Cloud Security Best Practices: **CISO Secrets Revealed**

Introduction: Empowering cloud security through collaboration

Enterprise adoption of the cloud during the past five years has been "staggering", according to Pete Chronis, CISO of Paramount, who recently participated in our CloudSec 360 event series.

However, this rapid adoption has revealed a troubling problem: silos within organizations, which create barriers between key players like CISOs, DevOps, and engineering teams.

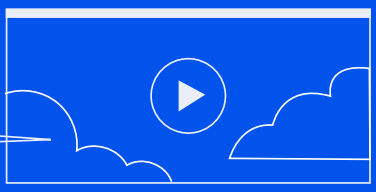
To address this issue, we brought together leading CISOs and industry analysts for our CloudSec 360 event series, where they shared insightson why collaboration is key to success.

This ebook is the result of those discussions and contains valuable takeaways for anyone looking to improve their cloud security strategy.

You'll learn

- How to normalize security-first behavior in teams across your organization and why this is central to scaling cloud
- Key steps towards rolling out the perfect cloud security strategy, including promoting greater collaboration.
- The biggest cloud security threats of 2023 and how to mitigate them

Watch the sessions now and discover more ways to scale your security program



Embedded security is key to scaling your strategy

Software development is now a sprint, not a marathon. Cloud has empowered DevOps teams to work at high speed, but security teams must keep pace or risk blocking innovation.

The answer is customer-centric security – closely collaborating with stakeholders, such as DevOps and engineering, as if they were customers. Security teams must evolve beyond looking for faults in code and policing non-compliant behavior to become the facilitators of innovation.

"Many security teams now realize that building adds a lot more value than finding bugs and breaking things," says Clint Gibler, Head of Security Research at Semgrep. "It's the difference between helping stakeholders do the right thing, rather than acting as a gatekeeper and preventing people from doing what they need to do."

In 2023, scaling your security program in a customer-centric way involves:

Creating self-service resources with security baked in
Security teams need to move their attention from finding weaknesses downstream to implementing security-by-design at the development stage. This involves building the tools and resources that dev teams need to perform successfully, with security already factored in. For example, they can collaborate with the platform engineering team in order to build security controls into standard tools and libraries across your company.

Embedding security team members in DevOps and vice versa
Think about starting an ongoing job swap between security, DevOps and engineering to help create a customer-centric security function. "When security team members embed in DevOps, for example, they should be taking tickets, building out features, shipping code for production and doing exactly what developers are doing," says Gibler. This can reduce silos and increase empathy, so the security team will appreciate their impact on DevOps and engineering and will be more inclined to design something with comprehensive benefits. This also works in the other direction, with engineers spending time embedded in the security team.

Ensuring security is easily embedded and consumed
Systems and processes should be designed so that taking the safest and most secure route makes absolute sense to all the teams involved. In Gibler's words it should be "as easy as clicking a button or configuring a line of code." He says, "If developers aren't behaving as the security team wants, it's not because 'they don't get it'. It's because the value proposition hasn't been made clear enough, or because security measures take too long."

Building shared capabilities
Design security tools and initiatives should deliver value across the organization. For example, an asset inventory gives security teams greater visibility, but it can also help finance understand your cloud bill and engineering knows which teams own what services. Similarly, security teams can use code scanning to find vulnerabilities or opting out of secure defaults, and engineering teams can use it to enforce coding standards or do code refactoring at scale. Gibler describes this approach as "hitching your security wagon to developer productivity."

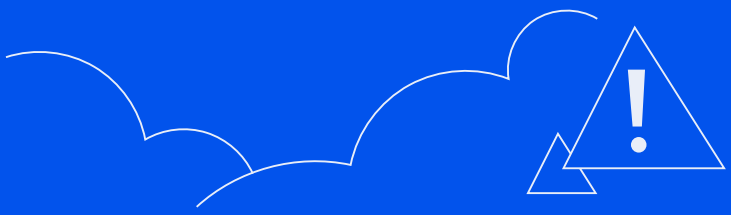
Watch "How to scale your company's security in 2023" and discover more ways to scale your security program

The era in which security teams work in isolation is over. CISOs must ensure they switch from being gatekeepers and blockers to becoming enablers and builders of guardrails. Security teams can do this by providing stakeholders with the tools and resources they need, but with security baked into their design.

Mitigating the biggest cloud security threats of 2023

Cloud attack surfaces are growing larger and more complex, while security budgets are being squeezed and criminals are getting smarter.

Even some of the biggest multinational corporations have fallen victim to cloud security threats in the past 12 months.



In many ways, cloud security teams face a perfect storm of risks during 2023. Here are some of the biggest threats:

API attacks – criminal exploitation of poorly configured and secured APIs
APIs are great at seamlessly connecting different systems and data sets, but they also add a level of insecurity on the cloud. This digital doorway is being increasingly exploited by criminals looking for an easy way to access critical networks. For example, hackers can access APIs if object-level permissions are not activated properly when APIs are configured. This back door can be closed by ensuring rigorous authorization policies are in place and all logged-in users are authenticated.

