Your Guide to Secure by Design and Data Protection

Contents

Introduction	3
Origins of Secure by Design	3
Security Standards	4
CISA's Promotion of Secure by Design	5
The Secure by Design Pledge	6
Secure by Design Principles	7
Secure by Design Tactics	9
CISA Secure by Design Pledge Principles and Tactics	10
Secure by Design for Data Backup and Recovery Environments	11
Benefits of Secure by Design	12
Final Thoughts	13

Introduction

Secure by Design is a strategy in the software industry that continues to gain traction over time. To counter the growing cyberthreats and cyberattacks, it just makes sense for organizations and software developers to improve the security of their software and to ensure their software development, functionality, and deployments are safer. Secure by Design shifts the focus from reactive security measures to building security into the digital asset, software, system, application, and of course data environments.

With more industry awareness about security, Secure by Design adoption has grown, and it emphasizes architecture considerations to build more secure systems from the start of the software development process.

Origins of Secure by Design

Secure by Design has gained significant traction in recent years in part due to a more educated professional workforce in the security space, paired with the increased need to respond to growing cyberthreats. Some industries, such as Financial Services, have been at the forefront of cybersecurity, and have recognized that security must be a key requirement and prerequisite on every software or system.

Another reason to think about adopting Secure by Design has been the growing disclosure of vulnerabilities in all software, including open source components that are widely used. Once a vulnerability is disclosed, organizations must react and apply fixes via patches. Why not prevent all of that in the first place by exploring ways to integrate security during and into the development lifecycle?

Going back in history, one of the earliest attempts to formalize secure system design came from the U.S. Department of Defense (DoD) in 1983, when the DoD introduced the Trusted Computer System Evaluation Criteria (TCSEC), commonly referred to as the "Orange Book," because of the color of its cover. US government systems followed the Orange Book for a couple of decades. This TCSEC and newer security standards set guidelines for building systems with security features from the start. It clearly marked an acknowledgment that security must be intrinsic from the design phase.

Security Standards

While the Orange Book was followed for a long time in the US, a number of newer standards have been created by a variety of global organizations. They continue to be relevant and are key elements of security audits and certifications. Here is a brief list of the most common standards:

Common Criteria (CC)

A standardized framework for evaluating the security of information technology products and systems.

National Institute of Standards and Technology (NIST) Standards

Provides a structured approach to managing risk in US federal information systems, focusing on security controls and continuous monitoring.

Center for Internet Security (CIS) Controls

A set of cybersecurity best practices designed to mitigate the most prevalent cyberthreats.

ISO/IEC 27001

It focuses on maintaining the confidentiality, integrity, and availability of information through a systematic risk management approach.

Payment Card Industry Data Security Standard (PCI DSS)

A security standard to ensure the security of card payment data.

Health Information Trust Alliance (HITRUST) CSF

Certifiable framework that integrates various standards, including ISO 27001, NIST, HIPAA, and others, to create a comprehensive security framework tailored to healthcare organizations.

CISA's Promotion of Secure by Design

The Cybersecurity and Infrastructure Security Agency's (CISA) involvement in the initiative can be traced back to its establishment in 2018, when it was tasked with protecting critical infrastructure and promoting cybersecurity across the United States. Recognizing the importance of proactive security measures, CISA began to emphasize the need for organizations to adopt a Secure by Design approach.

CISA has played an important role in promoting and advancing the Secure by Design initiative, aiming to integrate security into the development lifecycle and deployment of products and systems by raising awareness, providing guidance, and fostering collaboration among industry stakeholders.

Recognizing the importance of proactive security measures, CISA began to highlight the need for organizations to adopt a Secure by Design approach.

Some of the activities driven by CISA include the development of guidance and frameworks for implementing Secure by Design principles that go from threat modeling to secure coding practices and vulnerability management. CISA has also facilitated collaboration among industry stakeholders, government agencies, and academia to promote the adoption of Secure by Design.

Promoting awareness has been CISA's largest initiative. CISA has conducted outreach campaigns to raise awareness of the benefits of Secure by Design and encourage organizations to adopt this approach. To encourage participation among organizations, CISA created the Secure by Design Pledge.

