DARKReading RESEARCH

AUGUST 2021

# The State of Cloud

Censys

## Executive Summary

Recent tech headlines tell a clear story that cloud governance and security issues are getting worse. Cloud-originated breaches and data exposures continue to mount, and it is clear that adversaries are increasingly targeting cloud assets to their criminal ambitions.

There are number of reasons that cloud risks are growing, but data from Dark Reading's The State of Cloud Survey 2021 indicates that one of the biggest is a persistent lack of visibility in organizations, paired with what appears to be overconfidence among IT pros in their capability to keep track of cloud assets and their risk levels.

In this year's survey, we get a glimpse into not only the most common cloud architectures utilized by organizations today and the tools they use to track and manage their cloud assets, but also the perceptions of IT and cloud decision-makers about the overall security afforded by these tools. We then validated those perceptions against an existing body of research data from Censys security experts across real-world cloud deployments observed on the Internet to compare practices reported in the survey to realities in the field.

This comparison uncovers what appears to be a perception gap between organizations' confidence levels in their visibility and control over cloud assets and the actual state of affairs.

# Key Findings

The study found that:

## Visibility and Tracking of Cloud Assets Remain Lackluster

- 52% of respondents say they either don't know what they use to track their cloud assets, don't track them at all, or use manual means of tracking such as spreadsheets.
- Fewer than one-third of organizations use cloud-specific tooling to track cloud assets.
- The most commonly named obstacles that keep them from tracking cloud inventory are time, budget, and lack of headcount.

## Respondents Exhibit Overconfidence in Their Ability to Manage Cloud Exposures

- Despite low rates of consistent tracking and high rates of misconfigurations such as database exposures to the public Internet, 57% of respondents are "very confident" to "confident" in the visibility their organizations have into their cloud assets.
- 58% of respondents say they are "very confident" or "confident" that their assets and deployments are properly configured, and 52% are similarly confident they don't have cloud exposures.
- This contrasts with the high incidence of exposed services and resources in Fortune 500 cloud deployments; data from Censys found 1.9 million Remote Desktop Protocol (RDP) exposures in just a dozen common cloud providers.

## Rogue Cloud Assets are More Common Than Respondents Realize

- 82% of respondents say they use four or fewer public cloud providers.
- Only 2% of organizations indicate they use more than seven providers.
- Deployment statistics show Fortune 500 cloud environments use an average of 25 different cloud providers.

## Cloud Security Tooling Still Needs Work

- 83% of organizations say identifying and remediating Internet risks is a top cloud security priority.
- Yet only 57% say maintaining a comprehensive inventory is a top concern, meaning many organizations can't identify risks in assets they don't know about.
- The top security tool respondents use to control cloud assets is vulnerability management, and only 43% of organizations use it.

## The Perception vs. Realities of Cloud Sprawl

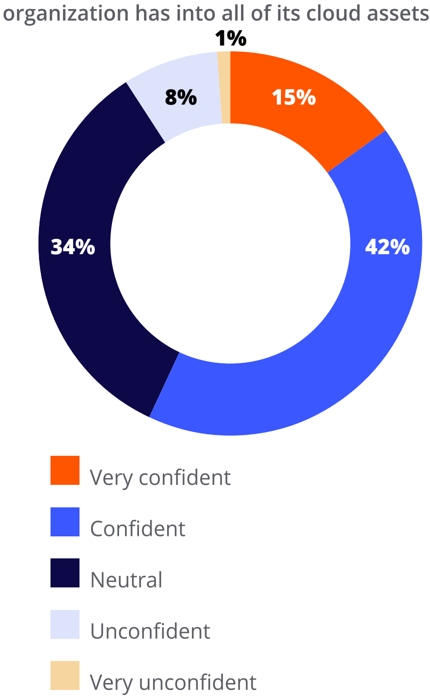
Despite a steady stream of very public cloud exposures in the news and increasing evidence that organizations struggle with cloud visibility and control, a small majority of IT decision-makers remain chipper about the state of affairs within their respective environments. Approximately 57% of organizations are "confident" to "very confident" in the visibility their organizations have into their cloud assets **(Figure 1)**. This appears to be overconfidence in the face of mounting evidence to the contrary.

