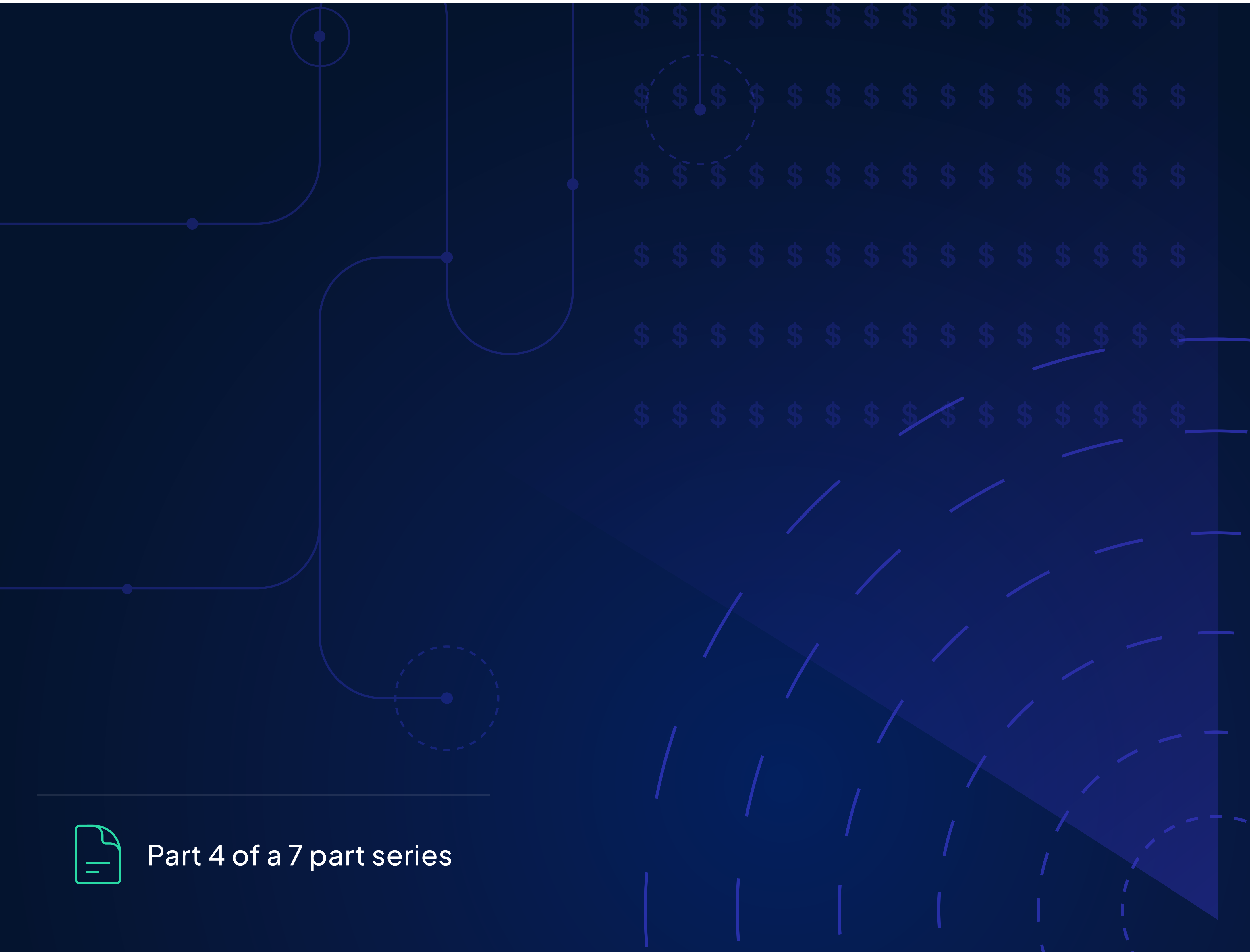
digital hands®

The Third-Party Problem That Can Become Your $12 Million Problem:

How MDR Defends Against Supply Chain Exploits



Part 4 of a 7 part series

Table of Contents

In the interconnected digital economy, your cybersecurity is only as strong as the weakest link in your supply chain. Cyberattacks that target third-party vendors, suppliers, or software providers with the goal of infiltrating their partners or customers have been growing rapidly. These attacks essentially use trust as a vector because they typically exploit your trusted providers.

Supply chain attacks have a high return on investment for bad actors because a single compromise can affect hundreds or thousands of organizations. These attacks can be used for a variety of malicious purposes en masse, from deploying ransomware or malware, to disrupting operations, stealing data, and installing backdoors into systems.

Why every CISO and SOC Should Care About Supply Chain Vulnerabilities

Digital supply chain compromises are one of the most difficult threats to detect and mitigate because they bypass traditional perimeter defenses. More than half of organizations say they don't have sufficient understanding of cybersecurity vulnerabilities in their supply chain. Not surprisingly, assessing security threats from third-party suppliers and supply chain partners was identified by surveyed security leaders as their SOC's second biggest challenge.

