ActiveState

THE BENEFITS OF MODERN SOFTWARE FACTORIES AND AN OUTSOURCED SOFTWARE SUPPLY CHAIN

Decrease risk & costs by outsourcing the security & maintenance of the open source components from which your software is assembled.

Executive Summary

The concept of a modern software factory applies the principles of manufacturing to software creation, in which automation, efficiency and quality are achieved by establishing a repeatable process based on a set of tools, processes and third-party components. With measurements in place at each point in the software development process, it's possible to increase value and remove costs in order to maximize efficiency.

One of the key areas of efficiency and cost improvement centers on the software supply chain. Modern software is more assembled than written today, with >80% of an application's codebase being composed of reusable, third-party open source software components. Today, implementing, managing, securing and maintaining the software supply chain is primarily done in-house, acting as a drag on throughput.

Much like manufacturers realized gains in productivity and efficiency by outsourcing their supply chains successfully decades ago, the software industry is now poised to do the same.

Outsourcing the software supply chain delivers:

- **Decreased Risks** - placing the burden of cybersecurity on an outsourced vendor reduces errors that occur due to a lack of internal expertise or lapses in focus resulting from internal cybersecurity burnout.
- **Lower Costs** - dramatically reduce the overhead of managing a software supply chain with a single hand to shake, rather than multiple third-party sources to manage.
- **Increased Revenues** - developer time spent managing and maintaining the supply chain can be repurposed to creating more features that close competitive gaps, increasing win rates.

This paper describes how an emerging class of software supply chain providers can help software vendors realize security, efficiency and productivity gains.

Introduction

The modern software factory is a result of the fact that software is more assembled from existing components rather than written from scratch. In fact, 80% or more of a modern application may be composed of open source components.

> As a result, software vendors are now in the software supply chain management business, whether they realize it or not.

Open source software is generated by third-parties that are rarely under control of a software vendor. However, third-party code imported into the enterprise must be managed and maintained in order to benefit from the innovation that open source provides, while avoiding security issues that expose the organization to exploitation by bad actors.

Unfortunately, only the largest enterprises can afford to spend the time and resources to create and manage their open source software supply chain in a robust and sustainable manner. Smaller organizations typically cobble together a set of point solutions (SCA tools, repositories, build tools, binary scanners, and so on) just to be able to compete. Given such a system, it's no wonder that most organizations take an ad hoc approach to maintaining and updating their software supply chain, which is the equivalent of running a factory with malfunctioning assembly lines.

The consequence is that managing and maintaining a software supply chain costs far more than many organizations believe. Worse, the practice is failing to help them meet security goals in the face of a 633% growth year-on-year in software supply chain attacks.

> In fact, as many as 91% of companies experienced a software supply chain attack in 2023.

It may be time to draw inspiration from the manufacturing industry and outsource the software supply chain. Like manufacturers have done for decades, outsourcing allows companies to better focus on their end product, while deriving additional benefits:

- Decreased security risk
- Minimized maintenance costs
- Increased productivity

Forward-looking organizations that take the step of outsourcing their software supply chain stand to gain a significant competitive advantage over their slower-moving counterparts.

Decrease Risk by Securing the Software Supply ChainChain

With twice as many software supply chain attacks in 2023 as the three previous years combined, 2023 was a costly year for businesses who paid $46B to address 245,000 supply chain incidents.

In line with these numbers, the Application Security Posture Management (ASPM) 2024 report, which surveyed 500 US-based CISOs, found that 77% recognize that software supply chain security is a blind spot for Application Security teams (AppSec).

AppSec is inundated with cyberattacks, which have more than doubled since the pandemic. At the same time, cybersecurity budgets have been negatively affected by the current economic uncertainty, allowing AppSec to merely tread water in the face of:

- An ever-growing number of open source vulnerabilities.
- The exponential growth of software supply chain attacks, driven primarily by malware.
- Record-setting ransomware payouts.

The result has been a crisis among cybersecurity professionals, reflected by increasing stress, cynicism and exhaustion. Attack vectors have evolved quickly post-pandemic when bad actors adopted economies of scale. By compromising open source code included in a popular software application, hackers embedded their malware in that software's customer environments. Rather than probing corporate networks one by one, bad actors exploited their embedded malware to steal data, install harmful software, gain control of networks, and so on at thousands of compromised customers.

> While the DevSecOps value proposition of "shifting security left" could help to relieve some of the AppSec burden, it remains aspirational for most organizations who are unwilling to accept the slower rate of code delivery that the DevSecOps approach entails.

As a result, cybersecurity professionals are increasingly burdened with triaging an ever-growing number of alerts. Unsurprisingly, a number of recent surveys reflect this trend, including a Cyberark survey that found 59% of cybersecurity employees were simply worn out, even as there's a growing shortfall of almost four million cybersecurity workers globally.

Without replacement workers burnout surges, leading to lax security as exhausted teams lose focus. For example, the software supply chain attack on VOIP software vendor 3CX in 2023 resulted in more than 600,000 client systems being compromised. While it was the VOIP software installer that included a malware-infected open source package, the root cause of the incident was alert fatigue: analysts ignored alerts that they believed to be false positives.

Outsourcing minimizes the cognitive load on cybersecurity and DevOps teams, allowing them to focus on the finished product. When a third party is responsible for discovering, investigating and remediating open source security issues, internal cybersecurity teams can focus their investigations on flaws in their proprietary code, instead.