For example, almost the same proportion of organizations that are confident in cloud visibility admit they don't have very good means to actually track that visibility. Some 52% say they either don't know what they use to track their cloud assets, don't track them at all, or use manual means of tracking such as spreadsheets to keep tabs on their cloud asset portfolio. The obstacles that keep them from achieving a complete inventory of their Internet assets are unsurprising: time, budget, and lack of headcount top the list **(Figure 2)**.

*Figure 1.*

### Confidence in Cloud Asset Visibility

How confident are you in the visibility your organization has into all of its cloud assets?

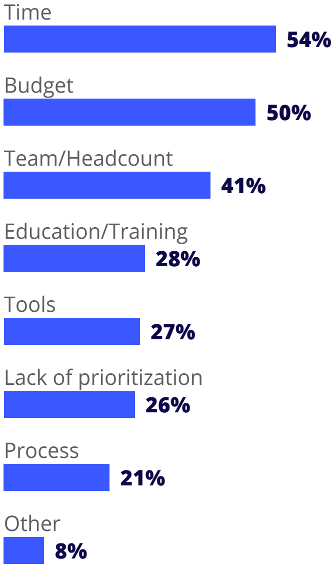


Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

*Figure 2.*

### Challenges in Achieving Complete Inventory of Internet Assets

What is preventing you from achieving complete inventory of all your Internet assets?



Note: Multiple responses allowed
Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

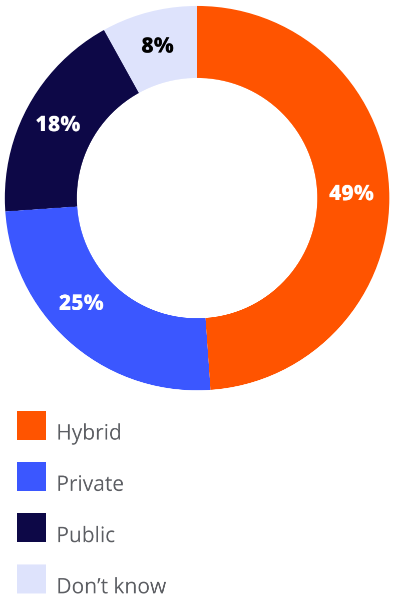
In spite of these lackluster mechanisms for keeping tabs on cloud assets, the overconfidence many organizations exhibit translates to a perceived surety that unauthorized cloud assets are not a problem in their environments. Only about 25% of respondents admit that their organization struggles with rogue cloud infrastructure. Tellingly, six in 10 flat out say they do not have rogue cloud assets in their organization.

When we think about this in light of the high rates of manual or non-existent tracking, the picture starts to crystallize: Organizations are counting on their policies to shield them from rogue assets and untracked cloud sprawl. Our survey shows that 75% of organizations have corporate policies around how and by whom cloud services are provisioned and managed.

*Figure 3.*

## Top Cloud Deployment Model

What is the prevalent cloud deployment model in your organization?



Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

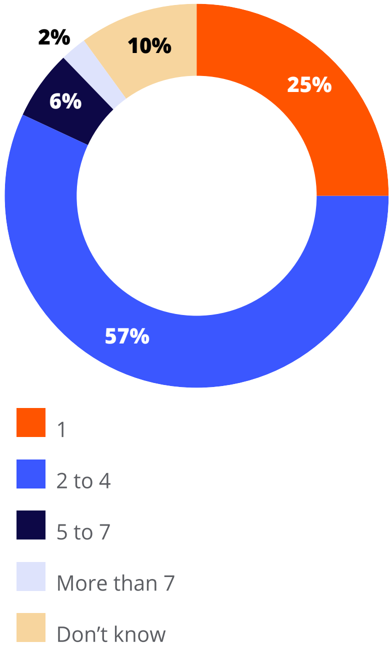
We can show incontrovertibly that these policies don't work nearly as well as IT leaders think, though. We've accomplished this by comparing the average volume of cloud provider relationships reported by this survey's respondents to the volume measured on publicly observable Internet infrastructure.

