Osterman Research

RESEARCH PAPER

Research by Osterman Research
Published **April 2021**
Sponsored by **Sonrai Security**

The State of Enterprise Cloud Security: The Good, The Bad, and The Ugly

Executive Summary

2020 was an unprecedented year where remote work exploded, and enterprise organizations were forced to take a quantum leap forward on cloud computing. This rapid cloud migration has created an entirely new set of security challenges around managing identities – both people and entities – and the many different ways they can access data. What we've seen is that these challenges have not been adequately met, and failures continue to happen when the combinations of people, processes, platforms, and priorities break down.

To better understand these issues, Sonrai Security engaged Osterman Research to conduct an in-depth survey of public cloud security and how larger enterprises address them.

KEY TAKEAWAYS

- Eighty-six percent (86%) of organizations surveyed consider their cloud operations to be "business-critical." Most organizations are operating in hybrid or multi-cloud environments, and only one-half (54%) of organizations are making the necessary investments to address solving cloud security problems.

- Close to half of those decision makers agree that a lack of visibility into their cloud operations, data loss, and overprivileged identities are "high risk." Twenty-five percent (25%) of those surveyed are aware of the risks but are not making the necessary investments to address them.

- The three most significant risk categories are: (1) data protection, (2) maintaining consistency of security across the data center and public cloud environments, and (3) identity access. Organizations are using various cloud security tools to reduce risk in these areas, but in most cases, they rely heavily on cloud provider's tools.

- Misconfiguration risk is at best "not getting better" or, more concerning is "getting worse" for seventy-five percent (75%) of organizations. The most commonly cited reason for misconfigurations is the complexity of the computing environment.

- Executives have a false sense of confidence in the security of their cloud. The majority (63%) of organizations surveyed spend no more than 20 person-hours per week managing auditing and report requests in their cloud environment while citing security risks are a top challenge.

86% of organizations surveyed consider their cloud operations to be "business-critical".

ABOUT THE SURVEY

The survey conducted for this paper focused on larger enterprise organizations. Here are the parameters we used to conduct the research:

- Organizations had to have at least 1,000 employees to qualify for the survey. The median number of employees at the enterprise organizations surveyed was 8,000.

- Organizations had to have at least $50 million in annual revenue.

- Most (90%) of the organizations surveyed were in the United States, but respondent organizations were also from the United Kingdom, Canada, Germany, Romania, and Switzerland. Sixty-seven percent (67%) of the

enterprise organizations surveyed operate locations outside of the United States.

- Organizations could serve any industry other than non-profit. A wide variety of industries were represented, including financial services (16%), health and life sciences (14%), manufacturing (14%), education (8%), government (8%), software/Internet/technology (8%), and insurance (6%), among others.

