EXTRAHOP 2021

Cloud & Hybrid Security Tooling Report

ExtraHop

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Where organizations choose to host their critical workloads and data is as varied as the organizations themselves, but a significant majority share one thing in common. They know they have gaps in their security toolsets.

According to a survey of IT and cybersecurity professionals conducted by an independent firm on behalf of ExtraHop, 62% of respondents believe they have gaps in their current toolsets. Almost two-thirds said they plan to migrate even more workloads and data to the cloud over the next 12 months, and roughly the same number plan to add new security tools in the coming year.

In this report, you will dive deeper into the survey results, as well as learn more about how network detection and response (NDR) can help fill in those security gaps, regardless of where you deploy your workloads and data.

Where Workloads Are Deployed

Hybrid and Multicloud Lead the Way

Every cloud service provider (CSP) positions itself as the best and only infrastructure-as-a-service (IaaS) choice for organizations seeking to take advantage of the speed, scalability, and elasticity of cloud computing. But the reality is, most organizations are not rushing to put all their eggs in one basket, choosing instead to go with on-premises data centers combined with one or more CSPs.

46% Hybrid with Multiple Public Cloud Providers

6% Multiple Public Cloud Providers

43% Hybrid with One Public Cloud Provider

6% One Public Cloud Provider

Almost half of respondents (46%) say they host workloads in hybrid environments with multiple cloud providers, and another 43% use hybrid environments with a single CSP.

Overall, 55% say they have workloads and data in AWS. Fifty-two percent use Azure for some or all of their cloud workloads, and 19% use Google Cloud.

> **Hybrid Growth Will Continue**
> Although 64% of people surveyed said they planned to migrate workloads to the cloud within the next 12 months, it seems unlikely that 2021 will be the year that a significant number of organizations ditch the on-premises data center. Currently, only 6% of respondents take a cloud-only approach, whether that's through using a single CSP or multiple providers.

State of Cybersecurity Tooling

Data Sources

Logging, whether on-premises or in the cloud, isn't going away anytime soon. However, organizations recognize the limitations of logging, and they are taking steps to fill in gaps with additional data sets that provide expanded visibility and a richer depth of information.

Almost half of respondents use logs as their primary data source for cloud (47%) and on-premises (44%) security. Given the ubiquity of logging tools, whether from third-party vendors or the CSPs themselves, those numbers make sense.

When we asked about secondary data sources, we began seeing a split between on-premises and cloud security tooling.

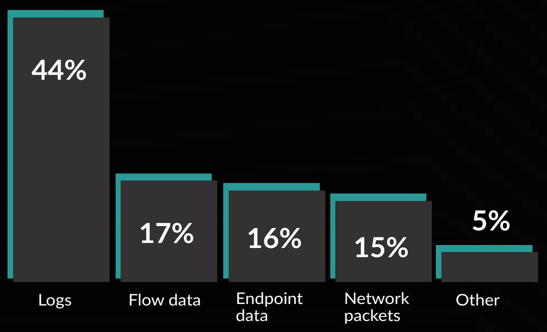
In on-premises enviroments, 17% of respondents use flow data as their secondary data source, followed closely by endpoint data (16%) and network packets (15%).

But in cloud environments, endpoint data has a fairly sizable lead (25% to 11%) when compared to flow data, with network packets sandwiched between at 17%.

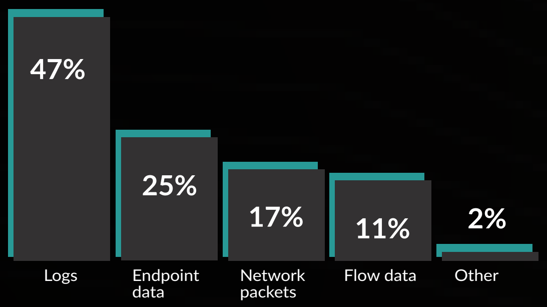
Logs Alone Aren't Enough

Logs are an important component of cybersecurity data sets, but ultimately, they should only be one component. In order to remove gaps and complete the SOC Visibility Triad, security teams also need endpoint and network data.