Approximately 67% of respondents say they work with public cloud providers, with 18% stating they utilize a fully public cloud deployment model and 49% saying they rely on a hybrid model **(Figure 3)**. The majority of our survey respondents say they limit the number of relationships they have with public cloud providers, with 82% stating they use four or fewer providers. A slim 2% of organizations report using more than seven providers **(Figure 4)**.

*Figure 4.*

## Number of Public Cloud Service Providers

How many public cloud service providers does your organization utilize?



Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

And yet, when you compare these statistics with data gleaned from readily available Internet sources, a different view of cloud reality begins to emerge. In its recent Cloud Misconfiguration Mayhem research report on Fortune 500 cloud environments' attack surfaces, Censys finds that organizations are using, on average, 25 different cloud providers in their ecosystems.

Even accounting for some sample bias and differences between each data set — which are likely minimal since the organizations in this survey were primarily large ones with more than 1,000 employees — the difference between what respondents think their cloud environments look like compared to what's observably lurking is extreme.

This is likely due to the inherent nature of cloud and the ability of individuals throughout an organization to easily create cloud instances outside the sanctioned IT environment and its security controls.

## The Hidden Cloud Service Exposures and Risks

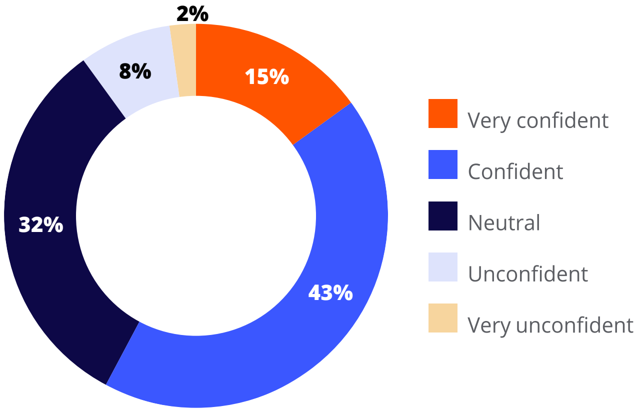
Of course, it isn't just cloud sprawl that organizations appear to have distorted perceptions about. Comparing the survey results to measurable observations from the public Internet also shows that the security exposure resulting from those non-visible cloud assets is much worse than many IT leaders understand.

Again, more than half of organizations believe their teams are doing a good job securing cloud assets. Some 58% of respondents say they are "very confident" or "confident" that their assets and deployments are properly configured, and 52% report they are "very confident" or "confident" that their environments are not at risk for exposure **(Figures 5 and 6)**.

*Figure 5.*

### Confidence in Proper Configuration of Cloud Assets

How confident are you that your organization's cloud assets and deployments are properly configured?

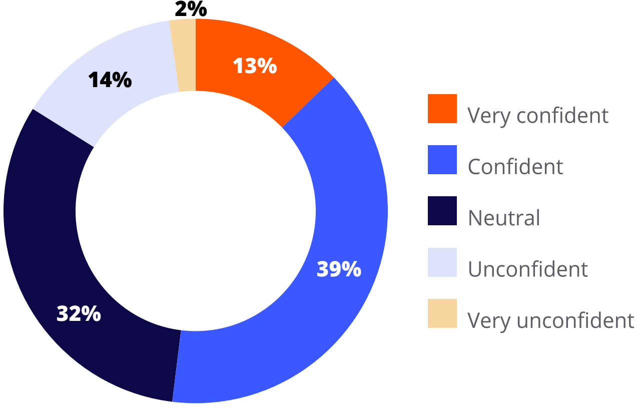


Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

*Figure 6.*

**Risk of Service Exposure for Cloud Environments**

How confident are you that your cloud environments are not at risk for service exposure?



Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

These high confidence ratings are likely misplaced, as real-world data shows that many organizations have hidden cloud services exposed on the Internet that they probably don't know about. When Censys examined common infrastructure elements exposed to the Internet by organizations using public cloud providers, it discovered uncommonly high numbers of exposures of sensitive services and resources.

Real-world deployment data from Censys found 1.9 million RDP exposures in just a dozen common cloud providers, as well as millions of database exposures from MySQL, Postgres, Redis, Elasticsearch, and others.

Censys Search 2.0 Stat: Internet-wide stats also contradict this:

| **Queries** | **Results** | **Date** |
|---|---|---|
| MySQL Query | 4,430,729 | May 14, 2021 |
| Postgres Query | 811,091 | May 14, 2021 |
| Redis Query | 193,190 | May 14, 2021 |
| RDP Query | 3,773,357 | May 14, 2021 |

Source

This is particularly problematic considering that other studies have shown that misconfigurations and exposures like these in the cloud are the number one cause of cloud-based data breaches.

While many respondents clearly still don't peg findings like these as relevant to their organizations, results from other questions show that the realities of cloud risks do produce at least some prickle of anxiety at many organizations. A resounding 68% of respondents admit that the worry of exposed services within cloud assets keeps them up at night. Other common worries include unnecessary functionality enabled, publicly accessible cloud stores, and default passwords in use.

## The Tools and Teams Currently in Place

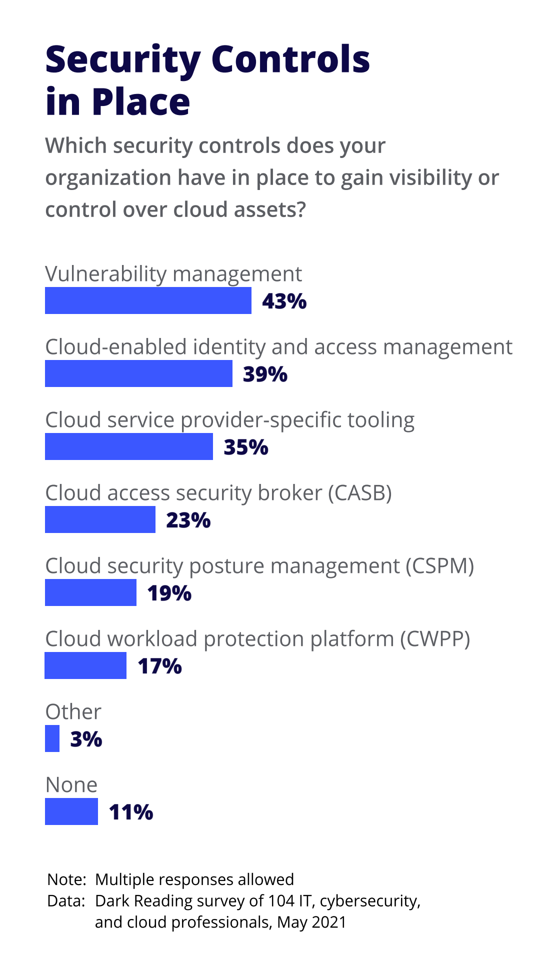
So why do risks remain hidden at so many organizations, and does the gap linger when it comes to perceived and actual risk of cloud exposure? Organizations are clearly struggling to gain visibility over the full portfolio of cloud assets, and a lot of this likely comes down to the tools they're using.

As mentioned above, more than half of organizations don't have an automated method for gaining visibility of their cloud environment in its entirety. Among those who do have tooling, the most commonly used tools are asset management tools (used by 38% of organizations) and cloud security posture management tools (30%), which are almost neck and neck in prevalence.

In many ways, they're similarly poorly equipped to control those assets they do know about. Disconcertingly, the most common tool used to gain "control" over cloud assets is not a cloud-centric tool at all.