Survey Findings

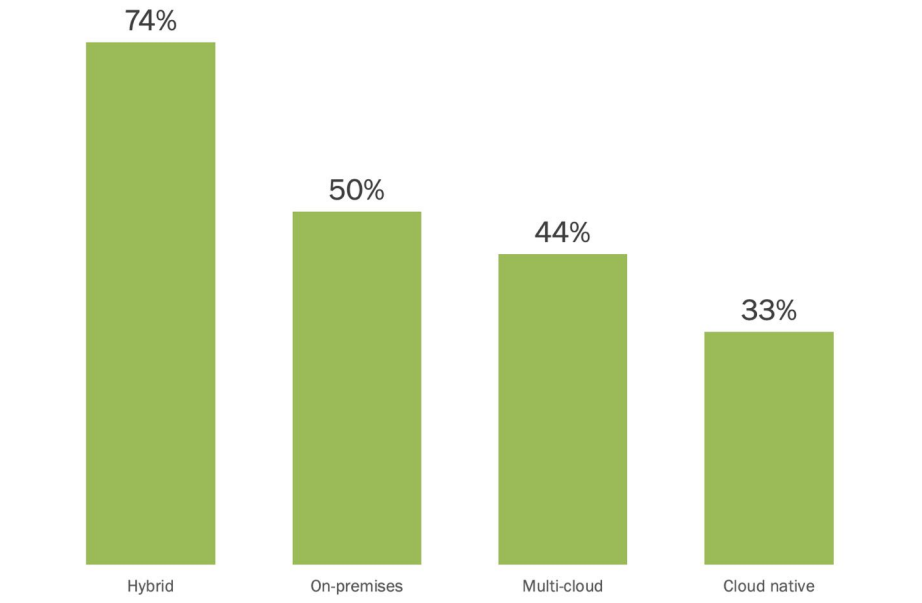
ENTERPRISES EMBRACE THE CLOUD

The vast majority (74%) of organizations surveyed describe their computing environment as hybrid, as shown in Figure 1. We are now in the age of interconnected clouds. There are many public clouds to choose from, such as AWS, Microsoft Azure, and Google Cloud. Enterprise organizations can also build a private cloud in a data center that's owned or rented by their organization – typically on their premises.

Our survey delved into the various cloud combinations used by enterprises with a hybrid strategy, as Figure 1 shows. Most enterprises are incorporating multiple public clouds, while others may be using more than one private cloud. The most common combination is a mix of various public and private clouds, taking a hybrid-cloud architecture approach.

Most enterprises are incorporating multiple public clouds, while others may be using more than one private cloud.

Figure 1
Description of the Computing Environment
(Respondents were permitted to choose more than one option)



Source: Osterman Research
Enterprises have almost entirely embraced the cloud, with seventy-four percent (74%) utilizing a hybrid model

The hybrid approach allows IT teams to choose where their data is located and where that data is processed. Decision makers can choose whether to use a private or public cloud and select which cloud to use. They can revisit those choices as situations change, such as when moving from public to private cloud. It is fair to say that enterprises have almost entirely embraced cloud.

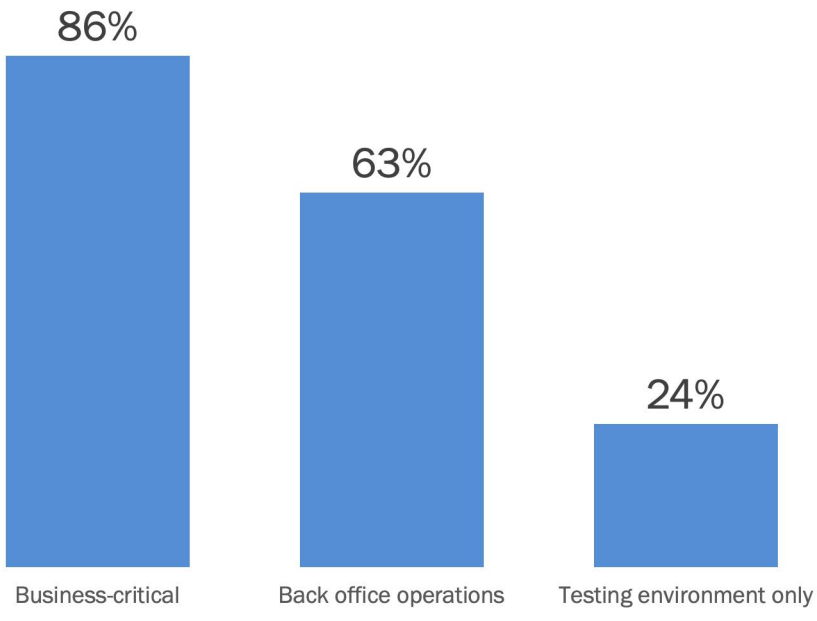
Additionally, research suggests 80% of the organizations in the cloud have adopted a multi-cloud strategy using multiple providers such as Amazon, Microsoft, Google, IBM, Oracle, and Alibaba. Also, the ease and benefits of creating cloud accounts ensure that having many AWS and Google Cloud accounts or Azure subscriptions is the norm.

Investment in public cloud and innovations in agile cloud development has led to an explosion of new data store options, with teams utilizing MongoDB, Elasticsearch, CouchDB, Cassandra, DynamoDB, HashiCorp Vault, and many more. Adding these to object stores, like AWS S3 and Azure Blob, makes it self-evident that new corporate infrastructures do not have a physical or logical concept of a 'data center.'

THE CLOUD IS FOCUSED ON BUSINESS-CRITICAL OPERATIONS

The vast majority of organizations (86%) describe their public cloud operations as "business-critical" as shown in Figure 2. Sixty-three percent (63%) of organizations focus their cloud operations on back-office operations, while only 24% are using the cloud for testing purposes only.

