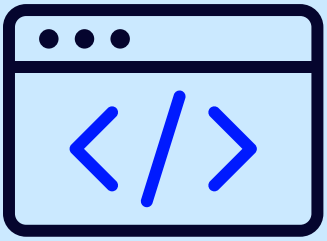


RESEARCH REPORT

Data Accelerator: Software Supply Chain and Cybersecurity

LevelBlue

Data Accelerator:
Software Supply Chain and Cybersecurity

The 2025 LevelBlue Futures Report calls on organizations to pay closer attention to the evolving security threats caused by AI disruption. It finds that companies are unnecessarily vulnerable to software supply chain threats: about half say they lack the visibility they need to fully understand—or even identify—the risks. This Data Accelerator is designed to help organizations better understand the challenges of securing the software supply chain and the opportunities to proactively lead in an area of emerging risk.

01

Part 1 Explores perceived risk factors and the drivers for transparency and security in the software supply chain.

02

Part 2 Compares data from survey respondents across four global regions.

03

Part 3 Offers four actionable steps to secure the software supply chain.

Software Supply Chains Need to Be Secure and Transparent

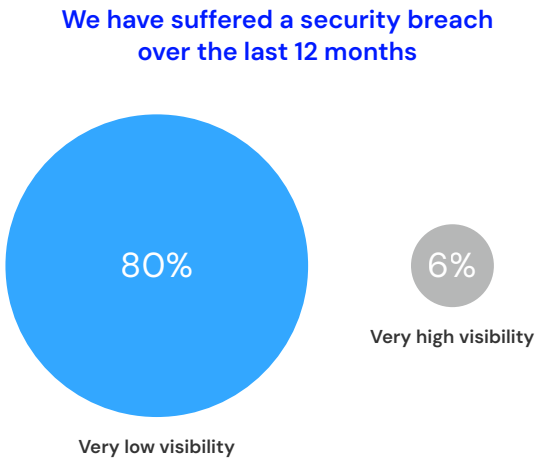
There is an urgent business case for investing in a more transparent and secure software supply chain. Of the organizations that say they have "very low visibility" across the software supply chain, 80% have suffered a security breach in the past 12 months—compared with just 6% of organizations that claim to have "very high visibility" (Figure 1).

In this LevelBlue Data Accelerator, we compare risk appetites, investment gaps, and overall preparedness to help organizations secure their end-to-end software supplier ecosystem.

Figure 1

Organizations with transparent software supply chains are far less likely to have suffered a security breach in the last 12 months

% of respondents Very high visibility N=348 | Very low visibility N=97



Part 1: Software Supply Chain Security is Moving Up the Agenda

Software supply chain security is a growing business concern in 2025. Partly, that is because regulatory frameworks such as the European Union Agency for Cybersecurity (ENISA) supply chain guidelines or mandates for Software Bill of Materials (SBOM) in the United States demand more transparency and accountability in software development.

It is also because the attack surface is expanding rapidly as organizations adopt AI-driven tools and integrate complex third-party ecosystems. Threat actors—from nation states to cybercriminal groups—are changing their tactics, targeting suppliers and development pipelines to gain access at scale.

There is also greater awareness, with recent global outages showing how operations can break down when a software supply chain is breached. In our research, 68% of organizations say that media reports have moved cybersecurity higher up the C-suite agenda.

