ExtraHop

EXTRAHOP 2022

Reducing Cloud Security Friction in the C-Suite

Understanding the CIO-CISO Balancing Act

TABLE OF CONTENTS

EXECUTIVE SUMMARY

When the subject of friction in the cloud comes up, it's often focused on security's effect on development. Of course, that's a legitimate concern because security teams have a reputation for slowing down application development and deployment to reduce risk. However, friction works both ways: Development and operations can also cause friction for security teams by leaving them out of the loop to ensure speedy deployments.

That bi-directional fiction can also affect the balancing act between chief information officers (CIO) and chief information security officers (CISO). The CIO often has a mandate to take advantage of the speed and efficiency of the cloud, while the CISO needs to ensure that the proper procedures and policies are in place to defend cloud environments.

To understand how friction affects security teams, ExtraHop commissioned an independent survey of IT and cybersecurity professionals, conducted by Virtual Intelligence Briefing (ViB). According to the survey, 67% of respondents experience friction in the cloud that makes security teams' jobs more difficult. Examples include visibility and communication gaps, difficulties integrating security into the software development lifecycle, shadow IT and unmanaged devices, and more.

In this report, you will learn more about the real-world challenges cloud-focused security and IT teams face as well as key takeaways to help you better understand the current state of friction in cloud security.

Setting the Stage

The cloud is proven to spur innovation and efficiency. It speeds software development, enables teams to quickly add third-party assets or spin up new instances, and allows organizations to connect with employees, customers, and clients. At the same time, the cloud's speed, scale, and complexity can introduce new security risks and increase friction. To understand what causes friction and how to overcome it, it helps to understand how organizations are using the cloud.

Cloud Initiatives and Security Use Cases

Organizations understand the benefits of cloud adoption, so it makes sense that transition from on-premises deployments to the cloud is a key initiative.

Almost half (48%) of survey respondents said that cloud migration and/or digital transformation are their most important projects. Another key initiative is cloud detection and response, with 25% of organizations saying it's their most important security use case. Container security (16%) and serverless security (9%) were the third and fourth most important use cases.

Q: *Which of these are your most important cloud initiatives and/or security*

Key Takeaways

Digital transformation and cloud migration projects are fundamental to enterprise growth, so it's not surprising that they're listed as the most important initiatives by a majority of respondents. But for security teams, ensuring safe cloud use stretches across numerous use cases and can put them at odds with their IT and operations counterparts. Balancing the need for speed and security can introduce friction between CIOs and CISOs. That friction also plays out downstream when projects are slowed down to reduce risk or when security best practices are ignored to keep projects on track. Providing security teams and their counterparts in development and operations with the tools and processes they need to understand inventory and risk before, during, and after migration is key to removing friction and defending against threats once assets are in the cloud.

Where Organizations Host Workloads and Data

Many, if not most, organizations host applications and data in the cloud, but that doesn't mean they have abandoned the on-premises data center entirely. A vast majority of respondents (80%) have workloads in hybrid deployments. More than a quarter leverage multicloud environments of two or more cloud service providers (CSP), while only 10% use a single provider.

Q: *Where are your workloads and data hosted/deployed?*

80% Hybrid Enviroments

27% Multiple Public Cloud

35% On-premises

10% One Public Cloud Provider

Cloud Workload Deployment

Almost every organization has some sort of cloud footprint, but where they deploy workloads in the cloud differs. A majority (67%) of respondents said they use infrastructure-as-a-service (IaaS) environments, which offer on-demand networking, compute, and storage resources.

Containers, which virtualize operating systems and can be deployed almost anywhere, are another popular choice with 52% of respondents saying they use them. Rounding out the top choices at 42% is platform-as-a-service (PaaS), which is similar to IaaS with the added benefit of greater support for developers. While function-as-a-service (FaaS), which supports serverless environments, is a hot topic among security and IT professionals, only 15% of respondents currently use it.

Q: *Where do you deploy cloud workloads?*

67% IaaS

42% PaaS

52% Containers

15% FaaS / Severless

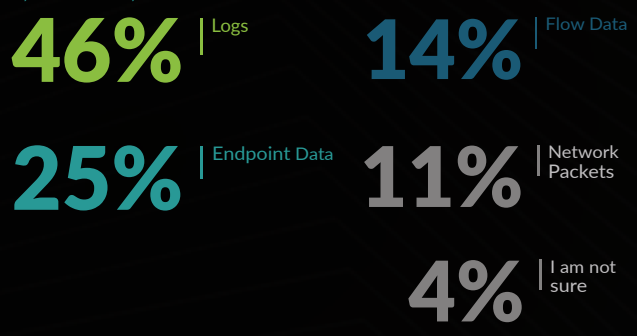
Key Takeaways

Cloud environments offer incredible flexibility. They enable organizations to mix and match the deployment of workloads inside a single CSP or spread their assets across multiple CSPs. While flexibility is a great benefit, it can also lead to tool sprawl and coverage gaps. To minimize this, organizations should carefully evaluate where to invest their tooling budgets, taking into account how many different environments their CSP-native or vendor products can reasonably cover, including hybrid.