Figure 2
Nature of Public Cloud Operations
(Respondents were permitted to choose more than one option)



Source: Osterman Research
Eighty-six percent (86%) of organizations surveyed consider their cloud operations to be "business-critical"

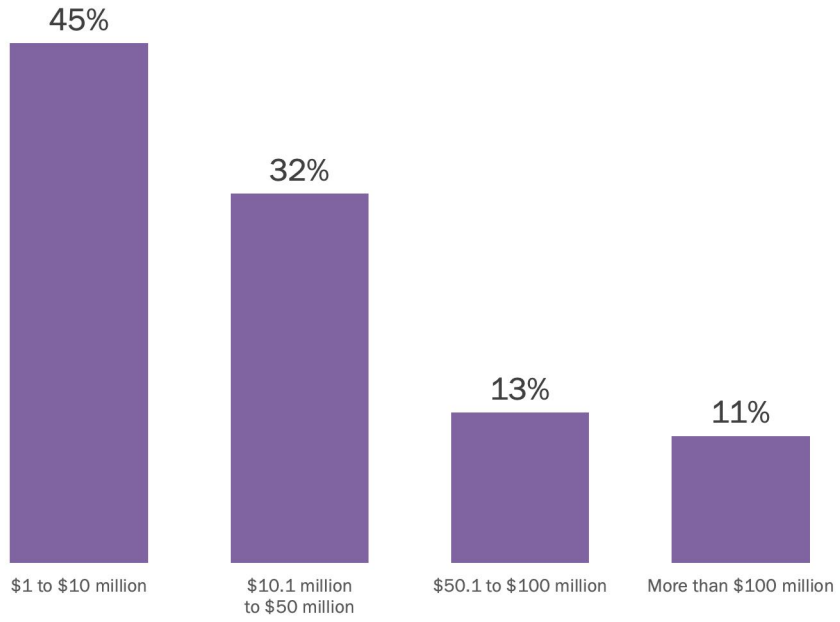
Investment in public cloud and innovations in agile cloud development has led to an explosion of new data store options.

With cloud operations trusted for business-critical applications, any application essential for business continuity is trusted by the enterprise. If a business-critical application fails or is interrupted, the organization's everyday operations cannot proceed as usual. This interruption can lead to short and long-term financial losses, decreased productivity, loss of brand authority, and loss of customer trust. The public cloud is now trusted with business-critical information.

CLOUD SPENDING SOARS TO OVER $10m IN ANNUAL SPEND

As shown in Figure 3, nearly one-half (45%) of the organizations we surveyed have spent between $1 million and $10 million on public cloud investments over the past three years. Another 32% have spent between $10.1 million and $50 million. A smaller proportion has spent more than $50 million.

Figure 3
Investments in Cloud Platforms Over the Past Three Years



Source: Osterman Research
Enterprise organizations have made significant investments in public cloud capabilities

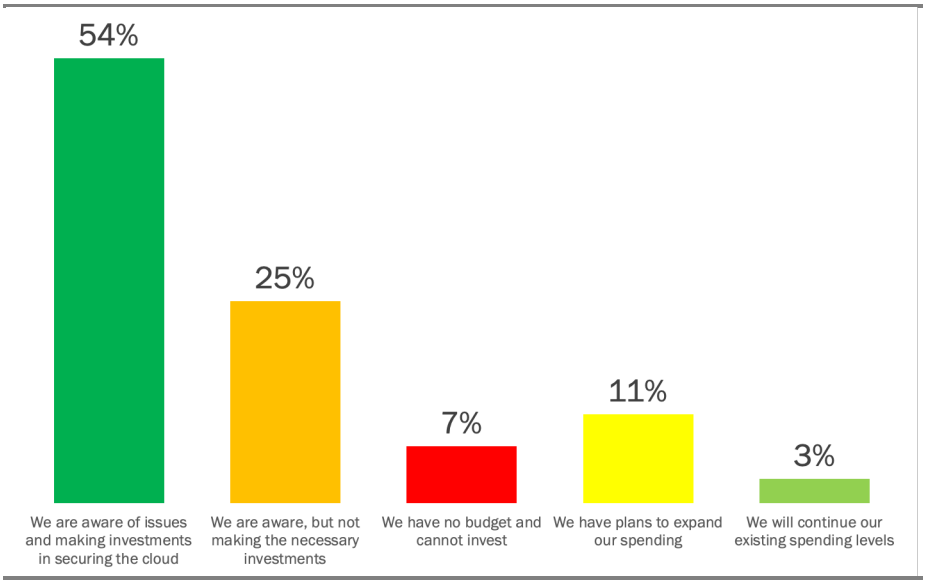
Our research focused on organizations that have made significant investments in public cloud capabilities, including the cloud platforms themselves (AWS, Azure, Google Cloud, etc.), as well as container platforms, cloud-native tools, etc. Consequently, we excluded organizations from the research that had spent less than $1 million in public cloud platforms and related investments over the past three years or those that did not have any sort of separate, identifiable spend in the public cloud space.

