WHITE PAPER

Cybersecurity in the Supply Chain

Best Practices and Solutions

SOPHOS

Introduction

The cyber threat landscape facing companies and public authorities is more serious and diverse than ever. Increasingly, attacks targeting the supply chains of both private and public organizations are presenting a greater risk to their cybersecurity. Managing supply chain risks is an essential part of all modern risk management programs and in many cases is legally mandated.

This guide will explain risks associated with supply chains, map out current legal requirements, outline best practices for cybersecurity management in the supply chain, and provide information on how Sophos products and services can support you in these efforts.

Cybersecurity risks in modern supply chains

Across the globe, the risks associated with cyberattacks have intensified significantly in recent years. The number of organizations that have become victim to a successful cyberattack is increasing rapidly. Likewise, the damage organizations suffer as a result of such incidents continues to rise — whether through revenue loss caused by production line stoppages or the often substantial costs of investigation and remediation. The question is no longer if a company will experience a cyberattack, but when.

The European Union Agency for Cybersecurity (ENISA) recently highlighted the potential threat arising from cyberattacks in the supply chain.[1] The agency noted that attacks on supply chains are increasing in volume and complexity. A study of selected cyberattacks showed that in almost two-thirds of the attacks, trust of customers in their suppliers was a contributing factor. ENISA strongly advises companies to review their cybersecurity mechanisms considering the risk of cyberattacks in the supply chain and to update them if necessary.

A further potential source of risks is the insufficient management of cybersecurity in the supply chain. According to a new survey by TÜV, a German technical service company, only a third of surveyed companies impose cybersecurity requirements on their suppliers and most suppliers are under no formal obligation to secure their systems. Worse, 83% of the companies surveyed do not carry out cybersecurity audits of their suppliers at all.[2]

83%

Of companies surveyed by TÜV recently who said they did not carry out any kind of cybersecurity audit.

Against this background, legal requirements for cybersecurity are becoming more stringent. Organizations are increasingly required by law to take targeted IT security measures, particularly within their supply chains.

Why supply chain cybersecurity matters

Ensuring cybersecurity in the supply chain is not an end in itself but lies in the best interest of every organization, public or private. Cybersecurity incidents in the supply chain can have immediate and severe consequences. In the manufacturing sector, for example, an IT failure at a supplier can interrupt operations, especially in just-in-time production environments.

In the worst-case scenario, a cybersecurity incident — such as a ransomware attack — at a cloud or IT service provider can lead to the failure of an organization's entire IT infrastructure, potentially forcing a temporary shutdown of operations. In addition to financial losses, there is the risk of reputational damage if the incident becomes public, even when it originates from a supplier or partner. Furthermore, inadequate oversight of supply chain cybersecurity may lead to regulatory sanctions, particularly as laws increasingly hold organizations accountable for third-party risks.

Potential effects of a cybersecurity incident targeting a supply chain supplier:

- Failure of the entire IT infrastructure.
- Temporary shutdown of operations.
- Financial losses.
- Reputational damage.
- Regulatory sanctions.

Legal requirements

A legal obligation to ensure cybersecurity in the supply chain arises from a range of legal acts — some explicit, others implied by their wording and intent.

Across the globe, governments and regulators are recognizing that cybersecurity is fundamental to economic stability, innovation, and public trust. As digital ecosystems become increasingly interconnected, legislation is evolving to strengthen resilience and transparency across entire supply chains. From data protection and operational resilience to software integrity and critical infrastructure security, these regulatory efforts share a common goal: ensuring that organizations manage third-party risks responsibly and maintain oversight of their extended digital networks. This reflects an international movement toward greater accountability and standardized security expectations across borders.

