Software Supply Chain Security

Solution Overview

Introduction

Modern software development methods for virtually any product, from enterprise software to mobile apps to embedded devices, involve the use of external open-source or commercial software components. The companies that develop, integrate, deliver, and deploy these products and their components form complex supply chains that are the lifeblood of today's digital economy—but they also pose significant risk management challenges.

The breadth of externally sourced software that exists in today's typical enterprise creates a vast attack surface for adversaries. The growth in connectivity makes products yet more complex and more accessible, increasing the likelihood of attack.

How can organizations enjoy the benefits of efficiency, agility, and choice that comes with the use of externally sourced software components and products while controlling exposure to supply chain risk? In this document, we discuss the sources of cyber-risk in the software supply chain and how Vdoo can help to manage and reduce these risks.

Overview of Software Supply Chain Security Risks

Software supply chain cybersecurity risks result from vulnerabilities intentionally, or unintentionally, introduced into an organization through the acquisition or integration of software from external sources.

Software supply chain vulnerabilities are extremely lucrative for attackers because they potentially give them the power to attack any organization that uses the software. As evidenced by numerous supply chain cyber-threats and attacks exposed in recent years, these vulnerabilities can be exploited to target specific organizations or individuals, or to create widespread impact. Depending on the attacker's goals, they can be used for the purpose of changing the behavior of products using the vulnerable software, or as a starting point to infiltrate organizational networks and systems.

Software Supply Chain Attack Methods

Zero-day vulnerabilities – Unknown code vulnerabilities in externally sourced software that, if discovered by attackers, can be used at will (overtly or covertly) until they become known and fixes are defined and implemented.

Malware – Malicious code that, if installed in addition to, in place of, or within legitimate external software, may be used by an attacker, for example to alter the functionality of products containing the software, disrupt operations, or steal sensitive data.

Known vulnerabilities – Vulnerabilities discovered in publicly available software that have been disclosed and may be exploitable if not remediated or mitigated in products and systems using the software.

Backdoors – An access method, implemented by malicious code or configuration, planted into a product or system to enable an attacker to bypass existing access controls and gain illegitimate access.

Insecure configurations – Configuration malpractices such as insecure privileged access permissions or weak authentication methods can lead to compromise of external software components or products.

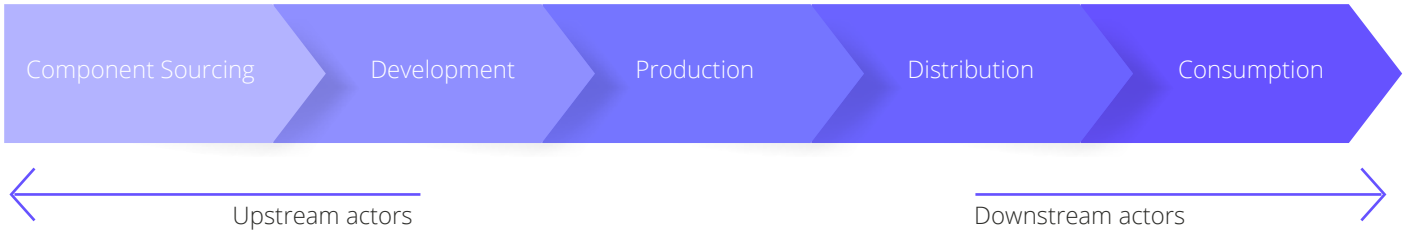
Bugdoors – A type of backdoor that is implemented as a software bug, hence harder to detect and to prove malicious intent if caught.

Risks Throughout the Software Supply Chain

Organizations' use of externally supplied software in products can be considered in two different levels:

- **In product development –** Software components such as open-source packages or commercial software packages are sourced for use as part of development, integrated into software or hardware products. The component software is typically maintained by the third party and therefore released products may not be updated with the latest or most secure component versions. Development of bespoke software components can also be outsourced to external suppliers as an alternative to internal development.

- **In product distribution and use –** Finished software or physical products (such as IoT devices or appliances) developed by third parties are sold and distributed to customers or deployed and consumed in the organization's IT and/or OT environments. In this case there is typically limited control over and visibility into the composition of the acquired product.



Basic Software Supply Chain Flow

The types and sources of risk related to external software vary by organization's role in the supply chain, between companies that develop products internally, companies that deliver products produced by third-party suppliers (possibly as part of a bigger system or service), and companies that consume products as end-users (asset owners).

