activestate

ASPM:
The Invisible Shield for your Open Source Ecosystem

activestate

Table of Contents

Introduction **3**

What is Application Security Posture Management (ASPM)? **5**

Why is ASPM important? **6**

U.S. Custom Software Development Market 6

ASPM vs. SAST 7

ASPM vs. DAST 7

ASPM vs. SCA 7

ASPM vs. AST 7

ASPM vs. ASOC 8

ASPM vs. CSPM 8

ASPM vs. Building It Yourself 8

ASPM: The Future of Secure Software Delivery **9**

ASPM and ActiveState:
Securing your Open Source at Scale **11**

Beyond the Hype:
6 Practical Uses for ASPM in Your Open Source Journey **12**

Discoverability and Observability:
Gaining Visibility into Your Open Source Landscape 12

Continuous Open Source Integration 12

Secure Environment Management 13

Governance & Policy Management 13

Regulatory Compliance 13

Beyond End-of-Life Support 13

activestate

Introduction

For decades, organizations in both the public and private sectors have steadily been increasing their use of open source software (OSS). In fact, nearly 100% of all organizations leverage some open source component (Intel).

Unlike traditional proprietary software development models, OSS is published with an open license, meaning anyone can modify or build upon it for their own purposes. This introduces a unique set of opportunities that proprietary software simply cannot, like:

- **Reduced Costs:** Most OSS tools are free to use, resulting in a lower total cost of ownership.
- **Flexibility and Customization:** With OSS, you have access to the source code, allowing you to modify and tailor the software to fit your needs.
- **Community Support and Collaboration:** Anyone can contribute to OSS, meaning features and improvements are often community-driven, leading to highly innovative software.

However, with the increased visibility and involvement from third parties, these benefits come with exposure to potential risk for enterprises, forcing developers - and the DevOps and InfoSec teams that support them - to constantly ask "what's in my code?"

In 2025, the answer to this question is more crucial than ever. With the use of third-party and AI-generated code on the rise, organizations must understand the security implications associated with reliance on open source—let's look at the implications:

- **More Cyber Attacks Overall:** Amazon recently reported that they're seeing 750 million threats per day, up from 100 million (reported within the same year, 2024). (The Wall Street Journal)
- **More Financial Impact:** IBM reported that the global average cost of a data breach increased to $4.88 million in 2024—a 10% increase over the last year and the highest total ever. (IBM)
- **More Regulations:** In the last two years, more than 170 data protection regulations have been drafted and/or passed (MIT Sloan)

DevSecOps teams need a solution that supports accelerated productivity while also protecting the business from potential attacks.

That's where Application Security Posture Management (ASPM) comes in.

In this whitepaper, we dive deep into what ASPM is, why it's important, and how a strong ASPM platform helps organizations mitigate vulnerabilities and unlock the full potential of open-source software.

Amazon recently reported that
they're seeing

750 million threats per day

up from 100 million
(reported within the same year, 2024)

IBM reported that
the global average
cost of a data breach
increased to

$4.88 million in 2024

a 10% increase over
the last year and the
highest total ever.

