kaspersky

Lock down the chain: essentials of product security evaluation for slashing supply chain risks

Modern businesses rely on countless digital tools and third-party components, meaning any supplier can introduce risk. As the recent Global Cybersecurity Outlook 2026 by WEF shows, there is growing concern among CEOs and CISOs with regard to the risks of software vulnerability exploitation, and so careful security evaluation of software vendors has become critical.

Many companies blindly trust the software without conducting technical assessments, and such an approach carries risks. Trust is a good starting point, but verified trust is what ensures security and confidence. This verification implies rigorous checks in choosing the best, most secure and cyber-resilient product through evidence-based technical assessments.

The evaluation method that we suggest is not a certification, it's an approach for how to select a better product available on the market. Below you can find action items on how to choose such a product to mitigate supply chain risks. There are three levels of assessment, depending on time constraints and resource limitations, customized to a company's size and needs.

Initial

1 Evaluate product security before purchasing and deployment using OSINT

Before purchase or deployment of the product, perform open-source intelligence (OSINT) on the vendor to evaluate its maturity. These include:

- Checking for vulnerability management and a disclosure program. A coordinated vulnerability disclosure (CVD) program that attracts researchers and shows dedication to the security of its products is a plus point for any organization.
- Looking for historical vulnerabilities (CVE records) and security bulletins or other forms of vulnerability fixes notification channels.
- Checking if a bug bounty program is in place. The program covers not only vulnerability management, but also its handling and, more importantly, disclosure. Such a program shows its clients that the company is ready to invest more than necessary to enhance the security of its products.
- Assessing how quickly the vendor fixes vulnerabilities. The optimal target is within 2–3 months for most issues.

Advanced

2 Evaluate the vendor's software development process

One of the ways to evaluate a product is to assess if the software development process is well-defined and comprehensive.

- The easiest option is to ask your supplier to provide access to software development documentation.
- If an organization is not ready to provide access and be so transparent, you should ask them to share summarized or redacted versions of these documents to measure the maturity of the software development process, including information on last updates, development methodology, risk management plans and coding and testing standards.
- It's also recommended to request certifications or independent audit reports on internationally recognized standards, such as SOC 2 security audit or ISO 27001, to ensure that security is embedded throughout the software development lifecycle.

3 Use structured questionnaires to assess vendor practices

Require vendors to complete standardized questionnaires covering software development practices and personal data protection practices. The questionnaire should include a vendor's:

- Compliance with the most advanced cybersecurity frameworks and standards, such as the NIST Cybersecurity Framework, ISO/IEC 27001, OWASP API Security Top 10, including security certification information and security policies.
- Secure development lifecycle (SDLC) practices.
- Risk assessment and management, including supply chain risk management.
- Specifics about data processing practices and type of information collected from a host system to understand how this information is protected before installing an application on a critical system.
- Access control and encryption policies.

Advanced Plus

4 Conduct practical technical checks before deployment

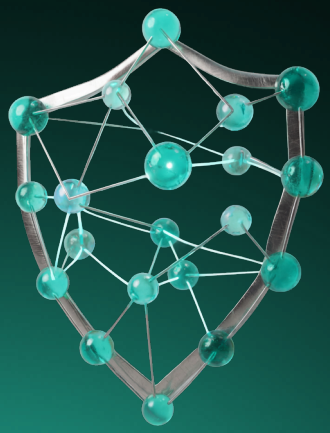
After OSINT and a software development process review and before approving a product, technical specialists can perform hands-on validation. Basic check includes:

- Verifying that all communications use encrypted channels.
- Checking for proper access control lists (ACLs).
- Confirming the product has a Role-Based Access Control (RBAC) model, ensuring the principles of least privilege and zero trust.
- Confirming that the list of third-party libraries and dependencies (software bill of materials) is up to date.
- Performing dynamic analysis (DAST), fuzzing, if possible, and in-depth penetration testing to validate that the running product behaves securely.

5 Conduct source code review when possible

For high-risk or critical systems, it is recommended that technical specialists conduct the most complicated and precise way of product evaluation and check its source code:

- Check application architecture and threat model for anomalies.
- Run automated static application security testing (SAST).
- Perform a manual review of critical components (communication, data processing, authentication).
- Conduct threat modeling to identify code areas requiring deeper review.
- Perform dynamic scanning with rebuild software.



6 Document all findings and maintain a supplier security register to ensure long-term supply chain resilience:

- A centralized record of all evaluated vendors.
- Risk ratings and justification.
- Required mitigations.
- Re-evaluation schedules.
- Incident history and patch timelines.

These action items create a repeatable, evidence-based process that strengthens supply chain security and ensures that only secure, resilient products enter the organization's infrastructure.

Kaspersky's approach to verify the trustworthiness of its products is called the Global Transparency Initiative (GTI). This project, launched in 2018, was initiated for providing an unprecedented level of transparency about how engineering and data processing practices work at Kaspersky. This includes ability to assess software development process, transparent reporting of the company's data management practices, transparent communication of the management-related and organizational processes, description and analysis of the surrounding business environment, software origins including legal factors and governing laws. All information required for the evaluation of our products is available in Kaspersky Transparency Centers. Learn more here.

kaspersky cybersecurity true to business

www.kaspersky.com