VECTRA®
SECURITY THAT THINKS

RESEARCH STUDY

State of Security Report: PaaS & IaaS

More People, More Access, More at Stake

VECTRA
SECURITY THAT THINKS

Table of Contents

Introduction

Organizations are rapidly embracing digital transformation—including always-on connectivity to support digital business—and this has resulted in the evolution of a hybrid infrastructure that combines on-premises and cloud-native architectures.

This transformation has led to a ramp-up of DevOps engineers using Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) for application development, thanks to their flexibility, scalability, and ability to dynamically spin up workloads. In fact, Gartner estimates that 70% of organizations employ or plan to employ a DevOps program. While the benefits of greater speed and agility that come with the cloud enable faster delivery of applications, these advantages need to be balanced against security risks that arise from increasingly complex and constantly evolving deployments—especially in public cloud services like Amazon Web Services (AWS). Gartner also states that through 2025, 99% of cloud security failures will fall on customers.

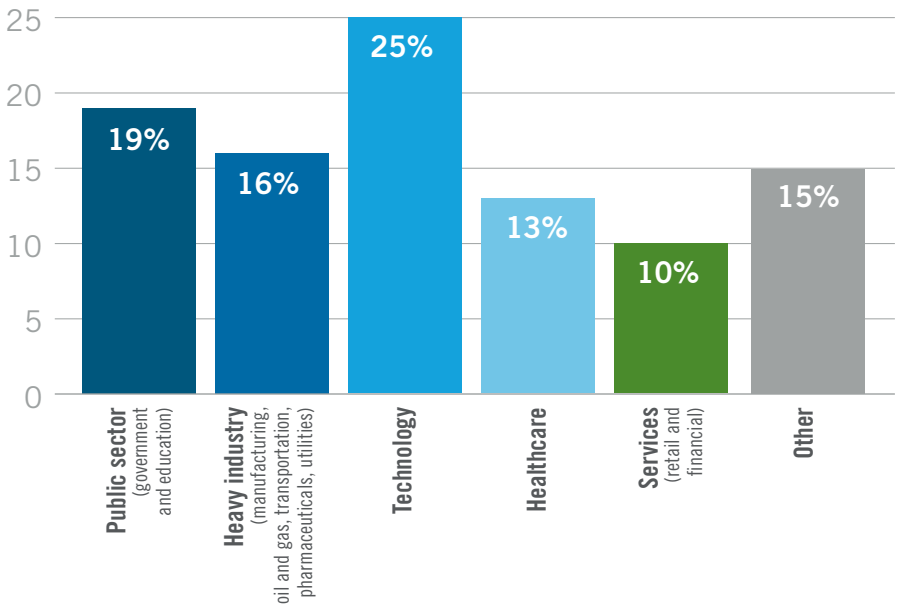
A survey commissioned by Vectra AI set forth to find out how organizations are addressing the security of their AWS deployments.

VECTRA
SECURITY THAT THINKS

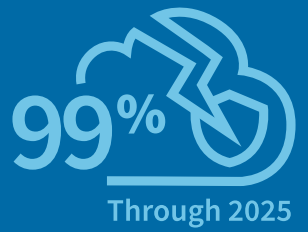
Survey Overview

A total of 317 IT executives took part in the survey. 70% of the companies surveyed were large organizations with more than 1,000 employees. All of the participating companies experienced a security incident in their cloud environment.