The Secure by Design Pledge

The Secure by Design Pledge is a voluntary pledge focused on enterprise software products and services, covering on-premises software, cloud services, and software as a service (SaaS). By participating in the pledge, software manufacturers commit to making a good-faith effort toward secure by design goal.

Organizations should document measurable progress toward security goals within one year of signing the pledge. For those unable to make measurable progress, the recommendation is to share with CISA their efforts and any challenges they faced within the same timeframe. In line with the principle of transparency, manufacturers are encouraged to publicly share their approach to help others in the industry learn from their experience.

The pledge is designed to complement and enhance existing software security best practices, including those developed by CISA, NIST, other federal agencies, and global industry standards.

Veeam Software is one of many organizations that have committed to the Secure by Design pledge. The pledge reinforces these organizations including Veeam's dedication to embedding security at every phase of the development process for products and services.

Secure by Design Principles

CISA, in collaboration with the National Security Agency (NSA), the Federal Bureau of Investigations (FBI) and the following international agencies, collaborated in the publication of "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default" a guide for Secure by Design with recommendations for software manufacturers. They include:

- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- Germany's Federal Office for Information Security (BSI)
- Netherlands' National Cyber Security Centre (NCSC-NL)
- Computer Emergency Response Team New Zealand (CERT NZ) and New Zealand's National Cyber Security Centre (NCSC-NZ)

Because the principles are not dictated or exclusive to CISA's guidance, there are a number of use cases and adaptations with regards to Secure by Design principles. The goal is to make sure software and systems are secure at every step of the development and implementation lifecycle, including secured architecture and features. The following list covers diverse opinions and publications related to the core principles:

Security requirements

First, incorporate security into requirements before software development and deployment. Integrate security considerations into the initial stages of the development process, from access controls to granular access and security in components.

Secure coding practices

Follow best practices for secure coding to prevent vulnerabilities in the software. All inputs to software or a system should be validated to prevent injection attacks, buffer overflows, cross-site scripting, code execution, and other vulnerabilities. Automate security scans during the development lifecycle and address all critical and high-severity vulnerabilities. Use secure coding standards and code reviews. Developers should be trained to follow secure coding practices to minimize vulnerabilities in the code.

Vulnerability management

Implement a program and tooling to identify, assess, track, prioritize, and remediate vulnerabilities in a timely manner. Use automated tools to continuously test for vulnerabilities throughout the development lifecycle. Keep up with the latest patches of all software including open source components and library dependencies.

Threat modeling and risk assessment

Threat modeling is a structured process to identify, analyze, and prioritize potential security threats. It involves identifying critical assets, potential attackers, and vulnerabilities, then assessing the likelihood and impact of each threat. Risk assessment is the process of evaluating and prioritizing potential risks based on their likelihood and impact. Use tailored threat modeling and risk assessment at every stage of the product or system development lifecycle.

Secure defaults

Design software and systems with secure default configurations to minimize vulnerabilities. Systems should be designed in such a way that if something fails, it should default to a secure state ensuring that do not expose sensitive data or leave software open to exploitation. Default settings should prioritize security without requiring user intervention. Ensure passwords have strong default complexity requirements.

Multiple layers of defense

Implement multiple layers of security controls to protect against potential attacks and vulnerabilities. If one control or layer fails, others are still in place to prevent intrusion. This includes the use of multifactor authentication (MFA), firewalls, network security, intrusion detection systems, API security, data access controls, and encryption of data.

Encryption and data protection

Safeguard all your data, especially sensitive data from unauthorized access both at rest and in transit. Use strong encryption and other data protection measures such as Veeam Data Platform — which complements data encryption by controlling data access, detecting malware and anomalies to prevent data loss. Together, encryption and data protection ensure confidentiality, integrity, and availability of sensitive data, protecting against cyberthreats and maintaining regulatory compliance.

Least privilege

Every component, whether user or system, should have only the minimum levels of access necessary to perform its function. This reduces the risk of unauthorized access and in the case of a breach, limits spreading throughout a network or system. Only grant administrative privileges to users who absolutely need them and restrict system access to essential functionalities.