If a business-critical application fails or is interrupted, the organization's everyday operations cannot proceed as usual.

MOST ENTERPRISES INVEST IN CLOUD SECURITY: 32% UNDER RESOURCE CLOUD SECURITY

As shown in Figure 4, more than one-half (54%) of survey respondents believe that they are aware of the critical issues surrounding public cloud security and are making the necessary investments to address them. However, 32% of respondents are equally aware of these security issues, but their organizations are not making the investments they need to make.

Figure 4
Organization Practices and Plans for Spending for Public Cloud Security



Source: Osterman Research

Thirty-two percent (32%) of respondents are aware of cloud security issues and are not actively working to solve these cloud security challenges

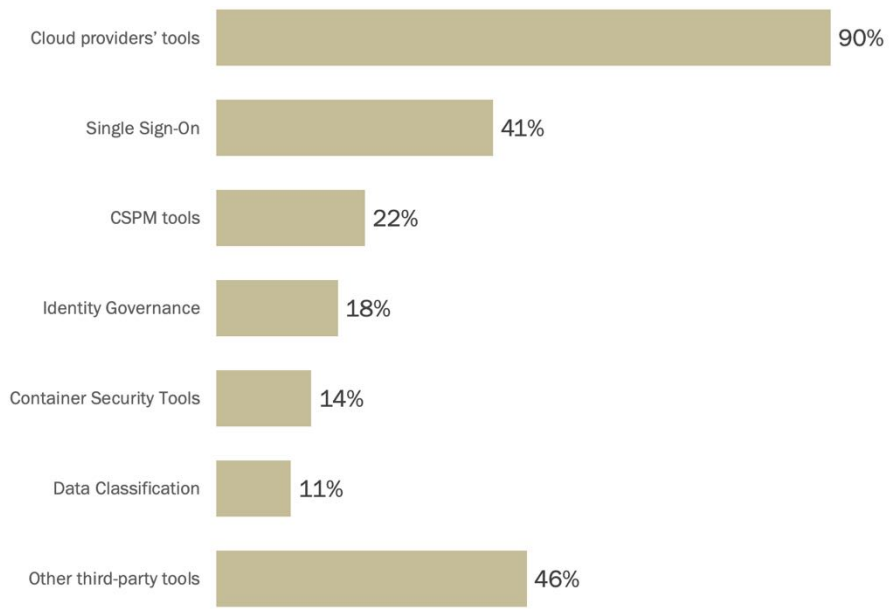
While 32% of respondents are aware of these security issues, they are not actively working to solve these challenges. This decision results from several issues, not least of which is that many organizations are budget-strapped and cannot address all of their vulnerabilities and risks. For those that do have a budget available, some decision makers may not consider a particular risk great enough to warrant the time and attention needed to address it adequately.

CLOUD SECURITY TOOLS ARE VARIED

The vast majority of organizations (90%) are using the security tools provided by their respective cloud providers, as shown in Figure 5. Another 41% use identity and access management (IAM) tools, while 22% are using Cloud Security Posture Management (CSPM) tools. Forty-six percent (46%) are using other types of third-party tools.

More than one-half of survey respondents believe that they are aware of the critical issues surrounding public cloud security and are making the necessary investments to address them.