While the specific frameworks differ between regions, their underlying principles are becoming more closely aligned. In Europe, regulations such as the NIS2 Directive, the Digital Operational Resilience Act (DORA), and the Cyber Resilience Act (CRA) set clear expectations for governance, reporting, and supply chain assurance. North American frameworks, including NIST's Cybersecurity Supply Chain Risk Management (C-SCRM) guidelines and recent federal executive orders on software security, pursue similar objectives. In Asia-Pacific, countries such as Japan, Singapore, and Australia have advanced national cybersecurity strategies emphasizing supply

chain integrity, critical infrastructure protection, and regional cooperation. Meanwhile, emerging legislation across Africa, the Middle East, and Latin America increasingly mirrors these principles, underscoring a global drive toward consistent and transparent cybersecurity standards.

For internationally operating organizations, this growing regulatory convergence highlights the importance of establishing clear governance structures and unified risk management frameworks that meet multiple jurisdictions' requirements. Building a comprehensive understanding of regional obligations — while aligning policies, documentation, and vendor management processes — enables organizations to demonstrate compliance efficiently and foster trust with partners, regulators, and customers alike. As global expectations continue to evolve, maintaining adaptability and visibility across complex supply chains will be key to achieving long-term compliance and resilience.

Best practices for defending against supply chain attacks

Given the complexity and nature of supply chain attacks, technology alone can't prevent them. Instead, these best practice guidelines are intended to enable you to minimize the risk associated with a supply chain attack.

1 Shift from a reactive to a proactive approach to cybersecurity

Recent supply chain incidents involving NPM and SaaS platforms such as SalesLoft underscore a hard truth for today's organizations: cybersecurity can no longer be reactive. In both cases, attackers exploited trusted software components and authorized integrations to gain access quietly, without triggering immediate alarms. By the time the activity was detected, sensitive data had already been exposed across hundreds of organizations.

This risk is being amplified by the rapid adoption of AI. Agentic AI systems and emerging protocols such as Model Context Protocol (MCP) depend on broad, automated access to data, APIs, and third-party services, often operating beyond traditional visibility and control mechanisms. While these capabilities enable scale and speed, they also expand the attack surface and complicate governance. As a result, organizations must adopt a proactive security mindset — continuously validating trust across both their software supply chain and AI-driven workflows. We will explore the technologies and services that enable this proactive approach later in this paper.

2 Monitor for early signs of compromise

During investigations conducted by the Sophos Managed Detection and Response (MDR) team, two things stand out as early indicators of compromise: The use of credentials for remote access and administrative purposes during off hours and the abuse of system administration tools to conduct surveillance and steal data from the network.

The use of legitimate accounts and your own tools to gain and retain persistence is often referred to as "living-off-the-land" (LoL). Detecting these behaviors requires vigilance and skill. However, they stand out clearly to a trained security operations analyst, alerting you to the attack before the bulk of the damage has been done. You should either invest in the technology and training needed to monitor for these indicators in-house or engage an MDR service provider to monitor on your behalf.

3 Conduct an audit of your supply chain

Conducting a structured audit of your supply chain is a foundational step in managing cyber risk. This begins with building a clear inventory of all third parties, vendors, and partners your organization depends on — often more than expected. Organizations should then evaluate suppliers in the context of their business relationship and access levels. Key considerations include the criticality of each supplier to operations, the sensitivity of the data shared (such as PII or intellectual property), and the organization's ability to continue operating if that supplier is disrupted or compromised. You can expect to be connected to third-party suppliers such as:

IT service providers	**Professional services**	**Suppliers**
MSP/MSSP	HR	Materials
Cloud providers	Finance	Services
	Legal	Labor
	Security	Logistics
	Janitorial	

Once you have a clear view of your third-party connections, the next step is to review how those organizations authenticate and what level of access their credentials provide, including the systems or data those credentials can reach. This includes evaluating the use of multi-factor authentication for user access, as well as the management of non-human credentials such as API keys and access tokens.

Practices such as API key rotation — the regular replacement and revocation of keys used by integrations and automated services — help limit the risk posed by long-lived credentials. Where access exceeds what is required for the business relationship, it should be reduced and constrained to the minimum necessary, with priority given to integrations that have broad or persistent access.

