SOLUTION BRIEF

Risk-Based Application Security Remediation

At Vulcan, we envision a world in which cyber security risks are fixed and eliminated rather than simply detected. We want our customers to proactively preempt attacks, and make sure that they are covered across *all* of their potential attack surfaces—infrastructure, cloud, or applications.

To make this vision a reality, the Vulcan Cyber® risk-based remediation platform has been built from the ground up to deliver a simple but powerful cyber hygiene value proposition:

Get fix done.

Vulcan Cyber risk remediation is based on four pillars:

- **PRIORITIZE**
  Using advanced security analytics, Vulcan Cyber prioritizes risks based on their severity in your unique environment, as well as your ability to fix them.

- **REMEDIATE**
  Vulcan's curated remediation intelligence matches the right remedies to prioritized risks, giving security teams ready-to-use solutions rather than to-do lists.

- **ANALYZE**
  Manage the entire risk remediation process from a unified interface, with full visibility into the fix/campaign status, quickly solving critical bottlenecks.

- **SCALE**
  Playbooks and orchestration campaigns automate and scale the fixing process, including remediation and mitigation actions, verification, and reporting.

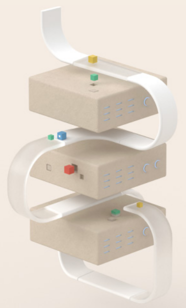
Improving your cyber hygiene programs across all exposed surfaces:

VULNERABILITY MANAGEMENT

Across all infrastructure and network endpoints, hosts, and servers.

CLOUD SECURITY

Across all public cloud providers and accounts.

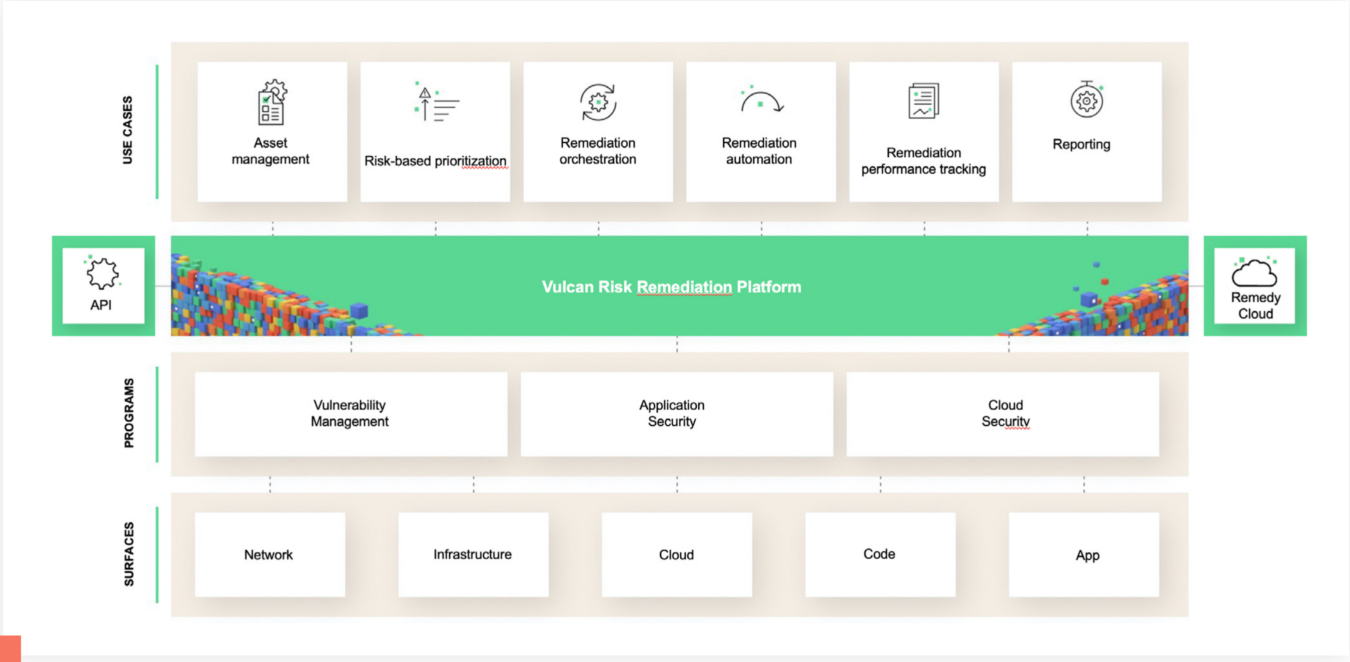


APPLICATION SECURITY

Across the entire code base and software development lifecycle (SDLC).

