Acronis

Closing the supply chain security gap: SSDLC evaluation checklist

Supply chain attacks are among the most critical and difficult cybersecurity threats to defend against. The SolarWinds, Polyfill.io, 3CX and MOVEit attacks demonstrated how targeting software suppliers enabled attackers to compromise entire industries at scale.

30%

of all breaches in 2024 now involve a third party, up 15% since 2023[1]

Traditional supplier evaluations focus on financial health and infrastructure security, but they miss where most vulnerabilities originate: the software development process.

The hidden vulnerability: Software development process

History-making supply chain attacks

Company	Industry	Date	Impact
Polyfill.io	Content delivery network (CDN)	2024	Thousands of websites affected
3CX	VoIP services	2023	Thousands of enterprises affected
MOVEit	File transfer	2023	2,000+ organizations affected
SolarWinds	IT software	2020	18,000+ organizations compromised

Security controls at runtime cannot retroactively fix insecure code. If vulnerabilities are introduced during design or coding, customers wait for vendors to patch while remaining exposed.

The secure software development life cycle (SSDLC) incorporates security into every stage of software development, from design to post-release maintenance.

How to evaluate software development

Evidence-based assurance requires evaluation across six dimensions:

Governance and policy:

Documented policies, formal security roles and executive oversight.

Risk management and design:

Threat modeling, security requirements and design assessments.

Implementation practices:

Developer training, secure coding standards and code review.

Verification and validation:

Automated testing, penetration testing and third-party validation.

Release and deployment:

Hardened pipelines, code signing and environment segregation.

Maintenance and monitoring:

Vulnerability disclosure, patching timelines and customer notifications.

Acronis: Certified SSDLC excellence

Acronis demonstrates SSDLC leadership through independently verified certifications:

IEC 62443-4-1
Secure product development for OT environments

ISO/IEC 27001
Information security management

ISO/IEC 27017/27018
Cloud service security and privacy

CSA STAR Level 2
Independent cloud security assessment

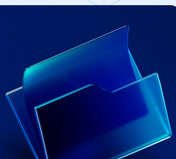
These certifications are rare and difficult to obtain.

IEC 62443-4-1 represents the gold standard for secure product development in industrial environments, validating that Acronis products are engineered with security at their core. OT customers and partners can be confident that Acronis solutions reduce their supply chain risk and simplify compliance across NIS 2, DORA and other regulations.

IEC 62443-4-1 CERTIFIED

Learn more

Strengthen your supply chain security with Acronis' certified approach:



- View Acronis IEC 62443-4-1 certification
- Read the full SSDLC white paper
- Explore Acronis cyber protection solutions
- Schedule a 1-on-1 consultation with an Acronis solutions engineer

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses. Learn more at www.acronis.com

[1] Verizon. "2025 Data Breach Investigations Report."