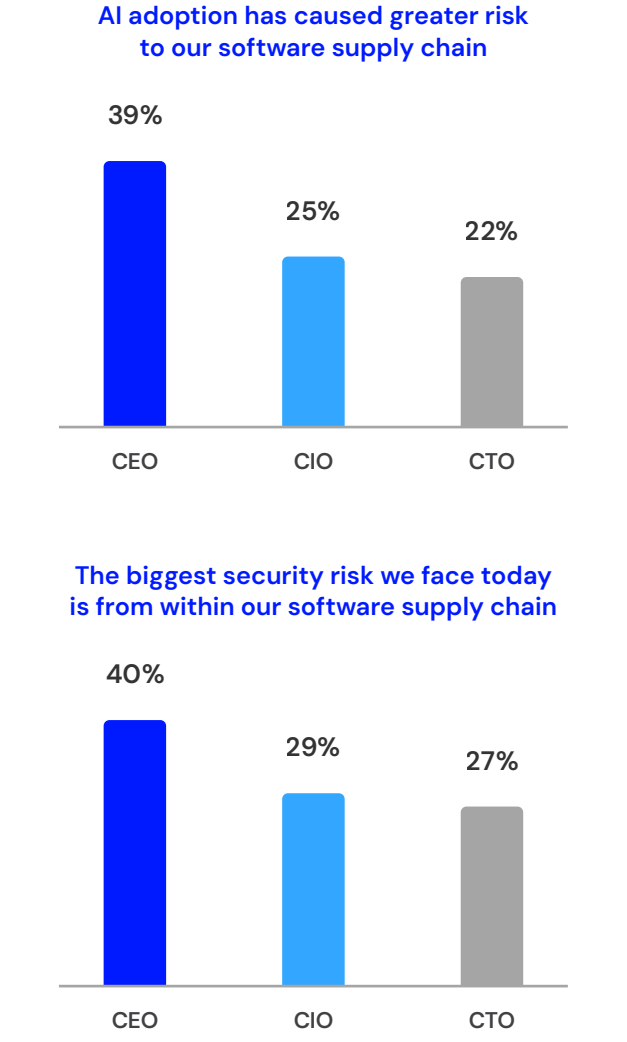
CEOs are particularly attuned to the evolving risks: 39% say AI adoption presents a greater risk to software supply chain, compared with only 25% of CIOs and 22% of CTOs. And 40% of CEOs believe that the biggest security risk the organization faces today is from the software supply chain, compared with 29% of CIOs and 27% of CTOs (Figure 2).

This suggests there is pressure on IT decision-makers to fortify operations across the supply chain, even if they do not see it as a high-risk area.

Figure 2

CEOs are more likely than IT executives to worry about software supply chain risks

% of respondents Each role N=100



Organizations Cannot Agree About How to Secure the Supply Chain

Software supply chains are interconnected ecosystems that create challenges when it comes to cybersecurity. Lack of visibility across suppliers and complex third-party development pipelines make it difficult to assess the risks. Open-source software exposes organizations to potential backdoor threats.

Beyond source code issues, organizations are finding it difficult to identify drivers to improve their software supply chain visibility. Organizations might be indecisive because they lack awareness of today's specific threats, or it could indicate a failure to implement solid software lifecycle engineering practices.

Without an obvious reason to improve visibility, organizations are failing to prioritize strategic action to increase transparency. Only 23% of organizations are currently confident that their visibility of the software supply chain is "very high."

A Secure Software Supply Chain Increases Overall Cybersecurity Confidence

Organizations that have very high visibility of the software supply chain are far more confident about managing risks across the entire ecosystem (Figure 3). Less than 20% of this group say that custom-developed source code, commercial off-the-shelf (COTS) software and app and API integrations are "somewhat risky" or "very high risk". By contrast, 80% or more of organizations with very low visibility of the software supply chain describe these factors as either "somewhat risky" or "very high risk."

Lack of visibility across suppliers and complex third-party development pipelines make it difficult to assess the risks.