Participating organizations belonged to the following industries:



451 Research shows that the #1 challenge with cloud native adoption is security and compliance risks.[1]



Through 2025, 99% of cloud security failures will fall on customers.[2]

50% year-over-year increase in data breaches targeting cloud infrastructures.[3]

[1] 451 research
[2] Gartner report
[3] Verizon Data Breach Industry Report 2020

Key Findings

The cloud has changed everything we know about security, while organizations are left with blind spots as they continue to expand IaaS and PaaS deployments:

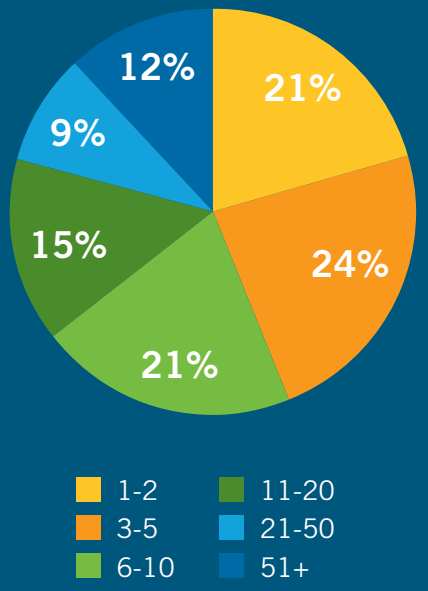
- The results of the survey clearly demonstrate that companies are investing heavily in security operations. Over half the companies surveyed had double-digit security operations center (SOC) headcounts. Other data sources confirm this increase in headcount and point to rising salaries for security analysts—a position currently in high demand.
- Both security and DevOps personnel are looking to be proactive and preventative in their roles. Security analysts want to be empowered to anticipate potential threats or vulnerabilities before the bad guys do. DevOps personnel are frustrated by avoidable crises that burn up resources.
- Risk exponentially increases as more people are granted access to the AWS environment. The challenges of securely configuring the cloud are expected to continue for the foreseeable future due to sheer size, scale, and continuous change.
- Organizations are looking for coverage beyond the bottom three AWS services. If there isn't a solution in place to monitor a particular service, security teams don't have a way of knowing whether that service is being exploited, which exposes a tremendous blind spot.
- The cloud has expanded so much that securely configuring it with continued confidence is nearly impossible. Almost one-third of organizations surveyed have no formal sign-off before pushing to production, and 64% of organizations are deploying new services weekly or even more frequently.
- There is a need for a solution that provides security holistically across regions. Security professionals are looking to automate activities in order to enhance their effectiveness. Increasing their workload with manual tasks will only hold them back.

Companies Are Investing Heavily in Security Operations

Over half of the companies surveyed have more than 10 employees in their SOC, while both SOC job opportunities and salaries are increasing. According to a recent survey by the Ponemon Institute, one-third of organizations are planning to increase security analyst headcounts. Ponemon also reports that, from 2019 to 2020, the average salary for a security analyst jumped from $102,000 to $111,000. Given the high demand for this profession, security analyst salaries are expected to continue to rise.

Organizations have made the human resources investment to protect against the threats they face daily like ransomware. The next step is to empower people in those roles with the tools and processes to help them be as effective as possible.

How many individuals are members of your security operations center (SOC) team?



VECTRA
SECURITY THAT THINKS

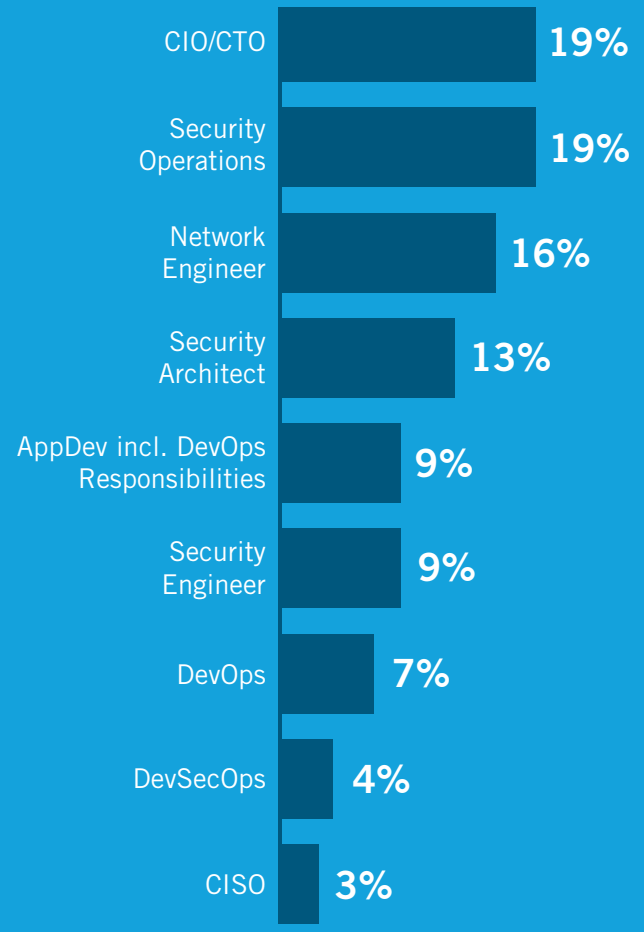
Both Security and DevOps Are Looking to Be Proactive and Preventative in Their Roles

