Defending the Next Generation of Software Supply Chain Attacks

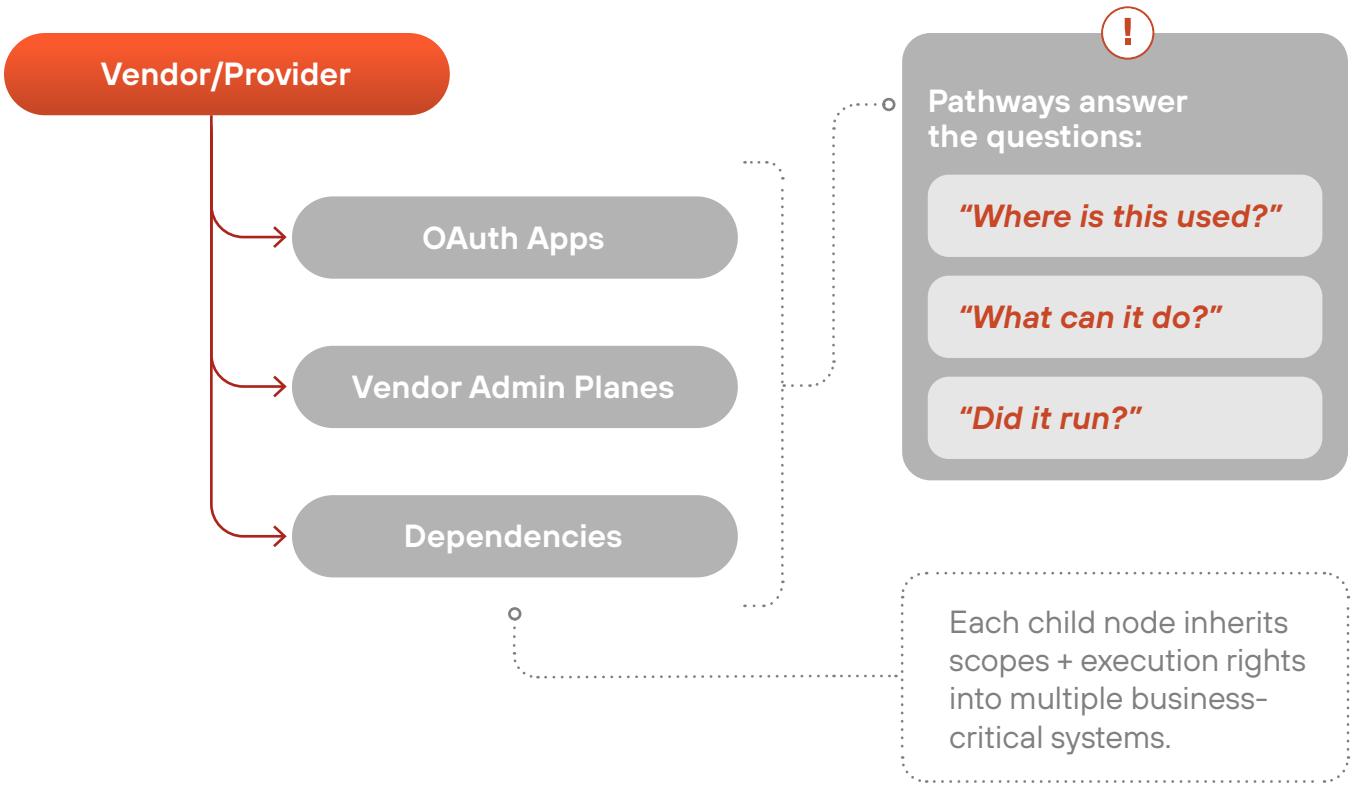
Executive Insights from the 2026 Unit 42 Global Incident Response Report

Supply chain risk is no longer limited to vulnerable code.

In 2025, we saw the supply chain expand to include SaaS integrations, vendor management planes and complex dependency ecosystems. Compromising these elements of the supply chain lets the attacker inherit the immense privileges of the vendor and weaponize that access downstream, causing one-to-many impact and disruption.

Our investigations revealed that when an upstream provider reported a compromise or outage, customers could not easily assess whether they were affected. On an individual level, such uncertainty delays containment and slows down operations. At scale, when numerous organizations are assessing compromise in parallel, it creates new issues, interruptions, and risk. Uncertainty becomes the disruption.

Defending the supply chain requires reducing the time needed to assess exposure and the areas of impact, yet inventory gaps, permission opacity, and telemetry gaps amplify the uncertainty caused by disruption.



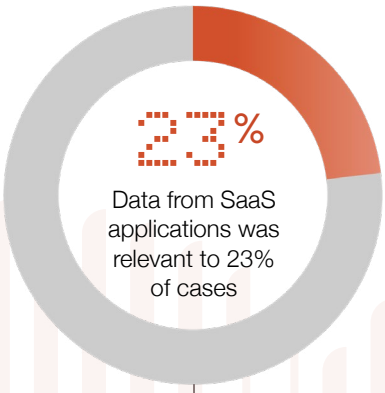
Risk Areas

SaaS Integrations

SaaS environments are stitched together through OAuth apps, API keys and workflow automation. These connections routinely carry access to data and business processes. For attackers, compromised integrations can become a lateral movement path that looks like normal automation.

