SOLUTION BRIEF

Risk-based cloud 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.

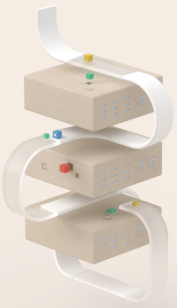
Improving your cyber hygiene programs across all exposed surfaces:

VULNERABILITY MANAGEMENT

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

CLOUD SECURITY

Across all public cloud providers and accounts.

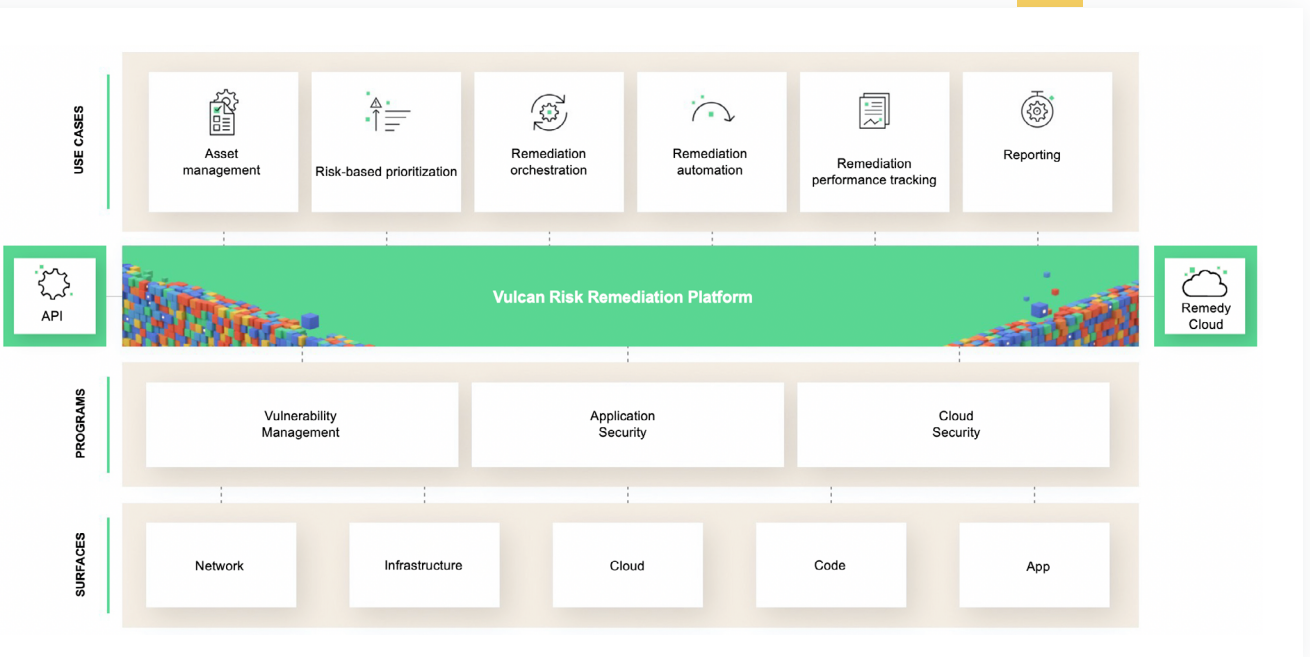


APPLICATION SECURITY

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

RISK-BASED REMEDIATION FOR CLOUD SECURITY

This solution brief focuses on how the Vulcan Cyber risk-based remediation platform accelerates your cloud security program, making sure that your cloud infrastructure strengthens your business rather than making it vulnerable to the overall cyber security risk.



Keeping your cloud secure

Challange

Your cloud environment is getting more complex all the time. Your data storage is growing exponentially, including your most sensitive data assets. Your apps are going cloud-native, riding the wave of containers, microservices, and open source. And more likely than not, you are using multiple-cloud and hybrid architectures.

So many configurations to manage. So many users to track. And as we see in Figure 1, keeping your cloud security, DevOps and developement teams in sync often feels like mission impossible. And you are more vulnerable than ever.

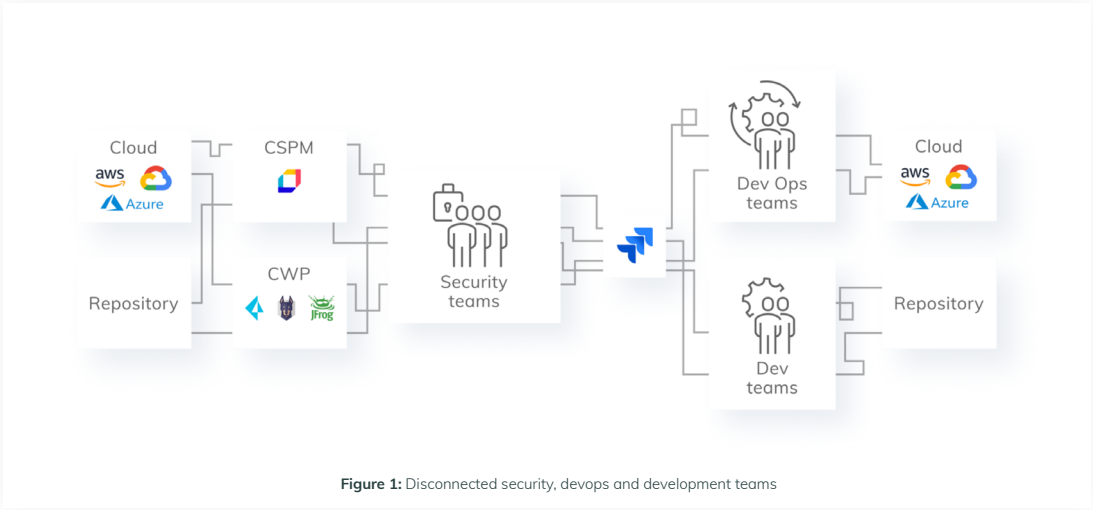


Figure 1: Disconnected security, devops and development teams

Solution

The Vulcan Cyber risk-based remediation platform streamlines cloud security programs, giving your cloud security and DevOps teams everything they need to get fix done. Tight integrations with Kubernetes, all the major cloud service providers, and other leading cloud security tools mean that everyone can see your risk in one place and manage it together. As shown in Figure 2, Vulcan Cyber lets security teams own the full cloud security program, and not just be another step along the way. Now your process is streamlined, faster, and closes the gap between security and development.