On-Premises



Cloud

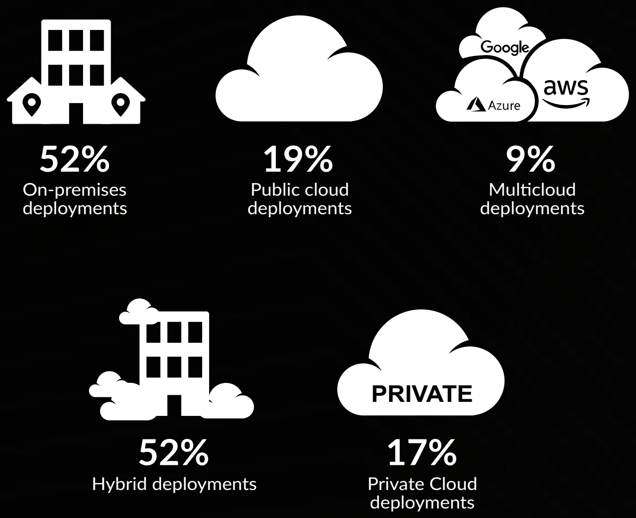


Where Tools Are Deployed

The majority of survey respondents deploy cybersecurity tools in on-premises or hybrid environments, but with almost two-thirds saying they plan to migrate workloads and data to the cloud over the next 12 months, expect those percentages to change in 2021.

Currently, 52% of respondents say they deploy cybersecurity tooling in on-premises environments. The same percentage deploy tooling in hybrid environments.

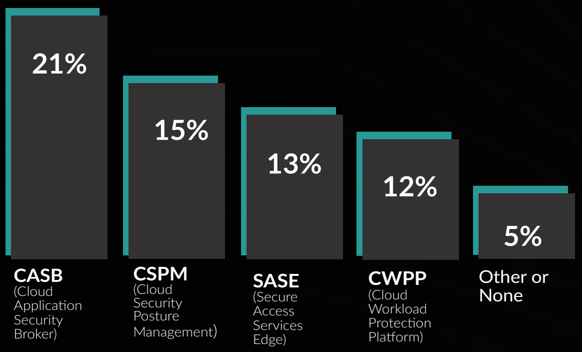
When it comes to cloud environments, 19% and 9% use tooling dedicated to securing public cloud and multicloud deployments, respectively. Let's dig a little deeper into the security tooling landscape.



Cloud-Focused Security Tooling

While the on-premises cybersecurity tooling market has had decades to sort itself out, the cloud-focused tooling market is more dynamic. New categories constantly emerge and join more established technologies.

With that in mind, we gave respondents a list of four specific categories and asked them to select all that they're using. Twenty-one percent of respondents say they currently deploy a cloud access security broker, or CASB. Cloud security posture management (CSPM) tooling was the next most popular category, at 15%, followed closely by secure access service edge, or SASE, at 13%, and cloud workload protection platforms (CWPP) rounding out the group at 12%.



Cloud-Focused Tooling Market Sorting Itself Out

Although CASB is the current leader among cloud-first products, it's beginning to be swallowed up by SASE. Additionally, it can be difficult to tell what you're getting from one vendor to the next, regardless of category.

CSP-Native Tooling

The “big three” cloud service providers in the United States—AWS, Azure, and Google Cloud—each have their own roster of native security tooling, and they are all quite popular with surveyed organizations that run on each environment.

AWS-Native Tooling

Among AWS-native tools, respondents use Amazon CloudWatch, a log-based centralized monitoring service, at a 45% clip. AWS CloudTrail, which logs activity across AWS environments, is used by 35% of respondents, followed by AWS Config (28%) and VPC Flow Logs (18%). More than 1/5 of respondents say they do not use any of the top four AWS-native monitoring tools.

> ### AWS Monitoring & Auditing Tools Lead the Way
> Survey respondents often use two or more AWS-native auditing and/or monitoring tools as part of their toolset, which makes sense. One advantage those tools generally have over most third-party tooling is their ability to seamlessly integrate with each other.

45%	Amazon CloudWatch
35%	AWS CloudTrial
28%	AWS Config
18%	VPC Flow Logs
21%	Other or None

AWS-Native Security Management and Threat Detection

Although tools such as Amazon CloudWatch do a good job of monitoring and/or auditing, they’re not truly standalone products for managing security and detecting threats. In order to gain those capabilities, 40% of respondents say they deploy Amazon Security Hub, an alert aggregation and prioritization tool, and 20% use Amazon GuardDuty, a threat detection tool.

> ### Third-Party Vendors Popular for Threat Detection
> Even with AWS Security Hub, Amazon Detective, and Amazon GuardDuty available to them, 33% of respondents say they look outside of the AWS ecosystem for security management and threat detection tooling.