In the last two years, more than

170 data protection regulations

have been drafted and/or passed

activestate

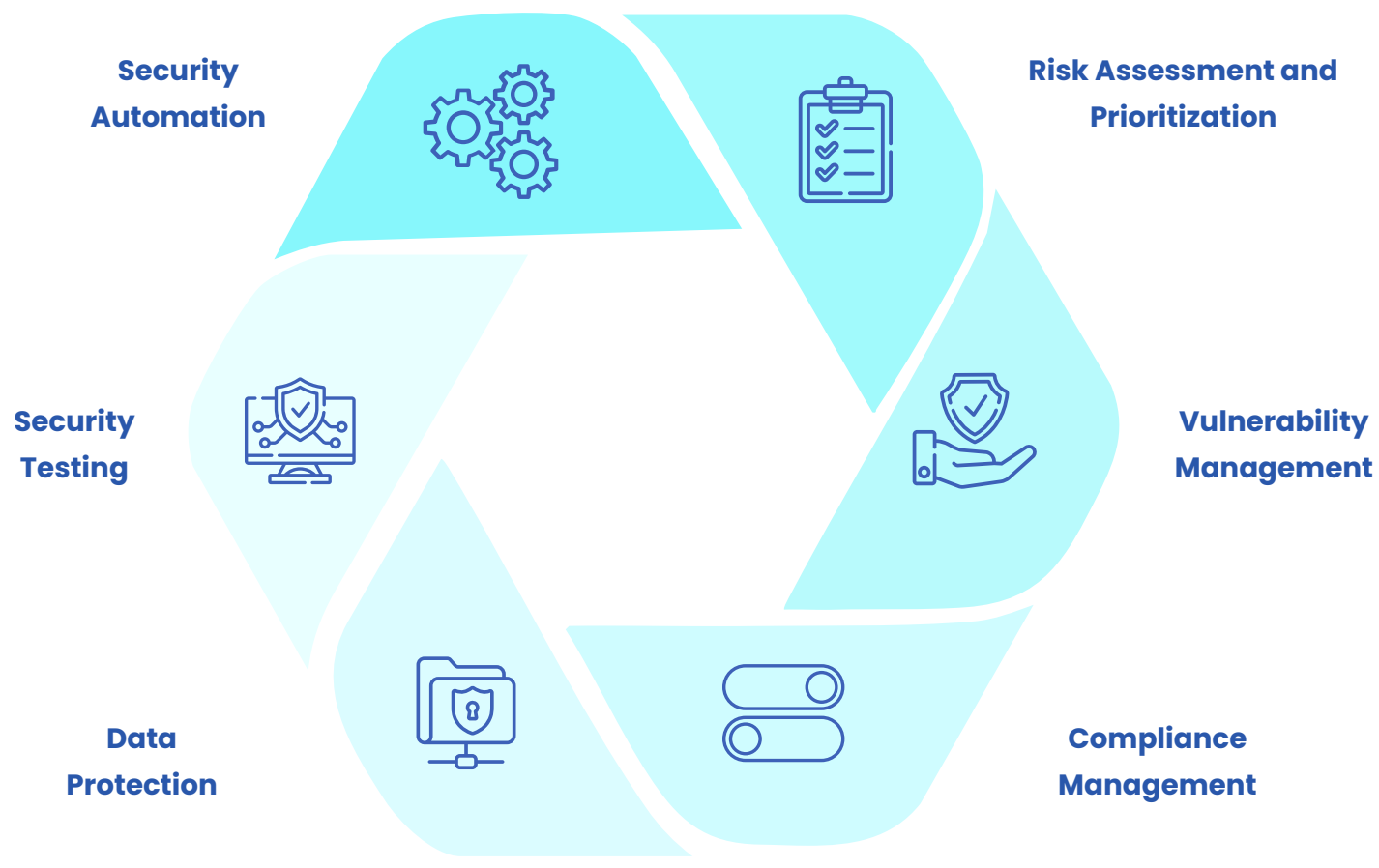
What is Application Security Posture Management (ASPM)?

Before we dive in, let's define what application security posture management (ASPM) is:

> "ASPM analyzes security signals across software development, deployment, and operation to improve visibility, better manage vulnerabilities, and enforce controls. Security leaders can use ASPM to improve application security efficacy and better manage risk."
>
> (Gartner).

