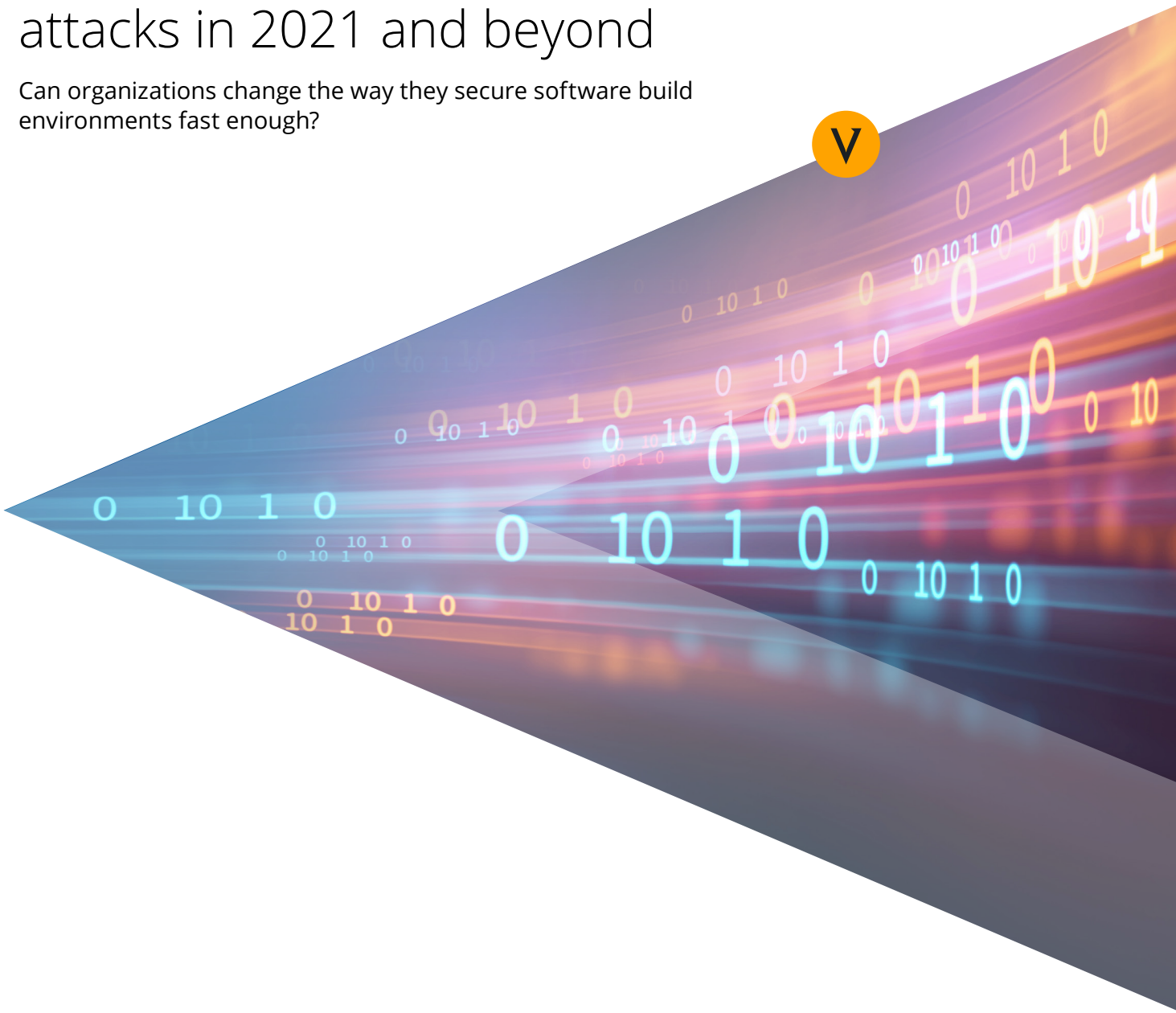
VENAFI®

// Survey: Tech professionals expect more SolarWinds-style software supply chain attacks in 2021 and beyond

Can organizations change the way they secure software build environments fast enough?



