paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Defending the digital supply chain in the era of frontier AI

Table of Contents

Undercutting the fabric of trust	2
The new cyber landscape: Trust has become the attack surface	2
The attackers' AI advantage: The 72-minute exfiltration window	3
Shifting from perimeter control to systemic resilience	5
The economic and operational dividend of digital supply chain resilience	6
A framework for board governance: Five key questions for supply chain oversight	7
Conclusion	8

Undercutting the fabric of trust

The long-standing model of enterprise security – defending a well-defined perimeter against external threats – no longer applies. Sophisticated attackers have identified and are now targeting vulnerabilities in the wide mesh of third-party software and services, using the complexity of organisations' existing trusted connections to compromise them. Trusted supply chains are being aggressively and effectively turned against enterprise security frameworks, transforming them into increasingly significant threat vectors. The emergence of frontier AI has exacerbated this challenge: Threat actors are now leveraging powerful AI models to compromise cybersecurity and gain access to sensitive digital assets.

This whitepaper explores the challenges of defending the digital supply chain in the face of frontier AI's substantial impact on the long-established fabric of trust woven through third-party interdependencies in infrastructure, applications, and architecture.

The new cyber landscape: Trust has become the attack surface

The digital supply chain – made up of hundreds, or even thousands, of third-party software, data, and services in a typical large enterprise – isn't just important: It's essential. Organisations trust the security of their digital supply chain for activities as critical and diverse as analysing sales trends and reducing manufacturing errors to filing intellectual property patents and processing employee benefits claims. Without a safe, secure, and hyper-available digital supply chain, organisations simply cannot maintain resilient operations in today's environment.

This reliance represents an opportunity for attackers. Today's threat actors have extended beyond opportunistic, single-organisation targets and are increasingly recognising the value of sophisticated, pervasive, and high-impact attacks on supply chains that offer the returns associated with a one-to-many impact. Attacks have been made even more likely by the rapid development of frontier AI. These cutting-edge AI models were initially designed to help software developers spot potential problems, but now they're also being exploited by bad actors to spot gaps, exposures, and weaknesses in source code. AI models are already being weaponised against foundational trust models of third-party interdependencies – everything from SaaS applications and open-source toolkits to cloud services and application programming interfaces. The more advanced models will only accelerate this development of attacker tools and techniques, effectively lowering the bar for creating impact.

These developments have transformed the digital supply chain from a strategic, trusted asset into a primary vector for systemic risk. There is ample evidence that this is not theoretical but happening as we speak:

- One in three data breaches now involves a third-party vendor – double the rate of just two years ago.[1]
- Third-party breaches cost organisations on average 40% more to resolve than internal incidents.[2]
- The global cost of software supply chain attacks will reach $138 billion annually by 2031.[3]
- Sixty per cent of vulnerabilities in cloud-native applications reside in transitive dependencies/ libraries.[4]
- Attacks involving third-party SaaS applications have surged 3.8x since 2022, accounting for 23% of all attacks.[5]

Adversaries are systematically and efficiently bypassing cyber defences by corrupting the core components of modern software development and delivery. The industrialisation of these automated attack vectors allows adversaries to target vulnerabilities across the broader digital ecosystem, scaling compromises to maximise operational disruption and financial impact.

As the digital supply chain has expanded far beyond proprietary code and direct vendor relationships, organisations now find themselves in a strategic paradox. The large and growing number of third-party relationships necessary to drive business velocity and automation-based efficiency have become the battleground for cyberattacks that threaten organisational viability.

Wendi Whitmore, Chief Security Intelligence Officer at Palo Alto Networks®, put it succinctly and powerfully: "Organisations are realising that frontier AI is not just a threat they need to defend against. It is a test of every vendor relationship they have."[6]

The attackers' AI advantage: The 72-minute exfiltration window

The introduction of frontier AI models represents a massive step-change in adversaries' capabilities because these models can act as autonomous agents, capable of, amongst other things, analysing massive, complex codebases to uncover vulnerabilities and build and execute critical exploit paths, and granting threat actors the ability to coordinate machine-speed exploits at scale – leveraging velocity as their primary tactical advantage.

