Maturity of software supply chain security practices 2024

Security is essential for modern software supply chains

Software supply chain security helps to ensure integrity, confidentiality, and availability throughout software development life cycles. Through advanced practices, processes, and technologies, IT operations and development teams can prevent, detect, and respond to threats, vulnerabilities, and malicious activities. By systematically and proactively managing security throughout the entire software supply chain, organizations can improve resilience, manage costs, and increase customer satisfaction.

Commissioned by Red Hat and authored by SlashData, the Maturity of software supply chain security practices 2024 report[1] assesses software supply chain security practices used by organizations worldwide.

Evaluate your software supply chain security

Protecting software supply chains can be significantly challenging due to their inherent complexity and global reach. Addressing these challenges requires a holistic approach that combines technological solutions, regulatory compliance, and stakeholder collaboration.

Here are 5 indicators that can help you understand the security of your software supply chain.

Assurance

Software efficacy measures how consistently an application performs over time. Practices that increase software efficacy provide users with assurances of predictable, stable operations with minimal disruptions. For example, dependency management tools, open source software governance policies, and centralized risk management systems can help you predictably deliver effective applications and services.

Key insight: While 51% of development teams ensure the trustworthiness of open source packages through either vulnerability and dependency management tools or responsible disclosure policies, only 11% of organizations currently have some form of open source software governance policy.

Transparency

Transparent processes, clear guidelines, and standardized approaches for software development increase the integrity of applications and services. Software with high integrity performs without failures or errors. Consistent security scanning, software artifact authenticity validation, strong integrated development environment (IDE) and plug-in policy enforcement, and automated communication methods can increase software integrity and lead to improved customer satisfaction.

[1] Dodd, Liam and Korakitis, Konstantinos. "Maturity of Software Supply Chain Security Practices 2024." 18 April 2024.

Key insight: 54% of developers actively implement vulnerability discovery practices in their own code, but only 20% apply standardized security practices each time a pull request is made.

Compliance

Applying security practices and controls—in compliance with industry standards—to build systems can prevent vulnerabilities, ensure authenticity, and speed delivery of critical features. Additionally, using automation to deliver more frequent, security-focused builds reduces software rollbacks that delay delivery schedules and lead to dissatisfied customers. Detailed provenance, signed attestations, standardized base images, and automated image assessments can help you increase software delivery quality and frequency while remaining in compliance with regulatory requirements.

Key insight: While 52% of developers apply mature software delivery performance practices in the build stage, 57% do not use build information to verify if pipeline compliance has been met.

Consistency

Automated build and deployment processes help deliver more consistent software while reducing the potential for errors and vulnerabilities. Continuous integration/continuous deployment (CI/CD) pipelines with automated, embedded security checks increase workflow efficiency, allowing you to deliver applications and services with minimal disruptions. And CI/CD pipeline features like security scans, digital signatures, and infrastructure as code (IaC) capabilities—along with dedicated workflow ownership—can mitigate security risks in your automated software delivery processes.

Key insight: 67% of development teams include multiple security practices in their CI/CD pipelines, helping to eliminate repetitive tasks and configuration drift. And 83% engage in pipeline security risk mitigation to support continuous deployment to an auditable, immutable state.

Resilience

Rapidly identifying and remediating threats and vulnerabilities at runtime is critical to delivering resilient, robust services across environments. Processes that let you promptly prioritize and respond to security issues according to severity—and without alert storms that can disrupt operations—limit users' exposure to potential threats. For example, real-time protection mechanisms, comprehensive container management solutions, policy enforcement points, and continuous analysis of stored images help you increase resiliency and avoid critical IT incidents.

