6 Strategies to Empower Secure Innovation at Enterprise Tech Companies

RAPID7

If we had to make a bet, we would wager that your team sees a similar dynamic play out on a weekly basis: Your development teams are under pressure to deliver new products and features at lightning speed. They view security as an afterthought or a hurdle that they jump over to get to market as fast as possible and then circle back to make improvements after an initial release. Engineering spins up new workloads or tests new apps, and the "critical" alerts start rolling in. And those are just the alerts for the workloads you know about, because rest assured, there's some shadow IT lurking out there.

As much as you might like to just hit "pause," investments in cloud aren't slowing down anytime soon. According to Gartner, public cloud spending will exceed 45% of all enterprise IT spending by 2026 – an increase of 28% in five years.

However, while the cloud enables development teams to move faster, it's easy for security teams to feel as though they're viewed as the ones responsible for slowing down progress. This is especially true at technology companies, where speed and innovation are prized above all else.

Yet a strong cloud security posture is arguably more essential than ever. In a study conducted by IBM, 80% of the decision-makers surveyed said that having data security embedded throughout cloud architecture is important or extremely important.

It's time to change the dynamic between security and engineering. This eBook is designed to help security professionals successfully partner with engineering and DevOps colleagues, turning cloud security into an enabler — not a blocker — of innovation.

THIS GUIDE IS FOR YOU IF:

You're a security leader or senior security practitioner at a large tech organization with a multi-cloud environment.

IN IT, WE'LL SHARE:

1. The unique security challenges that tech companies just like yours face

2. Six strategies to overcoming these challenges

3. Practical ideas to start implementing changes right now

THE PATH FORWARD: INTEGRATING SECURITY, DEVELOPMENT, AND OPERATIONS

Your security team and your dev colleagues don't need to be frenemies anymore.

It's possible – and beneficial for everyone – for you to partner with engineering to release secure products and services without slowing down innovation.

Security needs to become an enabler rather than a blocker, and a business driver rather than a cost center. With the right technology, processes, and people in place, great security can be integrated seamlessly into technology innovation cycles.

Let's explore how to do exactly that.

1 Create a culture of security.

Cybersecurity is about far more than technology. Equally important are the behaviors your employees exhibit with emails, data, and apps, all of which impact your organization's overall security posture. And there's no better time to start creating a culture of security if you don't have one already at your organization.

This is especially important when it comes to your organization's engineering teams that typically have the freedom, the know-how, and the access to stand up new tech as they please. For example, helping your developers get in the mindset of turning on multi-factor authentication (MFA) when testing out new software is a great first step in cultivating that culture of security.

Another example we increasingly see among tech companies that are adopting a culture of security is the move from DevOps to DevSecOps. Building security into the development process before deployment benefits everyone. According to a report from Chef.io, "DevSecOps adopters are three times as likely as non-adopters to see security as something that speeds software delivery and most organizations (84%) agree security improves quality as well." (Pro tip: You can even share these stats with your own team and your friends in engineering as you're making the case to implement DevSecOps processes.)

DevSecOps increases operational efficiency across various departments, including your own security team.This means earlier detection of code vulnerabilities, enhanced product reliability, and ultimately fewer PagerDuty notifications jolting your analysts out of bed at 2 a.m.

Above all else, DevSecOps allows organizations to provide their customers with increasingly secure products at an accelerated rate – a win-win for everyone. And it's easier to advocate for and make these culture shifts in a company when all employees already view security as part of their core responsibilities, whether the word "security" is in their job title or not.

GET STARTED:

Creating a culture of security starts with education. Hold a lunch-and-learn session for the whole company about common security issues, or host a security awareness challenge. These can bring security best practices to light in a more interactive way. Take it a step further and identify a few potential security champions, particularly in technical departments. Create additional training opportunities and empower them to identify and bring security issues to your team.

2 Focus on security by design. Prioritize prevention.

The goal with cloud security should always be to prevent issues as early in the software development lifecycle as possible. While simple misconfigurations might seem easy to avoid, the reality is that 65-70% of all security challenges in the cloud arise from misconfigurations, according to TrendMicro. These vulnerabilities, if not caught before deployment, can have expensive consequences. The Ponemon Institute and IBM found that the average cost of a data breach increased in 2021 from $3.86 million to $4.24 million – that's the highest average cost of a data breach in the 17-year history of the report.

That's where security by design comes in. Security by design is the concept of making your organization's products as secure as possible before the code is deployed to your cloud of choice. By catching problems like misconfigurations or policy violations before they hit production, you'll improve efficiencies for both the development team and your analysts. This approach enables teams to correct issues once instead of repeatedly trying to catch and fix them when it's time to deploy a new release.

Making strategic changes to intrinsically build security into your development and operations processes can significantly improve developer productivity and stop security and compliance risks before runtime.

GET STARTED:

Work toward implementing Infrastructure as Code (IaC) security checks. This enables teams to embed security and compliance policies into the CI/CD pipeline, giving your team the ability to evaluate the risk of IaC templates before they're put into use. If you're looking for tips and advice on how to get started, we shared our best pointers for how to implement secure and compliant IaC in this blog post.

3 Choose dev-friendly security tools and services.

If you give a developer a credit card… …you'll probably get some shadow IT to go with it.