The time from an attacker's initial access to data exfiltration has collapsed from weeks or days to mere minutes. The traditional 'zero-day clock' and patching window have effectively been eliminated. Manual, human-speed defences are no longer fast enough to stop machine-speed attacks.

Data from Palo Alto Networks Unit 42® reveals that the fastest quartile of sensitive data exfiltration now occurs in under 72 minutes from initial compromise. This rapid exfiltration defines the new defensive speed baseline required of modern security operations.

1. Hylender, C. David, Philippe Langlois, Alex Pinto, et al., 2025 Data Breach Investigations Report (18th ed.), Verizon, April 23, 2025
2. Third-Party Cyber Risk Management, Gartner, 2023
3. Software Supply Chain Attacks Forecast, Cybersecurity Ventures, 2024
4. Unit 42 Global Incident Response Report, Palo Alto Networks, February 17, 2026
5. Ibid.
6. 'Frontier AI is now a test of every vendor relationship', Palo Alto Networks, June 2026

At present, security operations centres often rely on human review cycles – in which manual alert triage routinely takes upwards of 25 minutes, further investigation often requires requests to be raised manually, and containment of an affected system may take hours or even days.

These traditional, human-led security operations are now at a severe disadvantage: They are structurally incapable of intercepting machine-speed attacks and data theft. The scale and contextual awareness of frontier AI models enable adversaries to identify, map, and exploit digital supply chain vulnerabilities at a pace human-driven correlation and fragmented point solutions cannot effectively counter, necessitating automated, cross-business defensive frameworks capable of operating at machine-speed.

Until defensive teams are equipped with the rapid, machine-driven triage and automated threat containment they need to respond to machine-speed threats, AI-enabled threat actors will retain their current significant advantage.

Other considerations in evaluating digital supply chain risk include the huge and still-growing cybersecurity skills gap (as well as the newer AI skills gap), which may leave organisations that rely entirely or primarily upon human security teams without the resources they need to act at scale; and the reality of long waits for third-party suppliers to patch interconnected systems – a delay that is no longer feasible or acceptable. All 'fix' processes must become automated and as close to real time as possible to ensure digital supply chain vulnerabilities are detected and blocked before they can be exploited.

Unfortunately, the update mechanisms and open-source dependencies modern enterprise infrastructure relies upon so heavily are inviting targets for cyber adversaries, who are continually developing new methods to exploit new digital supply chain attack vectors – and other bad actors may inject malicious code into developer tools, continuous integration/continuous delivery/development (CI/CD) pipelines, or open-source libraries.

There are plenty of real-world examples of digital supply chain compromise. In the case of SolarWinds, Log4Shell, XZ Utils, TeamPCP campaigns, and Mini Shai-Hulud, attackers exploited vulnerabilities within third-party tools, applications, and services to facilitate a wide range of malicious activities, including credential theft, data extraction, nation-state attacks, and device compromise.

It's critical to note, however, that frontier AI's ability to dramatically increase the speed of attacks is not its only powerful impact: The new technology model also eats away at trusted vendor relationships by turning them into primary attack vectors. For instance, software vendors are routinely shipping new AI capabilities, agents, and integrations into enterprise software stacks through traditionally unremarkable updates. But C-suite executives – including many CISOs – often do not know which AI tools are operating inside their perimeter, or yet have governance frameworks in place to monitor them.

Organisations must also come to grips with the potential downside of one of the newest and most important trends in AI: agents. If an agent is compromised, it immediately becomes an insider threat, easily turned against the organisation's cyber defences because of its use of legitimate user permissions to bypass traditional security monitoring. Research predicts that more than 1.3 billion autonomous agents will be deployed by 2028.[7] Even a tiny fraction of those agents, or any other non-human identity, going rogue or being compromised could have a massive impact throughout a digital supply chain.

Finally, all executives, team leaders, board members, and security professionals need to bear in mind the reality of 'Shadow AI'. Tech-savvy employees, contractors, and business partners have long used unsanctioned technology such as PCs, local area networks, cloud services, and internet of things sandboxes without the knowledge or control of IT or SecOps. However, the massive adoption of AI – not only by enterprise IT but also by individual users – has created an even higher level of complexity and cyber risk. If an external AI service used by an employee or well-meaning partner is compromised, it creates an unmonitored backchannel straight into corporate data lakes.

