CloudBees Global C-Suite Security Survey

The state of enterprise security with input from 500 executives.

CloudBees

Supply Chain Security is Top of Mind But Reality Reveals Concerns

In light of the Solar Winds supply chain attack, we wanted to take a deep dive into the security consciousness and preparedness of executives around the world. We commissioned Regina Corso Consulting to survey 500 C-suite executives about the state of their organization's software supply chain. This ebook provides top-level results and insight into the inner workings of security in enterprise companies around the globe.

We discovered that as software becomes the primary source of customer experience and value, supply chain security is getting the attention it deserves and at the proper levels in the organization. However, this study reveals gaps that indicate supply chain security is not well understood, nor are systems as robust or comprehensive as they should be.

Bottom line, the results reinforce the concept that software supply chain security needs to go beyond "shift left" to "shift security everywhere" — *with automation.* The software you are developing must be as secure as possible, but it doesn't stop there. The delivery process itself must be protected, and you have to be able to detect and instantly mitigate problems in production to consider your software supply chain as secure.

As always, we're standing by to help you automate and manage your software delivery to ensure security and compliance and to streamline and accelerate DevOps. It's what we do.

Prakash Sethuraman
Chief Information Security Officer, CloudBees

95%

say their software supply chains are secure or very secure but…

64%

say it would take more than four days to fix a problem

CloudBees

Is supply chain security top-of-mind?

95%

When it comes to software supply chains, one thing is clear: almost all C-suite (95%) executives are actively discussing the security of their software supply chain. They also believe (96%) their architects and/or designers have the knowledge and expertise to build and/or ensure a secure software supply chain.

Are their software supply chains safe?

95%

SECURE

Almost all say their software supply chain is secure with over half (55%) saying it is very secure.

90%

COMPLIANT

Almost all say their supply chain is almost or completely compliant, with over half (52%) choosing completely compliant.

70%

PUT SECURITY FIRST

Many feel it is more important to be secure and compliant than fast and compliant. The remaining 30% rank speed and compliance first.

CloudBees.

Are they prepared for an attack?

93%

Nearly all C-suite executives feel prepared to deal with ransomware or cyberattacks on their software supply chain, and over half say they are very prepared. More than 9-in-10 believe they would be very comfortable in their ability to respond if their supply chain were attacked.

Are they *really* prepared?

64%

UNSURE

Almost two-thirds of C-suite executives (64%) are unsure who they would turn to first if their software supply chain were attacked.

45%

NOT THERE YET

2-in-5 C-suite execs are half of the way finished securing their software supply chain, while only 23% are almost finished.

89%

SHIFTING LEFT

Almost all C-suite execs agree that the need to shift left enables them to secure their software supply chain.

But, are they *ready* to react?

75%

Three out of four C-suite executives think that security can be the **“department of slow.”**

And how *fast* can they react?

C-suite execs estimated timeline to resolve a security incident:

1-3 DAYS	4-7 DAYS	2-3 WEEKS
30%	39%	23%

How vulnerable are they?

Almost three-quarters of C-suite executives would rather deal with a natural disaster than a security issue in their software supply chain. But overall, these executives now think more about securing their supply chain than they did two years ago. They worry about employee disruption (83%) as tech staff will stop innovating to 'fix the problem,' and that their brand will suffer (93%).

While they exude confidence about their readiness, digging deeper reveals there's more work to be done. More astounding is that almost two-thirds of C-suite executives are not sure who they would turn to first if their supply chain were attacked.

What would they do if attacked?

- 58% have no idea who to turn to
- 88% would get a consultant
- 86% would work internally without letting others know
- 76% would shut everything down for a few days to deal with the issue

And, is their software secure...

CloudBees.

Software Supply Chain Technical Checklist

C-suite executives agree they have these issues covered

Most executives (95%) say container images are checked for high or critical vulnerabilities and their automation access keys are set to expire automatically.

Use of GPG Keys

Company only accepts commits signed with a developer GPG key (92%)

Registries Limited

Dependencies to trusted registries are limited at their organization (90%)

Restricted Access

Administrative access to CI/CD tools are restricted (89%)

Software Supply Chain Technical Checklist

C-suite executives are split across the board on these issues

Just about half of executives say artifacts are stored in separate repositories in development and artifacts in higher repositories are signed.

Signatures Validated

Prior to deploying artifacts, signatures are validated against the digest (51%)

In Production

Artifacts are stored in separate repositories in production (49%)

Prior Validation

Digest is validated against the artifact before deployed in that repository (46%)

In Staging

Artifacts are stored in separate repositories in staging (42%)

Software Supply Chain Technical Checklist

C-suite executives are low on software automation

One-third of C-suite executives say their software delivery supply chain is completely automated, while over two-in-five say it is *almost* completely automated. One-quarter say it is about half automated or less.