Figure 5
Cloud Security Tools in Use



Source: Osterman Research
The majority of organizations (90%) are using the security tools provided by their respective cloud providers

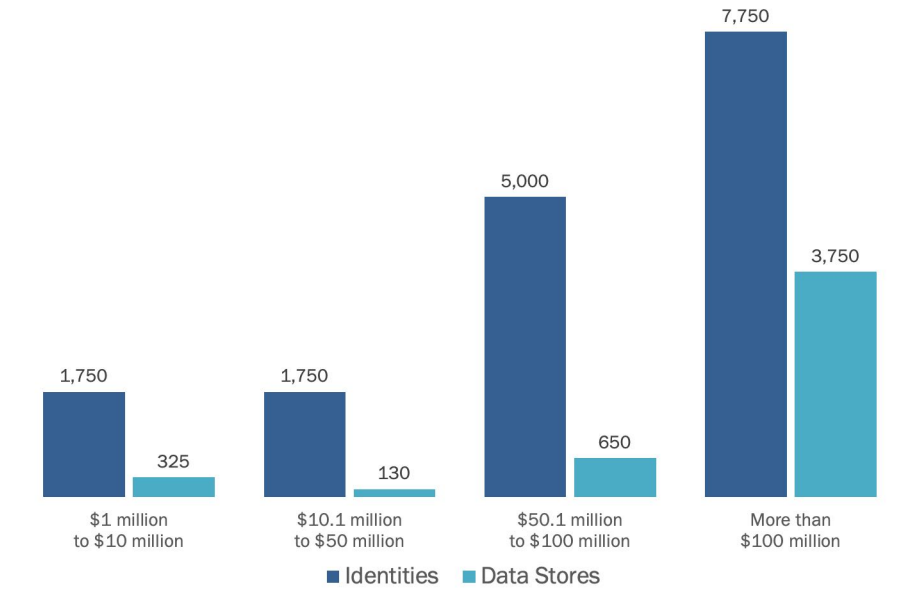
While many cloud providers – especially leading providers with large numbers of customers – normally take great pains to offer good security for their customers, the aggregation and concentration of large volumes of data make cloud providers an attractive target for bad actors. While these providers typically have better security capabilities than most organizations and suffer fewer data breaches, as a result, a successful data breach can open an organization to enormous financial penalties, regulatory fines, loss of customer confidence, and other consequences. Plus, it's essential to understand that there are many smaller cloud providers in use in some organizations, like Tencent Cloud, IBM, or Oracle, some of which do not have robust security profiles.

A successful data breach can open an organization to enormous financial penalties, regulatory fines, loss of customer confidence, and other consequences.

CLOUD IDENTITY AND DATA SPRAWL IS EVIDENT AS INVESTMENTS INCREASE

As shown in Figure 6, the number of identities and data stores increases exponentially along with the size of the investment in public cloud infrastructure. For example, organizations with up to $10 million in public cloud investments over the past three years have an average of 1,750 identities in their public clouds and operate an average of 325 data stores. At the opposite end of the spectrum, organizations that have spent more than $100 million on their public cloud infrastructure have an average of 7,750 identities and 3,750 data stores over the past three years.

Figure 6
Identities and Data Stores in Use by Size of Cloud Investment



Source: Osterman Research
Identities and data stores increase along with the size of the investment in public cloud infrastructure.

Most enterprise organizations consider identities to be related only to people. But people are just one part of the equation and increasingly a small part of that equation. As cloud adoption accelerates, there's been an explosion in non-people identities over the last few years. With container orchestration, the typical lifetime of a container is 12 hours. Serverless functions, already adopted by 22% of corporations, come and go in seconds. It is not unusual for enterprises to have hundreds and, in some cases, thousands of cloud identities, including data stores.