// Introduction

The SUNBURST malware attack on SolarWinds —first reported in December 2020—is not the first known software supply chain attack, but it is by far the most serious. The damage is already extensive, affecting around 80% of the Fortune 500, including giant corporations like Microsoft, Cisco, Intel, Belkin, FireEye and Deloitte, as well as numerous U.S. government departments and agencies, including the U.S. Departments of State, Defense, Homeland Security and Treasury. The attack was so extensive that its full impact probably won't be known for years.

The breach put a klieg light on how attackers are "shifting left" to successfully penetrate the defenses of a software provider in order to compromise their customers. Today's attackers are software developers who have already recognized software build environments as low-hanging fruit ripe for exploitation. In addition, they have discovered that infiltrating the software build pipelines of software providers is a force multiplier since a successful compromise of commercial software is an extremely efficient way to infiltrate a large number of a provider's customers.

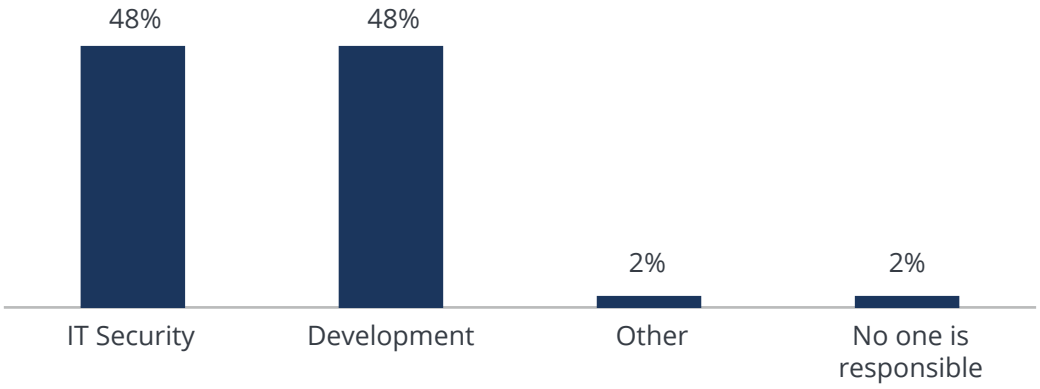
To defend against similar attacks in the future, all organizations that build software for commercial or internal use—which includes every software developer working in Global 5000 organizations—must shift their defenses left to protect all aspects of the software supply chain, including the entire build pipeline. "Directly targeting high-profile organizations is extremely difficult and time-consuming and tends to yield fewer results. Threat actors increasingly are taking the more covert approach of a supply chain attack to reach their targets instead. Taking advantage of the lack of security controls to the software development pipeline, these types of attacks are becoming more and more common—not only among state-backed actors, but also crime gangs and others—and it will take us a long time to discover them due to the nature of these attacks," explained Yana Blachman, threat intelligence specialist at Venafi.

Although the industry is clear that *something* needs to be done, the big question is which part of the organization should take primary responsibility for actually shifting security left. To better understand InfoSec and development teams—the two primary stakeholders in this matter—Venafi commissioned a global study of more than 1,000 development and InfoSec professionals in English-speaking countries. The results show a troubling lack of consensus on how best to move forward.

// Who will ensure software supply chains are secure?

