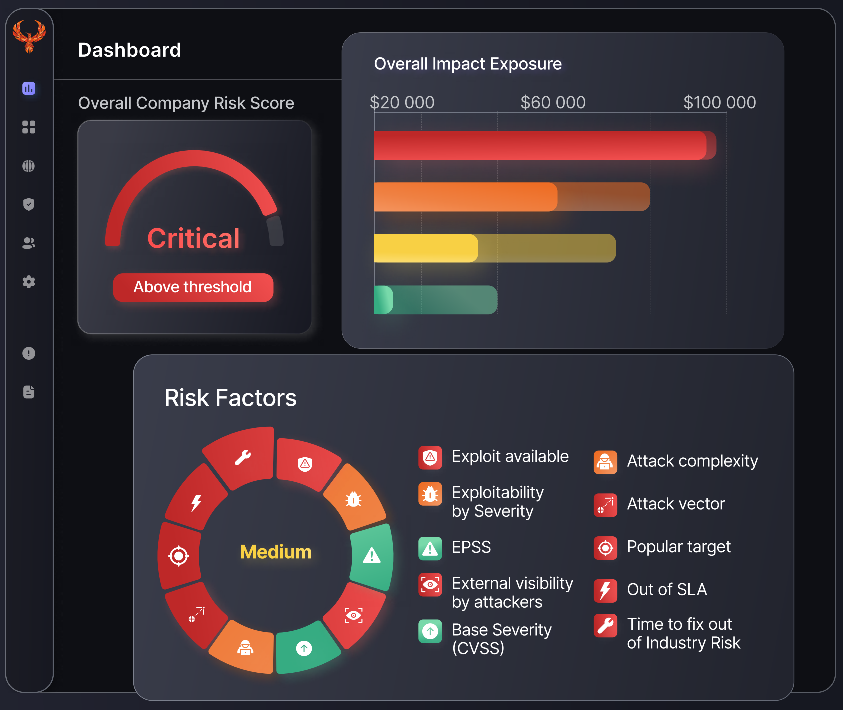
AppSec Phoenix is a **SMART Risk-Based Vulnerability Management** system that is contained in one easy-to-use UI. For organizations that don't have large security departments but still want to ensure the overall safety of their applications, AppSec Phoenix delivers a suite of tools that can act as a substitute while you grow.

It is a complete toolkit for developers at every stage of the SDLC. But unlike other SDLC tools, AppSec Phoenix was designed to give key intelligence to non-technical stakeholders and developers alike.

Understanding AppSec Phoenix

Gather data and use it to strengthen your security posture

- AppSec Phoenix uses 15 data points to build complete pictures of potential application vulnerability, examining the risks in the context of internal and external intelligence.
- The simplified flow aggregates and contextualizes data for ease of analysis.
- Dark Web Insights give you data on your attackers, including an extensive dark web database.



Automate your security response to save time for your business

- AI & Machine Learning provides risk impact analysis and remediation intelligence.
- AppSec Phoenix prioritizes and organizes threats into a hierarchy of risk, allowing for easier analysis.
- A prioritized list automatically accounts for your threshold and the areas which need the most urgent attention.

Prioritize the most dangerous threats and deal with them head-on

- Quantification of the potential risks gives clear financial indicators for high-risk threats.
- Developers and C-level executives alike can see the areas that need urgent attention and if there is one team in particular that needs more guidance.
- Push actions out to Jira or Slack and integrate them with your existing Kanban board.

The Problem It Solves

Cut the Cost of a Breach

A data breach on average costs a company $2 million in the post-breach window, but the overall fallout can rise to as much as $2 trillion. That's why 60% of businesses end up shutting down after a severe data breach.

By automating and fully integrating security tools through AppSecurity, you can minimize the risk of a serious data breach in your organization. Using AppSec Phoenix's wide range of tools to scan and secure your applications can strengthen your security posture and defend against a breach.

Make up for small security departments

Right now, there are 750 developers for everyone 1 security professional. On the ever-expanding attack surface, this lack of trained threat response workers is only going to hand the initiative to threat actors.

In place of a dedicated team of security professionals, AppSec Phoenix can provide a wide range of analysis and automated response tools to complement the toolkit of a small security team.

Improving DevSecOps

Moving from a DevOps organization to a DevSecOps organization is a difficult process. The entire development pipeline needs to be reconfigured and proper security tools need to be integrated.

Thanks to AppSec Phoenix's suite of security tools, you will make the jump to DevSecOps easier for everyone involved. The data collection and automated response aspects of AppSec Phoenix's approach to help the team collaborate better.

AppSec Phoenix does more than integrate tools. It augments the humans that use them and improves the security capabilities of a DevOps team without hiring expensive security professionals.

Speed Up Response Times

Critical data breaches can take up to 60 days to fix and potentially up to 280 days for smaller attacks. For smaller organizations, the associated downtime and costs can be enough to send a company under.

AppSec Phoenix automatically detects and analyzes errors in your applications, meaning that attackers will have a harder time penetrating your defenses and cutting the severity of a serious risk by as much as half.