36% of the respondents reported being in security-related roles. In addition, 20% of survey respondents stated they are in DevOps-related roles. As security professionals on the front lines of cloud security management, they are acutely aware of the issues associated with mounting threats and the deluge of alerts they receive daily.

- Security analysts are focused on monitoring and flagging events, running down high-priority tasks, and working with other teams to implement new systems. They seek to be more proactive than reactive and anticipate potential threats or vulnerabilities before the bad guys do. They are looking for comprehensive dashboards that give them a global overview of their company's infrastructure and threat activity.
- Security operations engineers focus on preventing malicious attacks and mitigating active risks to their organization. They are expected to act quickly and maintain composure in stressful situations. The role requires them to think like an attacker as well as a defender.
- DevOps engineers want to be more efficient with the time they spend on implementing features and bug fixes as well as helping developers deploy, build, and release software. They are frustrated by avoidable crises that burn up resources. They also want to be proactive and avoid unnecessary, reactive work.

Regardless of their roles, all security professionals need tools that help them use their time wisely in order to prioritize what matters, forestall security incidents, and anticipate attackers' moves.

What is your role within the organization?



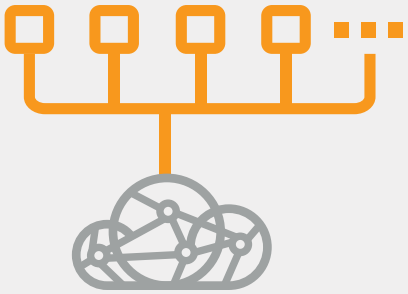
Organizations Are Looking for Expanded Security Coverage Beyond What's Offered by Cloud Providers

According to the survey, 71% of respondents use more than four services, leaving themselves even more vulnerable to exploitation, while only 29% use three AWS services—S3, EC2, IAM. 64% of DevOps respondents are deploying new services at least once a week.

