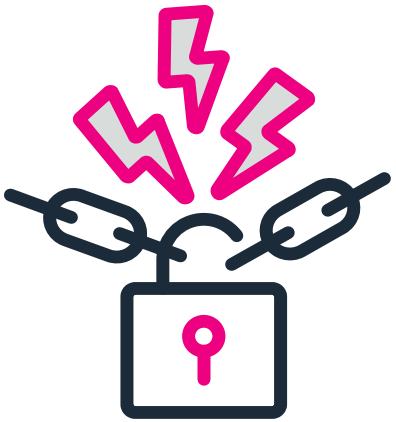
A Guide to

Protecting Against Supply Chain Attacks

How a data platform can help protect organizations from threats like the SolarWinds attacks

splunk> turn data into doing™

A supply chain attack is a powerful cyberattack that can breach even the most sophisticated security defenses through legitimate third-party vendors. Because vendors need access to sensitive data in order to integrate with their customers' internal systems, when they are compromised in a cyberattack, often their customers' data is too. And because vendors store sensitive data for numerous customers, a single supply chain attack gives hackers access to the sensitive data of many organizations, across many industries.



The severity of supply chain attacks cannot be overstated. And the recent spate of these attacks suggests this method is now the state actors' attack du jour.

The SolarWinds supply chain attacks were likely the most dramatic to date due to their unprecedented scale. More than 18,000 organizations and several U.S. government agencies were impacted, and it will be months before the full brunt of these attacks is known.

The SolarWinds attacks are just one example of why organizations must prioritize their security initiatives to detect and defend against these threats because it's clear the likelihood of other large-scale attacks will only increase.

How a supply chain attack works

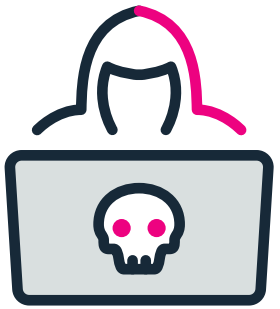
A supply chain attack uses legitimate, trusted processes to gain full access to organizations' data by targeting the vendor's software source code, updates or build processes. Supply chain attacks are difficult to detect because they happen at an offset to the attack surface.

Compromised vendors then unwittingly transmit malware to their customer network. Victims can be breached through third-party software updates, application installers and through malware on connected devices. One software update can infect thousands of organizations, with minimal effort from the hacker, who now has "legitimate" access to move laterally across thousands of organizations.

Here's how it works: After sneaking through the vendor's security defenses, often using multiple attack vectors, the malicious code embeds itself into a digitally-signed process of its host.

The digital signature verifies the software's authenticity, permitting its transmission. Hidden within, malicious code is then free to roam the updated traffic between the vendor and its customer network. The malware contains a backdoor that communicates with all third-party servers, which is how it's distributed. A single software update from a compromised vendor could breach thousands of organizations — in the case of the SolarWinds attack, it was over 18,0000.

A single software update from a compromised vendor could breach thousands of organizations — in the case of the SolarWinds attack, it was over **18,0000**.



What happened with SolarWinds

The SolarWinds attacks are a prime example of the magnitude of damage a supply chain attack can inflict. Sophisticated nation-state actors compromised SolarWinds' software and embedded it with malware.

The malicious software avoided detection by disguising its network traffic as legitimate protocol and storing reconnaissance results in legitimate files. Once embedded, the malicious code was deployed through a SolarWinds Orion product update, giving attackers backdoor access to all of SolarWinds Orion customers' networks.

The investigation into the threat campaign continues to develop, but at least two distinct malware threats have already been identified — Sunburst and Supernova, which may have come from two different threat actors.

SolarWinds is used by over 30,000 organizations as a network monitoring tool, and up to 18,000 of those customers installed updates that left them vulnerable to hackers. Confirmed victims include Fortune 500 companies and multiple agencies in the U.S. government, including the Pentagon, Department of Homeland Security, State Department, Department of Energy, National Nuclear Security Administration, and the Treasury. The full extent of the damage remains to be seen, but some experts are calling this one of the worst series of cybersecurity attacks in history.

Enter Splunk

To stay ahead of supply chain attacks, organizations need to modernize their security programs across hybrid and multicloud environments. Specifically, security teams need to normalize, manage and provide visibility into critical and disparate data sources and workloads so they can identify potential threats and conduct investigations and analyses in near real time.

Splunk's Data-to-Everything™ Platform helps organizations gain insights into their data no matter where it resides to better protect against security threats and vulnerabilities.

The platform helps protect organizations from supply chain attacks by detecting threats, recovering visibility into IT infrastructure and protecting customers, applications and development resources.

Securing the business

The Splunk platform helps organizations detect, protect and respond to supply chain attacks — similar to the SolarWinds attacks — by easily onboarding and searching for threat indicators in their environment.

The platform also helps security professionals review and update log types ingested into Splunk, which can lead to analysis of domain name systems (DNS), network and host traffic logs for evidence of malware activity. Security teams can also look at the results of vulnerability scans, hashes and proxy logs to search for evidence of webshell attacks (like the Supernova attack that was part of the SolarWinds attacks).

Organizations can also search for unusual activity from their directory and authentication providers for indications of a follow-on attack after a supply chain attack has been detected. The same data can also be used to look for other signs of lateral movement from compromised hosts.

Put an eye back on IT

One of the many reasons the SolarWinds attacks were so devastating was because customers lost visibility into their IT infrastructure as a result of the breach. Thankfully, the Splunk platform helps organizations restore that visibility, and monitor health and operations across their IT stack. This helps organizations improve their services, prevent outages and accelerate the time to remediate a problem.

Protect customers, applications and development resources

As application velocity has increased, enterprises need to re-evaluate their organizational structure and how they create visibility across their software delivery chain. Why? Because while increased delivery velocity has reduced mean time to value for customers, it can also increase attack vectors and expand attack surfaces for hackers to exploit.

Enter DevSecOps — the integration of security practices throughout the software development life cycle (SDLC) to ensure that secure services are brought to market. Through implementing DevSecOps practices, it's possible to secure both the service delivery chain itself and the software being delivered in it. To be successful, the DevSecOps practice needs to be observable, with actionable insights and incident response capabilities.

By making vulnerability scans visible, the Splunk platform helps organizations measure the coverage, effectiveness and activity of their vulnerability scanning processes, which helps them secure applications. Visualizations can also help organizations establish cross-team KPIs and metrics to measure the success and performance of DevSecOps practices.

Splunk also helps to protect supply chains by securing access to tool chains and monitoring, identifying and alerting on suspicious access and activity in an organization's dev/test environments. The platform also supports the resilience of an organization's critical SDLC infrastructure, including CI/CD, secrets management, code repositories and artifact management. It can be used to secure production apps by activating continuous verifications, alerting on new production vulnerabilities and then activating remediation before they can be exploited.

Learn More.

Ready to learn more about how Splunk's Data-to-Everything Platform which can help you stay ahead of supply chain attacks?

Learn More

21-17322-SPLK-AGuidetoProtectingAgainstSupplyChainAttacks-EB-108

splunk> turn data into doing™