4 Assess the security posture of your suppliers and business partners

There are many approaches to making an assessment, but one popular approach for large service providers, cloud operators, and payment processors is to determine what types of certifications and audits they are subject to.

For example, a payment processor will be subject to compliance with PCI DSS. If they are subject to PCI DSS level 1 or 2, you should request their report on compliance (RoC) issued by their QSA/ISA. You should review these RoCs on a quarterly basis to ensure they are meeting your expectations.

Another popular certification to confirm audits is SOC 2/2+/3 for your cloud service providers. SOC audits assess security controls and mitigations covering five Trust Service Principals: privacy, security, availability, processing integrity, and confidentiality.

Just as with an organization's own security posture, no single audit or assessment can provide absolute assurance, but it can indicate how seriously a supplier approaches security and compliance. In addition to formal audits, organizations may consider requesting evidence of independent security testing, such as penetration test reports.

Other useful signals include how transparently a supplier communicates about security issues — for example, whether they publish security advisories or release notes for patches, disclose vulnerabilities through CVEs, or provide post-incident communications such as root cause analyses. For publicly traded companies, regulatory filings may also offer insight into how security incidents are disclosed and addressed.

5 Continuously review your own IT security operations hygiene

While the posture of your suppliers is critical in safeguarding against supply chain attacks, do not neglect your own cybersecurity hygiene. Many organizations ignore it either because they didn't know where to start or they believed they weren't important enough to be targeted through the compromise of a trusted partner. Your cybersecurity practices could mean the difference between a mild inconvenience and a catastrophic data breach.

- Enable multi-factor authentication (MFA) where remote access is granted.
- Automate rotation of API keys for sensitive applications.
- Move away from providing suppliers with VPN access and adopt Zero Trust Network Access (ZTNA) as an alternative.
- Review supplier access and application privileges.
- Request SBOMs (Software Bill of Materials) from software and hardware suppliers and refresh annually.
- Proactively monitor supplier security bulletins.
- Review your cybersecurity insurance policy (if you have it).

How Sophos solutions protect against supply chain attacks

Sophos Endpoint

Sophos Endpoint provides critical protection against supply chain attacks through a comprehensive, prevention-first approach to security that blocks threats across every device, reducing pressure on stretched IT teams. The unique CryptoGuard capability automatically detects and rolls back unauthorized file encryption, even when adversaries have breached the network and bypassed other organizational defenses by compromising the supply chain.

Powerful endpoint detection and response functionality (EDR) adds further assurance by enabling teams to identify, investigate, and respond to suspicious activity across endpoints and servers. Sophos Extended Detection and Response (XDR) extends this visibility across the entire attack surface, with turnkey integrations with an extensive ecosystem of tools and technologies.

Collectively, these capabilities limit the blast radius of a compromise within the supply chain and prevent a single foothold from escalating into a wider incident.

Learn more about Sophos Endpoint

Sophos MDR

Sophos Managed Detection and Response (MDR) is a service delivered by a global team of cybersecurity experts who monitor environments for threats around the clock, including supply chain attacks. Expert analysts continuously monitor, investigate, and respond to suspicious activity, taking immediate, human-led actions to stop and remediate confirmed threats.

Sophos employs hundreds of global security analysts across nine regional hubs, enabling rapid containment and remediation with an industry-leading average response time of just 38 minutes, which is 96% faster than the industry benchmark for in-house SOC teams. This level of support is particularly valuable in supply chain attacks, where adversaries often enter through trusted software, services, or credentials and can remain hidden for long periods.

With 32% of ransomware attacks beginning with exploited vulnerabilities and nearly a quarter (23%) starting with compromised credentials, the ability to identify subtle anomalies is critical. Sophos analysts perform proactive threat hunts to detect adversarial behaviors that only a human can identify, providing essential protection against the concealed lateral movement and stealthy techniques typical of supply chain compromises.