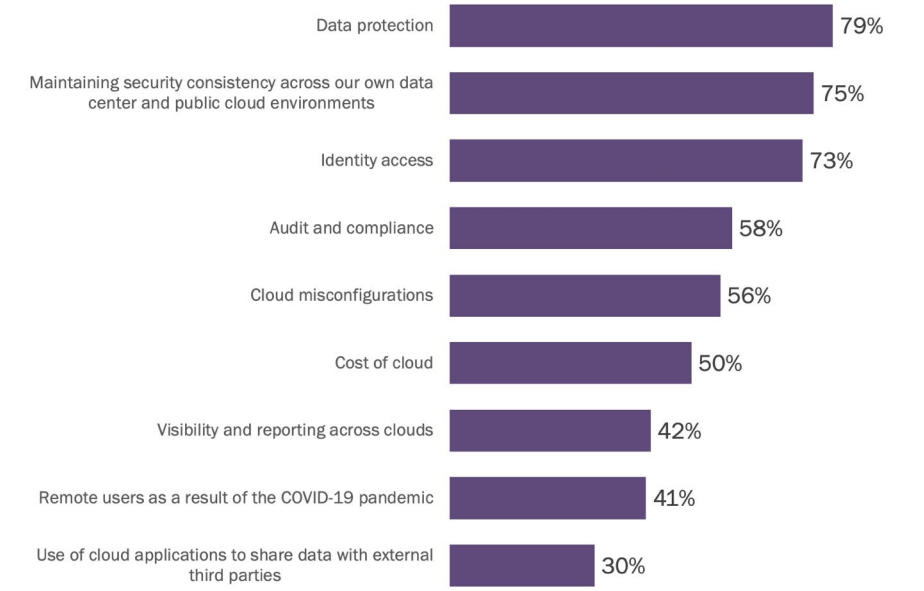
As cloud investments grow to accommodate workloads, so has the need to manage thousands of people and non-people identities. More than ever, enterprises are increasingly relying on automation and services — a trend that's going to keep accelerating as more organizations move away from monolithic paradigms to the cloud, which includes microservices, containerization, and serverless paradigms.

As cloud adoption accelerates, there's been an explosion in non-people identities over the last few years.

IDENTITY AND DATA RISKS DOMINATE EXECUTIVES' CONCERNS

Cloud influencers and decision makers are concerned about a wide range of issues relative to public cloud. As shown in Figure 7, four out of five of those surveyed (79%) are very concerned about data protection in the cloud, followed by 75% who are concerned about maintaining security consistency across their data center and public cloud environments. Another 73% are concerned about identity access. Also, more than one-half of those surveyed are very concerned about audit and compliance issues in the public cloud, as well as cloud misconfigurations.

Figure 7
Concerns About the Public Cloud
Percentage responding with "significant" or "huge" concern



Source: Osterman Research
Executives top concerns relative to the public cloud

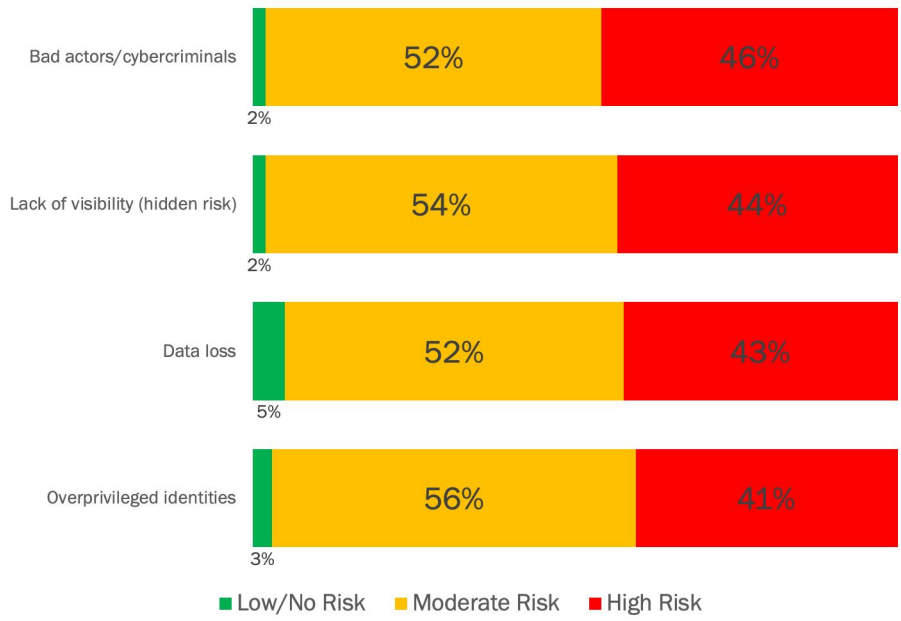
Cloud Risk Findings

TOP RISKS FOR PUBLIC CLOUD DATA AND IDENTITY

As shown in Figure 8, 46% of survey respondents consider that bad actors and cybercriminals represent a high risk to their public cloud operations. However, nearly as many respondents (44%) consider lack of visibility – what we term hidden risk – to be a serious threat. Other leading threats that are considered high risk include data loss and over-privileged identities.