of those surveyed

71%

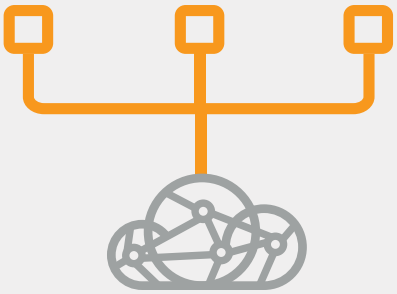
use 4 or more services



while only

29%

use only S3, IAM, EC2



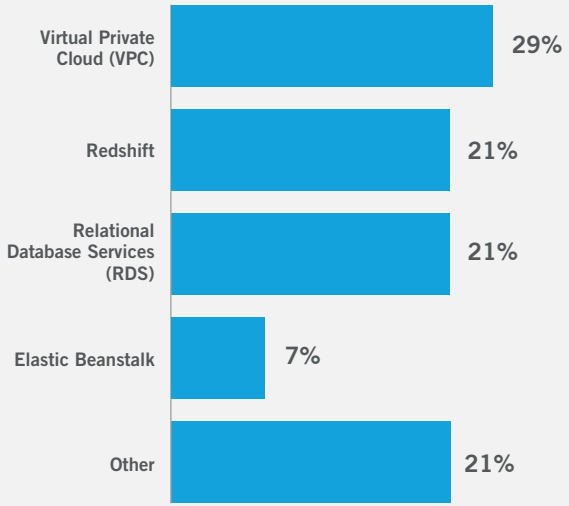
Introducing Vectra Detect for AWS

For those who need to secure and monitor applications running on AWS IaaS and PaaS, Vectra Detect for AWS provides behavioral threat detection, investigation, and automated response to attacks targeting applications running on AWS. Detect for AWS protects identity, compute, and storage instances at runtime, holistically across all AWS regions. The solution is designed for SOC professionals and DevSecOps engineers who want to deploy applications faster without undue risk and cloud operations/infrastructure specialists who need to reduce the risk of services being exploited.

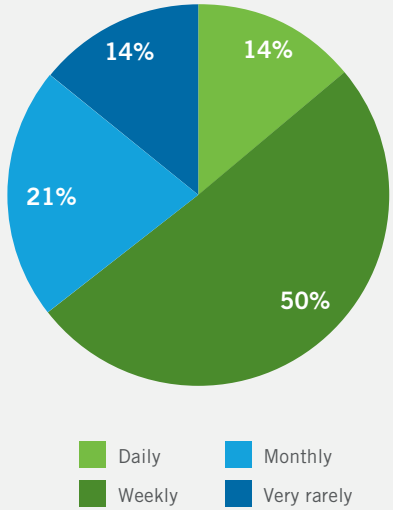
This begs the question: ***If there is nothing in place to monitor a particular service, how do we know it is not being exploited?*** As enterprises move their high-value data and services to the cloud, it's imperative to control cyber risks that can take down their businesses. Traditional security tools and approaches fall short in their ability to provide effective threat detection and response.

Based on the findings, most organizations are aware of this deficiency, as 71% stated that they need a solution that covers more than what is currently available from AWS.

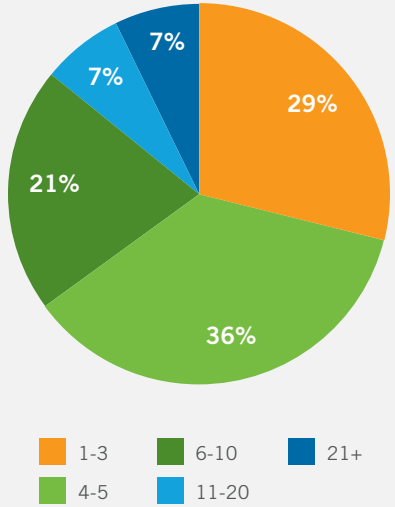
Which AWS service do you use the most outside of S3, EC2, IAM?



How frequently does your organization deploy new workloads/services?



How many AWS services do you estimate your organization is using today? (example: S3, EC3, IAM, RDS, or others)



How can we be certain cloud services aren't being exploited when cloud service providers offer limited threat detection capabilities?

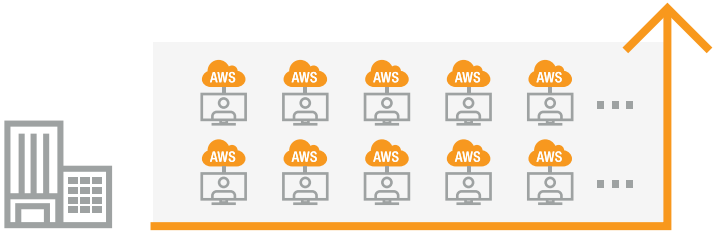
More People, More Access, More at Stake

Due to the many challenges organizations face without complete visibility across their environments, many security-minded enterprises are adopting a Zero Trust framework. This requires all users to be authenticated, authorized, and continuously validated for security configuration and posture before access is granted for applications and data.