Continuous monitoring and logging

Implement monitoring, error handling, and logging mechanisms to detect, respond to, and analyze suspicious or abnormal events or potential security incidents. Ensure logs are securely stored and regularly reviewed. Use SIEM tools to collect and analyze log data in real-time and detect anomalies that may indicate security incidents.

Security education and awareness

Educating developers to apply security best practices including knowledge of the OWASP top 10 for the most critical security risks in web applications is a critical step to secure by design. Users should have knowledge of how to protect sensitive information and systems. Training should include regular security awareness sessions, where users learn about various threats such as phishing, smishing, and social engineering.

The essence of Secure by Design lies in incorporating security principles into the very architecture and deployment of a system, ensuring that it remains robust even under attack.

Secure by Design Tactics

Now that we know about the Secure by Design Principles, let's talk about tactics to implement those principles. The Secure Software Development Framework (SSDF), or NIST's SP 800-218, outlines secure development practices to integrate into each stage of the software development lifecycle. Adopting these practices helps organizations detect vulnerabilities, mitigate risks, and prevent cyberattacks.

Memory safe languages

Use memory safe languages like C#, Rust, and Go, and replace legacy code written in C and C++ which provide freedom in memory management, this in turn results in exploitable vulnerabilities.

Secure hardware foundation

Use fine-grained memory protection architectures, such as those describe by Capability Hardware Enhanced RISC Instructions (CHERI).

Secure software components

Use secured commercial, third party, and open source components to reinforce product security. Release cadence, vulnerability disclosure, and patch delivery are good indicators of secured components.

Parameterized queries

Employ parameterized queries to prevent SQL injection attacks.

SAST, SCA, and DAST tools

Regularly analyze code for flaws and vulnerabilities by integrating static analysis software testing (SAST), software composition analysis (SCA) and dynamic analysis software testing (DAST) tools. These tools scan code bases and applications for known vulnerabilities.

Code review

Implement peer review for quality control.

Software Bill of Materials (SBOM)

Generate SBOMs of all your software and systems to enhance visibility into product components. An important asset to help with identifying software that needs to be patched due to vulnerabilities.

Vulnerability disclosure

Organizations should report documented vulnerabilities and fixes to improve secure for all.

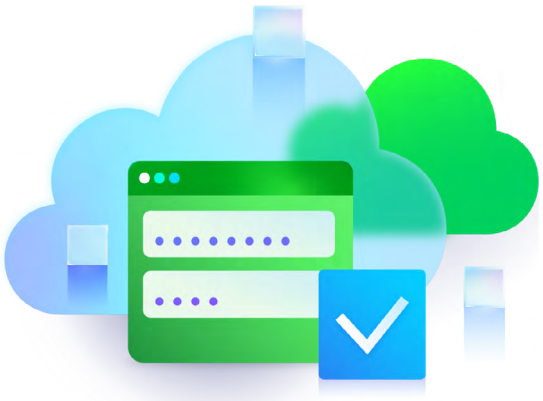
Organizations are encouraged to prioritize these tactics for new software and incrementally to legacy codebases.

CISA Secure by Design Pledge Principles and Tactics

Having reviewed the different secure by design principles and tactics, the following principles only cover the goals outlined in the Secure by Design pledge:

- Increasing the use of multi-factor authentication (MFA)
- Reducing the use of default passwords
- Reducing entire classes of vulnerability
- Increasing security patch installation by customers
- Publishing a vulnerability disclosure policy
- Demonstrating transparency in vulnerability public disclosure
- Demonstrating an increase in your customers' ability to gather evidence of cyber intrusions

All companies offering software products should commit to the pledge.



Secure by Design for Data Backup and Recovery Environments

Integrating the foundational elements of Secure by Design principles into backup and recovery platforms and environments emphasizes a resilient approach to data protection by aligning with the core principles of information security — Confidentiality, Integrity, and Availability (the CIA triad).