How Organizations Are Securing the Cloud

No matter the cloud environment, logs reign supreme as the data source of choice for organizations. A plurality (46%) of survey respondents said they use logs for cloud security, with endpoint data coming in next at 25%. Telemetry from flow data (14%) and network packets (11%) round out the top four. When combined, logs, endpoint data, and network telemetry allow organizations to take a defense-in-depth approach to securing critical assets and data in the

Q: *What is your primary data source for cloud cybersecurity?*



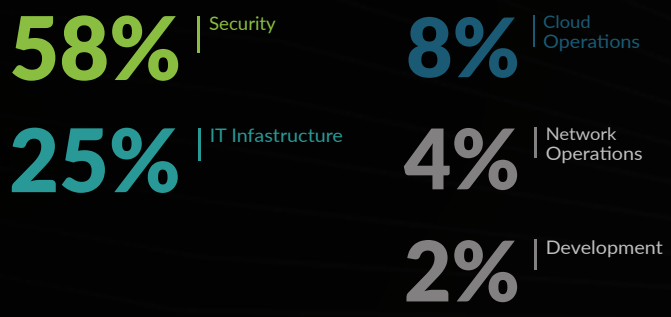
Key Takeaways

While the cloud thrives on change, cloud security data sources have remained consistent over the last year. The percentages of logs, endpoint and flow data, and network packets used as primary data sources are basically unchanged since we released our 2021 Cloud & Hybrid Security Tooling Report. Sixty-seven percent of respondents to the 2021 survey admitted to having coverage gaps. This year, 67% of respondents to this year's survey said they experience friction that includes visibility and coverage gaps. Organizations may want to reconsider their mix of data sources in an attempt to monitor more traffic flowing in, out, and across their cloud environments. The availability of telemetry like flow logs and CSP-native packet mirroring offer ways for organizations to expand their use of network data without the need for agents.

Expanding the Cybersecurity Toolset

Organizations of every size expect to add cloud security tools, with 69% of respondents saying they plan to bring in new products over the next 12 months. The teams in charge of purchasing tools vary by organization. More than half of respondents (58%) said security has buying power for cloud security tools, more than doubling the next closest group, IT infrastructure at 25%. Cloud operations (8%), network operations (4%), and development (2%) round out cloud security tooling purchasers.

Q: *Which team is in charge of purchasing new cloud security tooling?*



Key Takeaways

Who controls the budget can become a point of friction when organizations decide to add new cloud security tools. For a majority of respondents, security owns the power of the purse, which means they choose the new products and data sources they will use. For the remaining 42%, there's no guarantee that the preferences of security, or more specifically the CISO, will carry the most weight. Organizations with CIOs in charge of security tooling purchases could choose to go a different direction, even if it's against the desires of a CISO. Finding tooling and data sources that deliver value to both leaders is one way to remove that friction.

Who Handles Security in the Cloud?

There's a perception that security teams stand alone, or at least mostly apart from their colleagues in development and operations. The reality is that security works with several groups. Nowhere is this more apparent than in the cloud, where 93% of security teams share job duties.

Cloud Security is a Team Sport

Incident response and remediation in the cloud is one area where cooperation is the norm, not the exception. Nearly 40% of respondents said security works with developers or application teams to investigate and remediate security incidents. Almost one quarter (23%) said security works with NetOps, while 22% said Cloud Ops and security are partners. Only 14% of those surveyed said security works alone to investigate and remediate incidents in the cloud.

Q: *Who investigates and remediates security events and/or incidents in the*

39% Security team works with developers, app teams, etc.

23% Security team works with network operations

22% Security team works with cloud operations

14% Security team works alone

Key Takeaways

Providing security teams with the tools they need to work better together with other teams is an essential component for reducing friction in the cloud. If those teams can share a data source as well as a UI, it's even better. Not only does working with common tools and data help eliminate silos between teams, it also aligns CIOs and CISOs and makes the business case for adding a new tool even stronger.

Two Major Points of Friction in Cloud Security

Friction is an innovation killer in the cloud, but it's also bi-directional. However, the idea of friction is usually centered on security slowing down the application development that drives line of business. What's talked about less is the effect friction has on security. Regardless of the team, friction affects everyone from the C-suite down. Two-thirds of survey respondents (67%) admitted there are areas of friction that make their jobs more difficult, and they identified a few key areas of concern.