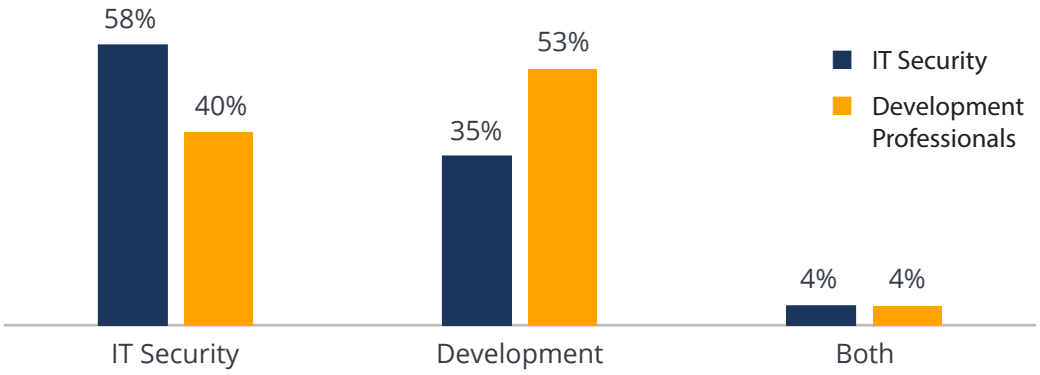
Respondents were nearly unanimous in the belief that the attack techniques used at SolarWinds will be used in future attacks. However, no consensus was evident about which of the two functional teams is responsible for solving this problem. In fact, respondents were split down the middle regarding which department is responsible for securing the software build pipeline in their organizations.

Which team or role in your organization is primarily responsible for in securing software build pipelines within your organization?



As far as which department *should* be responsible for securing software build pipelines, there still was no clear consensus, even when respondent data was analyzed by job function:

In your opinion, which role or team SHOULD be responsible for securing software build pipelines?



"Traditional roles are unclear about who is responsible for securing software pipelines: Engineers build code, while security teams protect the business. But who protects software developers and who can understand how to protect the code developers write? That's why we see development teams hiring security engineers, and security teams recruiting coders," said Kevin Bocek, vice president, security strategy and threat intelligence at Venafi.

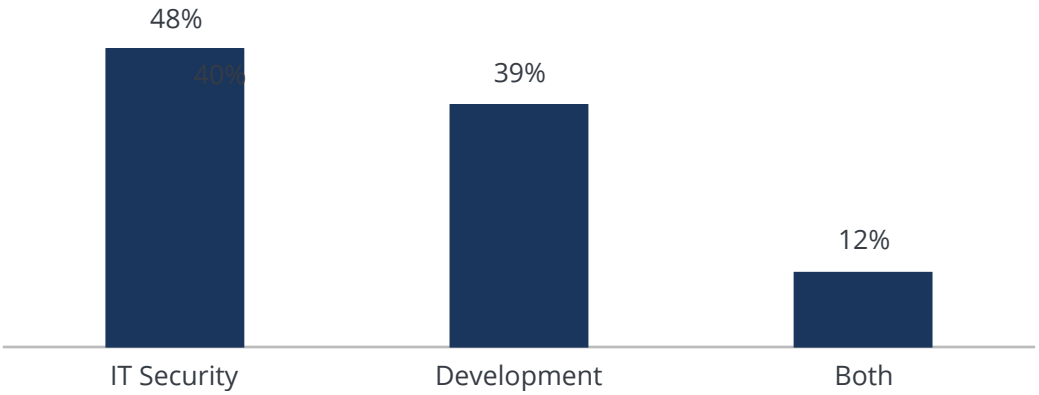
This lack of alignment in who should be responsible for shifting security further left to protect build pipelines extended to executive leadership. According to survey data, executives favored InfoSec over developers, but it was only a plurality—nothing close to a clear mandate.

Although the percentage of executives who believed both InfoSec and developers should share responsibility was double that of the IT and development professionals surveyed, the overall numbers pointing toward shared responsibility were still abysmally low. These numbers suggest that executives lack vision on how to manage the shift-left challenge, so it's not surprising the individual contributors and teams don't appear to have clear guidance on who is responsible for driving change.