In this way, forward-looking organizations that outsource the securing of their software supply chain will benefit from enhanced productivity, while reducing the kinds of cybersecurity burnout that result in security lapses.

Minimize Costs of Software Supply Chain Maintenance

Software supply chain maintenance is the new tech debt, and it's set to explode as applications are increasingly built on top of open source libraries.

But this approach to building software raises two key issues:

- Software supply chains facilitate continual production at scale, yet too many software vendors are in the habit of using their software supply chain exactly once per project in order to import the required open source components and create the environment on which the software will run.
- Developers prefer not to maintain and fix code they didn't write, especially when doing so might result in breaking the build. For this reason, codebases are rarely updated unless a critical vulnerability is encountered.

> These issues beg the question, if the software supply chain is not being leveraged to make continual updates, why incur the overhead of one?

The reality is that software vendors MUST continually maintain their software supply chain in order to avoid breaking their application, and/or becoming a target for bad actors due to both short and longer term issues that include:

- **Vulnerabilities** - security flaws in both open source packages and programming languages are constantly being found and reported, requiring frequent patching and/or updating of not only the open source components but also proprietary code.
- **API Changes** - software supply chains often include APIs that are constantly in flux as they're versioned, deprecated or deleted, requiring frequent code updates.
- **Outdated Packages** - IT policies may require open source packages to be updated on a 3 to 6 month basis in order to reduce risk. These updates may also require code fixes.
- **Language Upgrades** - longer term, programming language versions will go EOL. Unless upgraded on a regular basis, organizations will inevitably be confronted with a "big bang" upgrade that can be both complex and costly.

For organizations that regularly update their software supply chain, these tedious and repetitive maintenance tasks can take up to 30% of developer time, significantly hampering productivity. The reasons for this include:

- The maintenance overhead associated with integrating multiple point solutions in order to manage multiple open source ecosystems, or
- Stretching the capabilities of a single software supply chain to cover multiple ecosystems, where it may be a poor fit.
- Volatility within one or more open source ecosystems as a result of security, performance, stability or other concerns.

The root cause for these issues is the fact that software development organizations are not in the business of software supply chain management, and thus rarely invest the time and resources required to create a fully integrated software supply chain that can scale with their business needs.

Much like the manufacturing industry before it, the software industry has reached an inflection point where gains in productivity and efficiency can most easily be realized by outsourcing the management of commoditized components to a third party. When the third party understands how those components fit into the finished product, they can also add value by ensuring the application doesn't break when changes are introduced into the supply chain.

As a result, forward-looking organizations that outsource the maintenance of their software supply chain will benefit from enhanced developer productivity and organizational agility.

Increase Productivity by Outsourcing While Retaining Visibility & Control

One of the biggest concerns of organizations that adopt an outsourcing model is the loss of control over and visibility into their software supply chain. While handing over the reins requires trust, the outsourcing vendor must also provide a way to verify the efficacy of their model, as well as ensure all stakeholders have visibility into the results.

ActiveState has been a key player in the open source industry for more than 20 years, engendering the trust of 97% of the Fortune 1000. Their comprehensive software supply chain model has been honed over decades to address the key open source concerns of enterprises, including:

- **Scalability** - all open source dependencies are securely built in a reproducible manner from vetted source code using a SLSA Build Level 3-compliant hardened build system, thereby ensuring security for runtimes that can scale from a single, one-size-fits-all environment to hundreds of per-project runtime environments deployed across the extended enterprise from developer desktops to production servers.
- **Upgradability** - code scans regularly recommend updates to packages and programming languages that can be largely automated by resolving dependencies, refactoring code and rebuilding the application in a branch that can be pulled at any time. Breaking changes, as well as the need for manual interventions are minimized, essentially future-proofing applications.
- **Observability** - for all stakeholders, enterprise-wide insight is centrally provided into who is using which dependencies deployed to which environments, as well as dependency-specific information including licenses, vulnerabilities, datedness, etc to address key security, compliance and IT concerns.

Software vendors turn to ActiveState to be their outsourced software supply chain so they can meet their productivity and security goals by focusing on their application, rather than maintaining the open source their application requires.

Conclusions: Outsourced Software Supply Chain Benefits

Unlike the old version of tech debt that was based on each developer fixing mistakes in the code they wrote, organizations have very little control over today's software supply chain tech debt since it is entirely composed of third-party code.

Only the largest enterprises can afford to spend the time and resources to create and manage their open source software supply chain in a robust and sustainable manner. Others are absorbing the overhead of integrating multiple point solutions (SCA tools, repositories, build tools, and so on) just to be able to compete. Given such a system, it's no wonder that most software vendors rarely maintain or update their software supply chain, which is the equivalent of building a house on a shifting foundation.

An outsourced software supply chain provides direct benefits in the form of:

- **Increased Revenues** - redirect the 30% of developer time currently spent on maintenance toward closing competitive gaps that increase opportunity win rates.
- **Reduced Risk** - eliminate the barriers to updating dependencies, reducing vulnerability security threats, while avoiding the risks that come with cybersecurity burnout.
- **Lowered Costs** - gain a single hand to shake rather than individually managing the hundreds of third-party open source components in the software supply chain.

Software vendors that adopt the principles of a modern software factory, including an outsourced software supply chain will gain a significant competitive advantage that allows them to achieve their cost-cutting, productivity and security goals.

To learn more about outsourcing your software supply chain, contact ActiveState.

ActiveState

Secure open source integration

www.activestate.com
Toll-free in NA: 1-866.631.4581
solutions@activestate.com