Cloud Environments with Visibility Gaps

The cloud is notorious for visibility gaps that can introduce friction for security teams and make detecting and responding to advanced threats more difficult. Those visibility gaps are present regardless of the deployment environment. More than half (53%) of respondents said they experience gaps in IaaS environments, the cloud's most popular deployment environment. Containers (44%) and PaaS (43%) follow just behind IaaS and are nearly identical to each other in terms of visibility and coverage gaps. Although function-as-a-service (FaaS) and serverless environments were only listed by 17% of respondents, once organizations increase their FaaS and serverless adoption, that percentage is likely to rise.

Q: *In which environments have you identified visibility and/or coverage*

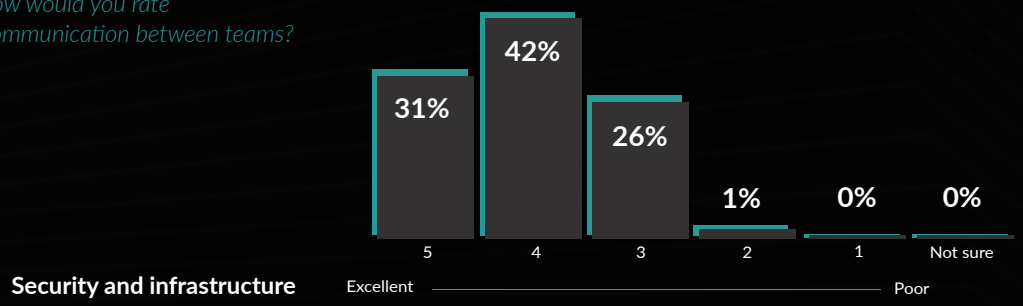
Key Takeaways

One thing to keep in mind is that respondents could choose numerous environments where there are gaps, and some surely did. What that means for security is that they're tasked with defending environments without a full understanding of assets in those environments or what those assets are doing. Gaps across deployments could be from using tools that only provide visibility into one environment or they could come from relying on incomplete data sources. For instance, it's impossible to log or deploy agents on every asset or workload. Ephemerality is also a contributing factor to container security coverage gaps. Choosing a tool that works across cloud environments is one way organizations can mitigate visibility and coverage gaps.

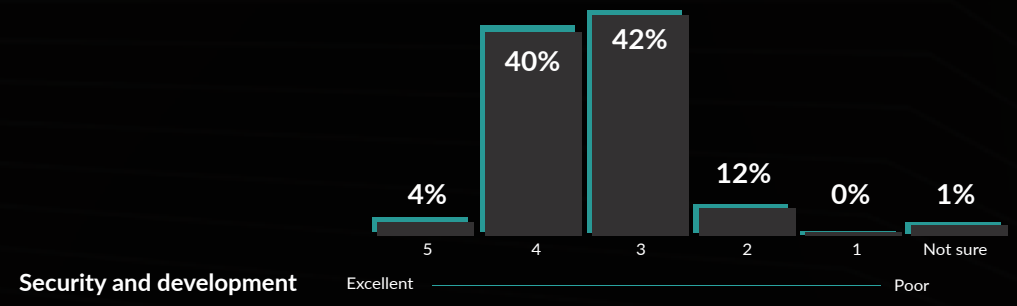
Communication Issues

Of all the groups security works with, they communicate best with the infrastructure team. More than 70% of respondents rated communication between those teams as excellent or good. Security and cloud operations also appear to communicate well, with 56% of organizations rating it as excellent or good. However, security and development often struggle to communicate well. Only 4% of respondents rated security-development communication as excellent, with an additional 37% rating it as good. Although 44% of respondents rate communication between developers and security teams as neutral, 12% of those surveyed gave that inter-team communication the second-worst rating possible.

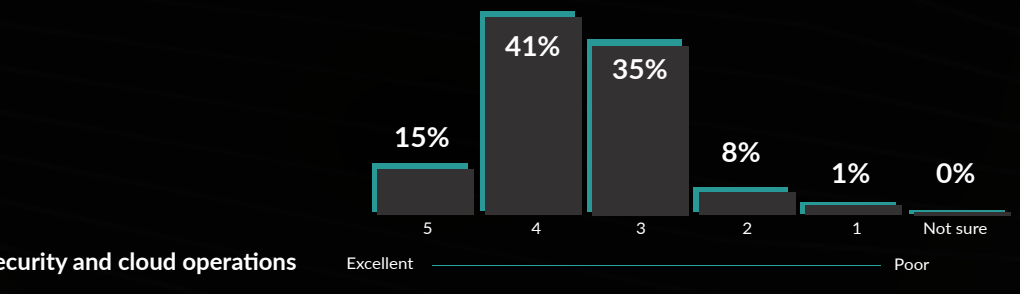
Q: *On a scale of 1 to 5, with 1 being poor and 5 being excellent, how would you rate communication between teams?*