Many organizations fall into more than one category. For example, a telecom service provider likely develops software in-house, acquires software applications such as mobile apps or devices such as networking equipment from external vendors for distribution to customers, and consumes third-party products such as connected printers and enterprise software.

Developers and Vendors

For organizations that develop product software internally, virtually any software project includes the integration of external software components. As a result, they face the risk of vulnerabilities in third-party components being exploited, or of malicious code being inserted into their products. The risk may originate from vulnerabilities or malicious code within the software components that are introduced into the product via these components' integration, from the way the software is configured in the product, or from security gaps in the organization's software development tools.

In case a new vulnerability is exposed, or a cyber-attack occurs, the vendor would likely be held accountable for the repercussions and responsible to address the issue (via a fix, mitigation, etc.) as soon as possible.

Asset Owners

Organizations face the risk of being affected by any security issue anywhere upstream in the supply chain of products they deploy and use.

Asset owners typically deploy a great diversity of software and hardware products in their IT and OT networks. Gaining visibility into the full scope of assets deployed in the organization, and their security vulnerabilities and associated risk, is a known and significant industry challenge. Attackers commonly seek vulnerable connected devices, applications or services exposed to public networks, and try to use them as an entry point to extend their reach into organizational networks and data.

Service Providers

Organizations that deliver products acquired from third-party suppliers to their customers face the risk of cyber-attacks due to product software vulnerabilities in their supply chain. Service providers may deliver, for example, externally developed networking and IoT edge devices, or mobile or server applications, associated with their services. In some cases, these products are acquired as white-label and delivered under the provider's brand without any indication of the source vendor. Though service providers can set software security requirements to their vendors, the products' security posture is not in their direct control. Still, vulnerabilities can lead to severe consequences, hurting their brand reputation and reliability.

In case of an attack, customers would likely hold their service providers directly accountable for damages they incur due to service downtime, data theft, or other attack related issues. Also, attackers may exploit product software vulnerabilities as an entry point to penetrate and compromise the organization's networks and systems.

Security issues in vendors' products, regardless of whether they are in code developed by the vendor, code from the vendor's external suppliers, or in non-code elements such as software configuration, create risk for the service provider. The company has limited control over the vendor's software development and security practices, and when software is delivered as binaries, it is hard to get accurate information on their software composition and security posture.

Sources of Risk

Following are a few key sources of software supply chain security risk for organizations:

Vulnerable Software

Open-Source Software (OSS) Components

The use of OSS components is extremely common in modern software development. Vulnerabilities discovered in these components are typically publicized and tracked as Common Vulnerabilities and Exposures (CVEs); larger components may have hundreds of CVEs associated with them. In addition, even the most well-maintained OSS may have unknown zero-day vulnerabilities that can be discovered and exploited by malicious actors. Once they become known, these vulnerabilities may be fixed in later versions of the OSS component, or a patch may be provided for existing versions.

Developers who integrate open-source components in their code don't always have the expertise, awareness, or tools to see all their dependencies and associated vulnerabilities, and to prioritize the vulnerabilities that are truly important to resolve. Beyond direct dependencies—the open-source components referenced directly in the code—transitive dependencies are also introduced by these components calling code from other OSS components, making the task of assessing the software security posture and identifying all issues very difficult and resource-intensive. Also, for various reasons, developers do not always update open-source dependencies to the newest versions with the latest security fixes.

Third-Party Non-OSS Software

Organizations may integrate external components into their products such as commercial software packages, hardware modules with embedded software, or outsourced development. In addition to the challenges with addressing known and unknown vulnerabilities as described for open-source components, the use of closed-source external software presents a further challenge: a lack of transparency. The company using the software components has limited control over software development and security practices, and when software is delivered as binaries, it is hard to get accurate information on their software composition and security posture.

Vulnerable Infrastructure

Software Development Infrastructure

Beyond finding security gaps in the product software itself, attackers can seek vulnerabilities in the systems used throughout the software development lifecycle to inject malicious code while evading existing software security and integrity controls. For example, an attacker gaining unauthorized access to the organization's build tools or repositories can integrate arbitrary code without anyone noticing, and before applying a valid cryptographic signature, so it is trusted as the vendor's legitimate code.