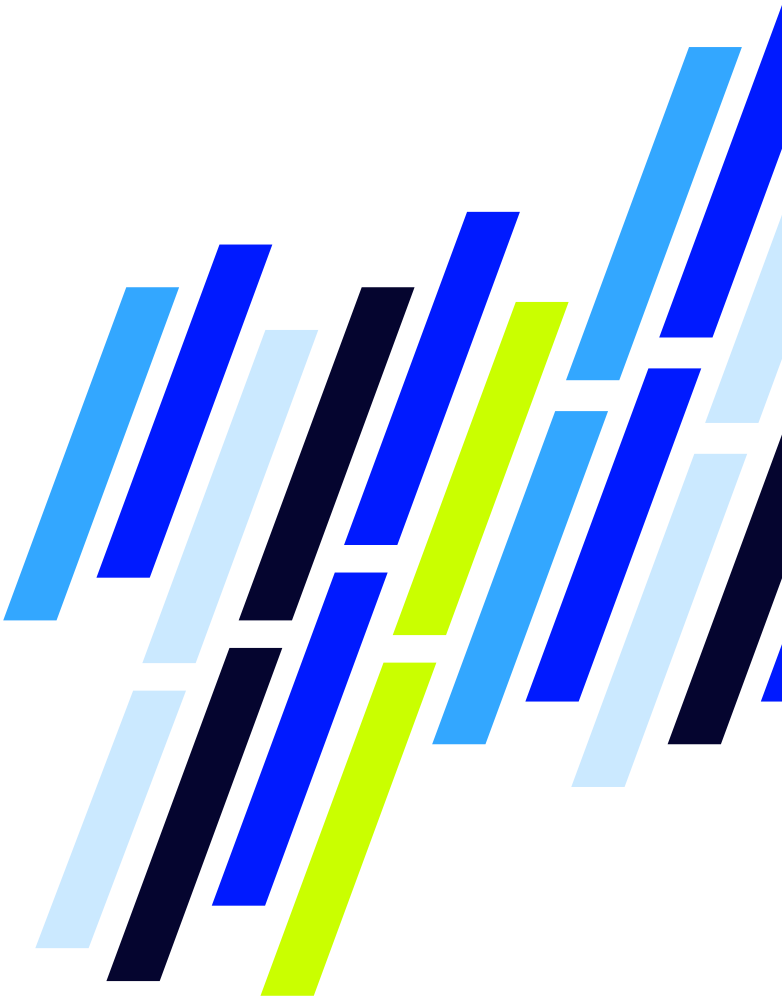
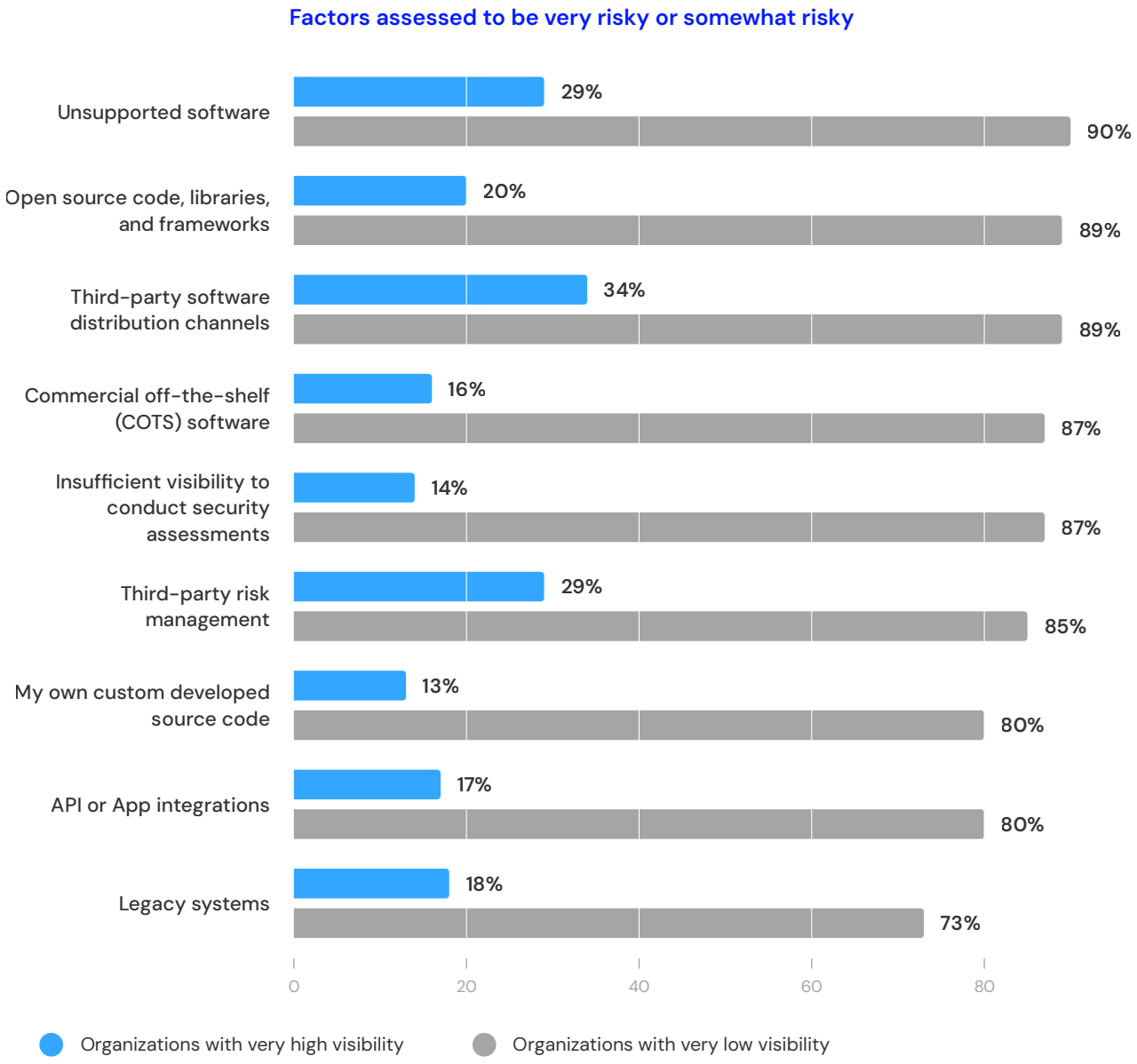