Use Cases for AppSec Phoenix

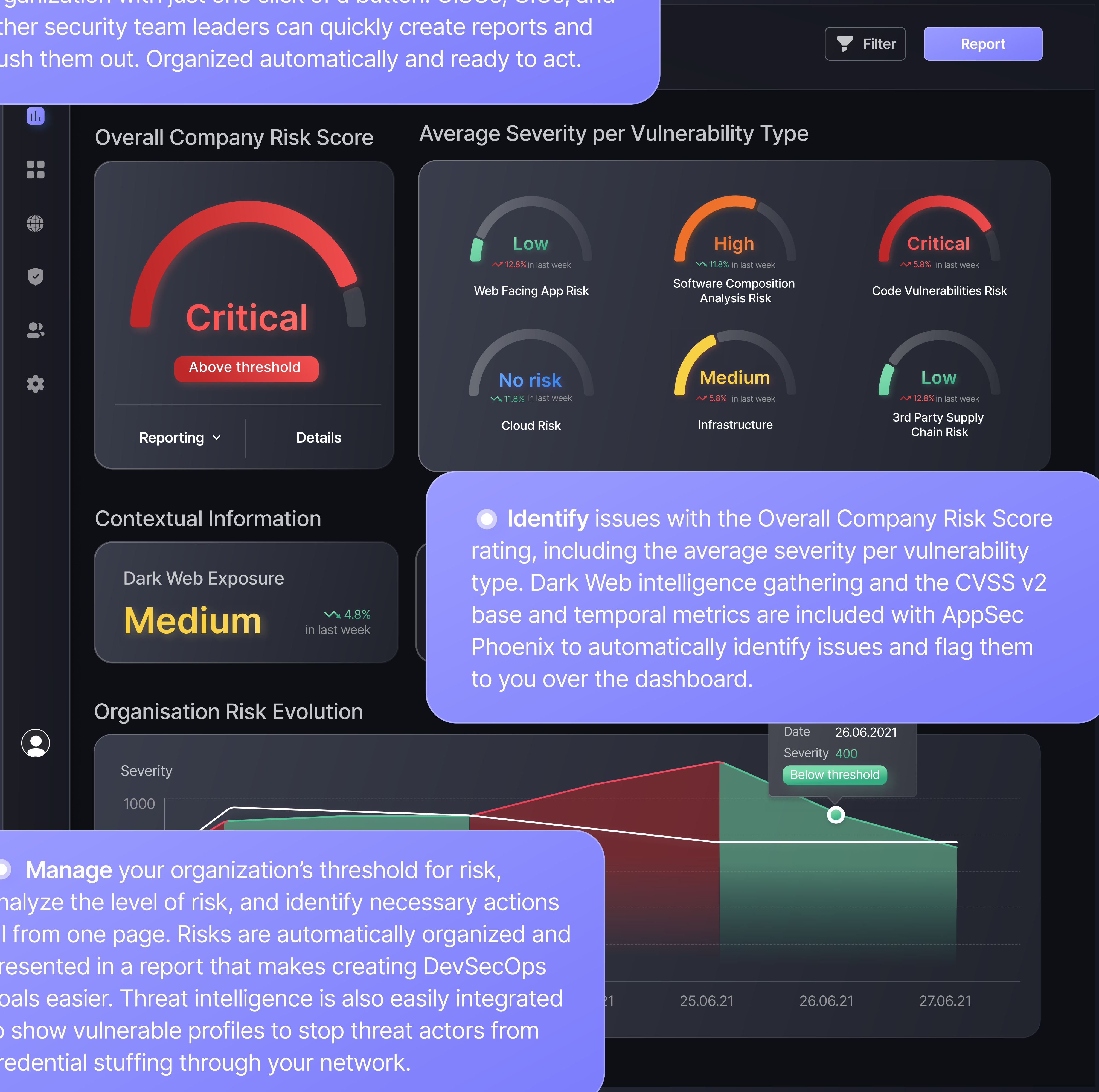
AppSec Phoenix is a unified tool that has a wide range of integrated tools to help you **identify, manage, and analyze risks and threats in your organization.**

1. Vulnerability Management

Finding vulnerabilities in software can be difficult. Not only finding threat intelligence but also implementing requires a dedicated professional, something not every organization can afford.

AppSec Phoenix provides effective vulnerability management through a three-part process.

- **Action** appropriate responses from the dashboard to send specific action plans to security professionals in your organization with just one click of a button. CISOs, CIOs, and other security team leaders can quickly create reports and push them out. Organized automatically and ready to act.



- **Identify** issues with the Overall Company Risk Score rating, including the average severity per vulnerability type. Dark Web intelligence gathering and the CVSS v2 base and temporal metrics are included with AppSec Phoenix to automatically identify issues and flag them to you over the dashboard.

- **Manage** your organization’s threshold for risk, analyze the level of risk, and identify necessary actions all from one page. Risks are automatically organized and presented in a report that makes creating DevSecOps goals easier. Threat intelligence is also easily integrated to show vulnerable profiles to stop threat actors from credential stuffing through your network.

2. AppSec Program Development

Throughout the development pipeline, security can be overlooked. A DevOps team that does not include security concerns until the pre-production phase will find time is wasted by simple security concerns that should have been addressed earlier.

AppSec Phoenix's DevSecOps tools include:

- Application Scanners
- Dependency Checkers
- SAST
- Web
- DAST
- Threat Intel

3. CloudSec Development

As more companies move their operations into the cloud, security professionals are finding it more difficult to ensure that data is stored securely. Full cloud integration is a challenge for all, especially in a fast-paced environment such as development.

AppSec Phoenix has a selection of security tools for:

- Container Security
- Data Control
- Governance
- Scanning
- Secure Cloud-Native Applications
- Visibility

With these tools, an organization can automate affect cloud security without hiring large security teams. Integrating the AppSec Phoenix suite provides you tools to integrate with some of the biggest cloud providers, including **AWS**.