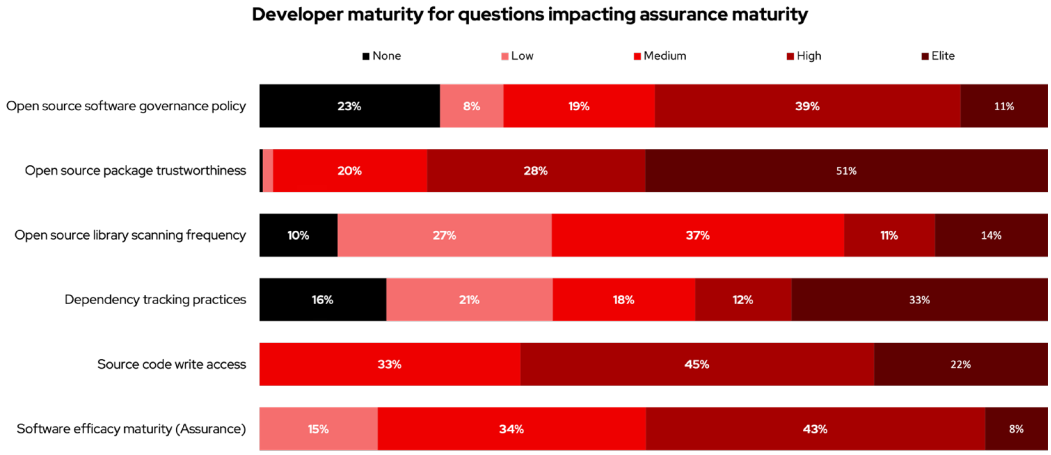
Key insight: While 53% of developers track container images according to mature security practices, only 15% scan their container images with high frequency.

Overall software supply chain security maturity

Survey responses from 5 areas of software supply chain security—along with an overall combined score—reflect the maturity of security processes for development organizations of all sizes and geographies.

Here are a few key insights from these survey results.

- Developers at organizations in the elite maturity group engage in more mature security practices across all 5 areas, while those in the high maturity group score lower in only 1 area.
- Organizations with more mature security practices have greater awareness of potential vulnerabilities and the associated risks for their customers.



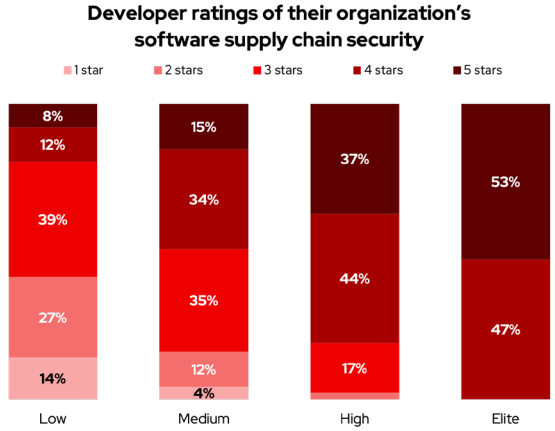
- For many development organizations, investing in practices that help rapidly detect and remediate vulnerabilities can greatly improve their software supply chain security.

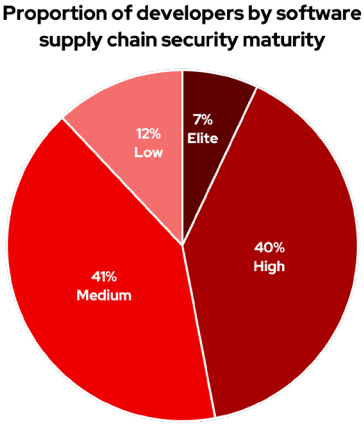
Developer assessment of organization security

As individuals, developers often engage in more software supply chain security practices than required by their organizations. Developer assessments of their organization's software supply chain security can highlight gaps between an organization's perceived and actual security practices.

Here are a few takeaways from this assessment.

- While developers at organizations in the elite maturity group are aware that their organization engages in security-focused practices, they also focus on continuous improvement of their software supply chain security.
- Organizations with less mature practices are unaware of their exposure to vulnerabilities, while also overlooking potential security improvements.





Question asked: On a scale of 1 to 5 stars, where 5 stars is exemplary and 1 star is poor, how would you rate your organization's software supply chain (SSC) security?
% of developers in each SSC security maturity group | % of developers (n=791)