When asked about the security controls they have in place, the most common answer (endorsed by 43% of respondents) was vulnerability management tooling, followed by cloud-enabled identity and access management (39%), and cloud service provider-specific tooling (35%), the latter of which does not do a good job of managing a portfolio, especially when dealing with dozens of different providers **(Figure 7)**.

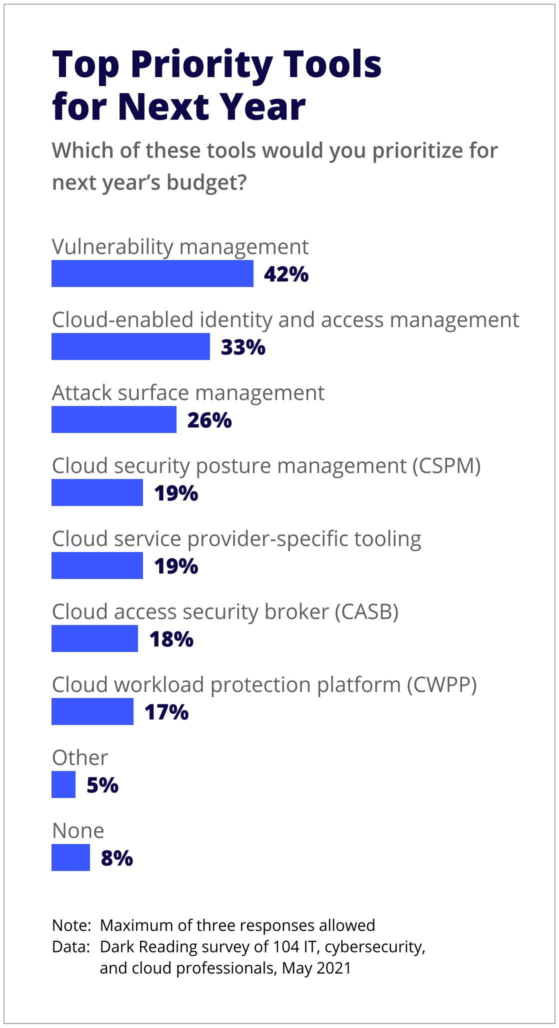
*Figure 7.*



Note: Multiple responses allowed
Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

Other frequently used tools include cloud security posture management and cloud workload protection platforms. When looking at funding priorities for cloud controls, we shouldn't expect any big shakeups in these percentages, as vulnerability management again leads the pack at 42%, followed by cloud-enabled identity and access management (33%) **(Figure 8)**.

*Figure 8.*



**Top Priority Tools for Next Year**

**Which of these tools would you prioritize for next year's budget?**

Note: Maximum of three responses allowed
Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

The use of attack surface management, which continuously discovers, manages, and remediates exposures in cloud assets, is definitely still nascent. Only 34% of organizations say this is a line item in their budget, with the rest saying they don't use it or don't know about it.

When queried about the priority areas of risk that concern their security teams about cloud assets, survey respondents resoundingly named identifying and remediating Internet risks as their top worry — this was named by 83% of organizations. Interestingly, number two was maintaining a comprehensive inventory of assets — named by 57% of respondents. This hints that many organizations don't recognize they may be putting the cart before the horse since it is very difficult or impossible to identify or remediate risks in assets they don't know about.

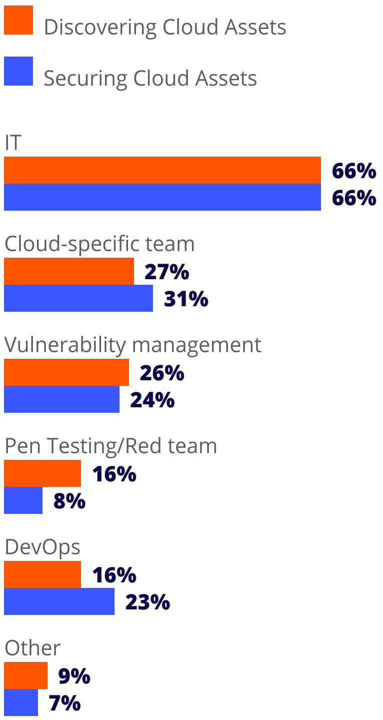
These teams say their top three cloud security concerns among cloud assets (in priority order) are securing user access, computing services, and exposed hosts. Other concerns include storage buckets and, to a lesser degree, containers and spoofing.