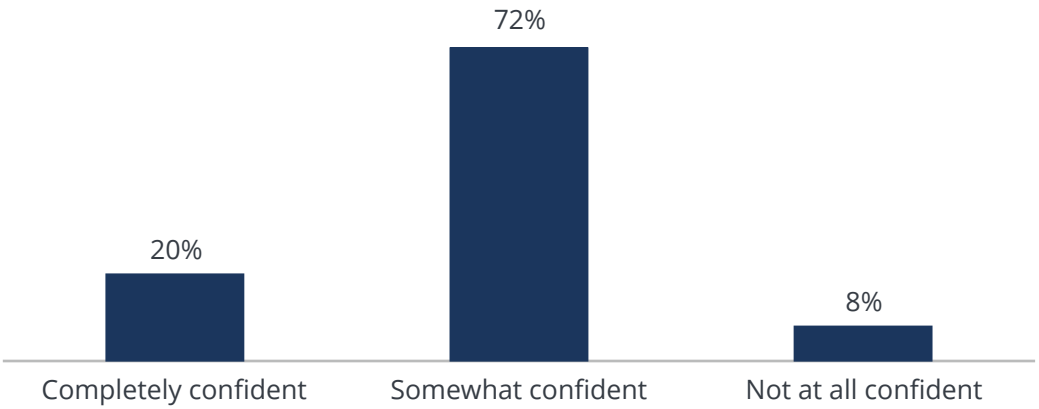
These findings are especially troubling given that 80% of all respondents said they were not completely confident in their organization's ability to defend their software build environment.

"Most respondents are fundamentally ambivalent about their ability to defend against attacks on software development, and this is a clear indication that leadership teams need to establish clear priorities and strategies for this critical area of security. After all, we're talking about intellectual property that makes up organizations' competitive advantage. In the age of digital transformation, there is nothing more important than protecting the code that makes your business competitive," Bocek said.

Executives: In your opinion, which role or team SHOULD be responsible for securing software build pipelines?



How confident are you about your organization's ability to defend against a cybersecurity attack that targets your software build environment?



// Why is there so much confusion about protecting software build environments?

Application developers, of course, are the closest to software build pipelines, and it makes sense that they would play a key role in securing these pipelines. And no developer wants to put out insecure code. However, it's also important to remember that developers are incentivized to deliver features and functions required to meet business goals. And the pressures that leadership puts on developers to meet aggressive development goals means that developers are often put in an either/or position, where they have to choose between features and security. And because most developers lack the deep security expertise needed to manage such a complex problem, it isn't surprising they focus on their primary area of expertise, which aligns with their organizational goals and incentives.

This situation will continue to worsen as more organizations embrace DevOps because this development approach requires shorter release cycles. Minimizing release cycles further reduces time set aside to address technical debt and improve security. It doesn't help that most organizations expect InfoSec to be responsible for all infrastructure security. On the other hand, InfoSec teams face constraints that prevent them from taking on this challenge. For one thing, most InfoSec teams don't have a charter from senior management to improve the security of software development environments.

But even if InfoSec teams had explicit organizational support to improve security across the build pipeline, they wouldn't necessarily have the deep software expertise needed to effect change. Moreover, they don't have visibility into the intricacies of the software build pipeline, nor do they understand the pressures developers face. InfoSec teams simply don't have the leverage to effect meaningful change—at least on their own.

To shift security left quickly, it's clear that application development and InfoSec teams need to combine their expertise to defend the software development pipeline against attacks.

"Developers are being told to build more, faster. Security is being told to protect more, faster. The fundamental problem is that these are still seen as two separate and distinct goals. What engineering and security teams need is the goal to move fast and staying secure—the mission that Formula 1 engineers know best. You can't operate at the extremes of performance without being safe. Until executives make "fast, secure" their business's mantra, we won't see the fundamental changes required to shift security left without compromising engineering productivity," said Bocek.