Figure 3

Organizations with very high visibility are less concerned about managing risk factors

Q: How do you view the following risk factors in your software supply chain?

% of respondents
Very high visibility N=348
Very low visibility N=97



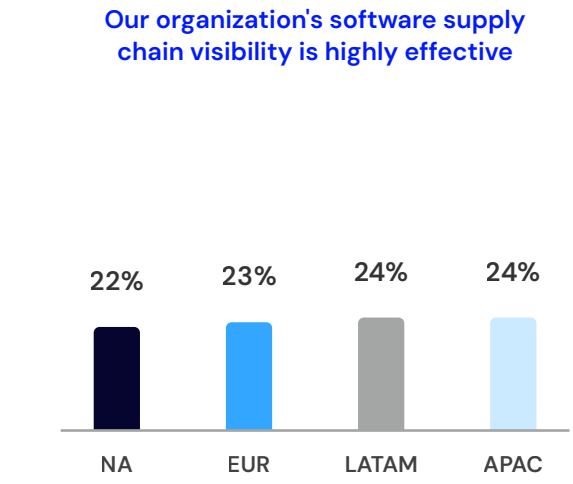
Part 2: How Are Different Regions Approaching Software Supply Chain Security?

Globally, software supply chain visibility is low. Less than one-quarter of organizations across all regions say that they have achieved very high visibility of their software supply chain.

Figure 4

Small numbers of organizations in each region have very high visibility

% of respondents N=1500



Despite these similarities in software supply chain visibility, preparedness for an attack varies widely across the four regions (Figure 5). In North America, organizations are far more likely to say they are prepared for attacks (57%) than organizations in APAC (44%). In Europe and Latin America, 51% and 50% say they are prepared, respectively.

This is worrying because at least 40% of organizations in every region believe that a software supply chain attack is likely to affect them within the next 12 months.

Figure 5

Less than half of organizations in APAC can handle an attack on their software supply chain

Q: How likely is it that a software supply chain attack will occur in your organization over the next 12 months?
Are you prepared?