Another potential attack vector, which illustrates the complexity of controlling supply chain risk in modern development environments, involves package managers. Package management tools enable automated operation of tasks such as installing, updating, configuring, and removing software packages as part of the software build process. They provide simplicity and speed, but they also open a potential method for attackers to install malicious code into products without accessing the organization's internal systems and without being noticed. For example, security researcher Alex Birsan recently exposed how "dependency confusion" in package managers can be exploited to install malware, simply by creating a malicious package with the same name as a legitimate package and placing it on a public repository (for example, PyPI for Python software packages).

Software Update Infrastructure

After deployment, products can be compromised via software update mechanisms. For example, by obtaining illegitimate access to the update server, an attacker can plant a malicious payload into update packages and have that payload delivered inside the target organization. This was the method used to distribute malicious updates to the SolarWinds Orion network monitoring platform as part of the highly publicized SolarWinds supply chain attacks on FireEye and other organizations. Another example is the backdoored version of the ASUS Live Update tool which was signed with a valid ASUS code-signing certificate, hosted on their update servers for months unnoticed, and pushed to over 1 million ASUS computers.

Managing Software Supply Chain Risk – the Vdoo Approach

To protect their business and customers from cyber-risk related to externally sourced software, organizations must implement cybersecurity controls throughout the supply chain flow, taking into account that access to source code is in many cases partly or completely unavailable. First, software security analysis and validation should be implemented at predefined checkpoints. Based on analysis insights, it is possible to assess security gaps and determine actions, including:

· **Decision to approve or deny** an external component or product for onboarding, or selection of the optimal product or component among multiple alternatives based on their security posture.

· **Independent implementation of mitigations** when possible to resolve issues determined as required for fixing, for example through added protection mechanisms such as a firewall, or through configurations.

· **Collaboration with supply chain upstream actors** to fix required issues, for example through code fixes, component version upgrades, patching, or implementation of mitigations in the product.

In addition, continuous vulnerability monitoring and protection capabilities are critical for detecting and quickly responding to new software supply chain related security issues or attacks that emerge after deployment.

At Vdoo, our goal is to empower product security, supply chain security, and development teams to achieve these security capabilities in a seamless, automated, efficient, and scalable manner. Explanations of the software supply chain security measures recommended by Vdoo and enabled by our product security platform are described below.

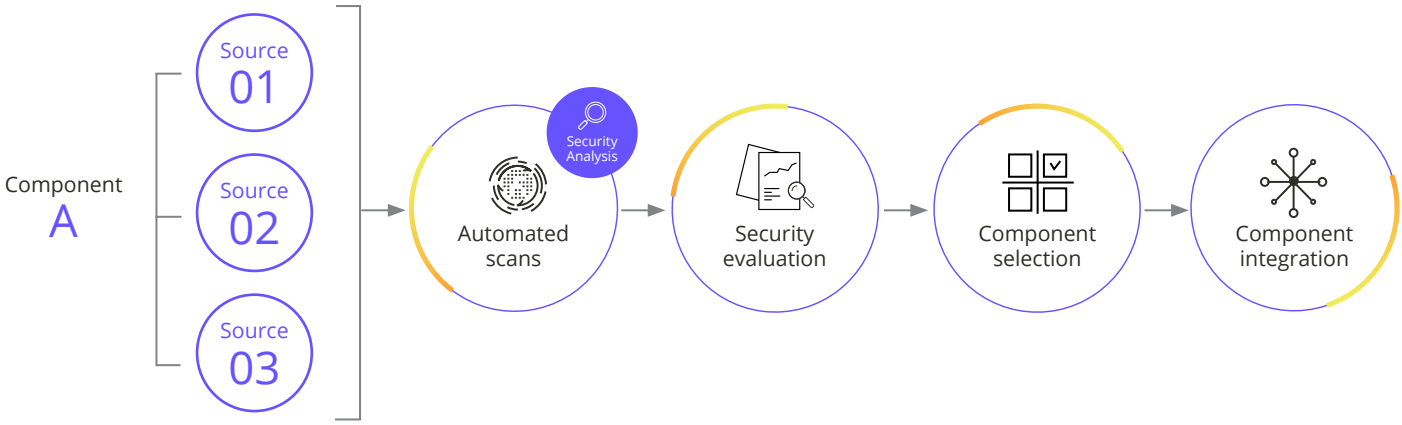
Managing Risk in Product Development

For organizations developing software internally, the optimal approach to reduce software supply chain risk is to combine informed decision making on the inclusion of specific third-party software components into the product, together with product security analysis as part of CI/CD build and release pipelines. This allows vendors to detect supply chain security issues, prioritize them by assessing their exploitability and impact in the whole product context, and resolve only the issues that matter from a risk perspective. In addition, this approach allows vendors to release highly secure products and reduce risk for their customers further down the supply chain.