Process Defined

All steps in the process are clearly defined (73%)

Use People

Relies on people in every step (62%)

Use Automation

Supply chain incorporates automation (71%)

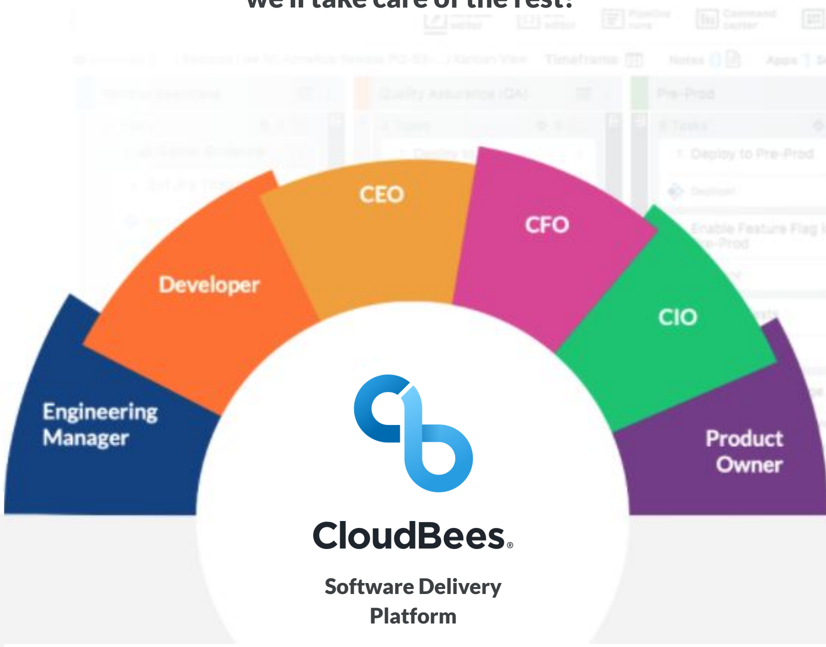
Secure Your Supply Chain With Software Delivery Automation

CloudBees provides the leading DevOps solutions for large and compliance-first organizations. We enable developers to focus on delivering great software, while providing higher-order visibility and management with powerful risk mitigation, compliance and governance capabilities.

Our software delivery automation platform powers:

- **Continuous Integration:** Integrate and automate the build, test and packaging of code to artifacts.
- **Continuous Delivery:** Eliminate scripts and automate deployment pipelines while verifying performance, quality and security.
- **Release Orchestration:** Model, orchestrate and visualize complex application releases and deployment models, with built-in audit trails.
- **Engineering Efficiency:** Track, measure productivity data and optimize delivery.
- **Feature Flags:** Release and manage new features rapidly across the entire SDLC.
- **Value Stream Management:** Visualize value flow and access key analytics.

You develop great software, we'll take care of the rest!



Engineering Manager

Developer

CEO

CFO

CIO

Product Owner

CloudBees.

Software Delivery Platform

Transform your software delivery with CloudBees.
Click to connect with one of our DevOps experts today.

BOSCH · Capital One · Nationwide Building Society · PEGA · THE HARTFORD · Fidelity INVESTMENTS · Allianz · DZ BANK · AUTODESK · Vrbo · HSBC · STADIUM GOODS

About the Survey

CloudBees commissioned Regina Corso Consulting to survey 500 C-suite executives from companies with at least 250 employees to understand how they feel about their software supply chain. Of the C-suite executives participating in the survey, 150 were from companies in the United States, 125 each were from Germany and the United Kingdom, and 100 were from France.

The Global C-Suite Security Survey was conducted online between August 9 and 18, 2021.

CloudBees.

About CloudBees

CloudBees, the enterprise software delivery company, provides the industry's leading DevOps technology platform. CloudBees enables developers to focus on what they do best - build great software - while providing peace of mind to management with powerful risk mitigation, compliance and governance tools. Used by many of the Fortune 100, CloudBees is helping thousands of companies harness the power of continuous everything, setting them on the fastest path from a great idea, to great software, to amazing customer experiences, to being a business that changes lives.

For more information, visit www.cloudbees.com

CloudBees

CloudBees CI is built on top of Jenkins, an independent community project.
Read more about Jenkins at: www.cloudbees.com/jenkins/about

CloudBees, Inc. 4 North Second Street | Suite 1270 San Jose, CA 95113 United States
www.cloudbees.com nfo@cloudbees.com

0921v00

CloudBees®