% of respondents N=1500

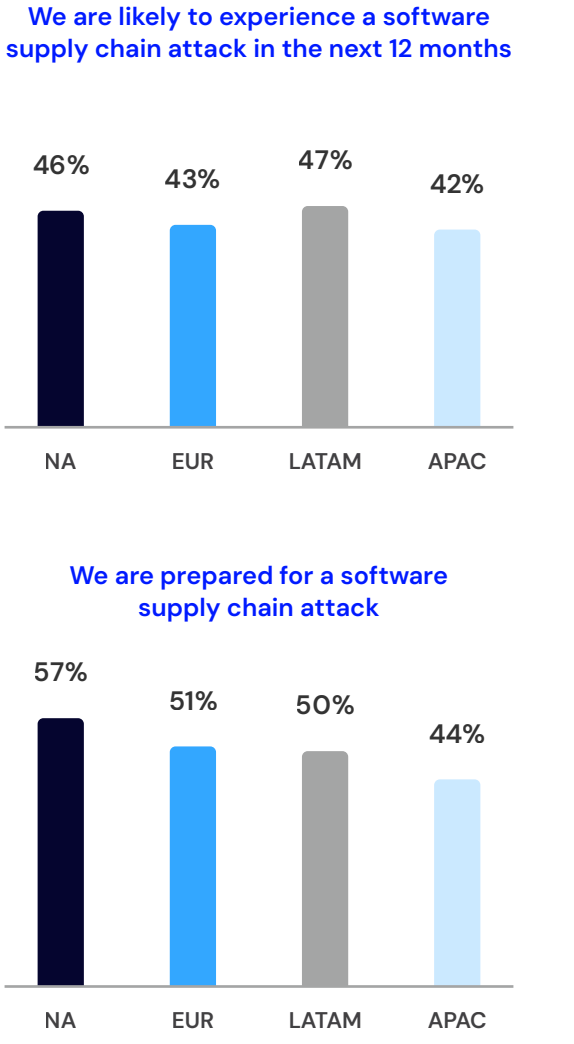
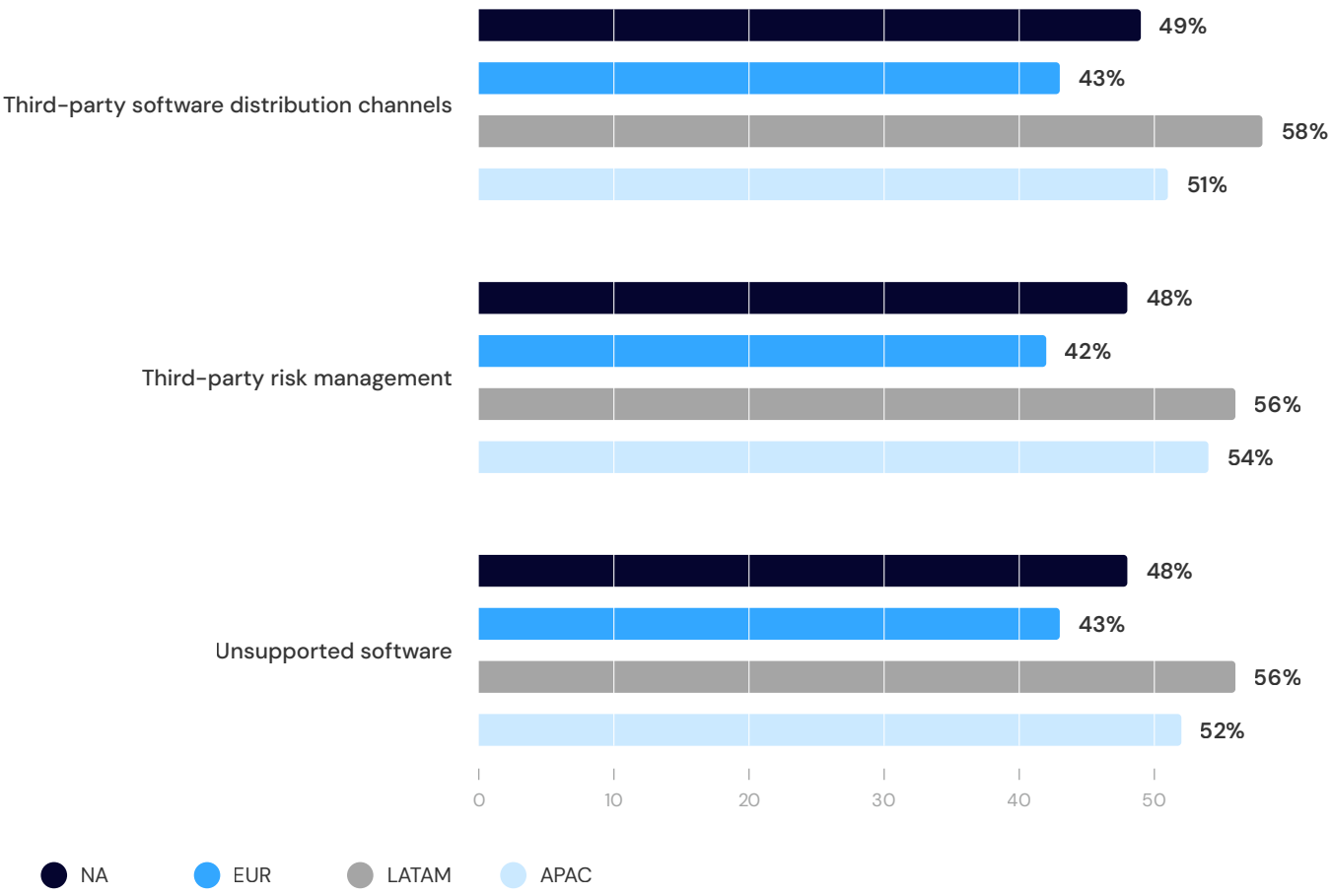


Figure 6

Third-party risk management is one of the top three risk factors for all regions

Q: How do you view the following risk factors in your software supply chain?