Component Selection and Onboarding

By assessing the security level of external open-source and commercial software components as part of the sourcing decision making process, product security and development teams can take action to reduce supply chain risk early in the development lifecycle.

Vdoo provides the capability to perform automated security analysis on externally supplied binaries as part of the acceptance workflow. It provides detailed security findings to support component evaluation and selection without access to source code. In case identified issues in a desired component are determined as feasible for fixing, Vdoo provides clear step-by-step resolution guidance so developers can implement their own mitigation measures if possible, or work with their suppliers to incorporate the needed security measures.



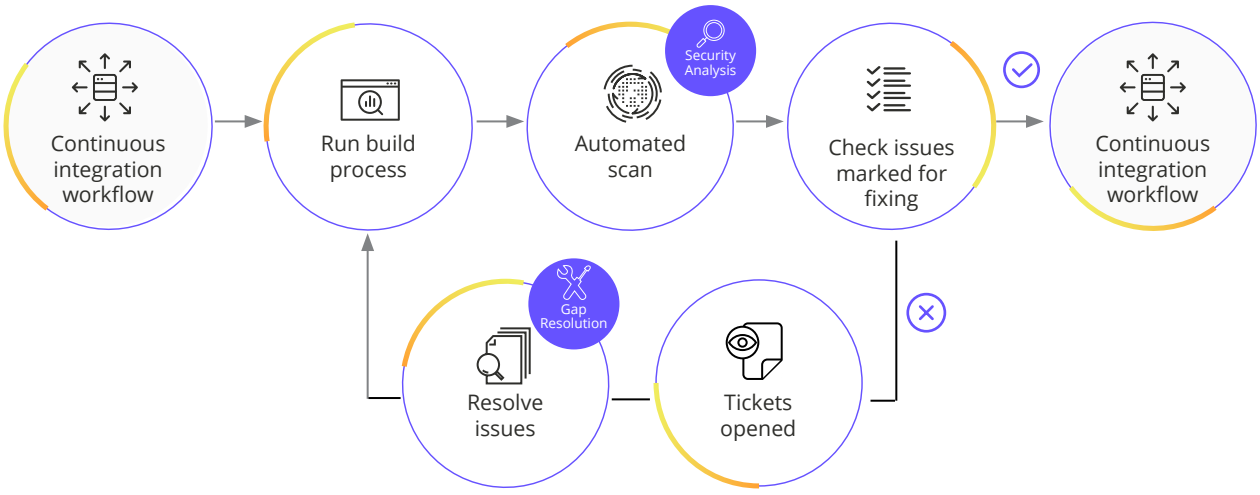
Security Implementation in CI/CD Processes

Automated security analysis scans can be used for security validation as part of nightly builds, checking whether any issues that require fixing are still unresolved to determine whether to continue or fail the build. If any such issues remain, tickets can be automatically opened in the ticketing system used by the organization for issue tracking and resolution.

The Vdoo platform's automated analysis provides a comprehensive and accurate view of product security issues, covering internally developed as well as third-party commercial and open-source software. It analyzes software artifacts to identify their software bill of materials (SBOM), open-source software licenses and versions, and complete product security information (CVEs, configuration issues, potential zero-days, malware, and more) in minutes. Vdoo provides clear step-by-step resolution guidance, so for each supply chain security issue detected, developers can choose the optimal resolution method: implementing their own mitigation measures if possible, updating or replacing vulnerable components, or working with their suppliers to incorporate the needed security measures.

Vdoo's approach is to perform the analysis of the entire build in order to accurately identify and prioritize security issues in the context of the product and not only at the component level. This helps organizations focus their efforts on fixing the relevant supply chain security issues. For example, a vulnerability in an HTTP server component may not be exploitable if the server is only listening on a local interface and/or the port is filtered by a software firewall.

This approach also enables detection of a broader range of issues, covering non-code elements such as configuration files, databases, keys and credentials, encryption mechanisms, and compiler security features. Though not discovered by typical application security testing tools, exposures related to these elements may have significant impact on the security posture of externally sourced software components and of the overall product, therefore their detection is critical for software supply chain security.

