A THREAT STACK REPORT

52% of Companies Sacrifice Cybersecurity for Speed

BRIDGING THE GAP BETWEEN SECOPS INTENT AND REALITY

threat stack

CONTENTS

EXECUTIVE SUMMARY

The majority of organizations are, at least in practice, willing to sacrifice security at the altar of speed. As long as this is the case, the long-held dream of marrying DevOps and Security simply won't come true. And that's bad news for everyone.

To better understand why SecOps has stalled out, we recently surveyed a group of development, operations, and security professionals about their attitudes toward security.

We found a huge gap between intent and reality when it comes to practicing SecOps. Most organizations agree that everyone should be responsible for security, but this principle is not being upheld in day-to-day practice.

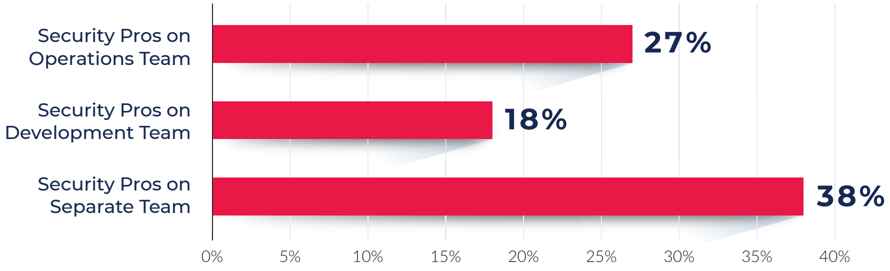
In this report, we examine why the vision for SecOps hasn't become a reality at most organizations. We look at specific obstacles and attitudes to illuminate what is standing in the way, even at organizations where a stronger security posture is an explicitly stated goal. This report explores these struggles and provides actionable steps for getting security and operations better aligned at your organization.

> "If there is no struggle, there is no progress."
>
> FREDERICK DOUGLASS, 1857

THE PLAYERS INVOLVED

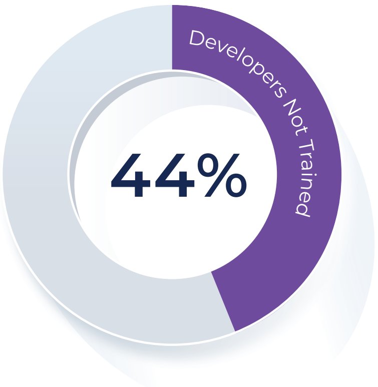
Security is (Still) Siloed

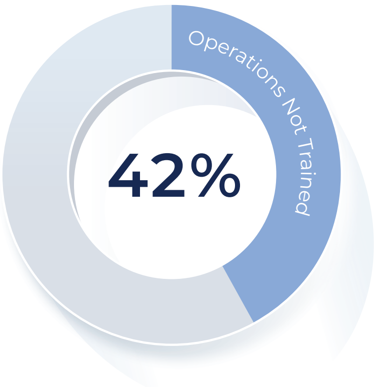
A security specialist is assigned to the operations team at only 27% of the organizations we surveyed, and security pros are on board with development teams in just 18% of cases. At 38% of organizations, security is a completely separate team that is only brought in “when needed.”



Developers Can’t Code Securely

It wouldn’t be such a big deal for security to be siloed if it weren’t for the fact that 44% of developers aren’t trained to code securely. Without this basic knowledge, coding is often done without security in mind. This forces security to become a bottleneck when they must inevitably step in and intervene. This not only slows down the process, but also creates resentment between these teams, making it even harder for them to cooperate.





Operations Doesn’t Have Security Training

A full 42% of operations staff admit that they are not trained in basic security practices, which means that they can’t configure servers securely. It also means that they don’t see deploying security as part of the configuration management process, which allows security best practices to fall by the wayside. When ops pros aren’t trained in security, there’s no way SecOps can succeed.

Given the above, it’s no surprise that 60% of respondents admit that security is not being integrated into DevOps processes today.