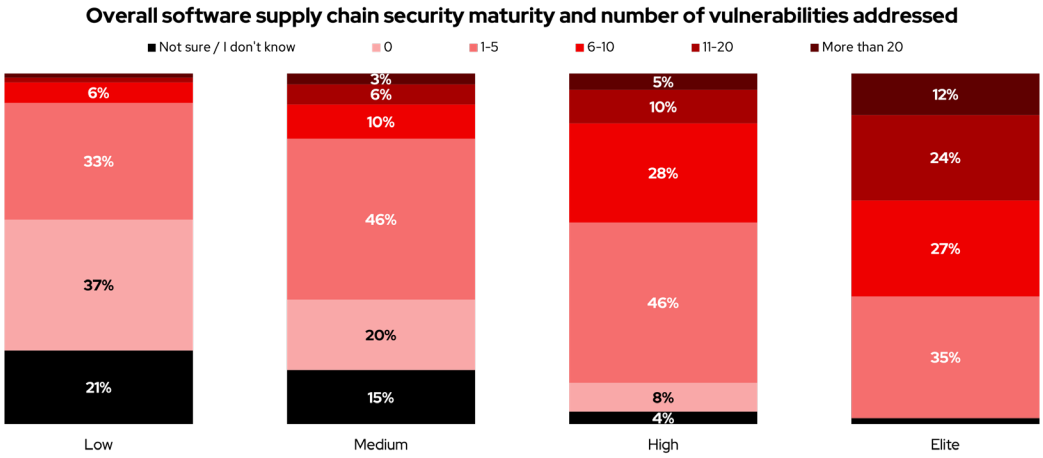
- Developers participate in more mature security practices for activities under their control, while engaging in less mature practices at the organizational level.

Resolution of security vulnerabilities

Mature security practices help organizations rapidly identify and remediate existing vulnerabilities while minimizing the introduction of new threats into the software supply chain. An analysis of the vulnerabilities addressed by an organization can indicate the maturity of their security practices.

Here are a few key points from this analysis.

- Organizations that engage in more mature security practices resolve more vulnerabilities while giving their developers a greater awareness of security-related incidents.
- Mature practices are key to building more secure software, as developers who engage in more security practices are more proficient at identifying and addressing issues.



Question asked: In the last 12 months, how many security vulnerabilities or threats required your team's immediate attention due to their impact or severity?
% of developers in each SSC security maturity group (n=751)

- Many organizations with less mature security practices are unaware of vulnerabilities in their software supply chain and underestimate their risk exposure.

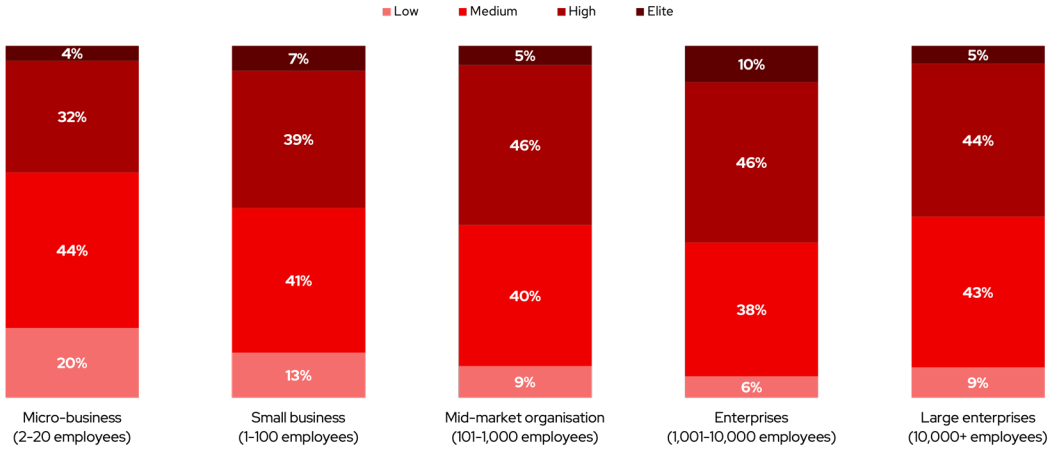
Impact of organization size on software supply chain security

Many factors—including corporate culture, technology resources, and regulatory concerns—affect how organizations operate. The relationship between organization size in number of employees and mature security practices illustrates the influence of these factors on software supply chain security.

Here are several key insights from these results.

- Larger organizations with more staff, greater financial resources, and dedicated security teams generally have more mature software supply chain security practices.
- The largest enterprises engage in slightly less mature security practices, possibly due to inefficient corporate policies that slow adoption of new technologies and processes.

Overall software supply chain security maturity for different organization sizes



Question asked: What is the size of the organization that you work for?
% of developers at each organization size (n=658)

- Although small organizations have fewer resources, they can rapidly implement new practices that continuously improve their software supply chain security.

Learn more

Read the Maturity of software supply chain security practices 2024 report to see the complete survey results and learn how you can improve your software supply chain security. Then, discover how Red Hat® Trusted Software Supply Chain can help you implement security-focused components, processes, and practices in your software factory to prevent vulnerabilities during development and anticipate security issues at runtime. Learn more at red.ht/trusted.

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

redhat.com
1100820_0424_KVM