When it comes to discovering and securing cloud assets, the team in charge tends to heavily trend toward IT generalists and the broader security team, rather than specialists. IT teams (including cybersecurity pros) were named by 66% of respondents as the main responsible party for both discovering and securing assets. Meanwhile, just under a third of organizations named cloud-specific teams as the team responsible for each **(Figure 9)**.

*Figure 9.*

**Discovering and Securing Cloud Assets**

Which team is responsible for discovering cloud assets, and who is responsible for securing cloud assets??



Note: Multiple responses allowed
Data: Dark Reading survey of 104 IT, cybersecurity, and cloud professionals, May 2021

At the programmatic level, the majority of organizations say they do have some kind of third-party risk management program to manage cybersecurity risks from cloud and other vendors. However, among those that have a program, fewer than half are staffed by dedicated cybersecurity professionals to run them. About a third of these programs are shouldered by cybersecurity pros with other duties, which could be a sign they may be programs in name only for the sake of compliance.

Overall, the teams tasked with cloud security are most likely to be governed by precepts in the NIST Cybersecurity Framework (CSF), which 58% name as the most used compliance framework in use at their organization.

## DevSecOps and Cloud Visibility

As DevOps and self-service precepts increasingly take hold within enterprise organizations, the role of developers spinning up and down their own cloud resources for test, dev, and production environments continues to grow.

As enterprise security teams try to stay aligned with these trends through DevSecOps practices, many are grappling with how they can control and monitor configuration issues, storage buckets, and containers leveraged by developers without impeding their autonomy.

Enterprises are gaining steam with this, with about 40% claiming they have built developer guardrails into the self-service toolchain to govern how they set up cloud storage buckets, containers, and other cloud infrastructure.

## Conclusion/ Recommendations

Organizations clearly operate with a false sense of security about their exposure to cloud vulnerabilities, and this survey indicates they'll need to get back to the basics in how they identify and monitor their cloud assets as they sprawl over the Internet.

You can't protect what you can't see, and cloud visibility is particularly challenging given its ephemeral nature and companies' cloud sprawl outside of sanctioned IT. While many IT practitioners believe that rogue cloud assets aren't a problem at their organizations, our field data shows otherwise. The first step to bolstering cloud control is gaining visibility into the assets that aren't supposed to exist.

Censys Attack Surface Management (ASM) continually uncovers unknown assets ranging from Internet services to cloud storage buckets and comprehensively checks all your public-facing assets for security and compliance problems regardless of where they're hosted. Censys ASM provides easy routes to creating workflows for remediating and tracking the disposition of known assets through integration with major providers like Qualys, Tenable, ServiceNow, Jira, and Splunk.

## Survey Methodology

Censys commissioned Dark Reading to conduct an online survey in May 2021 to explore trends in cloud security. The final data set is made up of 104 IT, cybersecurity, and cloud professionals at primarily North American organizations. Fourteen percent of respondents have IT executive titles such as CIO or CTO, 26% are IT directors, managers, or networking professionals, and 16% are cybersecurity directors or managers. Cloud-related titles such as cloud security, cloud engineer, or cloud architect make up 12% of the final data set. Fifty percent of respondents work at companies with more than 1,000 employees, and respondents come from more than 18 industries.

The survey was conducted online. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa Tech was responsible for all survey administration, data collection, and data analysis. Informa is the parent company of Dark Reading. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

Contextual field data analysis provided by Censys came from its 2021 Cloud Misconfiguration Mayhem report, with data based on analysis of the attack surfaces of Fortune 500 cloud environments. Data was collected in March 2021 through Internet-wide scanning across the globe in the United States, Europe, and Asia.