The risk is inherited permissions. When an organization integrates a third-party app via OAuth, that application receives whatever rights were originally granted, sometimes including the ability to read sensitive data, manage users or modify records. If the upstream provider is compromised, those same permissions can be misused downstream.

Data from SaaS applications was relevant to 23% of cases we investigated last year, up from 18% in 2024, according to the 2026 Unit 42 Global Incident Response Report.

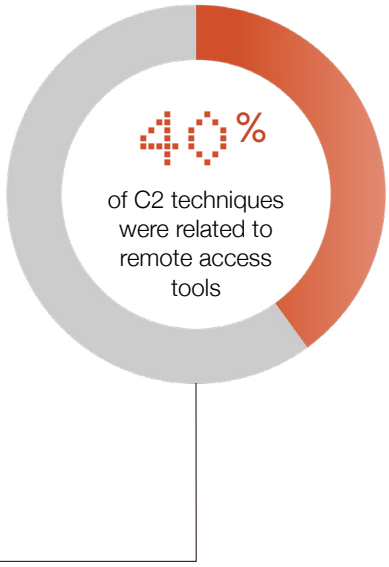


Weaponized Vendor Management Channels

Vendor tools like remote monitoring and management (RMM) and mobile device management (MDM) platforms enable privileged administrative action at scale. When attackers gain access to a vendor's management infrastructure (or the customer's tenant), they can push malware, run commands or change configurations in ways that blend into routine and administrative traffic.

Enterprises also inherit risk from opaque third-party applications running inside critical workflows. When customers can't inspect a vendor's codebase or validate security assumptions, then latent backdoors, hard-coded credentials or exposed interfaces can persist unnoticed.

Almost 40% of command-and-control (C2) techniques were related to remote access tools, according to the 2026 Unit 42 Global Incident Response Report.



AI Dependency Sprawl & Build-Time Compromise

In building or using AI systems, the risk lies in the indirect dependencies in the open-source ecosystem. Think of an "indirect dependency" as the silent elements used by the package, library or service you explicitly choose to add to your project or pipeline. These assets aren't named in your requirements file, but they're still brought into your environment and add to your attack surface.

We've observed threat actors injecting malicious code into upstream packages to execute during the install and build steps, which compromises pipelines before deployment and expands the blast radius across environments. As development teams adopt GenAI-assisted coding, they ingest more code and more dependencies faster—without sufficient scrutiny of provenance, maintainer trust, and downstream package behavior.

Over 60% of vulnerabilities in cloud-native applications reside in transitive libraries, according to the 2026 Unit 42 Global Incident Response Report.

Keys for Defense

Map SaaS Ownership & Scope

Many organizations lack a unified view of SaaS connections, vendor agents, and transitive libraries, making it hard to answer "Where is this used?" Teams should inventory OAuth apps and integrations, assign owners, and remove dormant interactions and integrations tied to departed users.

Design "Break-Glass" Severing Plans

Without manual review, it's tough to inventory the privileges that integrations, agents, and tooling possess, which makes impact assessment and containment unclear. While teams should mitigate that opacity as much as possible, they should also be proactive in designing revocation mechanics, rather than improvising them in the heat of an incident.

Log Vendor and Integration Activity at Audit Depth

Activity arriving through trusted channels like API calls and admin tooling can often look legitimate in the logs, delaying detection and increasing investigation time. Take steps to ensure you can answer what was executed, where and by whom. Alert on permission changes, token grants, and anomalous admin actions.

Harden Build Ingestion

The web of dependencies and indirect dependencies in the open-source AI ecosystem can be dizzying. Use software composition analysis (SCA) and provenance controls to quarantine and validate open-source components before deploying them into your environments. Pin versions, restrict new repositories and require review time for new dependencies, especially those that execute at install or build time.

Safeguarding Your Software Supply Chain

Minimizing supply chain risk isn't about avoiding dependencies or open-source resources. It's about gaining granular visibility into the hidden areas surrounding them. By gaining this visibility, the supply chain goes from a black box to a governable surface to which you can apply least privilege and interrogate unknown components before they land in production. When an upstream provider is compromised, rather than suffer prolonged disruption and broad isolation actions, you can execute a fast, targeted containment playbook.

Cortex Cloud gives you the visibility to actually understand your software and identity supply chain—from open-source dependencies to the integrations and permissions connecting your environments. It helps you answer the critical questions quickly: what's exposed, who has access, and what's actually happening. Instead of guessing during an incident, you can see the impact clearly and respond with precision.

Learn more in the 2026 Global Incident Response Report about how Palo Alto Networks can help you safeguard your software supply chain against the risks of today and tomorrow.

CONTACT US TODAY

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com