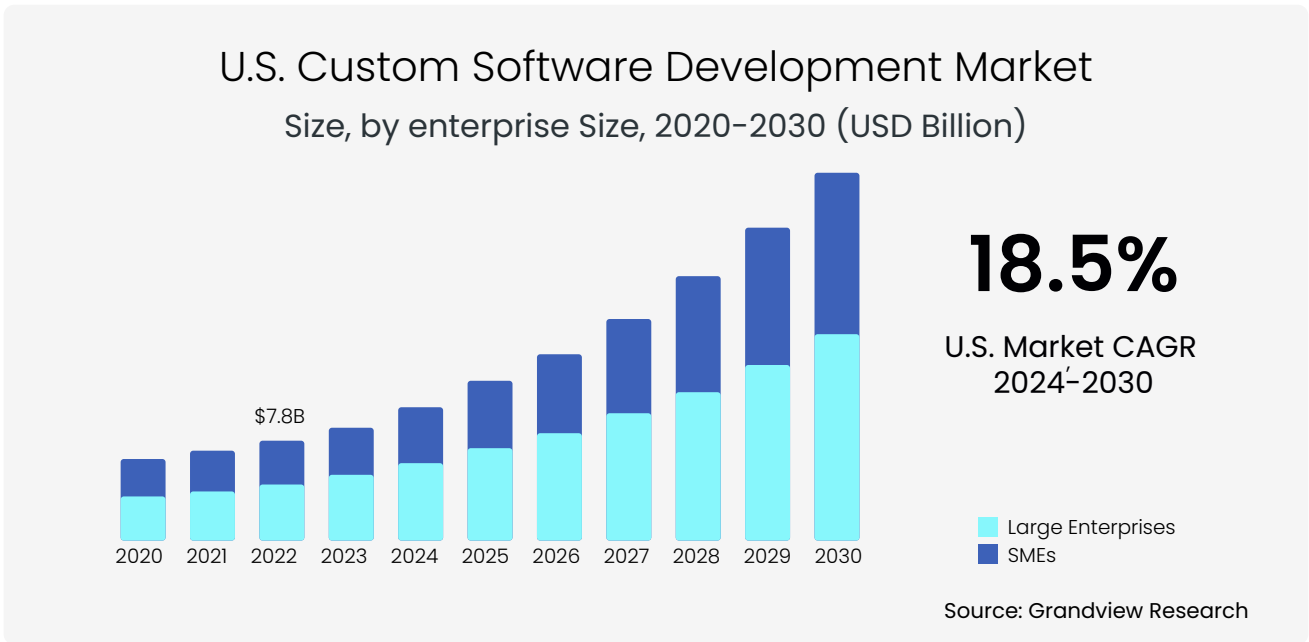
In other words, ASPM provides AppSec teams and their DevOps counterparts a holistic view of their application's security posture throughout the development lifecycle. An ASPM solution helps teams identify vulnerabilities, assess risk, and prioritize remediations across the entire attack surface.

Elements of ASPM



Why is ASPM important?

Businesses are building applications faster than ever with AI and low-code development platforms—Grandview Research estimates that the global custom software development market size was $35.42 billion in 2023, and expects it to grow at a CAGR of 22.5% between 2024 and 2030.



Traditional AppSec programs can't keep up with the pace of development. ASPM has emerged to address common challenges security teams face, such as:

- **Accelerated Development Cycles:** With software being developed and deployed faster than ever before, security teams are struggling to keep up, exposing the business to vulnerabilities slipping through the cracks.
- **Widening Attack Surface:** Modern applications are made up of microservices, APIs, and external components, significantly widening the attack surface, and making it harder than ever to maintain a comprehensive view of an organization's security posture.
- **Vulnerabilities in the Software Supply Chain:** With the number of attacks increasing year over year, organizations need better visibility and control over the security of third-party components and dependencies integrated into their applications.
- **Regulatory Compliance:** As previously mentioned, over 170 regulations related to data protection and privacy have been introduced in the last two years; organizations need more robust processes to manage risk and demonstrate compliance.

ASPM has become a vital practice, so much so that, Gartner predicts that by 2026, over 40% of all organizations developing proprietary applications will adopt ASPM to identify and resolve application security issues quickly. The rapid adoption of ASPM makes sense when you consider the dynamic landscape of software development. ASPM ensures applications are being rigorously and continuously tested, allowing organizations to quickly detect, prioritize, and remediate.

Over 40% of all organizations developing proprietary applications will adopt ASPM to identify and resolve application security issues quickly

activestate

ASPM vs. SAST

Static Application Security Testing (SAST) is a security testing method that analyzes the source code, bytecode, or binaries of an application. It's a critical component of a robust security strategy, and is part of ASPM platforms.

ASPM platforms integrate advanced SAST tools to help pinpoint vulnerabilities during the development phase of an application. SAST can help identify issues like buffer overflows and SQL injection.

