activestate

The 2026 State of Vulnerability Management & Remediation Report:

CONTAINER SECURITY EDITION

activestate

Contents

activestate

Executive Summary

In this second edition of the State of Vulnerability Management and Remediation report, we deep dive into the world of container security. Two-hundred and fifty (250) DevSecOps leaders in North America shared their perspectives on how they're using containers to build their applications, the risks they perceive - and experience - when containers contain vulnerabilities, and what they're excited about for the future.

In short, containers are proliferating across software development teams, but still represent a significant attack vector and companies don't always have the processes, tools, and best practices in place to quickly and efficiently remediate CVEs. There's hope that AI will improve remediation turnaround times and results, and that adopting compliance and policy enforced containers will help reduce future risk.

How Modern Build Practices Increased Exposure

According to Linux Foundation, 91% organizations use containers in production[1] and open source can be found in 49% of containers,[2] yet IDC reports that only 33% of organizations have adopted some form of managed or trusted open source[3].

The use of containers has become the standard for production environments, yet security practices haven't kept pace. While nearly all organizations rely on containers, the prevalence of unmanaged open source software within them creates a massive, unprotected attack surface.

Two Thirds of Organizations Are Running Blind

91% Adoption
Organizations using containers in production

49% Integration
Open Source Software (OSS)

33% Governance
Organizations using managed or trusted open source

[1] CNCF Cloud Native 2024 Report (Linux Foundation)

[2] Linux Foundation

[3] The Secure Base Race: Why Hardened Images Are Gaining Ground Fast. May 19, 2025. By Katie Norton, IDC.

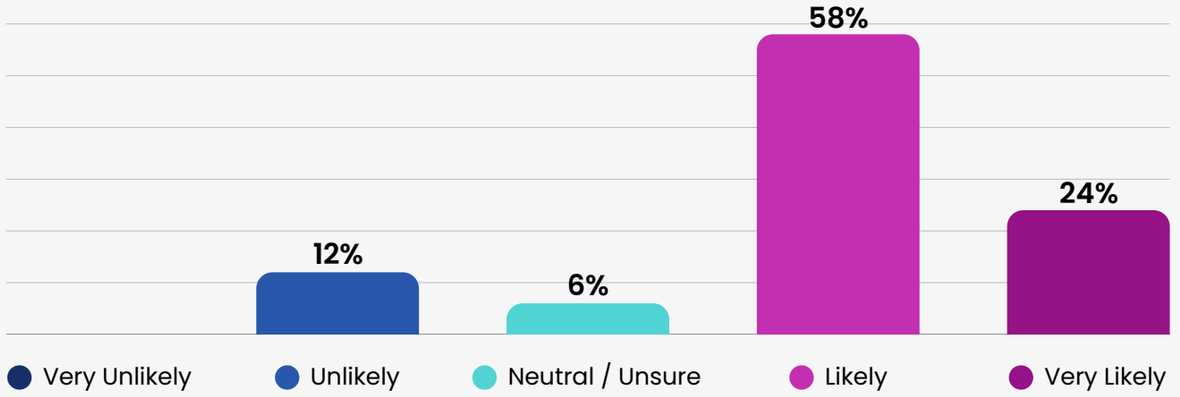
According to survey respondents, while all (100%) organizations report containerization as critical to their production strategy, 82% admit they've likely suffered at least one container-related security breach in the past 12 months. This is similar to what RedHat reported in their 2024 State of Kubernetes Security Report, where nearly 9 in 10 (90%) of organizations experienced at least one container or Kubernetes security incident in prior year.

Why This Matters:

Universal adoption without universal security controls turns containers into systemic risk multipliers.

How important is containerization to your organization's production strategy today?

How likely is your organization to have suffered at least one container-related security breach in the past 12 months?