WHEN SECURITY IS SACRIFICED FOR SPEED

52%

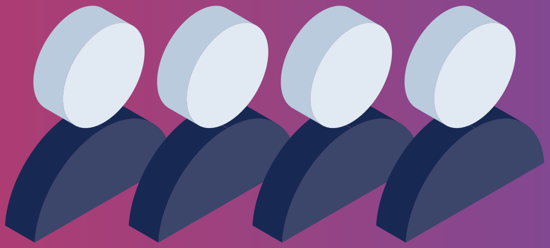
of companies admit to cutting back on security measures to meet a business deadline or objective.

And since the directive for speed starts at the very top, it's hard to ignore — even if it means that security becomes roadkill in the process.

68%

of companies state that their CEOs demand DevOps and security teams not do anything to slow the business down.

We can hardly blame them in today's fast-paced, competitive world. For rapidly scaling businesses, the speed of innovation and execution is what drives the business forward. Therefore, slowing down code reviews or deployment can mean a direct impact on the bottom line, as well as customer satisfaction.



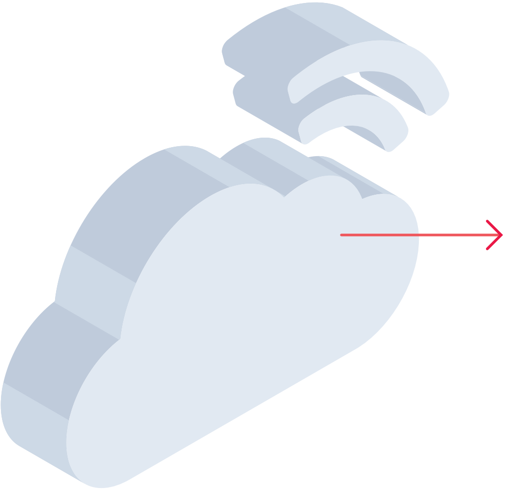
62%

say their operations teams push back when asked to deploy secure technology

57%

say their operations teams push back on security best practices.

While employing these doesn't have to mean slowing the business down — if it isn't done correctly, it certainly can. And that may feel like a risk that's too great to accept.



60%

of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures by 2018

ACCORDING TO GARTNER

So the lack of successful SecOps implementation impacts organizations in one area more than any others: the security of cloud infrastructure.

Running in the cloud has the obvious benefit of enabling organizations to move at the speed necessary to run a successful modern business. It's also more secure, at least when configured and deployed appropriately. Yet more than half of SecOps professionals rate the security of their organization's cloud infrastructure and environment as "average or worse." Without SecOps practices embedded from within, it's easy for cloud infrastructure-based threats to slip through the cracks and expose companies to attack.

CASE STUDY

Genesys Boosts Security and Compliance of Microservices Deployments on AWS

When Genesys transitioned their applications and workloads to AWS, the operations and security teams faced a new challenge: Ensuring complete security and compliance across an ever-changing environment. The environment supports Genesys' leading cloud contact center solution.

Threat Stack provides Genesys with security that accelerates the company's continuous deployment model and reduces the time to security incident detection.