If you don't want your counterparts in engineering to go around using whatever software and apps they want — and quite possibly releasing less-than-secure code into the wild — then you need to procure developer-friendly tools that also include built-in (and simple) security checks.

This means they need to be easy to use and not require a PhD in cybersecurity or handholding (or wrist-slapping) from a security professional to manage. Ideally, these tools should also offer the dev team periodic security checks as they're writing code. Your security team and engineering colleagues can work well together if you adopt developer-friendly security paradigms, like security by design and IaC.

What's the best way to bake security into development? By making sure security happens as early in the CI/CD pipeline as possible. While many security tools can only be used after code is submitted for deployment, developers prefer a command-line interface that can be installed anywhere, allowing them to run checks on-demand during the dev process to check their work before final deployment.

Catching security issues early and fixing them quickly allows the dev team to keep moving forward, meeting the demands of other stakeholders in your organization that expect new, innovative product features to be released constantly. If you want your team to be viewed as a true partner to development, the security tools and processes you implement must enable engineering to move at the speed of innovation.

GET STARTED:

Curious about what security tools your organization's developers might want to use? Ask them! Talk with your dev teams about what security tools they've used and liked. Ask them what they look for in a security tool (or tools in general). What features are helpful, and which ones slow them down? Use that information when you choose a cloud security platform or provider.

4 Improve visibility and assess risk, exploitability, and impact.

CVSS-based risk scores often result in thousands of "critical" vulnerabilities. No business, even one with an army of analysts, has the resources to immediately address each vulnerability across their environment as they pop up.

Because it's impossible to review and remediate every single vulnerability, it's important to prioritize issues based on risk, exploitability, and impact. For example, regardless of how critical a vulnerability is, if it lives in a development container with no access to the public internet and is scheduled for redeployment nightly, you likely don't need to spend time remediating it. Rather, focus on the issues that are exploitable and have the potential for significant impact.

In short, think like an attacker. Prioritize remediations by understanding which vulnerabilities would be most attractive to a bad actor. For example, understand where you have commercially sensitive assets and how those assets are connected to the organization's core business processes. Protect those first.

If you know where your biggest risks are, you can prioritize remediation effectively.

In order to do this, you need total visibility into all your cloud resources, paired with guidance for your analysts so they know which fixes to prioritize and which don't require their attention.

5 Automate, automate, automate.

Once you have full visibility into your environment and a strong sense of your organization's risk, identify the threats that are repetitive and predictable – or can easily be fixed when the right context is applied – and automate the remediation of those. Automation is essential if you want to achieve both security and speed to market at scale. Otherwise, you and your team will be stuck playing a never-ending game of whack-a-mole with an unmanageable amount of security alerts. And we all know the dev team won't be too happy with the endless rounds of code reviews.

Simplifying cloud security with automation will save time and money while reducing your organization's risk. Another benefit: Automation allows you to keep your talented team of security pros focused on the interesting, strategic activities — the stuff that made them want to join your team in the first place — rather than rote tasks.

Secure cloud configurations and workloads through automated security and vulnerability management, even across complex, ephemeral cloud environments. This is a great way to future-proof your security, making it even easier for teams across your organization to quickly adopt the latest and greatest tools without introducing unnecessary risks.

GET STARTED:

Make a list of the most common security activities your team is doing manually that could be automated. Prioritize them in order of "most time spent" and "most easily automated" and start there.

6 Build relationships to get a seat at the table.

Before the introduction of cloud computing, security teams like yours were primarily responsible for securing networks, servers, software, and storage. Fast forward to today, and the traditional "perimeter" no longer exists. Today, security teams are responsible for protecting so much more, ranging from identities to data to intellectual property.

No matter what assets you're protecting, security is rooted in improving business outcomes and reducing business risk. That's why it's essential for you and your team to build relationships with your colleagues across departments, from engineering to product to marketing and sales.

Start (or continue) implementing the strategies we shared in this eBook to show you're committed to making security easier. Demonstrate how better security will benefit the business, and you'll experience less resistance when asking for a role in executive-level strategic business discussions, the budget you need to be successful, or buy-in from other leaders across the company.

GET STARTED:

Set up time to get coffee (or chat on Zoom) with your counterparts across departments. Share specific examples of how you and your team are working to make security easier. Ask for their feedback on strategic projects you've planned that will impact the entire organization.

Once you've established these relationships, ask to attend board meetings, C-Suite meetings, or other high-level discussions to present about what you're working on when it comes to improving cloud security. Focus on topics like money saved and business deals won as a result of great security controls and compliance. Find ways to highlight the value and importance of security to the business's overall success.

RAPID7

ENHANCE YOUR CLOUD SECURITY FOR BETTER, FASTER INNOVATION

While aligning security with quickly-evolving technology shifts like cloud computing and devops is never an easy endeavor, it is exciting and well worth the effort. You can tackle each strategy in this guide one at a time, or implement them all at once, continuing to build as your organization evolves. Just remember that cloud security is a journey; regardless of where you begin, use this guide as a roadmap to further your progress and build a security-based mindset into the core of your business.

Whichever path you choose, know that you'll be taking steps to empower your development team to operate more securely in the cloud with dev-friendly tools, automation, and appropriate (but not restrictive) guardrails… and these changes will benefit the entire company.

Want more advice on how to start your journey to better cloud security? We're here to help. Watch a demo of Rapid7's InsightCloudSec platform now, and let's talk.