Eric Bauer, Director of Cloud Security at Procter & Gamble says "At P&G we focus on API visibility using specialist tools. I can't even begin to tell you how many APIs we have, so having a specialist tool that can correlate all that information, identify vulnerabilities where APIs have been misconfigured and provide useful remediation is vital. APIs need to be set up correctly, because they give direct external access to critical systems. Without exception, they need to be authenticated and encrypted."

Cross-tenant vulnerabilities – allowing unauthorized cloud tenants to access other tenants' data
Public cloud isn't always as secure as you'd expect. Recent breaches show how easy it can sometimes be for hackers to exploit security vulnerabilities and access other tenants' cloud data. Cloud users can assess the level of cross-tenant risk using the PEACH method:

Privileges – Ensure your choice of cloud provider offers minimal permissions within its service environment

Encryption – Is data encrypted with a unique key, regardless of where it's stored?

Authentication – Ensure communication between each tenant and the control plane is authenticated with a unique validation key

Connectivity – Check that all connectivity between tenants is blocked by default.

Hygiene – Ensure your cloud provider purges all unnecessary secrets, software and logs from your cloud environment, thus removing clues for hackers.

More threts on the next page

Cloud ransomware – enabling attackers to hijack entire cloud environments

Underestimate the cloud ransomware risk and you won't just have your data encrypted by a criminal - you could lose access to an entire cloud environment. That's because hackers create their own set of security keys once they hack into their victim's cloud environment, locking the legal owner out until they pay the ransom. Companies need to take a range of measures to address the cloud ransomware threat, including regular employee education, using anti-phishing tools, backing up data securely, blocking malicious websites and apps and ensuring security patches are regularly updated.

"Ransomware in the cloud isn't about spreading infected files," Bauer explains. "It's about compromising log-in credentials. Once criminals have gained access to your cloud environment, they can then create their own encryption keys and seize control, not releasing it until the ransom is paid."

Wiz's director of data & threat research, Alon Schindel, explains that in some instances criminals attack on-prem first, gain access and then they easily move across to the cloud. "That's why it's critical that the interfaces between on-prem and cloud are well protected," he says.

Cryptominer attacks – parasitic code inserted onto victims' servers to secretly mine cryptocurrency

Crypto miners can insert their malware onto a victim's server through code embedded in a website or an email phishing attack. Once in place, the malware can be difficult to detect manually. A behavioral analytics solution, however, may be able to identify unusual and unauthorized patterns of cloud server use triggered by crypto mining malware.

"Some of the most sophisticated cryptominers deploy their resources in the same way you do, so without a sophisticated behavioral analytics solution it can be incredibly difficult to spot," says Bauer.

Security teams must double down on key areas of vulnerability, ensuring they have fully audited their cloud environments, carefully authenticated and secured assets, ensured user access security is watertight and their data is encrypted.

Schindel says that employees have to be especially vigilant how they share login credentials. *"Ensure passwords are not shared via your Slack channels or stored on your SharePoint, which are relatively more vulnerable," he says.*

Get more information about this year's biggest cloud threats. Watch "View from the trenches: perspectives on the major threats of 2023."

4 steps towards rolling out your cloud security strategy in 2023

In less than a decade, enterprise cloud has transformed great swathes of the global economy.

In the rush to migrate and innovate, however, many C-suites have struggled to balance cloud security with innovation.

1 **The paved road approach:**
David D'Amato, CISO at financial services giant AON, says "The paved-road approach involves creating secure repeatable patterns. These enable you to lay the road on which your developers can roll out their products at speed, using that secure, sustainable and scalable foundation."

2 **Collaboration betweenDevOps and security:**
This expands data and insights, revealing exciting new commercial opportunities. "A great example of this is creating a remote development environment built with DevOps teams' needs in mind, versus them using their local laptops to build, with all kinds of horrible security controls that will slow them down," explains D'Amato.

3 **Switching from influencing individuals to guiding behavior:**
Security teams at high-growth organizations must make this transition if they are to succeed.

4 **Big companies generate big data:**
Security teams need to fully leverage and operationalize big data, using it to shape their cloud security strategy. "For example, if you have a bug bounty program, you can track where your bug reports are coming from – what percentage of bugs are discovered internally, versus those reported by customers," says Ryan Kazanciyan, CISO at Wiz. "This kind of data can reveal whether security teams are looking hard enough for bugs, or whether more prevention and design work is needed upfront."

Watch "Building a cloud security strategy: the #1 priority for CISOs for more tips on how to operationalize your cloud security strategy."

Can Wiz be a partner in your security strategy?

The world's fastest-growing start-ups, as well as 35% of the Fortune 500, have partnered with Wiz on their cloud security strategy. Discover how Wiz can help you achieve greater visibility by enabling collaboration between your security, dev, devops, and engineering teams.

See Wiz in action: wiz.io/demo

About WIZ

We're reinventing cloud security from the inside out.

Led by an experienced and visionary team, we are on a mission to help organizations create secure cloud environments that accelerate their businesses. By creating a normalizing layer between cloud environments, our platform enables organizations to rapidly identify and remove critical risks.

Find out more