Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem

Overview

Secure by design products are those in which software manufacturers—the companies that create, ship, and maintain software—make security a core consideration from the earliest stages of the product development lifecycle. Ensuring that the products they use and procure are secure by design is essential for organizations to be resilient against ransomware and other forms of malicious cyber activity. Software manufacturers strive to deliver the features customers request, so it is crucial that customers explicitly demand security as part of the procurement process.

In this guidance, we lay out questions and resources that organizations buying software can use to better understand a software manufacturer's approach to cybersecurity and ensure that the manufacturer makes secure by design a core consideration. This guidance is a counterpart to CISA's Secure by Design guidance for technology manufacturers, which lays out three secure by design principles:

(1) Take ownership of customer security outcomes,
(2) Embrace radical transparency and accountability, and
(3) Build organizational structure and leadership to achieve these goals.

Today, when companies perform due diligence of their software manufacturers, they often focus on the enterprise security measures of the manufacturers, such as by ensuring the manufacturers meet various compliance standards. Although enterprise security is important, customers also need to focus on how a manufacturer approaches product security. Enterprise security refers to practices to protect a company's own infrastructure and operations, while product security refers to actions the software manufacturer takes to ensure the products they deliver are secure against attackers. There are many compliance standards that organizations use during procurement that focus on enterprise security; conversely, relatively few focus on product security. This guide bridges that gap by offering resources organizations can leverage to assess product security maturity and whether a manufacturer follows secure by design principles.

Organizations can integrate product security considerations into various stages of the procurement lifecycle:

- **Before procurement,** by posing questions to understand each candidate software manufacturer's approach to product security.
- **During procurement,** by integrating product security requirements into contract language, as appropriate.
- **Following procurement,** by continually assessing software manufacturers' product security and security outcomes.

Below are questions that organizations can use as a starting point for assessing a software manufacturer's approach to product security. These questions are informed by the threat landscape we observe at CISA and are categorized by sets of actions that, if done correctly by software manufacturers, will drive down exploitable defects and misconfigurations. Customer organizations can also use this guidance in procurement discussions with third party resellers or service providers. For further guidance, CISA encourages organizations to read CISA's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force's Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle, the Minimum Viable Secure Product, and CISA's Secure by Design Pledge.

Software Manufacturer Questions

Customers should ask the following questions of their software manufacturers to understand the extent to which the manufacturer has designed the product with security in mind and to ensure quality and positive customer security outcomes.

General Questions

- Has the manufacturer taken CISA's Secure by Design Pledge? What progress reports has the manufacturer published in line with its commitments to the pledge?
- How does the manufacturer make it simple for customers to install **security patches**? Does it offer support for security patches on a widespread basis and enable functionality for automatic updates?

Why this is important: *a company that has made the Pledge has publicly committed to take and demonstrate steps towards producing software that is secure by design. In addition to helping secure the products you use, these commitments will help protect all Americans by securing the technology upon which our critical infrastructure relies.*

Artifacts you can collect from a software manufacturer:

- A Software Bill of Materials (SBOM) that lists third-party software components used by the product.
- Roadmaps that highlight how the manufacturer plans to eliminate classes of vulnerability, such as a memory safe roadmap.

Artifacts you can collect yourself:

- Whether the software manufacturer includes basic security features, like logging and single sign-on (SSO), in the baseline version of the product.
- Whether the software manufacturer operates a vulnerability disclosure policy (which should be a public webpage).
- Whether the software manufacturer files timely and correct Common Vulnerabilities and Exposures (CVE) records.
- Whether the software manufacturer has taken CISA's Secure by Design Pledge, and any progress reports published by the software manufacturer showing actions taken.

Authentication

The product should support **secure authentication**.

- Does the manufacturer support integrating standards-based **single sign-on (SSO)** for customers at no additional cost?
- If the software manufacturer manages authentication, does it enable **multi-factor authentication (MFA)** or other phishing-resistant forms of authentication like **passkeys** by default, and at no cost?
- Has the software manufacturer **eliminated default passwords** in its products? If not, is it working to reduce the use of default passwords across its product lines?

Why this is important: *Default passwords, which CISA defines as universally shared passwords that are present by default across a product, continue to enable malicious cyber activity. Default passwords should be replaced with more secure authentication mechanisms, such as random, instance-unique passwords. Additionally, MFA is the greatest defense against password-based attacks, such as credential stuffing and password theft. Any form of MFA has been shown to significantly reduce the success of such activity, with more secure forms of MFA, like phishing-resistant MFA, offering even more protection against targeted activity.*

Eliminating Classes of Vulnerability

The software manufacturer should systematically **address entire classes of software defects** across its products.