7%	Amazon Detective
40%	Amazon Security Hub
20%	Amazon Guard Duty
33%	Other or None

Azure-Native Tooling

Thirty-four percent of respondents say they use Azure Advanced Threat Detection, Azure Security Center, and Azure Monitor, a performance monitoring tool, in their Azure environment. Judging by the numbers, several survey respondents most likely combine two or more of those tools.

Microsoft Takes a Different Approach

Rather than focusing exclusively on cloud deployments, two of Azure's most popular native tools can be used for hybrid security. Azure Advanced Threat Protection allows users to detect and investigate threats, compromised identities, and insider activities, and Azure Security Center is a security posture management tool for hybrid cloud

34%	Azure Advanced Threat Protection
34%	Azure Monitor
34%	Azure Security Center
15%	Azure Network Watcher
13%	Azure Sentinel
29%	Other or None

Google Cloud-Native Tooling

Like AWS and Azure, logging and auditing tools are Google Cloud's most popular among survey respondents. Google Cloud Audit Logs, deployed by 52% of survey respondents, compiles information about admin activity, data access, and system events. Google Cloud VPC Flow Logs, deployed by 38% of respondents, can be used for network monitoring, forensics, and security analysis.

Chronicle Makes a Detection Play

With the addition of threat detection capabilities, Google Chronicle may see a jump up from its current 8% deployment among survey respondents.

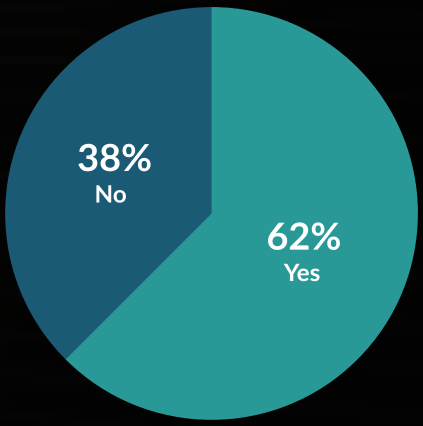
52%	Google Cloud Audit Logs
38%	Google Cloud Flow Logs
8%	Chronicle
27%	Other or None

CYBERSECURITY CHALLENGES

Gaps in Tooling

Securing the modern attack surface means protecting a complex web of workloads spread across core and cloud environments. Not surprisingly, that complexity forces infosec professionals to use a wide variety of tools, some of which only work in one environment.

Gaps in your current toolset?



As a result, 62% of survey respondents say they have gaps in their current toolset. Those gaps include:

- Visibility across workloads and CSPs
- A lack of real-time detection and reporting
- Disparate tools for on-premises and cloud environments
- Blindness into encrypted traffic
- Limitations of log analysis
- Challenges controlling shadow IT

In an attempt to fill in those gaps and keep pace in the cybersecurity arms race, 63% of respondents say they plan to add new tools within the next 12 months.

The ExtraHop Solution

The ability to unify visibility and security controls across hybrid and multicloud deployments has never been more important than it is today, but many organizations are missing a key input—data from network traffic packets.

With SaaS-based ExtraHop Reveal(x) 360, security teams can fill in gaps in their defenses with a cloud-native network detection and response (NDR) solution engineered to provide complete visibility, real-time threat detection, and intelligent response capabilities across deployment environments.

ExtraHop Reveal(x) 360 enables security teams to see every device, every workload, every user, everywhere—and detect and respond to threats anywhere—from a single management pane.