Security and infrastructure



Security and development



Security and cloud operations

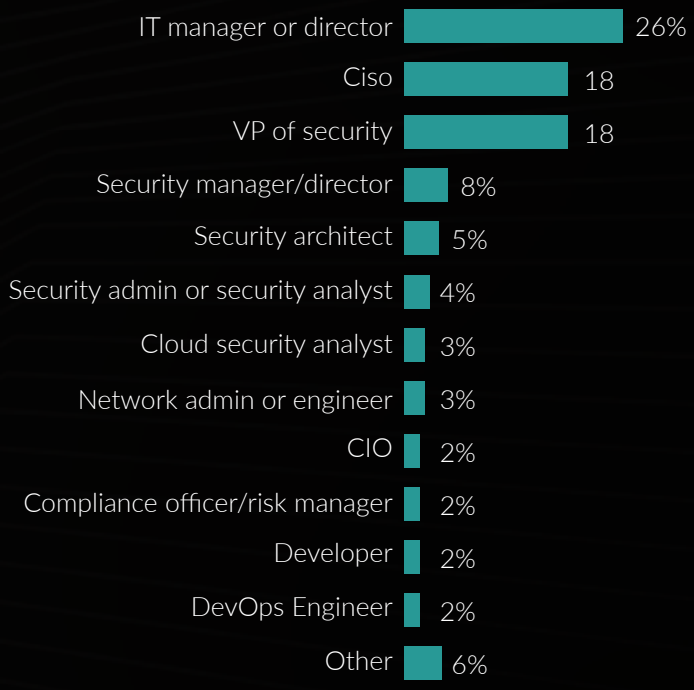
Key Takeaways

Communication challenges between security and development can work their way up to the CIO-CISO relationship. In an attempt to mitigate that friction, many organizations are turning to DevSecOps as a way to strengthen the bonds between security, development, and operations. In DevSecOps, security "shifts left" in the development lifecycle, meaning it's instituted early in the code creation process and verified by testing before releasing an application into a production environment. While DevSecOps is designed to mitigate friction, it's still more of a concept than an effective practice, meaning organizations still need to focus on threat defense.

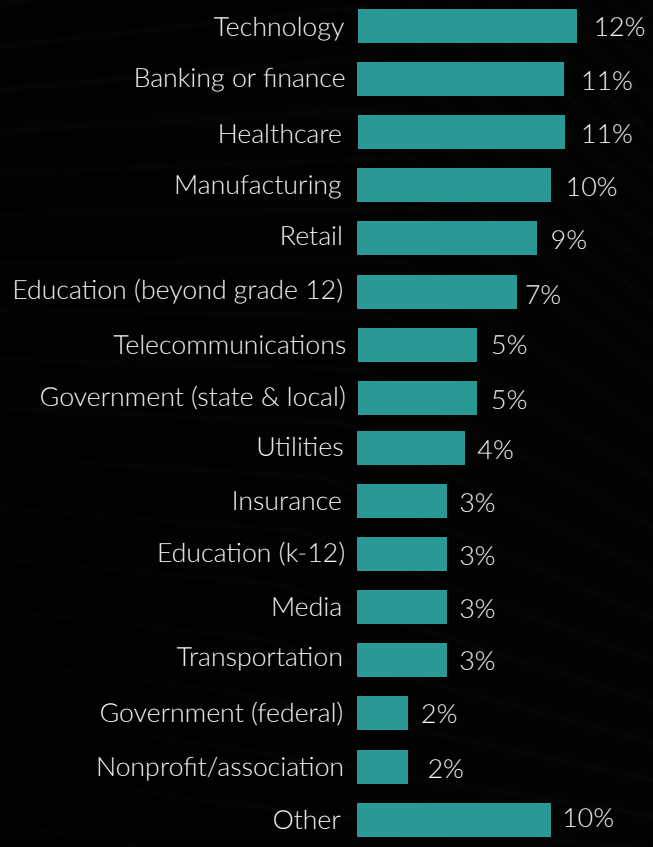
Survey Demographics

Virtual Intelligence Briefing conducted this survey of 126 security and IT professionals on behalf of ExtraHop in June 2022. The majority of respondents (70%) were managers or above in their organizations. Company size for this survey ranged from 1,001 employees to more than 100,000 and included members of the public and private sectors.

Job Role



Industry



Company Size