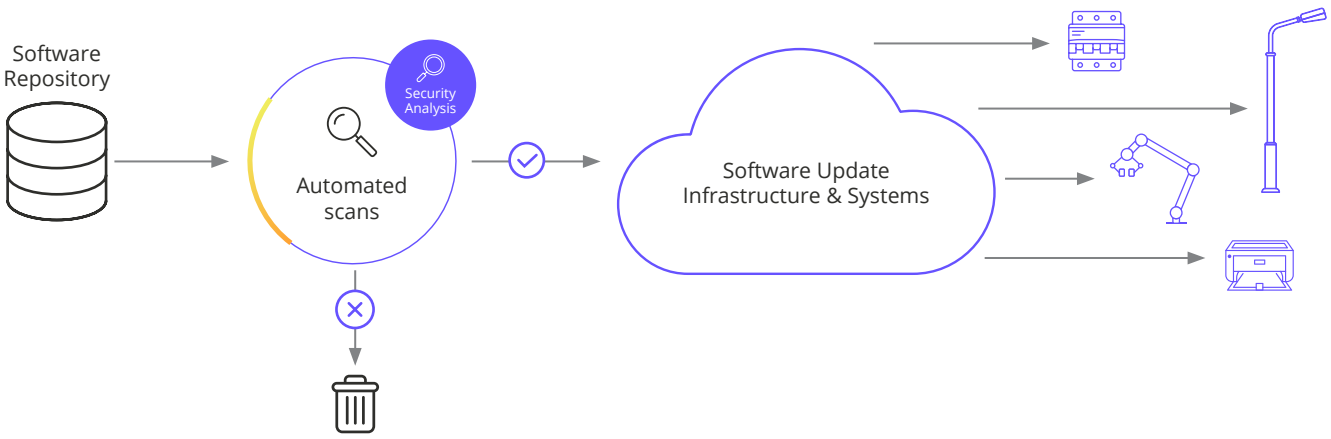


Security Gatekeeper for Product Releases

Automated security analysis scans can be used for security validation as part of a release approval process, checking whether any issues in the release build that require fixing are still unresolved. If any such issues remain, tickets can be automatically opened in the ticketing system used by the organization for issue tracking and resolution. This process can be performed iteratively until all issues required for fixing are resolved.

Security Gatekeeper for Software Updates

New software versions can be automatically scanned to validate they meet security policies before the software update deployment process. Software versions that do not meet security requirements can be rejected and not deployed.



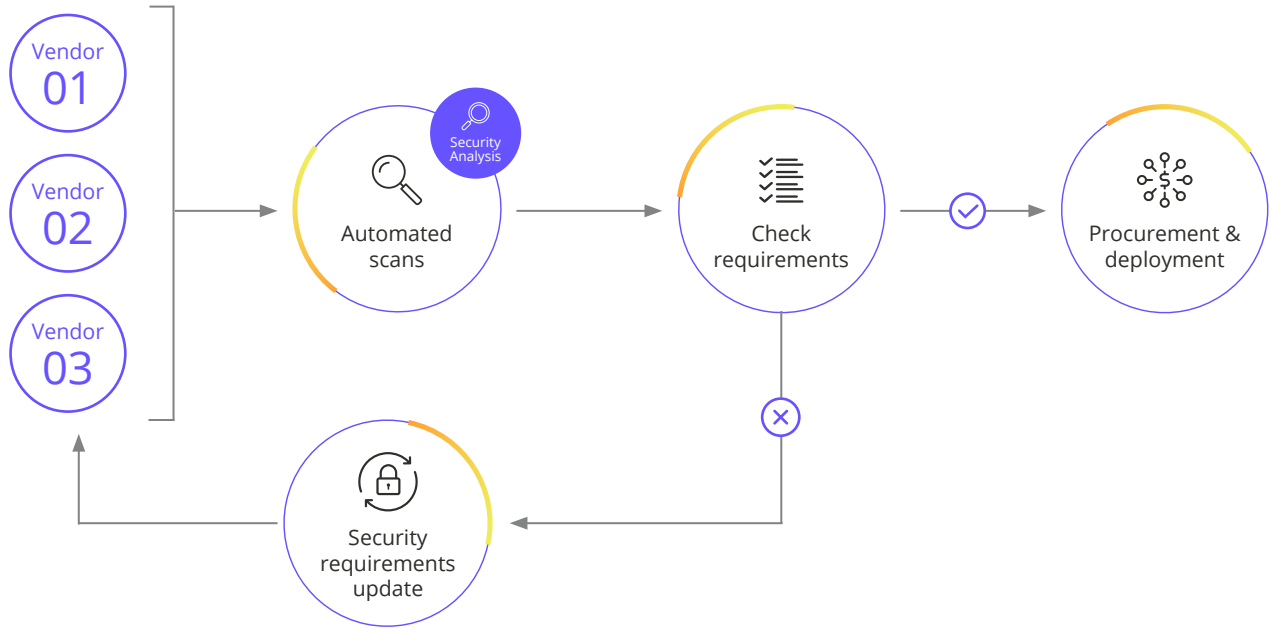
Managing Risk in Product Distribution and Consumption