% of respondents
N=1500



Perceived Risk Factors Vary Globally

Organizations in Latin America are more concerned about risk factors in the software supply chain than organizations in the other three regions (Figure 6), perhaps because around half (47%) are concerned that an attack is imminent. Significantly higher numbers than in other regions say they see third-party software distribution channels (58%) and third-party risk management (56%) as very risky or somewhat risky.

Organizations in APAC are more concerned about risk factors in the software supply chain than organizations in North America or in Europe, which could be because they are the least likely of all regions to be prepared for attack. Around half say they see third-party risk management (54%), and unsupported software (52%) as very risky or somewhat risky.

APAC's organizations are also far more likely to see open-source code, libraries, and frameworks as particularly risky: 53% compared with 44% in North America, 43% in Latin America and 37% in Europe.

In North America, the top three risks for organizations are third-party software distribution channels (49%), third-party risk management (48%), and unsupported software (48%).

In Europe, the top concerns are similar: third-party software distribution channels (43%), unsupported software (43%), and third-party risk management (42%) top the list of risk factors. European organizations are less concerned about their own custom-developed source code as a risk factor within the supply chain: 35% compared with 40% in North America, 47% in Latin America and 45% in APAC. This may reflect a culture of code reuse across systems.

Every Region Has to Increase Actions to Protect the Software Supply Chain

Organizations are aware of the risks to their software supply chains, but they are not doing enough to address them. They will need to commit to continuous investment, even if they feel prepared for an attack.

Figure 7

Evolving threats demand ongoing investment

Q: To what extent is your organization investing in enhanced supply chain security to prepare for new and emerging types of cyber threats?

% of respondents N=1500

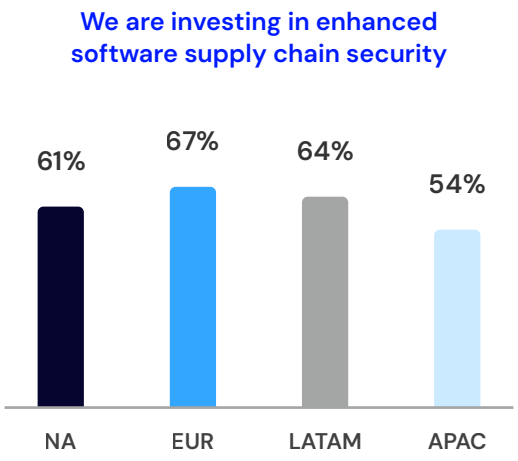
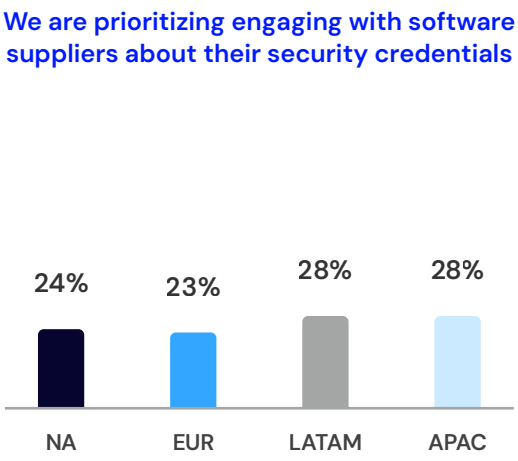


Figure 8

Only a quarter of organizations say engaging with software suppliers is a priority for the next year

Q: Which of the following will be a priority for your organization over the next 12 months as it seeks to improve its cyber resilience?

% of respondents N=1500



In North America, only 61% of organizations are committing moderate or significant investment to improve their software supply chain security (Figure 7). This might be because they are confident they can handle an attack—57% describe themselves as prepared—but complacency is dangerous.

European organizations are investing far more in software supply chain security than organizations in the US and APAC: 67% are making moderate or significant investments, even though 51% describe themselves as "prepared" for an attack.