Learn more about Sophos MDR

Case study: Stopping a supply chain email compromise attack (Sophos MDR)

Attack. An adversary group breached the email system of a legitimate supplier and used a compromised email account to create a phishing campaign hosted on Dropbox. The phishing email included a malicious PDF designed to capture the Microsoft 365 credentials and MFA token of one of their client's employees. Multiple email security controls failed to detect the threat, allowing the targeted employee to open the attachment and unknowingly provide their login details.

Detection. The supplier's client was protected by Sophos MDR which identified suspicious Microsoft 365 login activity based on an unusual user agent string, suggesting a potential session compromise. The Sophos MDR team investigated, using the client's Microsoft 365 Management Activity telemetry ingested by the Sophos platform. By comparing the detected behavior with the employee's normal login patterns, Sophos analysts quickly identified the behavior as anomalous.

Remediation. A Sophos MDR analyst terminated active sessions on the client's behalf and advised them to reset credentials and review their MFA. Once the client applied these steps, the account was fully secured, preventing the adversary from progressing beyond initial access.

With Sophos MDR

Attack detected and blocked immediately.

Without Sophos MDR

42GB of data exfiltrated, widespread encryption, and a demanded ransom payment.

Case study: Thwarting a supply chain attack through a compromised MSP tool (Sophos MDR and Sophos Endpoint)

Attack. Adversaries exploited three unpatched vulnerabilities in the SimpleHelp tool to access a Managed Service Provider's (MSP) cloud-based remote monitoring and management (RMM) console. Once inside, the attackers used existing SimpleHelp agents installed on the MSP's customers' networks to push malicious activity. The MSP itself was not compromised because it did not use the SimpleHelp agent on its own devices.

Client using Sophos. Among the MSP's customers, the difference in outcomes was stark. A customer using Sophos MDR and Sophos Endpoint saw the attack detected immediately when suspicious installer activity appeared. Attempts by the adversary to disable Sophos Endpoint failed due to tamper protection, and the Sophos MDR team neutralized the threat with zero data extracted and zero devices encrypted. Application Control in Sophos Endpoint was used to block the attacker's tools and cut off their access.

Client not using Sophos. The MSP's customers without Sophos protection were far less fortunate. One suffered 42GB of data exfiltration, widespread encryption, and a ransom demand before engaging the Sophos Emergency Incident Response team, who ultimately removed the adversary. The contrast highlights how significantly outcomes improve when Sophos MDR and Sophos Endpoint are in place, particularly in supply chain style attacks delivered through trusted tools.

Learn more about this incident

Conclusion

The threat landscape has evolved, and supply chain compromise is an issue for all organizations, large and small. We're all targets in someone's supply chain — and it's never been more important to minimize third-party supply chain risk. By following the guidelines in this paper, you can reduce your risk of falling victim to an attack and prevent an attack from significantly impacting your business:

1. Shift from a reactive to a proactive approach to cybersecurity.
2. Monitor for early signs of compromise.
3. Conduct an audit of your supply chain.
4. Assess the security posture of your suppliers and business partners.
5. Constantly review your own IT security operations hygiene.

In addition, consider adopting technologies and services such as EDR, XDR, MDR, and ZTNA to support your supply chain security objectives.

A proactive approach transforms supply chain cybersecurity from a defensive obligation into a source of strength and trust. By embedding protection, visibility, and continuous assessment into every stage of supplier engagement, organizations can stay ahead of adversaries and maintain confidence in an increasingly complex threat landscape.

1 ENISA, ENISA Threat Landscape for Supply Chain Attacks, July 2021, p. 3, available at https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf.

2 TÜV-Verband e.V., TÜV Cybersecurity Study 2025, p. 15, available at https://www.tuev-verband.de/fileadmin/user_upload/Content_local/Studien_local/2025_TUEV-Verband_Cybersecurity-Studie_Studienbericht.pdf.

SOPHOS

Ready to assess your cybersecurity program?

Speak to a Sophos expert today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com