Production Has Shifted to Containers and So Has Risk

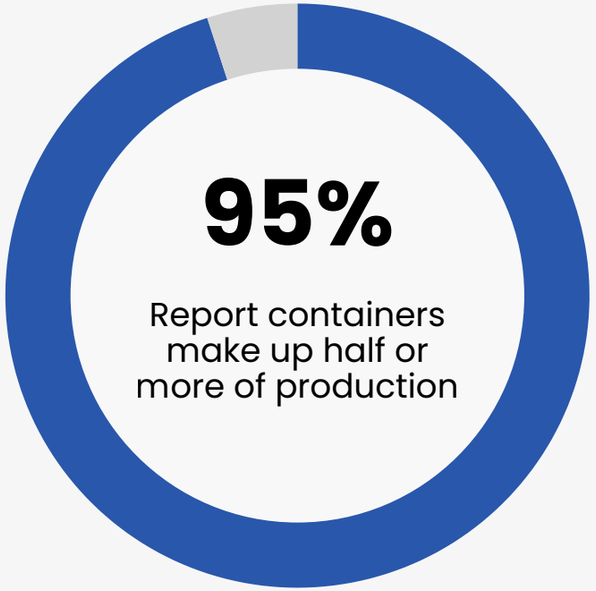
More Containers, More Problems

While 95% of DevSecOps leaders in our survey say container workloads account for half or more of their production footprint, 87% say they are likely to experience a container-specific security incident in a given year.

Key Insight

Container adoption has outpaced the maturity of enterprise security programs, making incidents an expected — not exceptional — occurrence. According to IBM's 2025 Cost of a Data Breach report, the global average breach costs $4.44 million; that number can more than double for a highly regulated industry like healthcare.

Container Adoption is Outpacing Security Programs



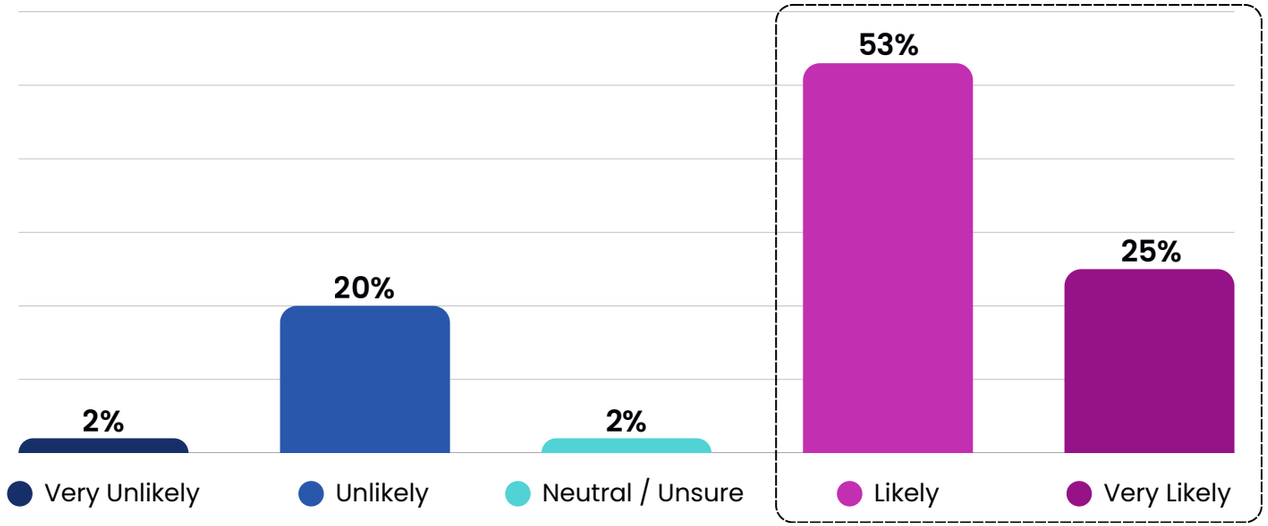
Audit Failures Reveal the Remediation Gap

Why This Matters

Persistent CVEs can translate directly into regulatory and reputational risk.

Regulatory authorities issued over **2,200 fines** for non-compliance in early 2025 alone, many linked to insufficient vulnerability management practices relating to open source and third-party components. Sysdig's 2024 Cloud-Native Security and Usage **Report** noted that 91% of runtime scans fail vulnerability policies, indicating that current scanning tools are catching issues far too late in the lifecycle.

78% of organizations have likely failed a compliance audit due to CVEs in container images.