Shifting from perimeter control to systemic resilience

One major reason the long-standing enterprise security model no longer applies is that one of the key elements of that model – the organisational perimeter it was designed to defend – has changed beyond recognition. Just as the cloud moved existing perimeter boundaries beyond endpoints, data centres, and wide area networks, AI has further reshaped and even eradicated the once well-defined perimeter. While the growing number of third-party dependencies is to blame for much of that transition, the increased sophistication, persistence, and innovation of bad actors in finding and exploiting weaknesses outside the traditional perimeter must also be acknowledged.

It's clear that breaches, incursions, incidents, and simple human errors represent tangible threats to organisations. Downtime cannot be managed away through service-level agreements, compliance audits, and periodic vendor assessments. And, as important as MTTD and MTTR are for any enterprise, the impact of a single incident along a digital supply chain can be catastrophic.

To regain the upper hand, organisations must shift digital supply chain security away from traditional perimeter-based controls and towards systemic cyber resilience.

One of the key steps in achieving systemic cyber resilience is to architect for it. Legacy third-party risk management relies on point-in-time assessments that are null and void by the time they are filed. Instead, organisations must shift to a new model: continuous, real-time mapping and risk assurance of the entire digital supply chain.

This approach calls for machine-readable visibility into transitive dependencies, which requires systemic generation and ingestion of Software Bills of Materials (SBOMs) and their AI counterpart, AI Bills of Materials (AIBOMs). Doing so sheds light on silent code dependencies and shadow AI integrations before attackers can turn them against defences.

It also necessitates continuous posture management, replacing legacy scheduled audits in order to provide continuous exposure management. This helps keep third parties aligned with the organisation's risk tolerance and reduces the potential for digital supply chain compromise.

7. IDC, 'IDC FutureScape 2026 Predictions Reveal the Rise of Agentic AI and a Turning Point in Enterprise Transformation', October 2025

Another important – and potentially controversial – issue is the notion of access. Organisations should adopt a policy that eliminates implicit trust as the basis for determining access and privilege, replacing it with identity – specifically, machine identity. Concepts such as just-in-time orchestration should replace standing privileges for vendors, partners, and APIs; this will severely limit an adversary's attack vectors. The zero trust mantra of 'never trust, always verify' must extend from applications to the identity layer in order to restrict the potential for a compromised vendor to become an exploit path.

Finally, digital supply chain resilience must be built on the same principle as the new AI attack model: speed. By building in machine-speed autonomous response, organisations take the burden off human analysts struggling to keep up with automated attacks. Just as attackers have automated their methods, so too must organisations automate their response posture. Techniques such as algorithmic containment and platform consolidation are key here because they reduce complexity. This positively impacts detection, analysis, response, and remediation, mitigating the risk of the digital supply chain being compromised and critical systems disrupted.

The economic and operational dividend of digital supply chain resilience

To identify machine-speed threats across such complex ecosystems, organisations must increase visibility and reduce complexity through a unified security architecture, enabling autonomous threat management that allows detection and response to happen in seconds rather than hours or days.

But locking down and ensuring the sustained resilience of an organisation's digital supply chain is not only good cybersecurity practice – it also delivers substantial operational benefits that translate into tangible returns, making cybersecurity a verifiable contributor to bottom line as well as overall operational success.

For instance:

- A zero trust architecture enhances cybersecurity through continuous verification and least-privilege access controls. But it doesn't just minimise the attack surface: It also aligns well with organisations' digital transformation efforts, facilitating innovation by enabling safe experimentation while simultaneously strengthening governance and compliance posture.
- Automated high-speed response – derived from pre-authorised containment playbooks that isolate threats and minimise attack impact in real time – improves mean time to respond. But this ability to prevent, detect, and respond to a machine-speed threat with a machine-speed defence doesn't just reduce the likelihood and impact of an incident: By doing so, it also cuts potential capital loss.