Given the quickly evolving threat landscape, relying on product security assessment and validation at a specific point in time or only in the development phase is not enough. Continuous product security mechanisms should be used to quickly detect and respond to new cybersecurity threats. Complementing network-based security solutions, such mechanisms enable organizations to reduce supply chain risk by detecting more threats on their deployed connected assets, triaging them faster, and better protecting against them.

Organizations that develop products should establish processes and capabilities to ensure the security of their products after they are released. In parallel, organizations that deliver, deploy and consume finished products should have the capability to independently check the security of all products they use, as part of procurement processes and on an ongoing basis.

Security Validation in Procurement Process

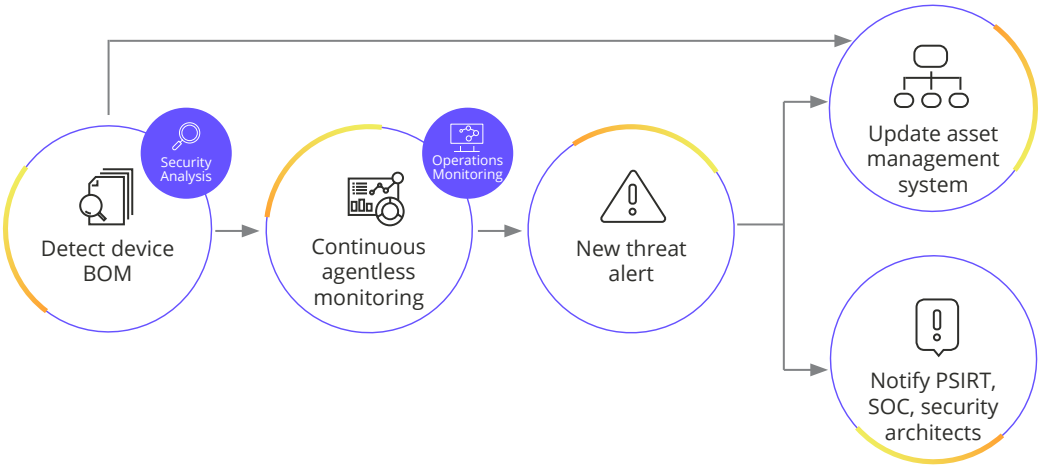
Automated product security analysis can be performed by asset owners as part of the procurement workflow. Vdoo provides detailed security findings without access to source code. Asset owners can use the detailed results to make informed product selection and procurement decisions. Should they wish to have identified issues fixed as a prerequisite for approval, Vdoo provides clear step-by-step resolution guidance so asset owners can implement their own mitigation measures if possible, or work with their vendors to incorporate the needed security measures.



Vulnerability Monitoring

Ongoing vulnerability monitoring allows rapid identification of newly discovered vulnerabilities in third-party commercial and open-source software for products developed, delivered, or deployed by the organization. It is important to assess these issues' potential impact, and quickly respond to the vulnerabilities that pose actual risk.