ASPM vs. DAST

Dynamic Application Security Testing (DAST) focuses on identifying vulnerabilities in a running application, typically by simulating external attacks. DAST tools simulate real-world attacks so security engineers can identify vulnerabilities that only become apparent during execution such as authentication issues, misconfigurations, and runtime exploits.

DAST tools are often one of the testing methods integrated within ASPM as part of a larger application security program. ASPM uses DAST to help contextualize security risks and provide a risk-based prioritization.

ASPM vs. SCA

Software Composition Analysis (SCA) is the practice of identifying and managing open-source and third-party components within a software application. SCA tools scan application codebases to detect open-source libraries and other external components, identifying vulnerabilities, licensing issues, and outdated or unsupported versions.

SCA is a component of an ASPM strategy. While SCA focuses on identifying and managing risks associated with third-party dependencies, ASPM takes a more holistic view of an application's security posture across the entire SDLC.

ASPM vs. AST

Application security testing (AST) tools are a subset of ASPM. They are designed to scan code and pinpoint security vulnerabilities, however they lack the sophisticated context provided by a complete ASPM platform.

On the other hand, a complete ASPM platform consolidates the findings of an AST tool to give security, development, and operations teams a broad picture of their risk. ASPM analyzes the findings from the scan and prioritizes them based on potential risk.

ActiveState takes it a step further and fully automates remediation. With ActiveState's ASPM solution, development teams can focus on building their core application, while we manage dependencies and configuration.

Learn more>

ASPM vs. ASOC

ASPM and Application Security Orchestration and Correlation (ASOC) both share methodologies that aim to enhance an application's security, but they take different approaches.

ASOC is an approach, not a tool, to coordinating and automating the processes and tools involved in vulnerability detection and management. Organizations adopt ASOC to have application security processes that are more efficient and effective than those of traditional manual security.

ASOC has evolved to become a part of ASPM, often viewed as a precursor to the broader and more holistic approach of ASPM. ASPM takes ASOC a step further, shifting from just managing vulnerabilities, to managing and scaling an AppSec program based on risk.

ASPM vs. CSPM

ASPM and Cloud Security Posture Management (CSPM) can work together to provide security, but there are some core differences between the two that are worth discussing, but first, what is CSPM?

CSPM visualizes and remediates risk in the cloud infrastructure layer. CSPM solutions are focused on monitoring and securing the cloud infrastructure itself.

While both powerful, they have several key differences:

- **Scope of Protection:** ASPM protects across the entire SDLC, while CSPM only secures the cloud-based environment in which the applications are deployed.
- **Security Concerns:** ASPM is focused on the security of each application and all connections made with it, while CSPM is focused on creating a secure cloud-based infrastructure which applications can be safely deployed

ASPM vs. Building It Yourself

There is a lot of open source software readily available to build your own code scanning and security toolkits to identify vulnerabilities in everything from your dependencies to containers. This does save your organization money purchasing several tools–SAST, DAST, SCA, or CSPM tool (to name a few), however the manual hours building and maintaining all the tools far outweigh the benefits.

Investing in an ASPM tool will provide you one workstream to manage the security of your entire SDLC versus working with various applications which don't communicate with one another, leaving your team more confused and frustrated. Additionally, most ASPM tools are customer-forward with a support team at hand to quickly resolve any bugs and a centralized dashboard to alert you to the newest vulnerabilities and remediate before they become a costly issue.

Building in-house is great for organizations with extremely large teams and unlimited budgets but for most organizations, you would rather your team build features than fix bugs.

activestate

ASPM: The Future of Secure Software Delivery

As we know, there are dozens of solutions that help organizations manage their applications vulnerabilities, but that's precisely where the problem lies.

> "Complexity is the enemy of security; yet the average organization works with 10 to 15 security vendors and 60 to 70 security tools."
>
> -Gartner

Security leaders are grappling with complexity, overlap, and blind spots that come from using multiple cybersecurity vendors and tools. Different teams are using different tools and different processes creating risk silos that are impossible for security leaders to manage.

The key is in detection, prioritization, and remediation with ActiveState's ASPM for Open Source Supply Chain Security.