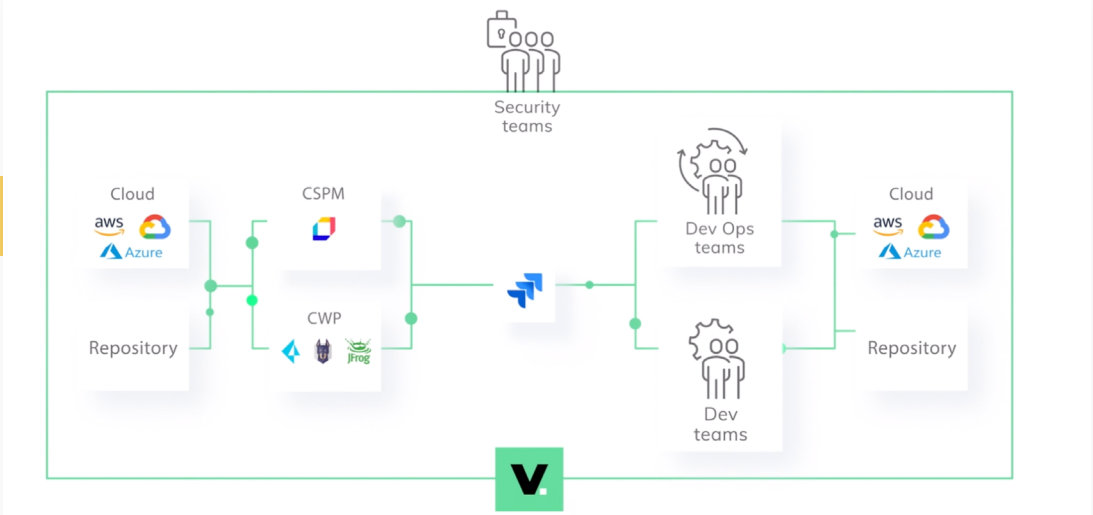


Figure 2: The Vulcan Cyber risk-based remediation platform streamlines processes to get fix done

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 cloud security program. The key use cases are:

- **Cyber asset management**, with continuous auto-discovery and centralized risk management for gaining control over all your cloud assets, including containers and services.
- **Risk-based prioritization of infrastructure-related vulnerabilities,** fully integrated with your multi-cloud security stack for full-context prioritization aligned with your company's unique business requirements.
- **Remediation orchestration,** with seamless cross-team and cross-tool collaboration to mitigate cloud vulnerabilities and misconfigurations. The right team handles the right vulnerabilities, at the right time, using the right tools.
- **Remediation automation,** for real-time fixing at scale triggered by automated remediation playbooks. Become a fixing machine.
- **Remediation performance tracking,** to authoritatively validate fixes and benchmark the efficacy of your cloud security program.
- **Reporting and BI dashboards,** for data-driven cloud risk mitigation programs powered by advanced analytics. Scan-to-fix visibility.

Benefits

ASSESS AND CONTEXTUALIZE BUSINESS RISK

The Vulcan Cyber risk-based prioritization engine ingests and enriches data from multiple sources, including cloud asset and configuration data. With Vulcan Cyber, IT security teams can track, consolidate, and prioritize all cyber vulnerabilities across all digital surfaces—infrastructures, networks, clouds, and applications. Your cloud security team gets a risk score that truly reflects the severity and the fixability of the cloud security vulnerability *for your organization.* You can be confident that your remediation efforts are focused on the cloud security weaknesses that present the highest business risk.

BUILD COLLABORATION

Our recent survey of cybersecurity leaders reveals that there are numerous stakeholders involved in cyber hygiene programs—from cybersecurity and IT executives to IT operations, developers, and DevOps practitioners. The Vulcan Cyber risk-based remediation platform provides your cloud security teams with workflows and integrations that help development teams and other stakeholders 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, AUTOMATE, AUTOMATE

Yet another revelation from our cybersecurity survey is that almost half still use manual processes to identify remediation and mitigation actions for detected vulnerabilities. Aside from manual processes being time-consuming and tedious, they are also highly prone to human error. Vulcan Cyber automates almost every step of the vulnerability remediation program, from highly contextual risk prioritization to recommended actions and preconfigured workflows that let you get fix done with minimal disruption to your business processes.

Integrations

Vulcan Cyber can integrate with virtually any cloud security tool in your stack. The following integrations are available off-the-shelf:

Ingest host data from AWS security tools such as AWS EC2, Docker container data from AWS ECR, or container data from AWS ECS to enrich asset risk posture and better prioritize vulnerabilities

Ingest aggregated data about security alerts and your security posture across all your AWS accounts

Ingest data from Azure security tools

Ingest data from GCP security tools

Ingest data from the Aqua Security CSPM

About Vulcan

The powerful Vulcan Cyber risk-based 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