2,200 + fines

for non-compliance in early 2025

91%

Runtime scans fail vulnerability policies

Visibility Isn't Optional, It's Foundational

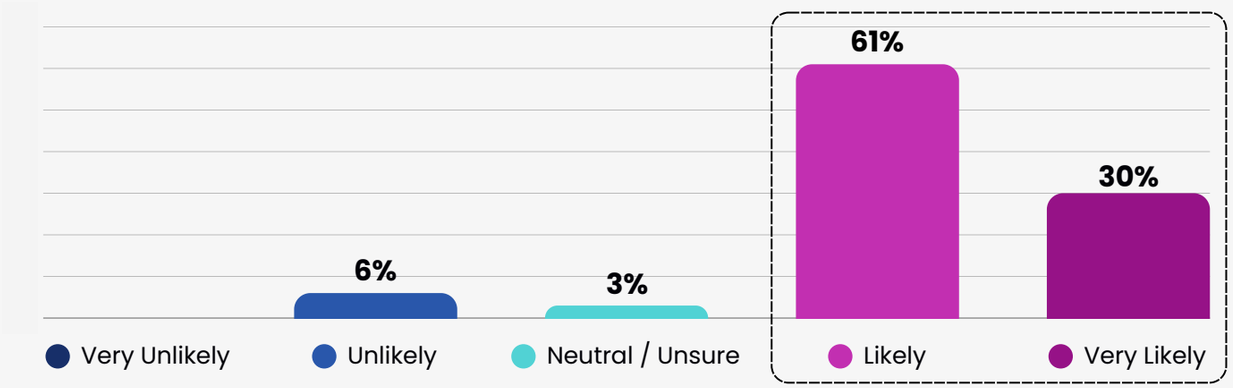
Short-lived containers, long-term consequences

91% of DevSecOps leaders report limited visibility into container components as their biggest security blind spot. 83% of DevSecOps leaders identified outdated base images as the root cause of their most recent vulnerabilities.

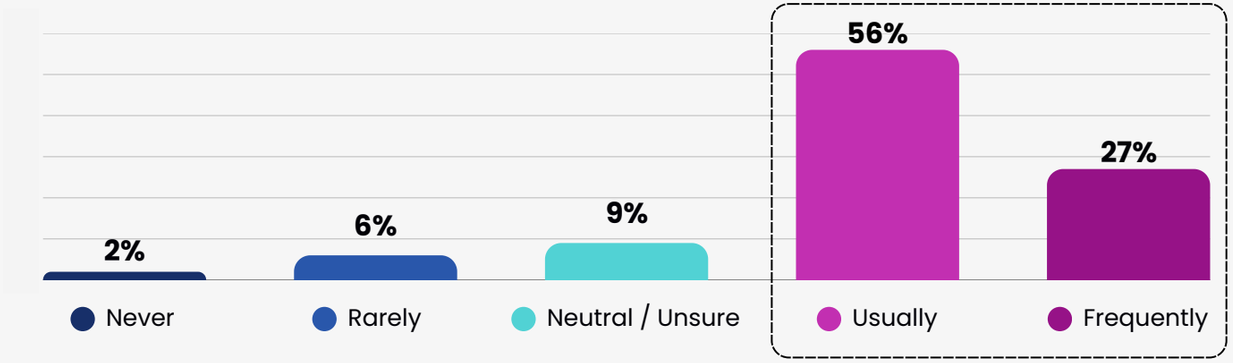
91% Visibility gaps

83% Outdated base images

How likely is limited visibility into container components to be your team's biggest security blind spot?



How often do outdated base images contribute to your most recent vulnerabilities?



Why This Matters:

Limited observability across containers creates unmonitored attack surfaces that complicates detection and compliance verification.

Sysdig **reported** that 70% of containers live for 5 minutes or less — humans cannot secure assets that vanish in 300 seconds. Furthermore, use of outdated components may violate both regulatory and internal compliance standards, particularly if exposed vulnerabilities remain unaddressed or contradict supply chain security policies.