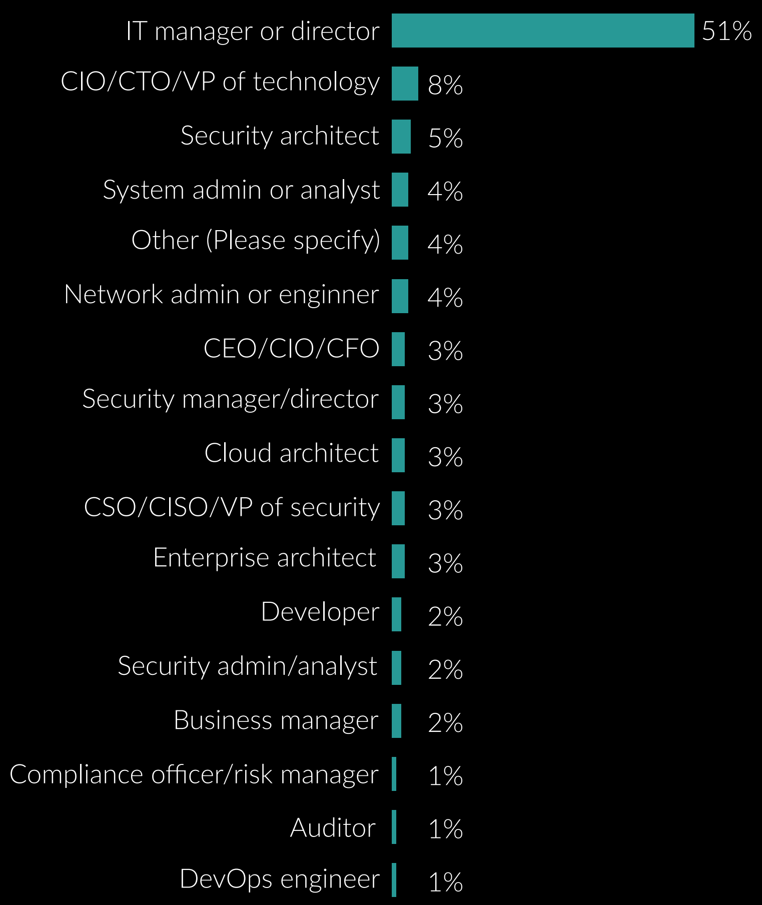
For cloud deployments, ExtraHop leverages native integrations with packet mirroring features from Amazon Web Services and Google Cloud, as well as the announced Microsoft Azure vTAP, to capture copies of network traffic data without the need for agents.

To learn more about how ExtraHop can help you detect threats 95% faster and reduce time to resolve breaches by up to 84%, visit our Reveal(x) 360 product page.

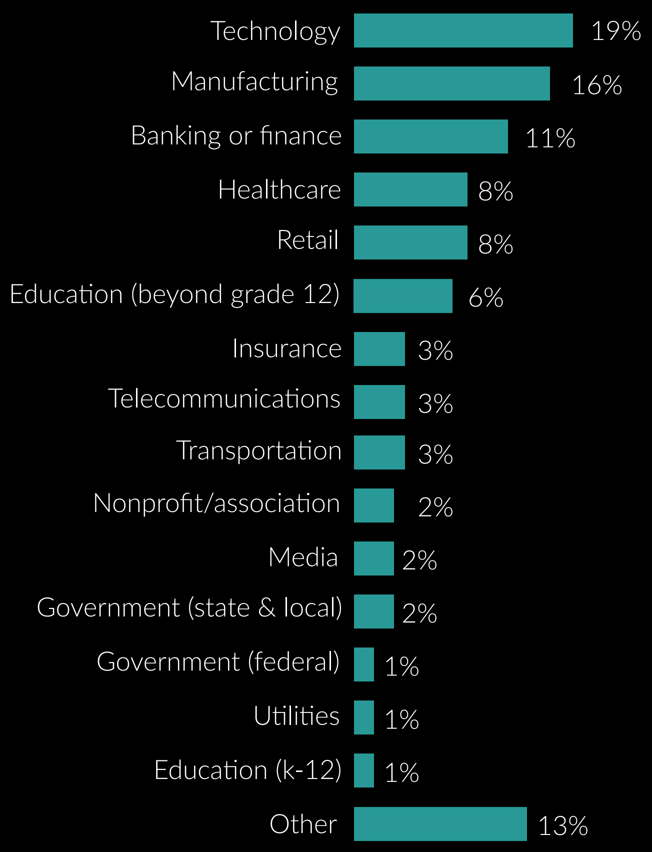
SURVEY DEMOGRAPHICS AND METHODOLOGY

This survey of 340 IT and cybersecurity professionals was conducted August 1–31 on behalf of ExtraHop by independent research firm Virtual Intelligence Briefing. The survey methodology incorporated extensive quality control mechanisms at 3 levels: targeting, in-survey behavior, and post-survey analysis. The calculated margin of error at a 95% confidence level is 3.9%.

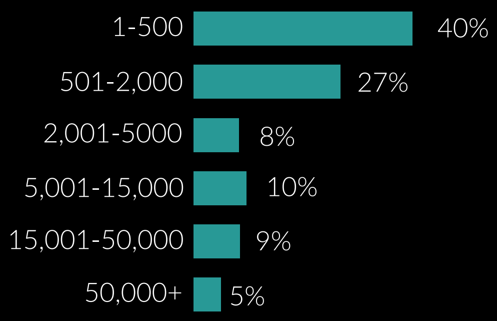
Job Role



Industry



Company Size


1-500 40%
501-2,000 27%
2,001-5000 8%
5,001-15,000 10%
15,001-50,000 9%
50,000+ 5%