RISK-BASED REMEDIATION FOR APPLICATION SECURITY

This solution brief focuses on how the Vulcan Cyber risk remediation platform accelerates your AppSec program, making sure that your applications strengthen your business rather than make it vulnerable to cyber security risk.



USE CASES

Asset management

Risk-based prioritization

Remediation orchestration

Remediation automation

Remediation performance tracking

Reporting

API

Vulcan Risk Remediation Platform

Remedy Cloud

PROGRAMS

Vulnerability Management

Application Security

Cloud Security

SURFACES

Network

Infrastructure

Cloud

Code

App

Keeping Your Applications Secure

Challange

Software application and website vulnerabilities have become the most popular external attack vector. Enterprises struggle to maintain their security posture in light of the API-based architecture of modern applications and the ever-growing usage of third-party open-source scripts and dynamic containerized workloads.

However, the biggest application security challenge is that security processes are viewed as a constraint by developers, who are under pressure to continually release new features. According to the Modern Application Development Security survey, almost half (48%) of the respondents admitted their development teams regularly pushed vulnerable code into production in order to meet critical deadlines.

Figure 1 shows how the current process of securing applications and websites is complicated and long. Its many and diverse "moving parts" make it hard to collaborate, which is critical for effectively maintaining security. Siloed workflows intensify the inherent tension between the security teams, who are tasked with reducing cyber security risk in the application layer, and the development teams, who don't really understand risk and have their own business targets to meet.

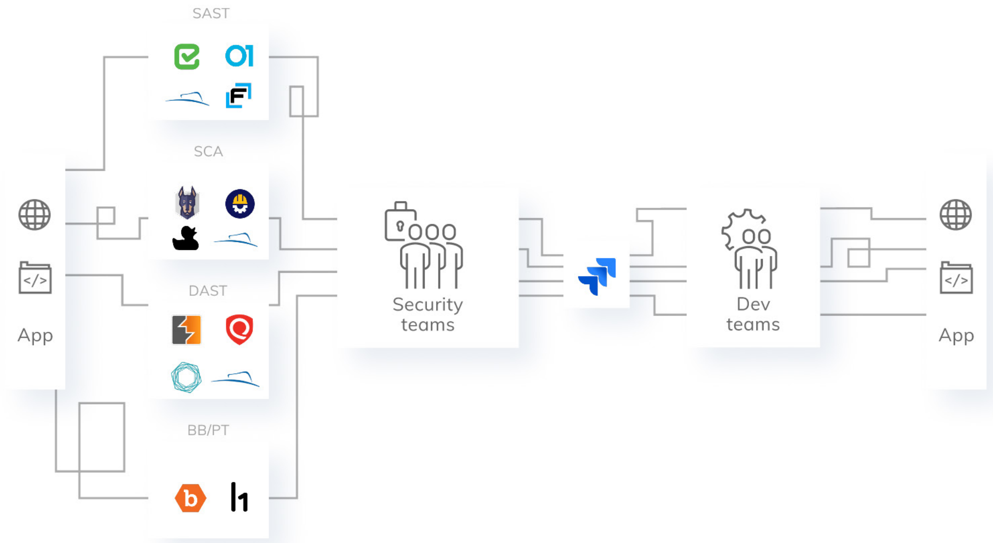


Figure 1: Disconnected security and development teams

The bottom line is that CWEs pile up and threat actors enjoy long windows of exposure for potential application exploits, since it takes companies 189 days on average — more than a half a year — to remediate a *critical* application vulnerability.

Seamlessly implementing application security policies and application security best practices throughout the SDLC is a must. We're here to fix this.

Solution

The Vulcan Cyber risk remediation platform connects to all application security testing tools in your stack to make sure that AppSec is fully integrated into your overall cyber hygiene program. As shown in Figure 2, Vulcan Cyber lets security teams own the full application security program, and not only be another step in the way. Now your process is streamlined, faster, and closes the gap between security and development.