Here's some data illustrating just how high the risks are:

- ✓ Supply chain attacks skyrocketed in the past five years: the number of organizations impacted grew by 2,600 percentage points between 2018 and 2023.
- ✓ 62% of small and midsized organizations say they've been impacted by a ransomware attack that originated from a supply chain partner.
- ✓ For nearly 40% of organizations, recovery from a supply chain attack takes more than a month.
- ✓ The consequences are significant, from financial losses (identified by 64% of organizations) and data loss (59%) to reputational damage (58%) and operational impact (55%).
- ✓ The magnitude of the attacks can be immense: the SolarWinds attack impacted 18,000 organizations, including many Fortune 500 companies and government agencies. According to a survey, affected organizations paid an average of $12 million in remediation alone, or about 11% of their annual revenue.

How a Supply Chain Attack May Unfold

To carry out a supply chain attack, malicious actors can use tactics such as installing malware on connected or integrated systems, exploiting IoT device weaknesses, and infecting software development tools. One of the rapidly growing tactics is to deploy malicious software updates, as was the case with Solar Winds. **Here's how an attack may unfold:**

STEP 1

Vendor system compromise

The attackers infiltrate a software vendor through tactics like spear phishing the vendor's employees or exploiting unpatched vulnerabilities in IT systems. For example, an attacker could use compromised user credentials to gain access into a software company's build server.

STEP 2

Malicious code injection

The attackers modify legitimate software updates to include malicious code. Because the code embeds itself into the vendor's digitally signed process, the compromised update is signed by the legitimate digital certificate, verifying the software as authentic and ensuring trust. In the case of the SolarWinds attack, malware was injected into the update of the company's Orion IT management platform.

STEP 3

Delivery to target organizations

Unbeknownst to the vendor, the compromised software updates are distributed to customers. The patches contain a backdoor to the third-party servers, enabling them to distribute the malware across the entire customer base.

STEP 4

Exploitation and escalation

Once the target organizations are infiltrated, the adversary can use the backdoors for a host of malicious actions, moving laterally within the networks to exfiltrate data, deploy more payloads, or disrupt operations. In the SolarWinds attack, Russian nation-state actors compromised several U.S. federal government agencies and prominent technology and cybersecurity companies, among others.

How to Mitigate Supply Chain Attacks with Managed Detection and Response (MDR)

Supply chain attacks are difficult to detect because you don't have visibility into your partners' environments. However, MDR can look for indicators of compromise and help contain these attacks to limit their impact, spread, and severity.

Here's what the playbook may look like, using a combination of automated tools and human experts:

1. Detection

The MDR vendor's detection platform sees across multiple technologies. This breadth and depth across systems allows it to detect abnormal behaviors that single point systems may miss due to the lack of curated threat intelligence and AI capabilities. The platform monitors for anomalies across vendor communications and software updates, such as:

- Unusual traffic between the organization and third-party systems *(e.g., file types, domain names)*
- Behavioral deviations in user account activity *(e.g., activity at unusual hours)*
- Behavioral deviations in software processes after updates
- Signs of lateral movement or backdoor access *(between internal systems)*

2. Automation

Automated MDR platform workflows enrich data by gathering information and context from other technologies in the customer's environment, providing a full picture to analysts for investigation. The automation also isolates systems that are interacting with suspicious or compromised third-party software and blocks malicious activity originating from external IPs associated with the vendor's compromised system.

3. Investigation

MDR analysts investigate potential compromises to determine whether third-party software contains malicious code and to identify any backdoors or lateral movement within the organization. They validate flagged anomalies as either real threats or benign vendor-related changes.

4. Action

The compromised systems are isolated while vendor access is temporarily disabled. Analysts provide guidance on removing malicious updates and patching vulnerabilities. MDR threat hunters use threat intelligence along with other techniques to proactively search for other suspicious activities and anomalies that are completely unknown and may not have been detected by automated means.

Benefits of MDR beyond supply chain attacks

Digital Hands' Real-World MDR offers much more than defense against supply chain attacks.

Your MDR partner can augment your in-house SOC or security team, enabling them to:

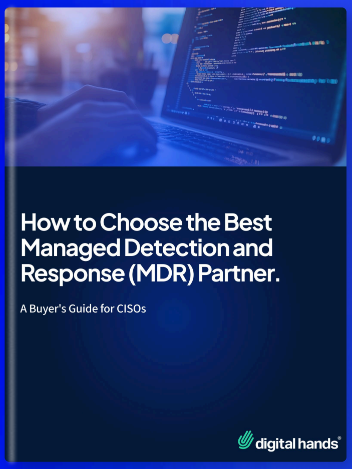
- ✓ See more — faster — to protect your environment holistically.
- ✓ Get higher-fidelity alerts and integrated, enriched telemetry.
- ✓ Improve operational efficiency while allowing you to automate your workflows based on your risk appetite.
- ✓ Increase response time with automated containment and expert-led investigations, reducing the window of opportunity for the adversary.

Buyer's Guide

Not sure where to start?

Get your MDR Buyer's Guide to understand key evaluation criteria and the 8 must-ask questions before you buy.

Download Now



How to Choose the Best Managed Detection and Response (MDR) Partner.

A Buyer's Guide for CISOs

digital hands