Risk Drivers

70%

Containers live under 5 minutes

Ephemeral workloads are impossible to secure manually

Unmonitored layers create hidden attack surfaces

Outdated layers introduce compliance risk

Security Loses When Convenience Wins

Shortcuts ship risk

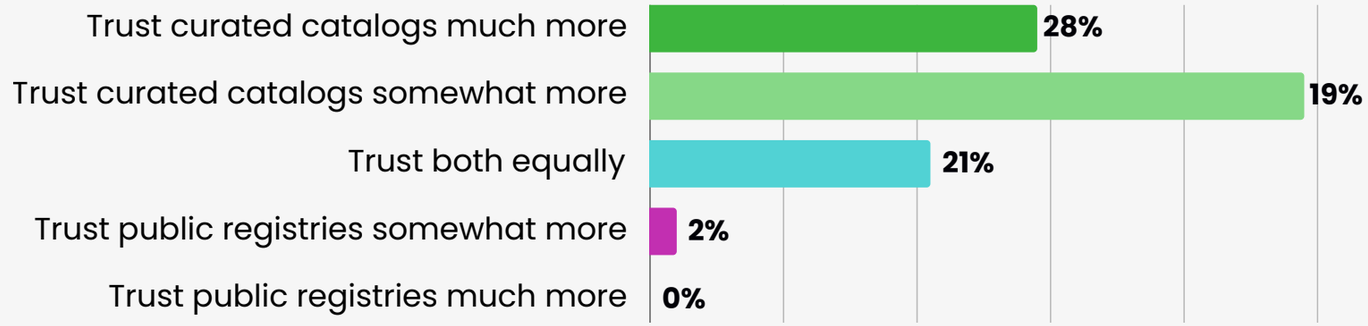
Although 77% of DevSecOps leaders trust curated catalogs more than public registries, 90% still use lightly modified public images with little to no hardening.

Root Causes:

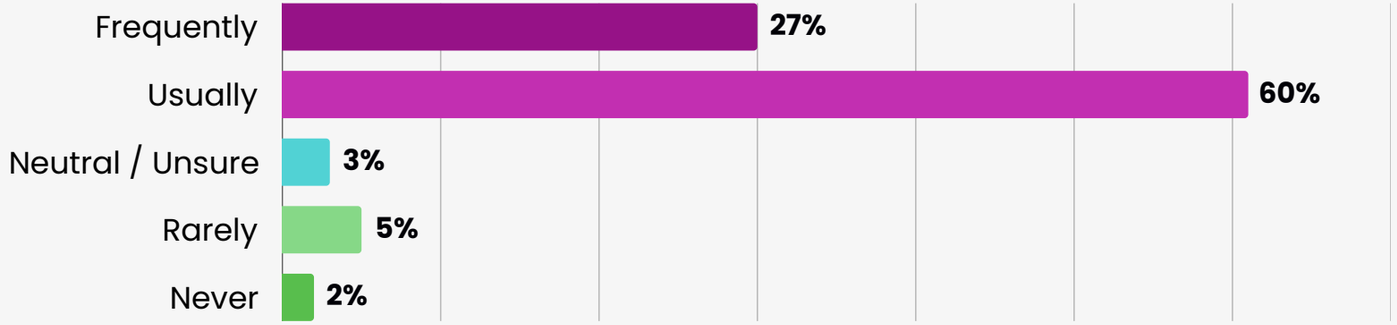
77% Trust curated catalogs

90% Still use lightly modified public images

How much do you trust curated catalogs compared to public registries for open source?



How frequently do your teams use lightly modified public container images with little or no hardening?



Why This Matters:

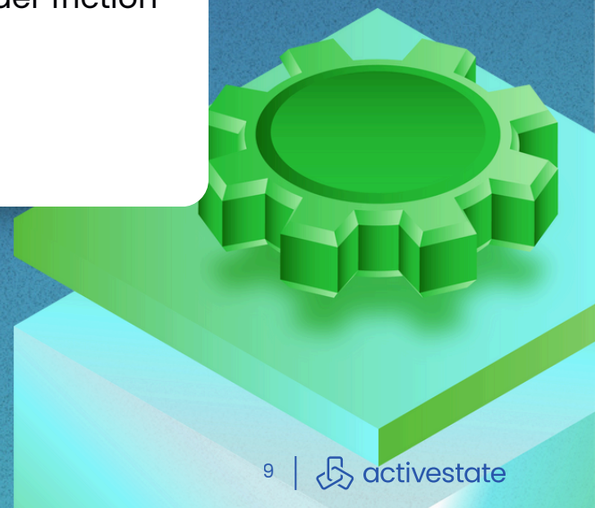
Convenience still trumps control, exposing production workloads to preventable risks. Unfortunately, curation typically doesn't scale: Platform Engineering teams attempt to manually curate approved package lists that include "*golden images*," "*blessed libraries*," "*approved dependencies*," but within months, these catalogs become bottlenecks and frustrated developers bypass platform controls entirely, pulling packages directly from public registries.

Key Drivers

Convenience outweighs control

Manual curation doesn't scale

Developers bypass controls under friction



Top Security Strategies Aren't Delivering Results

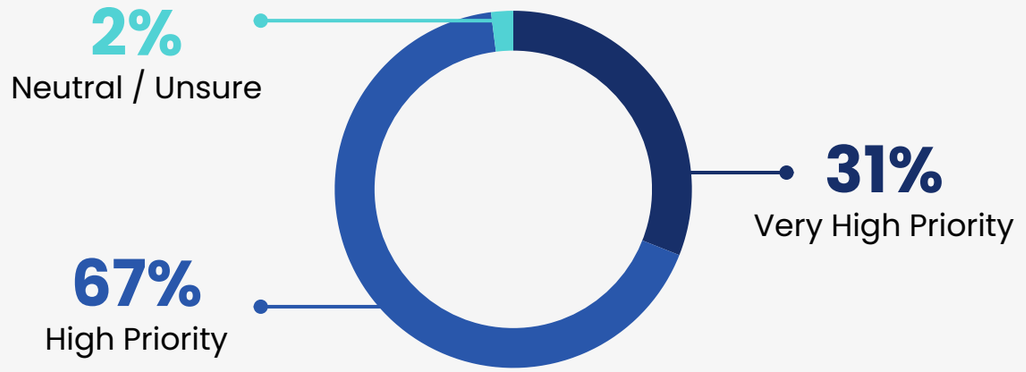
Harden everything, remove what's unnecessary.

98% of DevSecOps leaders rank hardened container solutions as a high strategic priority, yet 78% have likely failed audits due to container CVEs.

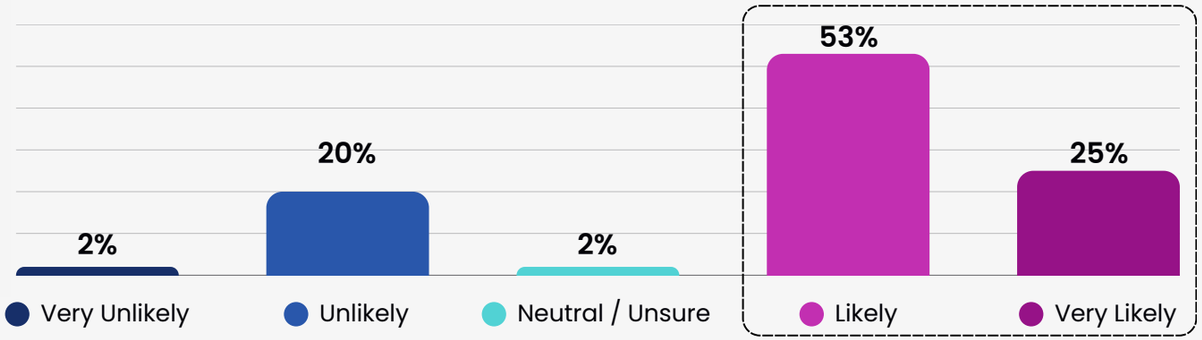
Key Insight

Investment momentum is strong — but execution gaps persist across remediation and governance.

How high a priority is investing in hardened container solutions for your organization's strategy?



How likely is it that your organization has failed a compliance audit due to CVEs in container images?



