Enterprise Strategy Group
by TechTarget

Optimizing Application Security Effectiveness to Scale With Rapid Development

As businesses modernize their development processes to increase productivity, security teams need an effective way to scale. TechTarget's Enterprise Strategy Group looked at best practices that drive the efficiency needed to rapidly remediate application security vulnerabilities in order to mitigate risk and prevent incidents.

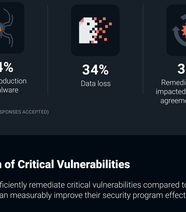
This Enterprise Strategy Group infographic was commissioned by Mend and is distributed under license from TechTarget, Inc.

The Need for Effective Remediation of Critical Vulnerabilities

Only **52% of companies say they can effectively remediate a critical vulnerability**, and even fewer application security practitioners (44%) agree. (N=350)

Similarly, just **41% are very confident in their ability to manage the security and compliance risks** associated with open source software components used within internally developed applications. (N=350)

The result: Organizations face serious consequences from security incidents.



Top 5 Impacts From Security Incidents

46% Application downtime

38% Unauthorized access to applications and data

34% The introduction of malware

34% Data loss

32% Remediation steps impacted service level agreements (SLAs)

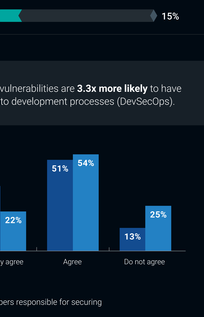
(N=228, MULTIPLE RESPONSES ACCEPTED)

Best Practices Enabling Efficient Remediation of Critical Vulnerabilities

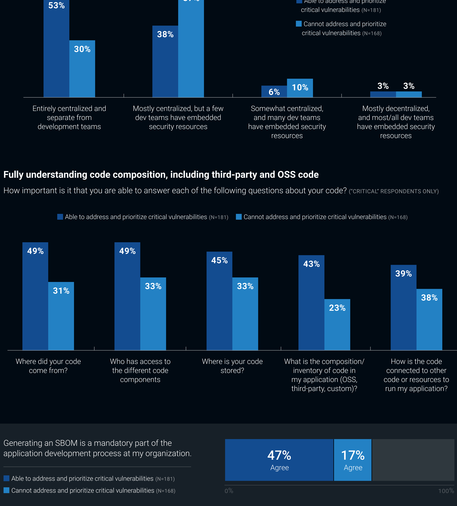
We identified key patterns among the organizations that could efficiently remediate critical vulnerabilities compared to those that could not. By following these best practices, organizations can measurably improve their security program effectiveness.

Aligning goals, along with collaboration

To build a culture of security, we encourage collaboration between application development, security, and operations.



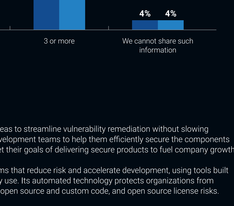
Reasons for incorporating security processes into DevOps processes and developer workflows



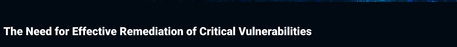
3.3x Organizations able to keep up with vulnerabilities are **3.3x more likely** to have extensively incorporated security into development processes (DevSecOps).

Shifting security responsibilities left to developers while security plays a centralized role

Our application development team is taking on more security responsibilities with support and help from the security team.



What organizational structure best describes how security team members responsible for securing internally developed applications are distributed in your organization?



Fully understanding code composition, including third-party and OSS code

How important is it that you are able to answer each of the following questions about your code? (CRITICAL* RESPONDENTS ONLY)

Generating an SBOM is a mandatory part of the application development process at my organization.

Measuring Program Effectiveness: Preventing Incidents

Organizations that report the ability to efficiently remediate vulnerabilities were nearly twice as likely to say they have not experienced any serious security incidents tied to a software vulnerability/web application exploit in internally developed applications over the last 12 months.

Conclusion

Organizations should leverage solutions that address these areas to streamline vulnerability remediation without slowing development down. When security teams can partner with development teams to help them efficiently secure the components of their software, both teams can work more efficiently to meet their goals of delivering secure products to fuel company growth.

Mend.io helps organizations build world-class AppSec programs that reduce risk and accelerate development, using tools built into the technologies that software and security teams already use. Its automated technology protects organizations from supply chain and malicious package attacks, vulnerabilities in open source and custom code, and open source license risks.

LEARN MORE