// The way forward: Engineering must take charge

To successfully shift security further left than attackers, engineering teams—which encompass product development engineering, infrastructure engineering and product security engineering, as well as application development—must take the lead. Only engineering has the visibility and span of control to effect the necessary changes. Unlike InfoSec, engineering intimately understands the complexities of the software build pipeline, as well as the deep knowledge base needed to ensure these changes work in concert with competing pressures to build and iterate software quickly.

But engineering can't take on this task alone. They need the guidance and expertise InfoSec can provide to ensure that security controls are effective and corporate policies are being enforced. This approach represents a sea change from the traditional infrastructure security model; it requires both teams to throw off old ways of thinking and collaborate in new ways.

Ultimately, it will be up to senior leadership to support the initiative to shift security left. Leadership needs to recalibrate the pressures currently placed on developers so that security of the CI/CD pipeline becomes as important as fast development cycles. In addition, leadership must supply the resources to support them, including incentives and guidance from InfoSec and outside sources as needed, along with technologies. Leadership must also get InfoSec on board to work closely with development to ensure that all security processes developed anywhere through the software build pipeline adhere to corporate and regulatory standards.

"All signs point to more engineering teams adding their own security experts. Increasing board-level and executive concerns will lead to less and less tolerance for breaches in software development. Just like we saw many CISOs quickly replaced after a breach, we're likely to see the same with engineering leaders. Over time, today's product security teams will merge with today's IT security teams. There must always be a team focused on defending the business from attack," said Bocek.

// How do we get there from here?

It's essential that security controls are pragmatic. This means that no security control will be implemented if it proves to be an impediment to the timely delivery of new software. In other words, security controls must not impose restrictions on process or tools. Moreover, they cannot slow down development teams the way old-school InfoSec processes too often did.

First off, all software build security controls should map to the four stages of software development pipelines:

- **Code:** Developers design software and commit code to code repositories.
- **Collaborate:** Developers include external and internal libraries and share software for review.
- **Staging:** Software is built and prepared for final delivery.
- **Production:** Software is run anywhere.

And all security controls designed for pipelines should also adhere to the following design philosophy tenets:

- **Principle of least privilege:** Grant only access and permissions required to accomplish a job.
- **Immutability:** Artifacts and infrastructure are not modified after deployment to an environment. Any necessary changes must be done in the image or script within the development environment and then promoted through the higher environments.
- **Everything as code:** Infrastructure, security policies and other parts of the pipeline are implemented as code and subject to the same controls as software artifacts.
- **Traceability:** All changes to any code must be revision-controlled. This principle works in concert with Everything as Code methodology.

// Conclusion: Time to shift security left and engineer attackers out of software build pipelines

We already know that the attack on SolarWinds was not unique. Experts are only beginning to understand the full scope of the damage brought about by the SUNBURST hack as new attacks—most notably the one on Codecov that affected IBM, HPE, Proctor & Gamble and potentially many other companies—are being reported. We all expect these types of attacks to continue and escalate. And we already know that the cost of cleaning up after a software supply chain attack are prohibitive. Solar Winds spent $19 million in the first quarter after the attack, but the price paid by their customers is incalculable.

Organizational change is hard, and that's all the more reason for executives and managers act now to empower the people closest to building software: engineers. They also need to clearly charter InfoSec teams to support them so the organization can remain agile and deliver secure software without compromising delivery schedules. However, we all know this type of change won't happen if organizations fail to clarify who is responsible for building a resilient environment that effectively defends against these types of attacks.

"Time is ticking. Boards and executives will be held accountable for failing to build secure software, much like executives at companies (e.g., Equifax) more traditional security breaches occurred were held accountable," Bocek said. Leadership must make decisions to designate accountability and clearly identify how the organization needs to change. If we fail to change quickly enough, we are putting our business and our customers at risk—and the damage could be immeasurable.

If you're looking for help to secure your software build environment—or you're otherwise interested in learning how Venafi has helped hundreds of the world's most security-conscious organizations build effective machine identity management programs, contact us at **venafi.com**.

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

About Venafi

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to- machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit venafi.com