ASPM offers security leaders with unparalleled visibility into their application's architecture, allowing them to better manage vulnerabilities and enforce controls. Some other benefits include:

- **Comprehensive View of Security Health**
  - » **Holistic Security Monitoring:** ASPM offers a unified, continuous view of the security health of an application, helping organizations understand the complete security posture of their applications across development, testing, deployment, and production stages.
  - » **Centralized Security Dashboard:** Security teams can access a centralized dashboard that consolidates vulnerability data, compliance status, and security risks, providing a clear and comprehensive understanding of where security weaknesses lie.
- **Proactive Risk Management**
  - » **Early Vulnerability Detection:** ASPM helps identify vulnerabilities early in the SDLC. This proactive detection reduces the changes of critical security flaws making it into production
  - » **Continuous Risk Assessment:** Continuous scanning for vulnerabilities, misconfigurations, and other security risks ensures that gaps are caught early and mitigated before they can be exploited.
  - » **Prioritized Remediation:** With automated risk assessment, ASPM tools prioritize security issues based on factors such as exploitability, severity, and business impact, allowing teams to focus their efforts on the most critical risks.
- **Enhanced Security Visibility**
  - » **End-to-End Visibility:** ASPM provides visibility across all layers of the application, including code, infrastructure, third-party components, and cloud environments, helping organizations track vulnerabilities in every part of the application.
  - » **Comprehensive Threat Landscape:** By continually monitoring and assessing security risks, ASPM offers insight into the evolving threat landscape, enabling organizations to better prepare for emerging threats.

- **Improved Compliance and Regulatory Adherence**
  - » **Automated Compliance Tracking:** ASPM can help organizations automate the tracking of compliance with various regulatory standards. This reduces the manual effort required to meet security and privacy regulations.
  - » **Audit Trails and Reporting:** ASPM tools generate detailed audit trails and reports that can be used to demonstrate compliance to regulators, internal auditors, and other stakeholders.
  - » **Ensure Security Best Practices:** By enforcing best practices and security standards, ASPM helps ensure that applications meet industry-specific compliance requirements without extensive manual intervention.
- **Increased Efficiency and Automation**
  - » **Automated Vulnerability Scanning:** ASPM solutions automate vulnerability scanning and risk assessments, freeing up valuable resources and allowing security teams to focus on remediation efforts.
  - » **Automated Remediation:** ActiveState's ASPM platform can automatically create full source code builds, speeding up the remediation process and removing the manual burden on development teams.
- **Cost Savings**
  - » **Reduced Breach Costs:** By identifying and mitigating security risks before they result in a breach, ASPM helps avoid the significant costs associated with data breaches, including fines, legal fees, reputation damage, and customer loss.
  - » **Reduced Remediation Costs:** Addressing vulnerabilities early in the SDLC is typically far less costly than fixing them in production. ASPM helps organizations catch issues before they become expensive to resolve.
  - » **Resource Optimization:** By automating vulnerability scanning, risk assessments, and reporting, ASPM reduces the manual workload on development teams.

However, like any approach, ASPM tools have some limitations, but perhaps the biggest are:

- **It's Not a Complete Fix:** ASPM tools don't automatically fix all vulnerabilities; they provide recommendations, but developers still need to manually address more complex vulnerabilities.
- **Tooling Gaps:** ASPM relies on integrations with other security tools, so its effectiveness in remediation depends on the quality and breadth of these integrations. If an ASPM tool isn't properly integrated with the development environment or CI/CD pipeline, it can reduce its effectiveness.
- **Resource Intensive:** Continuous monitoring and remediation workflows can be resource intensive—especially at enterprise-scale—oftentimes requiring dedicated resources for management and oversight.

activestate

ASPM and ActiveState: Securing your Open Source at Scale

OSS is the standard in enterprise software. For most organizations, identifying all the OSS deployed is difficult, but then we layer on the complexity of managing security, and now it's nearly impossible with traditional processes. A 2024 Gartner report highlighted that 83% of organizations experienced a security incident directly or indirectly related to open-source vulnerabilities in the past 12 months.