According to the findings, 71% of organizations who participated have more than 10 users with access and the ability to modify the entire AWS infrastructure. Compromising even one of these accounts can spell disaster for the organization, and while most are well aware that this level of access poses a real risk, only 9% of respondents are not concerned about AWS security threats.

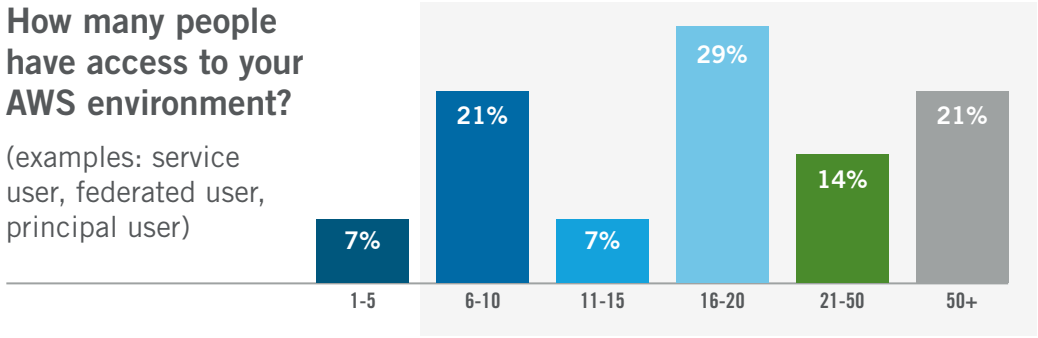
71%

have more than 10 people accessing AWS.



How many people have access to your AWS environment?

(examples: service user, federated user, principal user)



Comprehensive Coverage of Services

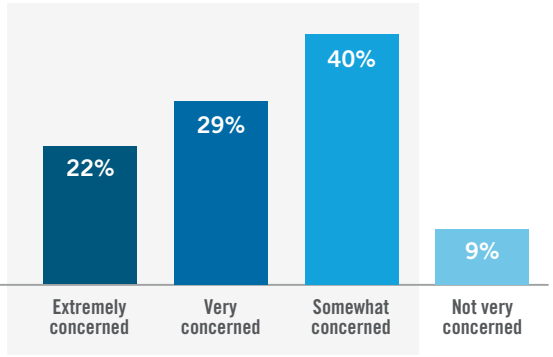
Today's tools cover only a fraction of the services deployed by most organizations. Vectra Detect for AWS uses AI to detect, prioritize, and automatically stop advanced attacks spanning global AWS environments. It helps DevOps confidently migrate, develop, and deploy more applications with speed, agility, and scale. Through its cloud-native threat detection and response capabilities, it reduces the risk that attackers will exploit AWS services.

Uncertainty for Those Tasked with Security Responsibilities

When asked in the previous cloud survey, Securing Cloud Assets conducted by the research firm EMA, "has your organization experienced an incident or breach within the past 12 months involving cloud service(s)?" 63% of respondents answered, "not that we know of." So, if security professionals can't see it, did it happen? The answer is "yes," but they aren't aware of the incident, which could explain why it can often take six to nine months to discover breaches.

As mentioned, by 2025 more than 99% of cloud breaches will have a root cause of customer misconfigurations or mistakes. The reality is that securely configuring the cloud will remain a daunting task due to the sheer size, scale, and continuous changes in workloads and infrastructure.

AWS has become a popular target for attackers in recent years, resulting in a large number of data leaks. How concerned are you about security threats within AWS?



Reduce Risk of AWS Services Being Exploited

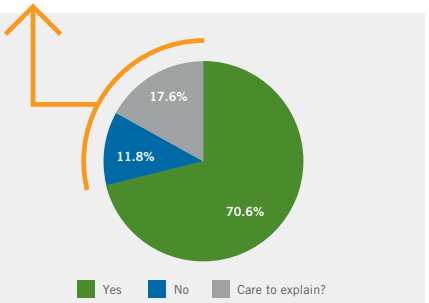
Detect for AWS sees what others miss, including creation of and changes to accounts and how services are being used. It prioritizes attacks across the AWS ecosystem without agents in the workload or static policy rules.