Balanced against the financial dividend of significantly mitigating regulatory compliance risks, legal liabilities, and potential brand damage stemming from data breaches, it's abundantly clear that ensuring cyber and operational resilience across the digital supply chain delivers tangible business value. It not only limits the potential for crippling downtime, but also cuts the economic impact of any incident, reduces total cost of ownership, and improves return on investment and return on assets.

A framework for board governance: Five key questions for supply chain oversight

The role of board members in cybersecurity governance has always been essential, and it has become exceedingly complex and challenging in the era of frontier AI. Because securing the digital supply chain has such far-reaching fiduciary responsibilities, board members need to ask tough, direct questions of all executives – not just the CISO. Here are five key questions that should be asked and answered:

1. **The velocity metric:** "If a highly trusted, digitally signed vendor integration is compromised upstream, can our security architecture autonomously detect and isolate the connection within a machine-speed exfiltration window?"
2. **The dependency blind spot:** "Do we possess continuous real-time visibility into the transitive dependencies and third-party AI models currently interacting with our production data, or are we relying on static vendor questionnaires?"
3. **The identity liability:** "Are our external vendors, CI/CD pipelines, and SaaS integrations operating with standing privileged access, or have we enforced ephemeral, just-in-time identity controls for non-human identities?"
4. **The complexity tax:** "Is our security estate structurally fragmented, creating blind spots that adversaries can exploit, or are we actively consolidating toward a unified, automated architecture?"
5. **The resilience test:** "Has our incident response plan been exercised for a realistic supply chain failure scenario in which a critical, digitally signed software update is the attack vector?"

Uncertainty in these areas indicates a significant gap in security posture that known adversaries will be equipped to exploit. Such findings should prompt the board to direct management to formulate a time-bound remediation plan.

Conclusion

The gap between machine-speed attacks and human responses is real – and growing. There is an emphatic need for autonomous containment methods, particularly because a growing wave of new regulations is putting pressure on board members and the C-suite to invest in proactive architectural modernisation to identify and plug digital supply chain gaps.

When designing and implementing strategies to secure the digital supply chain, there are important principles business and technical leaders should observe. Adhering to those principles will help leaders transform their enterprise from passive risk acceptance to proactive resilience.

One such principle is that assumed trust must now be augmented with continuous verification – a need that can be met by the zero trust model. Without it, the current exploitation of third-party vulnerabilities in digital supply chains – accelerated by the advent of frontier AI and the growing sophistication of adversaries – will continue to represent a fundamental erosion of trust between organisations and their partners.

Leaders must also bear in mind that this is a 'whole business' problem: A successful attack on an organisation's digital supply chain may infect every functional area within that organisation. Therefore, a whole-of-business approach to planning, constructing, and implementing solutions is required. Every department must be 'on the team'.

Since CXOs already have so many responsibilities, it may help organisations to have a North Star – a guidepost to help them identify and prioritise the actions that will have the greatest impact on the long-term security and safety of the digital supply chain.

With the core concept of resilience in mind, it's important that organisations map their 'minimum viable business' to clarify which capabilities cannot be compromised without severe, perhaps lasting, damage to the enterprise. These capabilities should be cross-mapped against known threats and the organisation's non-human identity landscape. Potential consequences of supply chain vulnerabilities and exploits must be rigorously evaluated so the organisation can understand its capacity to sustain critical functions and recover quickly from compromise.

Despite the significant threats to digital supply chains described in this whitepaper, there is good reason for organisations to be optimistic: All the countermeasures outlined herein are both well understood and readily achievable. Frameworks already exist to help identify vulnerabilities, close gaps, and automate response. It is up to the board, the C-suite, and all technical and business leaders to seize the initiative for digital supply chain resilience. The first step is to move from awareness to action. Organisations should begin by making a clear-eyed assessment of their specific exposure against the resilience metrics outlined in this paper.

Palo Alto Networks partners with enterprise leaders to diagnose these systemic risks and architect a defensible, resilient digital supply chain. If you are ready to transition from managing incidents to managing risk, we are ready to help you build your framework for resilience.

paloalto NETWORKS

22 Bishopsgate, Level 55
London, EC2N 4BQ
United Kingdom

0800 028 3904

www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

parent_ds_Defending the digital supply chain in the era of frontier AI_26.08.26