In Latin America, the investment outlook is similar to that seen in Europe. Half are prepared for attack and yet, encouragingly, 64% are committing moderate or significant investments in software supply chain security.

This suggests that organizations in both Europe and Latin America understand that security is an ongoing journey in today's evolving risk landscape.

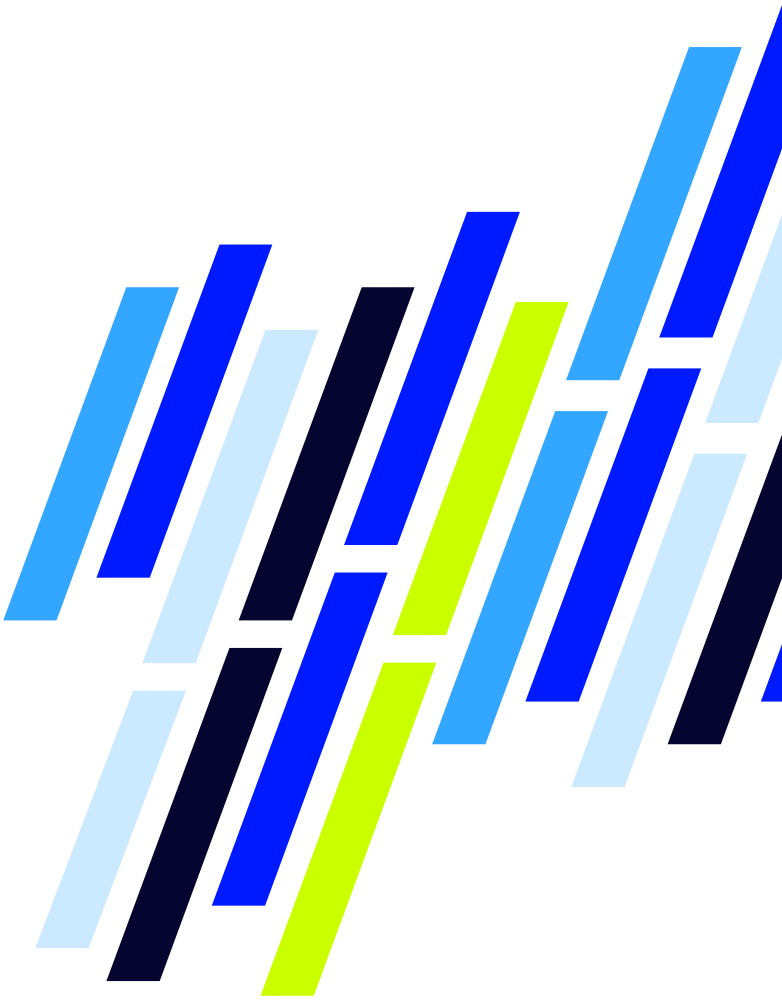
APAC organizations, on the other hand, must review their investment strategies. They are the least likely to feel prepared for an attack, but only slightly more than half (54%) are making moderate or significant investments to enhance their software supply chain security.

Organizations in Every Region Are Overlooking the Third-Party Supplier Threat

In APAC, Europe, North America and Latin America, organizations say that third-party risk management is one of the biggest threats they face. But only about a quarter in any location say that engaging with software suppliers about their security credentials is a priority for the next 12 months (Figure 8).

Proactively engaging with suppliers is a critical way to increase confidence in cybersecurity overall. It allows organizations to develop a benchmark and confidence level for suppliers, exposes hidden vulnerabilities, and helps to mitigate common risks relating to open-source components.

Proactively engaging with suppliers is a critical way to increase confidence in cybersecurity overall.



Part 3: **Four Ways to Secure the Software Supply Chain**

01

Take advantage of C-suite awareness of the risks to highlight specific threats and access budget for enhanced security measures.

02

Work with your organization to identify where the biggest vulnerabilities lie and to understand the potential business impact. Use this alignment to agree on the shorter-term priorities for building better visibility.

03

Proactively invest in cybersecurity measures such as advanced threat detection and response, and exposure and vulnerability management technologies to stay prepared for emerging and evolving threats.

04

Request evidence of suppliers' cybersecurity credentials so you can identify potential risks in your software supply chain. Carry out regular assessments of your software suppliers to build confidence and to maintain your organization's resilience.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence—this enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us today to learn more about how we can safeguard your organization's future.