Confidentiality requires organizations to secure backup data from unauthorized access and data exfiltration. Integrity focuses on preventing ransomware and other cyberthreats from corrupting or encrypting data, ensuring that data remains accurate and intact. Availability is critical for maintaining robust systems that can withstand outages or cyberattacks, and supporting rapid restoration of services and data post-incident.

Incorporating Secure by Design principles further strengthens backup and recovery environments by applying **timely patches and vulnerability management**, as well as **secure default configurations** to minimize vulnerabilities and attacks. Applying **multiple layers of defense** including MFA, **least-privilege** access controls, and regular auditing of backup access logs reduces the risk of malicious insider actions or external attacks on backup data.

By nature, backup and recovery environments are about **data encryption and data protection**, the goal is to have all the necessary capabilities to safeguard all your data, especially sensitive data from unauthorized access.

Backup and recovery environments secure by design should also include testing recovery processes and verifying backup integrity to ensure rapid recovery. By embedding these Secure by Design principles, organizations build a robust and resilient data protection strategy.

Benefits of Secure by Design

By incorporating Secure by Design principles, organizations significantly improve their security posture. Integrated security measures minimize system and application vulnerabilities, reducing exploitable flaws and weaknesses. This proactive approach enhances overall security posture, shielding against data breaches, financial losses, and reputational damage.

Financial benefits

- **Cost savings:** Early security integration reduces remediation expenses.
- **Decreased maintenance:** Secure designs simplify maintenance and updates.
- **Reduced downtime:** Minimized disruptions enhance productivity.
- **Protect intellectual property:** Secure software and operation protects key data from organizations including intellectual property.

Operational benefits

- **Improved customer experience:** Secure systems ensure reliability and uptime.
- **Increased trust:** Demonstrated security commitment builds confidence in customers, trust that private information is secured.
- **Customer trust:** Enhances customer trust and loyalty.
- **Competitive advantage:** Differentiates organizations through robust security.

Legal, regulatory, and compliance benefits

- **Enhanced compliance:** Aligns with standards and regulations like ISO/IEC 27001, PCI DSS, HIPAA, and more.
- **Simplified auditing:** Demonstrates security commitment with auditing and compliance reporting.
- **Risk reductions:** Reduces risk of non-compliance penalties.

Additional benefits

- Enhanced customer data protection
- Improved incident response
- Streamlined security updates
- Better resource allocation
- Proactive risk management

By integrating Secure by Design principles, organizations prioritize security, reduce risks, and optimize operations, ultimately driving success and safeguarding customer information.

Final Thoughts

As cyberthreats intensify, Secure by Design has become an essential part of any organization's digital strategy, covering software development lifecycle, security features, and secure implementations.

With the rise of new technologies from autonomous vehicles to cloud based services, Internet of Things (IoT), and of course, artificial intelligence (AI), everything is being driven by software and systems, all generating and keeping large amounts of data and all interconnected. Understanding and following the Secure by Design principles and tactics are more important than ever.

Looking ahead, we can expect Secure by Design principles to be further refined and expanded, especially as regulatory requirements increase across countries and industries. Secure by Design enables compliance with standards and regulations including PCIDSS, GDPR, HIPAA, SOX, DORA, and many others.

There are recent major initiatives such as the European Union's Cyber Resilience Act which further emphasizes the importance of Secure by Design. The Act requires manufacturers to implement security measures throughout a product's lifecycle to prevent the introduction of vulnerable products into the market.

Another example of a major global initiative is CISA's recently launched International Strategic plan where a key goal is to promoting a secure digital ecosystem. This objective seeks to promote security practices and digital infrastructure that are both secure and resilient, aligning global digital ecosystems with principles of Secure by Design.

Overall, Secure by Design principles integrated into each development phase empower organizations to protect their digital assets and enhance resilience, laying a proactive groundwork for secure, and compliant organizations.

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes every business should control all their data whenever and wherever they need it. We're obsessed with creating innovative ways to help our customers achieve data resilience. We do that by offering purpose-built solutions that provide data backup, data recovery, data data portability, data security, and data intelligence. Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

Latest Release:
New Veeam Data Platform

Powerful Data Resilience to Keep Your Business Running