AI is Redefining How Teams Fix Vulnerabilities

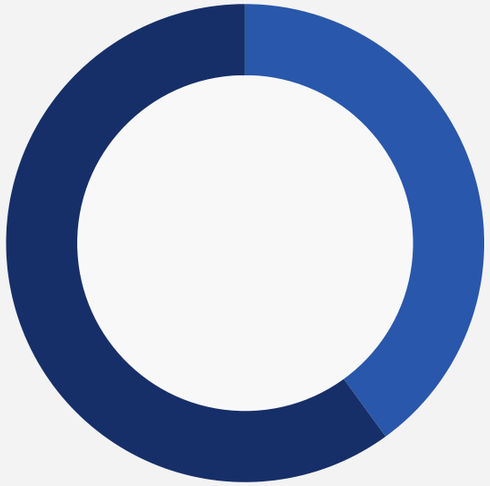
AI Takes the Wheel

100% of DevSecOps leaders are likely to use AI or automation to prioritize vulnerabilities, and 95% expect intelligent remediation to become standard by 2026.

The Future of Automated Remediation looks Br“AI”ght!

The main benefits of AI remediation are rapid and targeted vulnerability response, operational consistency, improved accuracy, and significant reductions in labor and business risk—providing a strong foundation for modern, scalable container security.

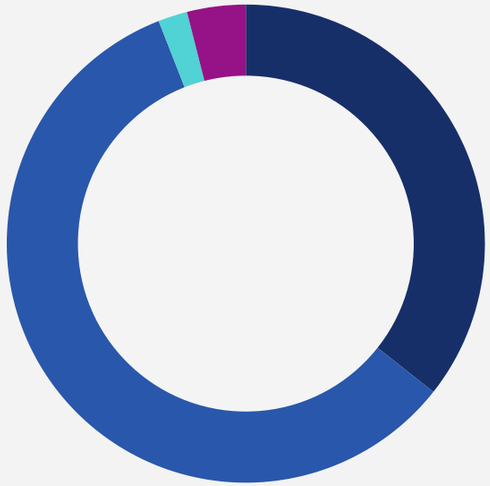
How likely are you to use AI or automated logic to prioritize vulnerabilities for remediation?



60%
Likely

40%
Very Likely

How likely do you believe intelligent remediation automation will become a standard practice by 2026?