46% of survey respondents consider that bad actors and cybercriminals represent a high risk to their public cloud operations. However, nearly as many respondents consider lack of visibility to be a serious threat.

Figure 8
Perceptions on the Public Cloud Threat Landscape



Source: Osterman Research
46% of survey respondents consider that bad actors and cybercriminals and (44%) citing lack of visibility as a high risk to their public cloud operations

DATA LOSS RISK AMONG TOP IMPROVEMENTS DESIRED

The survey asked, "If you could somehow wave a magic wand to improve your cloud security, what are the top two or three things you would improve?" Here's what we found:

- They are seeking higher levels of data protection, IAM, and reporting.
- Data classification and exfiltration protection, solid IAM, and quality security reporting are capabilities that need to be added.
- Data loss protection, vendor willingness to work with the customer to secure and harden the cloud, and more automation and visibility into the cloud environment for compliance are also on organizations' wish lists.

LACK OF VISIBILITY IS A MAJOR RISK

As the cloud grows, one of the biggest challenges for survey respondents, as shown in Figure 8, has been (44%) lack of visibility and hidden risks. Some organizations do not know what data they're storing in the cloud, who has access, when it was accessed, and/or by whom it was accessed. Many have experienced serious cloud security incidents resulting from poor cloud visibility into their data and identities. IT complexity is on the rise due to various factors, including a growing number of identities, data stores (Figure 6), and the remote workforce adding complexity to this lack of visibility.

OVERPRIVILEGED IDENTITIES ARE INCREASING

As shown in Figure 8, forty-one percent (41%) of respondents consider overprivileged identities as a serious or "huge" risk for their organizations, putting

Many have experienced serious cloud security incidents resulting from poor cloud visibility into their data and identities.

the risk of overprivileged identities only slightly below that of cybercriminal activity. When those who consider the problem to be merely "risky," that figure jumps to 68%. With identities expanding to people and non-people, the challenge will continue to grow. It is estimated that within two years, three out of four security failures in the cloud will be the result of improper identity, access, and privilege management[i].

MISCONFIGURATION RISK IS INCREASING

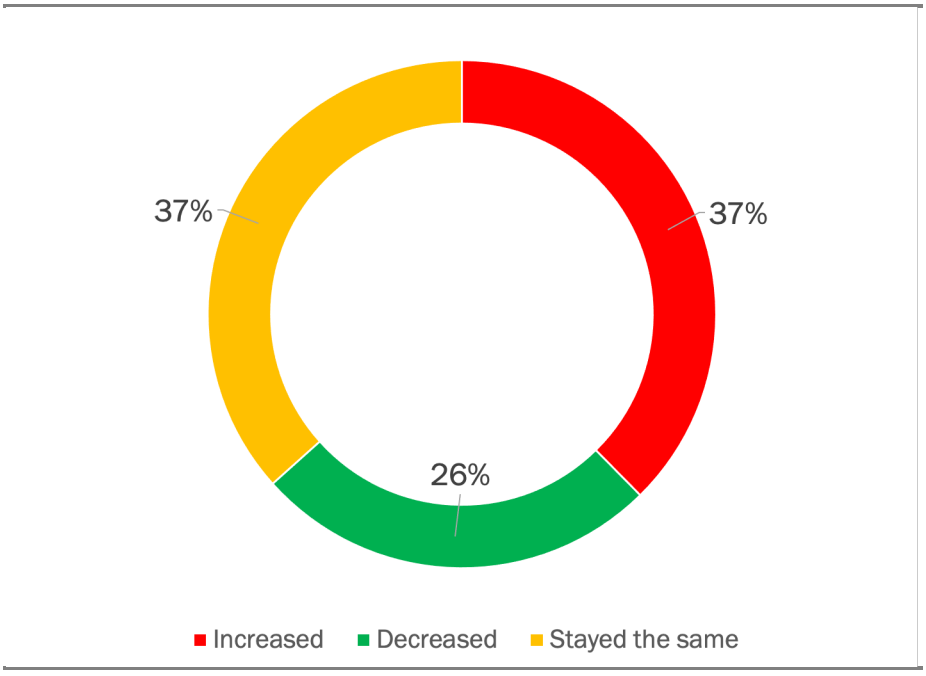
The research conducted for this survey found that the problem is not getting better for most organizations. As shown in Figure 9, 37% report that the risk of cloud misconfigurations is getting worse over time, while the same proportion reports that the problem is getting no better. In other words, 74% consider that the problem of cloud misconfigurations – which 95% consider to be a security risk – is not improving over time and is actually getting worse for many.

