

Are you the next victim of a shift left attack?

More than 80% of CIOs believe their software supply chains may be breached

Shift left attacks have metastasized since the notorious SolarWinds attack. And they have CIOs worried.

CIOs admit to vulnerability

82% of CIOs believe their organization is vulnerable to cyberattacks targeting software build pipelines.

82% Feel vulnerable to software supply chain attacks

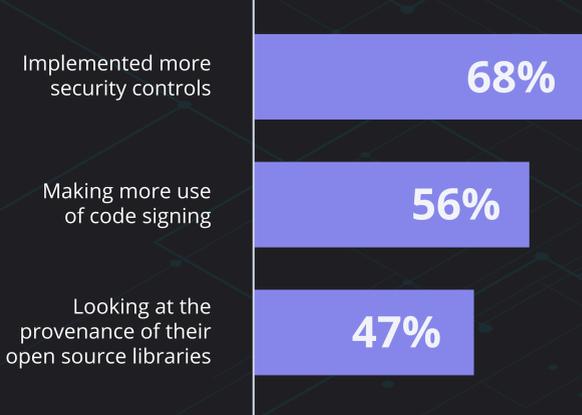
Pressure to protect intensifies

85% of CIOs are mandated by senior leadership to improve software build pipeline security—now.

85% Feel pressured to improve software build pipeline security

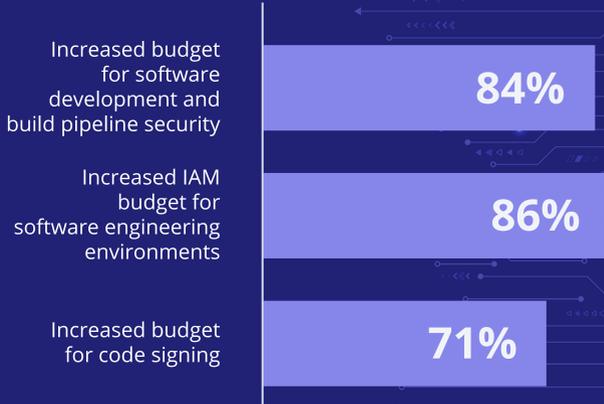
CIOs taking preliminary steps

The majority of CIOs have already started to change their approach to securing software development environments.



Majority are recalibrating budgets

CIOs are increasing their budgets dedicated to security, Identity and Access Management (IAM) and code signing for software development and build pipelines.



Security strategies not shifting left as fast as attackers

Engineering, which is closer to the epicenter of the attacks, is largely not responsible for securing software development pipelines.

InfoSec still holds that control.



61% Owns security of software build environments

62% Holds security budget for software build environments

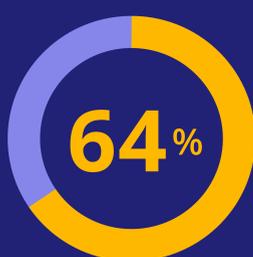
Security policies mainly unenforceable

CIOs are worried that software developers are likely to compromise on security policies to meet tight SLAs for new products and services.

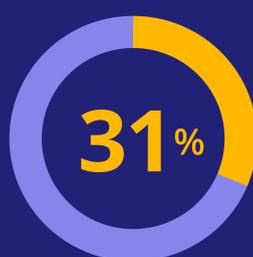


87% Agree software developers may compromise security for speed

95% of InfoSec teams have authority over security controls for software supply chains, but 31% have no way of enforcing them.



Can proactively recommend and enforce security



Can proactively recommend but not enforce security controls

What's really at stake?

Every piece of improperly secured code could serve as a portal for attackers to infiltrate—and destroy!

Ready to shift left to secure your software supply chain?

Visit venafi.com/platform/code-signing-checklist