3%
Very Unlikely

2%
Neutral / Unsure

59%
Likely

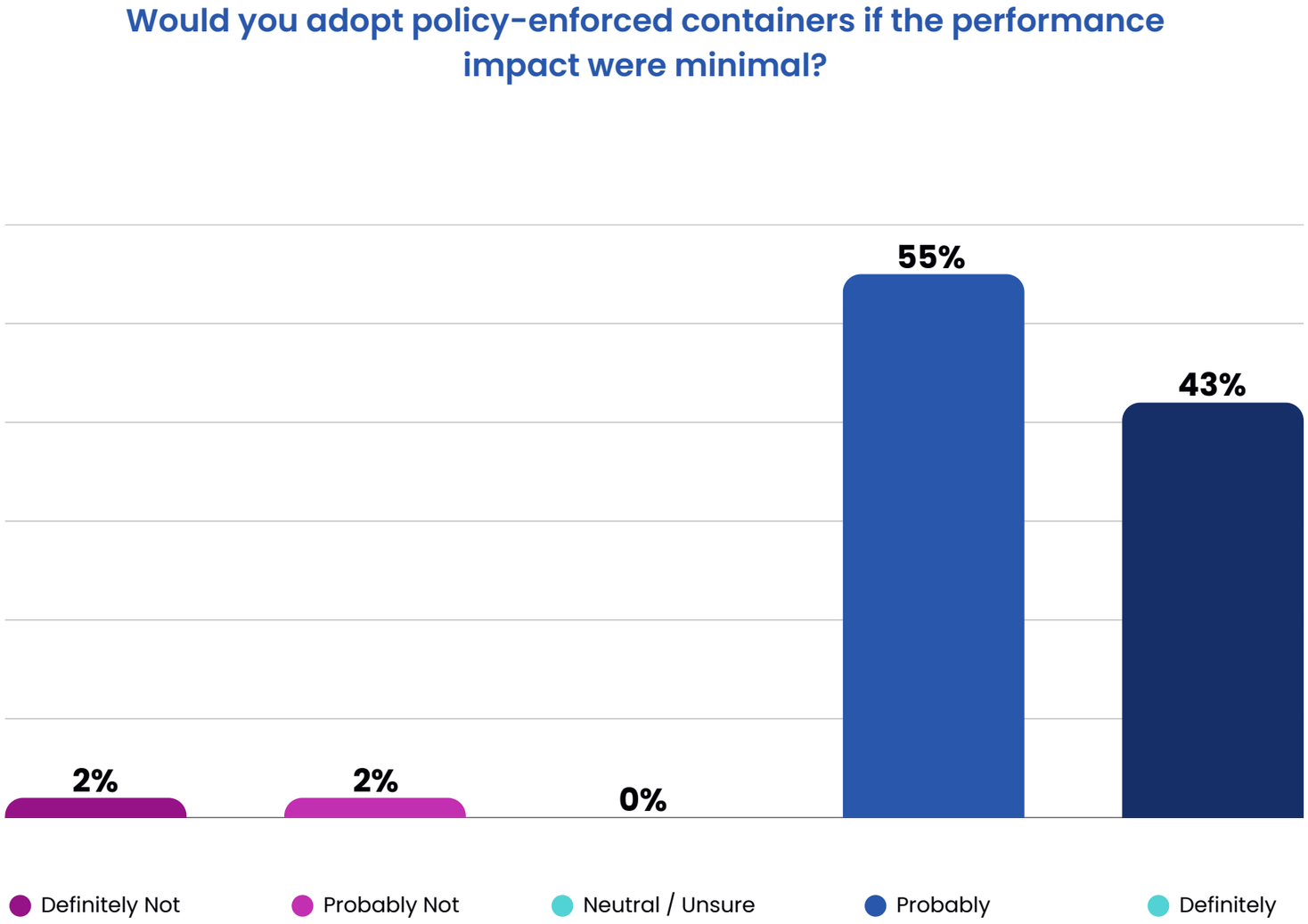
36%
Very Likely

Policy Enforcement Becomes the New Standard

97% of DevSecOps leaders would adopt policy-enforced containers if performance impacts were minimal.

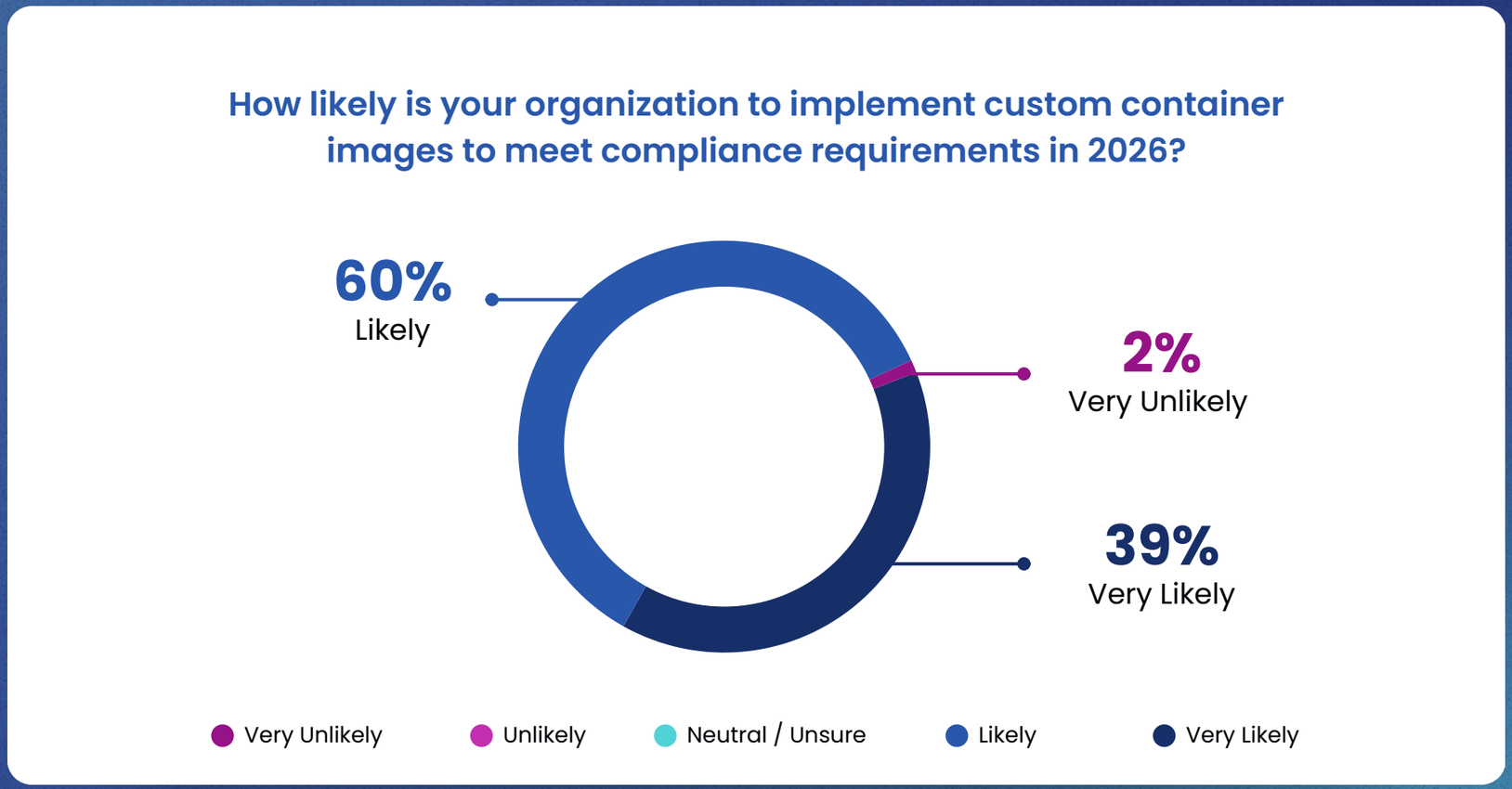
Why This Matters:

Runtime enforcement is poised to become a new baseline for secure containerization.



Custom containers are becoming the smarter path to compliance

98% of organizations plan to implement custom container images to meet compliance requirements in 2026.



To Do:

Standardize base image creation and approval workflows to meet compliance mandates efficiently. Work with providers like ActiveState, who focus exclusively on delivering secure open source into the software development lifecycle, and take on the full workload of providing, maintaining, and remediating open source libraries and containers. Your teams get the secure containers they need, without the overhead and headaches that typically accompany them.

activestate

Conclusion

The 2026 State of Vulnerability Management & Remediation Report reveals a critical paradox: while containerization is now essential to production strategies for 100% of organizations, security maturity lags dangerously behind, resulting in an 82% breach rate and widespread audit failures. The data confirms that manual curation and "golden images" are failing to scale, creating a clear mandate for leaders to shift toward curated catalogs, AI-driven automation, and policy-enforced runtimes to close these gaps. To secure the future supply chain without stalling innovation, organizations must immediately prioritize standardizing base image workflows and partner with dedicated providers like ActiveState to offload the burden of remediation and maintenance.

Make 2026 the year you focus on securing all the open source in your organization - from containers to packages to dependencies. An ActiveState Open Source Security Expert can show you how.

Contact Us Today

About ActiveState

ActiveState enables DevSecOps teams to improve their security posture while simultaneously increasing productivity & innovation to deliver secure applications faster.

The company provides a curated catalog of secure open source components and container images that can be consumed via artifact repository, CI/CD, IDE, or directly from ActiveState. For more than 25 years, ActiveState has been providing companies in regulated industries secure open source, beginning with Python, Perl, Ruby, and tcl, and now delivers more than 40+ million components across those languages as well as Go, Node, Java, Rust, R, and more. ActiveState continuously monitors and updates the open source components to help keep companies vulnerability-free.

Companies using ActiveState see a 60-99% reduction in CVEs, improving their security posture, and save as much as 30% of developer time, eliminating the engineering toil typically associated with using open source in commercial applications.

Learn to Secure Containers | *Free* Certification

Master practical container security: choosing base images, scanning for vulnerabilities, and securing production.

View Course