- What **classes of vulnerability** has the software manufacturer systematically addressed in their products?
- For those that they haven't yet addressed, do they have a **roadmap** showing how they plan to eliminate those classes of vulnerability? The following tactics are in line with a healthy secure development process:
  - Consistently enforcing the use of parametrized queries to prevent SQL injection attacks.
  - Adopting web template frameworks with built-in protection against cross-site scripting vulnerabilities.
  - Transitioning code to memory safe languages in a prioritized approach and writing new products in memory safe languages.
  - Providing secure defaults for developers, such as by providing "building blocks" of secure functions and libraries that make it impossible (or significantly more difficult) to introduce a certain class of vulnerability.

Why this is important: *The vast majority of exploited vulnerabilities today are due to classes of vulnerability (or product defects) that can be prevented at scale. Software manufacturers can reduce risk for their customers by working to prevent and eliminate classes of vulnerability across their products.*

Evidence of Intrusions

Software manufacturers should make available **security logs** to customers in the baseline version of the product. For cloud service providers and software as a service (SaaS) providers, the software manufacturer should retain and make available to customers security logs for at least six months at no additional charge. Logs should cover areas such as:

- Configuration changes or reading configuration settings;
- Identity (e.g., sign-in and token creation) and network flows, if applicable; and
- Data access or creation of business-relevant data.

Why this is important: *It is essential that organizations have the ability to detect cybersecurity incidents that have occurred and understand what has happened. Software manufacturers can enable their customers to do so by providing artifacts and capabilities to gather evidence of intrusions, such as a customer's audit logs. In doing so, software manufacturers embody the secure by design principle of taking ownership of their customers' security outcomes.*

Software Supply Chain Security

The software manufacturer should **maintain and share provenance data of third-party** dependencies and have processes to **govern its use of, and contributions to, open source software components.**

- Does the manufacturer generate a software bill of materials (SBOM) in a standard, machine-readable format and make this available to customers? Does the SBOM enumerate all third-party dependencies, including open source software components?
- How does the software manufacturer vet the security **of open source software components it incorporates** and **facilitate contributions back** to help sustain those open source projects? Does the software manufacturer have an established process to do so, such as through an open source program office (OSPO)?

Why this is important: *Software manufacturers should treat the security of their third-party dependencies as an extension of their own security. To that end, software manufacturers should continually maintain provenance data of their dependencies, share this with their customers, and establish processes (such as through an OSPO) to govern their use of, and contributions to, open source software components.*

Vulnerability Disclosure and Reporting

The software manufacturer should demonstrate transparency and timeliness in **vulnerability reporting for both on-premises and cloud products.**

- Does the software manufacturer include accurate **Common Weakness Enumeration (CWE)** and **Common Platform Enumeration (CPE)** fields in every CVE record for the software manufacturer's products?
- Has the software manufacturer published a **vulnerability disclosure policy** that authorizes testing by members of the public on products offered by the software manufacturer?

Why this is important: *In addition to serving as a standardized way to communicate actions that customers should take to protect against vulnerabilities; timely, correct, and complete CVE records allow for public transparency in vulnerability trends over time. This benefits both individual companies and their customers, and the software industry more generally, allowing software developers to better understand the most pressing classes of vulnerability. We note that issuing of CVEs is valuable even for SaaS products, while acknowledging that this is only now starting to become more standard practice. Coordinated vulnerability disclosure has emerged as a mutually beneficial norm for engaging with security researchers. Software manufacturers who establish a vulnerability disclosure policy benefit from receiving help from the security research community that can allow them to better secure their products. Security researchers receive authorization for testing under the policy, in addition to a clear channel to report vulnerabilities.*

Where to go for Further Information

This guidance serves as a starting point for software customers to generate the demand for more secure technology products. For more information, visit CISA's Secure by Design page to read our white paper, blogs, and alerts. The ICT SCRM Task Force's Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the C-SCRM Lifecycle, the Minimum Viable Secure Product, our Secure by Design Pledge, and NIST's Secure Software Development Framework contain additional measures that customers can leverage during procurement. We also encourage you to engage with your regional Cybersecurity Advisor and us at SecureByDesign@cisa.dhs.gov.