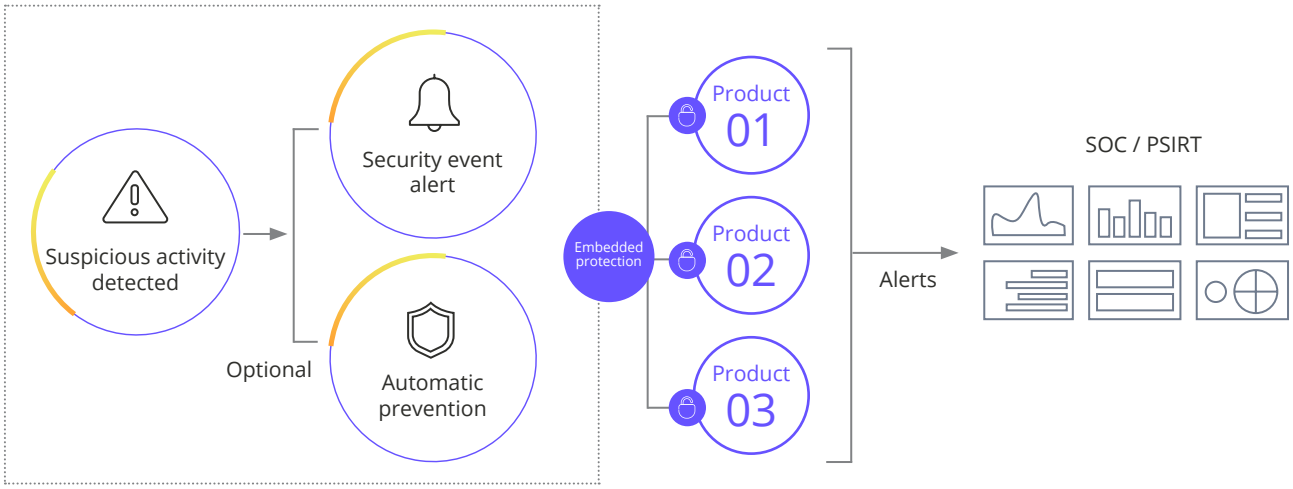
Vdoo provides real-time alerts on new vulnerabilities affecting products previously analyzed by the platform. Based on the components found on the product in the analysis, it is possible to correlate vulnerability information with the specific products that are impacted; this information can be quickly routed to the relevant security teams for handling.



Embedded Protection

Embedded protection mechanisms can reduce software supply chain risk by monitoring products in real time, alerting on security incidents, and proactively blocking supply chain attack attempts.

Vdoo enables such protection for devices and containers via an auto-generated tailored agent per product. The agents monitor for security events and create real-time alerts whenever a security event occurs. If desired, they can also actively prevent actions typically taken by attackers when attempting to exploit connected products. The agent enables mitigation of unknown or new vulnerabilities by blocking common attack vectors without any software modifications, which can be prohibitively expensive and risky, especially when the source of the issue is in third-party code which is out of the organization's direct control.



Securing the Software Supply Chain with the Vdoo Platform

Increase resilience and peace of mind – Address product security use cases across all parts of the software supply chain with one automated platform.

Gain control and visibility – Independently validate the security of components and products from external sources in binary form; no need for source code.

Reduce risk – Obtain comprehensive security findings on analyzed software including CVEs, configuration issues, zero-days, malware and more; implement continuous product security capabilities after deployment.

Reduce overhead – Empower development and security teams with accurate automated issue detection, contextual prioritization, and actionable resolution guidance, achieving high security at lower cost and effort.

Make security seamless – Use the platform easily without any setup required; integrate security capabilities smoothly with your organization's existing systems and processes using Vdoo's REST API.

Summary

The ability to independently analyze and validate the security of externally sourced software is key to controlling supply chain risk. The optimal approach to address all software supply chain use cases—from development to distribution and consumption—is to adopt technology that supports automated security validation of outgoing product software before it is released, checking of incoming software components or full products in whatever format they are available (source code, binary, or both) when acquiring them, and continuous security mechanisms to monitor and protect from new threats after deployment. Vdoo delivers all these capabilities in an automated platform that is easy to integrate and scale across diverse products and groups within the organization.

Beyond the technologies that facilitate security visibility and information sharing, the development of security awareness and processes among varied groups inside the organization (for example security, development, procurement, and IT), as well as increasing collaboration and transparency throughout the ecosystem, are needed to effectively manage supply chain security risk.

About Vdoo

Vdoo is a global leader in the complex and increasingly-critical product security space. With Vdoo, organizations can identify, prioritize, and mitigate a vast range of security issues. As the only automated platform that provides end-to-end product security, Vdoo helps development and security teams reduce time and effort while ensuring optimal product security. The platform addresses a diverse variety of security risks including supply chain threats, configuration risks, standard compliance, zero-day vulnerabilities, and more. Founded in 2017 by a team of seasoned cybersecurity entrepreneurs and product security experts, Vdoo is now a global company with offices in Israel, US, Germany, Singapore, Japan, and dozens of Fortune 500 customers representing the most security-diligent companies from various industries.

For additional information, please contact us at info@vdoo.com or visit vdoo.com