Unknowingly or not, developers would prefer to think of OSS as "my solution; someone else's problem". Unfortunately, that's rarely how things work out—issues inevitably arise, creating a bottleneck that's difficult to break out of, leading to consequences like:

- The creation of a "golden set of dependencies" for all projects
- Never updating the OSS components in a project's codebase for fear of breaking the build
- Artificially limiting your tech stack to limit maintenance work even though other ecosystems may offer better solutions.

These consequences increase security and performance risk over time, impacting the organization's ability to scale.

ASPM tools, like ActiveState, help manage OSS security by offering continuous monitoring, risk management, and remediation of vulnerabilities.

ActiveState's ASPM platform provides organizations the necessary visibility to manage open source software at scale—some key capabilities of ActiveState include:

- **Unprecedented Visibility:** ActiveState empowers your security team to catalog, monitor, and understand all the open source components within your organization, providing panoramic insights into the landscape of your open source components.
- **Faster Decision Making:** ActiveState provides a clear view of your open source so you can understand your risk profile, generate comprehensive dashboards, and share critical intelligence across your entire team, enabling informed and proactive decision-making.
- **A Single, Curated Source of Truth:** ActiveState replaces a multitude of insecure sources with a single, curated catalog of all open source components, ensuring alignment of all organizational policies and regulatory components to the SDLC.
- **Hardened Build System:** ActiveState allows you to leverage completely customizable build infrastructure without the hassle of building it yourself, freeing your developers to focus on your own mission-critical development tasks.
- **Intelligent Remediation and Deployment:** Unlike other platforms, ActiveState is able to automate remediation. Our solution automatically rebuilds code directly from the source and seamlessly integrates with your CI/CD system to get the fix into production, quickly.

activestate

Beyond the Hype: 6 Practical Uses for ASPM in Your Open Source Journey

The widespread adoption of OSS in enterprise applications unlocks a treasure trove of benefits. However, managing OSS at scale introduces new security complexities. Exploitable vulnerabilities in open-source components can expose your applications to data breaches, financial losses, and reputational damage.

ASPM empowers organizations to navigate these challenges and unlock the full potential of OSS. This section explores six key use cases where ASPM provides significant value, enabling you to achieve secure and efficient open-source integration at scale.

Discoverability and Observability: Gaining Visibility into Your Open Source Landscape

Managing OSS effectively is crucial in today's development landscape. However, achieving complete visibility into all the OSS components used across your applications and infrastructure can be a significant challenge. Traditional methods, like manual tracking and spreadsheets, are time-consuming, error-prone, and fail to scale. This lack of visibility exposes organizations to security vulnerabilities, licensing compliance issues, and version control problems.

ActiveState's ASPM solution addresses these challenges by providing comprehensive discovery and observability capabilities. It automatically scans your environment to identify all direct and transitive OSS dependencies, giving you a real-time inventory of your entire open-source footprint. This empowers you to make informed decisions about security, licensing, and overall application health. ActiveState differentiates itself by offering a holistic approach to OSS management, going beyond mere discovery to provide actionable insights and automated remediation guidance. This empowers organizations to not only see their OSS usage but also take proactive steps to mitigate risks and optimize their open-source strategy.

Continuous Open Source Integration:

The continuous integration of open-source components is essential for modern development practices. However, manually identifying, vetting, and integrating new open-source libraries can be a time-consuming and error-prone process. Additionally, keeping pace with the ever-evolving open-source landscape can be challenging.

ActiveState's ASPM solution addresses these issues by providing a streamlined approach to continuous open-source integration. It continuously monitors for new releases, vulnerabilities, and security advisories related to your existing open-source dependencies. This enables you to quickly identify and incorporate necessary updates, ensuring your applications are always running on the latest and most secure versions of OSS. ActiveState's platform simplifies the integration process, reducing development time and minimizing security risks associated with outdated or vulnerable components.

activestate

Secure Environment Management:

Developing and deploying open-source applications requires a robust security posture throughout the entire software development lifecycle. Traditional methods of managing development and production environments can leave vulnerabilities open to exploitation.