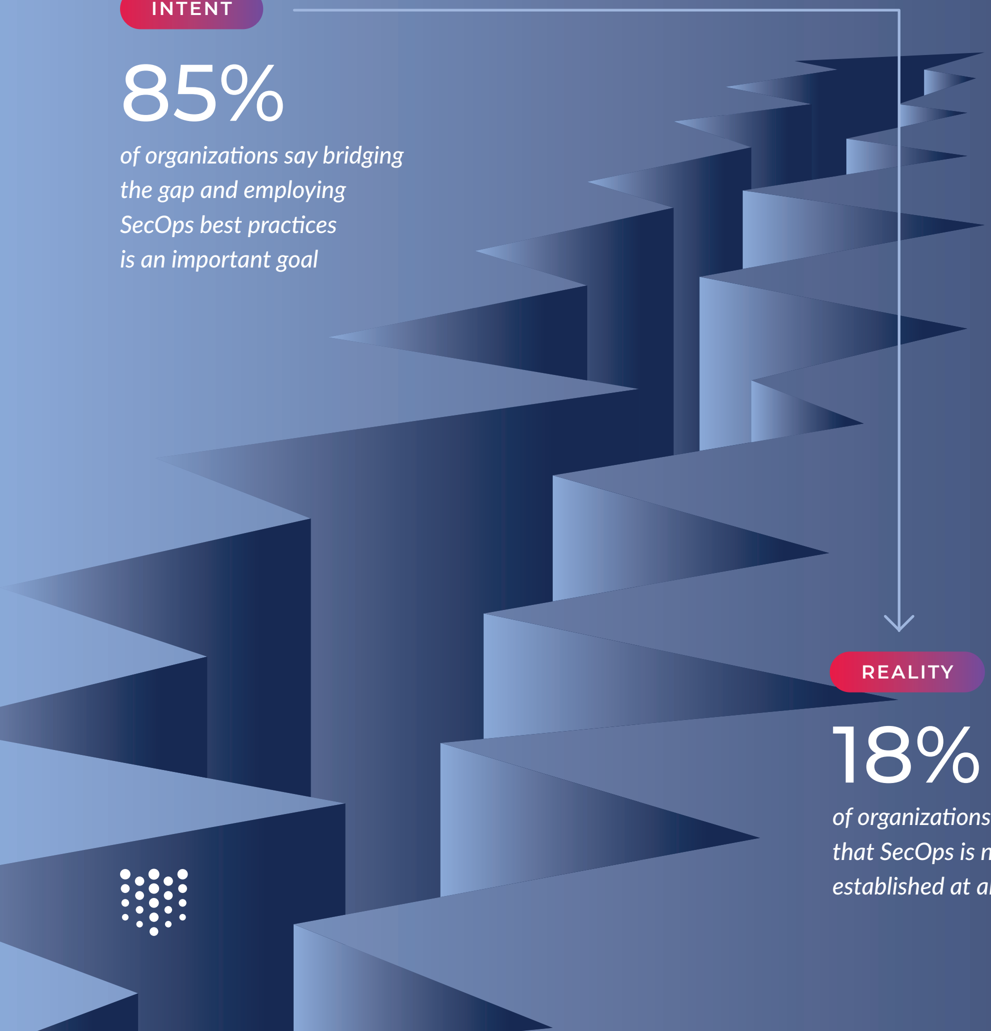
> **We don't deploy code to an existing server. Instead, we spin up a new microservice on a new server, go through the configuration management process, and tear down the old server. Monitoring for anomalous activity throughout this process is key.**

JARROD SEXTON
Lead Information Security Manager, Genesys

GENESYS™

THE CONFLICT

SecOps Intent vs. Reality



INTENT

85%

of organizations say bridging the gap and employing SecOps best practices is an important goal

REALITY

18%

of organizations say that SecOps is not established at all

The Divide

Given the findings stated earlier, you might be surprised to learn that the majority of organizations (85%) say bridging the gap and employing SecOps best practices is an important goal for them. Another 62% of operations pros and developers insist that security has actually become a bigger priority for them recently.

Yet just 35% say that SecOps is a completely or mostly established practice at their organizations, and 18% say it's not established at all.

What Gives?

The purpose and intent of SecOps is to build on the mindset that "everyone is responsible for security" with the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required.

But the obstacles we detailed on page 4, as well as the on-high directives we shared on page 5, mean that the gap between good security intentions and cold, hard reality remains a wide one today.

GOING DEEPER

Is SecOps in the Eye of the Beholder?

It's one thing to recognize the intent vs. reality gap and admit, "Yes, we mean to implement security, but we aren't doing it successfully. Time to shape up!" But what if different parts of your organization can't even agree about your current reality? In other words, what if some folks think you are running securely and others don't? Interestingly, our survey revealed that different team members in different departments often do not see eye to eye on whether SecOps is being implemented.