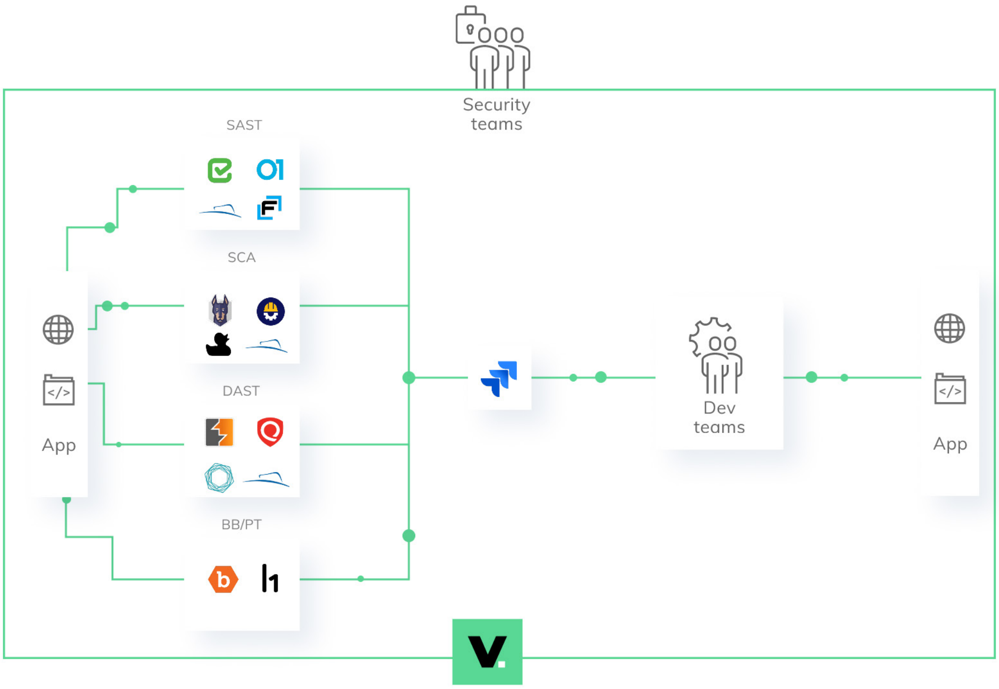


Figure 2: The Vulcan Cyber Risk Remediation Platform streamlines processes to get fix done

Use Cases

Through the Vulcan Cyber risk-based remediation platform and its intuitive user interface, you gain end-to-end control and visibility of your AppSec program. The key use cases are:

- **Cyber asset management**, with continuous auto-discovery and monitoring of code bases and other application-related assets
- **Risk-based prioritization of application-related vulnerabilities,** aligned fully with your company's unique business requirements
- **Remediation orchestration,** with seamless cross-team and cross-tool collaboration
- **Remediation automation,** for real-time fixing triggered by automated remediation playbooks
- **Remediation performance tracking,** to authoritatively validate fixes and benchmark the efficacy of your AppSec program
- **Reporting**, for insightful business and compliance documentation

Benefits

ASSESS AND CONTEXTUALIZE BUSINESS RISK

The Vulcan Cyber risk-based prioritization engine ingests and enriches data from multiple internal sources (scanners, testing tools, asset repositories, and so on) as well as from external threat intelligence feeds. The result is a risk score that reflects the severity and the fixability of the software vulnerability *for your organization*. With Vulcan Cyber, you can be confident that your CWE remediation efforts are focused on the weaknesses that present the highest business risk.

BUILD COLLABORATION

The Vulcan Cyber risk remediation platform provides your application security teams with workflows and integrations that help development teams be a seamless part of the remediation process. Now your security and development teams have a common language that lets them collaborate better and get things fixed faster.

AUTOMATE TO MAINTAIN BUSINESS CONTINUITY

Remediation must be a high priority, but it's critical that all departments be aware of the importance of not breaking applications already running in production. Vulcan Cyber allows you to put systems in place ahead of time to automate and streamline internal product patches for minimal disruption of business processes.

Integrations

Vulcan Cyber can integrate with virtually any application security tool in your stack:

WhiteHat SECURITY
Web app and code project scanner

Burp Suite
Web app and code project scanner

snyk
Open-source library and container scanner

JFrog
Container and app scanner

tenable.io
Dynamic web application and website scanner

CHECKMARX
SAST

VERACODE
SAST

FORTIFY
DAST and SAST

bugcrowd
Pen-testing and bug-bounty findings

hackerone
Pen-testing and bug-bounty findings

About Vulcan

The powerful Vulcan Cyber risk remediation platform hands teams the exact priorities, remedies, and automation they need to get fix done, in all layers of their cyber hygiene program: infrastructure, cloud, and applications. Unlike typical cyber security tools that simply give you an endless to-fix list, Vulcan prioritizes based on both severity and fixability, hands you the ideal remedy for the job, then orchestrates and automates the entire fixing process. That's why industry leaders like Snowflake, Zoom, Robinhood, and Blue Cross Blue Shield already use Vulcan to fix more risks while spending 85% less time doing so.

Get fix done.

Get fix done starting today by using Vulcan Remedy Cloud or by requesting access to Vulcan Free. If you'd like more information before diving in, we'd be happy to provide a custom demo for your team.

VULCAN.

Contact us at hello@vulcan.io
See more at www.vulcan.io