ActiveState's ASPM solution empowers organizations to create and maintain secure environments for their OSS-based applications. It provides a centralized platform for managing and deploying secure containers and images. This ensures your applications are built on a solid foundation of security from the very beginning, reducing the risk of introducing vulnerabilities through insecure environments. ActiveState's secure environment management capabilities empower organizations to confidently leverage open source while minimizing security risks.

Governance & Policy Management:

The widespread adoption of open-source software necessitates a well-defined governance framework to ensure security, compliance, and consistency across an organization. Manual enforcement of policies and best practices related to OSS usage can be cumbersome and error-prone.

ActiveState's ASPM solution addresses this challenge by providing a centralized platform for governance and policy management. You can define and enforce rules around acceptable open-source licenses, acceptable risk levels for vulnerabilities, and approved sources for OSS components. This ensures all developers within your organization adhere to established security and compliance requirements when working with open source. ActiveState's platform empowers organizations to achieve consistent and controlled OSS usage, minimizing risks and simplifying governance efforts.

Regulatory Compliance:

In today's data-driven world, adhering to regulations like GDPR and CCPA is paramount. However, managing the privacy implications associated with open-source components can be complex.

ActiveState's ASPM solution empowers organizations to achieve regulatory compliance by providing deep insights into the data handling practices of different open-source libraries. This enables you to identify potential privacy risks associated with your OSS usage. By leveraging ActiveState's platform, you can ensure your applications comply with relevant regulations and avoid costly fines or reputational damage.

ActiveState's ASPM solution empowers organizations to confidently leverage open source while navigating the ever-changing regulatory landscape.

Beyond End-of-Life Support:

Many open-source projects eventually reach their end-of-life (EOL), leaving applications built upon them vulnerable to security threats and compatibility issues. Traditional methods of manually tracking EOL announcements and migrating components can be resource-intensive and reactive.

ActiveState's ASPM solution addresses this challenge by proactively identifying and mitigating risks associated with EOL open-source components. It continuously monitors for EOL announcements and provides insights into potential security vulnerabilities and compatibility issues. This enables organizations to plan and execute timely migrations to supported alternatives, ensuring the long-term security, maintainability, and performance of their applications.

ActiveState's ASPM solution empowers organizations to proactively address EOL concerns and safeguard their applications from the risks associated with outdated open-source components.

activestate

> **"ActiveState's platform has revolutionized our approach to open sources. It offers complete visibility across our projects, preemptively tackles security vulnerabilities, and unifies our toolset, allowing us to focus on what truly matters—innovation."**
>
> - Jordan Lee, CTO at TechInnovators Inc.

At ActiveState, we help teams take a holistic, secure approach to open source management by ensuring unparalleled observability, robust vulnerability management, continuous upgrades, and governance support. With ActiveState's platform, organizations can gain a competitive advantage by

- **Minimizing Security Risks:** Proactively identify and mitigate vulnerabilities, reducing the risk of data breaches and reputational damage.
- **Improving Development Velocity:** Streamline development workflows and accelerate time-to-market by automating security checks and reducing manual effort.
- **Enhancing Compliance:** Ensure adherence to industry standards and regulations with automated compliance reporting and policy enforcement.
- **Driving Innovation:** Focus on core business objectives by offloading the burden of OSS management to a trusted partner.

We ensure a frictionless, scalable integration within your existing workflows and developer tools, so you don't have to completely overhaul your tech stack. Plus, we're compatible with any open source language or ecosystem.

Ready to gain full visibility and control over your software supply chain? Explore ActiveState's platform to enhance software supply chain security through a free Enterprise Trial.

About ActiveState

ActiveState enables DevOps, InfoSec, and Development teams to improve their security posture while simultaneously increasing productivity and innovation to deliver secure applications faster.

With a single platform that tames open source complexity, teams get a continuously secure software supply chain, unparalleled observability, robust vulnerability management, continuous upgrades, and governance support that enhance collaboration across the organization.

All from the trusted partner that pioneered and continues to lead enterprise adoption and use of open source software.

Start An Enterprise Trial

www.activestate.com • solutions@activestate.com