No Formal Deployment Sign-Off Before Pushing to Production

Surprisingly, the survey shows that 30% of organizations surveyed don't have formal deployment sign-off before pushing to production, and 40% have shared that they don't have a DevSecOps workflow. This shows that the cloud has expanded to such an extent that configuring it securely is nearly impossible. And while a few applications can be configured to reach into the right services, with so many people having access to modify both the applications and services—the risk is multiplied by an order of magnitude.

30%

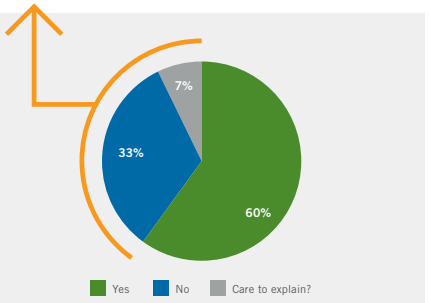
of organizations have no formal deployment sign-off before pushing to production



Do you have a formal deployment sign-off before pushing to production?

40%

have no DevSecOps workflow



Do you have a formal DevSec workflow that ensures configuration is correct/secure?

Designed for the Modern Cloud Deployment Realities

Detect for AWS is delivered as a service. It spins up in a few clicks and dynamically scales without the operational cost of agents or other ongoing configuration maintenance.

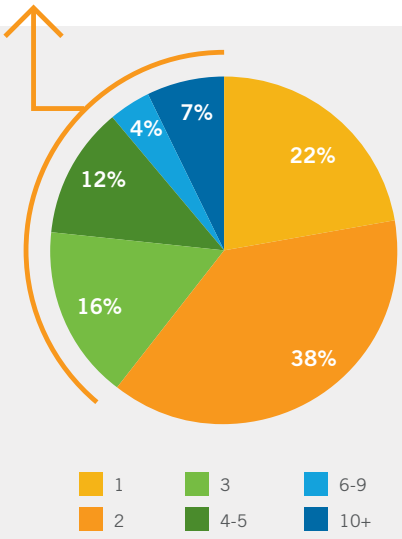
The Need for a Holistic Solution Across Regions

The survey reveals that 40% of organizations report running AWS across three or more regions. As the native threat detection tools offered by cloud service providers require a single console for each region, security professionals have to manually investigate the same threat in each regional console. For those attempting to automate activities to be more efficient, these native tools only serve to hold them back and may augment the risk of a successful breach.

40%

running AWS across three or more regions requiring multiple consoles

How many different regions does your AWS environment operate in?



Vectra Detect for AWS: Agentless Threat Detection for IaaS and PaaS

Vectra Detect for AWS offers continuous behavioral threat detection, prioritization, investigation, and automated response to attacks targeting applications running on AWS. It also protects identity, compute, and storage instances at runtime holistically across all AWS regions.

VECTRA
SECURITY THAT THINKS

Conclusion

Due to its rapid pace of innovation, securely configuring the cloud with confidence will continue to test many organizations' ability to defend against today's attacks. Defending against threats like ransomware, account takeovers, and supply chain attacks requires a new way of thinking as legacy and endpoint security tools are regularly bypassed by cyberattackers, meanwhile the new cloud landscape is like the Wild West for cybercriminals. As organizations continue to adopt cloud for all of the speed, scale, and connectivity benefits that come with it—accounting for security risks must remain a priority. How will organizations answer the bell when an attack is already underway?

Security can be enhanced by empowering security professionals and DevOps engineers to:

- Reduce the risk of cloud services being exploited
- Rapidly detect threats against IaaS and PaaS environments such as AWS
- Automate response to attacks on applications running on AWS

It's clear that next-generation security solutions must give organizations the confidence to migrate, develop, and deploy applications in AWS at scale while reducing the risk of introducing security issues.

Email info@vectra.ai vectra.ai