Respondents were asked whether SecOps is an established practice at their companies:

10% of DevOps professionals said "not at all"

25% of security professionals said "not at all"

In other words, there's a 15% gap that comes down to perception.

Respondents were asked to rate their organizations' awareness and ability to detect and remediate security incidents:

41% of DevOps professionals responded that their ability was "average or above"

35% of security professionals responded that their ability was "average or above"

This likely means that DevOps pros are overestimating their organizations' security capabilities, given that security pros tend to have their fingers pretty firmly on the pulse of these issues.

Respondents were asked if they have the ability to fix a security-related issue themselves:

44% of DevOps professionals said they would have to rely on someone else

35% of security professionals said they would have to rely on someone else

In other words, they do not have access to the tools or environment required to fix security flaws.

NOW WE MAKE PROGRESS

There is little controversy among either the DevOps or the security community around the general idea that security must be integrated into the entire development lifecycle.

THE CHALLENGE, CLEARLY, IS IN TURNING THIS WIDELY ACCEPTED IDEA INTO A WIDESPREAD REALITY.

There are several reasons why this has not been a linear path. Obstacles include a security talent shortage, siloing, and a need to update skills across teams — as well as some major rifts in perception. It's important that teams begin to work more closely together and to examine the reality of their organizations so they can agree on where the SecOps transition really stands and what it will take to move forward.

To help you meet these objectives, let's take a look at four concrete ways that teams can begin to close the SecOps chasm.

01 Start at the Top

If C-level executives value speed over security, there's no way SecOps can succeed. Remember: Security has ROI benefits, too, from speeding up sales cycles to opening up entirely new markets. Executives should understand the rewards of running both fast and securely, and should champion the need for secure processes and strategic investment in both people and tooling to support the SecOps cause.

02 Get Real

Survey your team and find out what various teams' and roles' attitudes are toward the value of security and the current reality of your organization's posture. This should give you a sense of where perception gaps exist and what it will take to open everyone's eyes to where you really stand, so you can move forward with purpose.

03 Teach Them to Fish

DevOps teams need to know how to use security tools and how to incorporate security best practices into their workflows. Security teams, likewise, need to learn how to code and integrate their efforts into continuous deployment cycles. Don't wait for this process to happen organically; you must make a conscious investment in alignment and education across teams. In other words, teach them to fish, and SecOps won't just be a pipe dream.

04 Prioritize by Risk

Overwhelmed by your security to-do list? Start with infrastructure because this area holds both the highest risk and the greatest reward. Make sure you are following configuration management best practices and implementing security alerts that are well-tuned to your unique organization. Securing your infrastructure will have a ripple effect throughout the organization, from app dev to operations.

METHODOLOGY

Research was based on the following:

- 200 Security, Development, and Operations professionals surveyed
- Professional companies ranging from SMB and mid-market to enterprise organizations in North America running one or more production app/ service in the public cloud (IaaS and/or PaaS)
- Organizations covered multiple industry verticals including manufacturing, information technology, business services, and financial

ABOUT

Threat Stack enables businesses of all sizes to securely leverage the benefits of cloud computing by identifying and verifying insider threats, external attacks, and data loss in real time. Purpose built for today's infrastructure, Threat Stack's comprehensive intrusion detection platform combines continuous security monitoring and risk assessment to help companies gain an unparalleled level of visibility at the speed and scale of today's business. Located in Boston, Massachusetts, Threat Stack works with nearly 400 security-minded customers.

www.threatstack.com
support@threatstack.com | sales@threatstack.com
617.337.4270 | @threatstack

Additional Security + Compliance Resources

Lean Cloud Security: Your Guide to SecOps Efficiency in the Cloud

DOWNLOAD

Compliance Playbook for Cloud Infrastructure: A Guide for Building Compliant Businesses in the Cloud

DOWNLOAD

SecOps Playbook: How SecOps Enables Secure Code Release, At Scale and At Speed

DOWNLOAD