As just one example of the problems that misconfiguration can cause, the now-infamous Capital One breach was the result of a misconfiguration error in conjunction with permissions that were too broadly applied. The result was the theft of data from more than 100 million credit applications, affecting nearly one-third of the US population.

Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes. Security and risk management leaders should invest in tools to identify and remediate these risks with a particular focus on identity and data access proactively and reactively.[ii]

The now-infamous Capital One breach was the result of a misconfig-uration error in conjunction with permissions that were too broadly applied.

Figure 9
Changes in the Risk of Cloud Misconfiguration Over Time



Source: Osterman Research
Cloud misconfigurations are considered a data security risk by 19 out of 20 IT decision makers and with 37% reporting they are getting worse

Cloud misconfigurations are damaging. One analysis found that for the two-year period that ended December 31, 2019, there were 196 data breaches caused primarily by cloud misconfigurations resulting in the breach of more than 33 billion records. Inadvertent mistakes in coding decisions can also have significant impacts on cloud services. Another analysis found that the average organization has thousands of misconfigurations every year, and 99% of them go unseen.

CRUSHING COMPLEXITY AND STAFF SKILLS LEAD TO RISKY MISCONFIGURATIONS

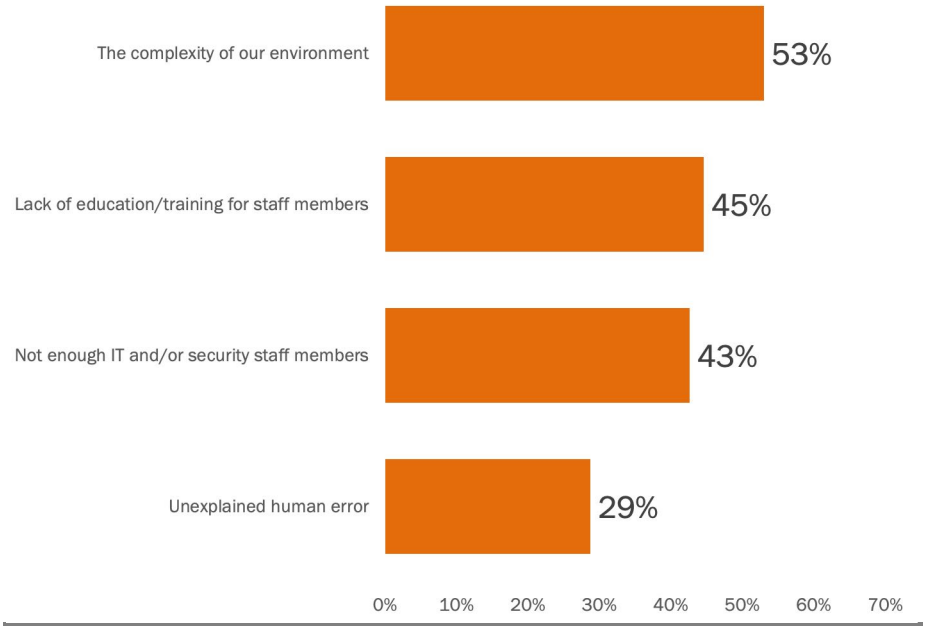
Cloud misconfiguration is preventable yet remains one of the most common security concerns for organizations. There are a number of reasons that misconfigurations occur. As shown in Figure 10, 53% of those surveyed believe that a likely or major reason they happen is because of the complexity of cloud environments – not surprising given that most organizations are operating multiple public clouds. Misconfigurations in the cloud aren't rare events. Another recent survey found that every organization running within the cloud had seen a misconfiguration incident at some point in the past. Most (73%) admitted to having over 10 misconfiguration incidents a day.

As shown in Figure 10, another leading reason that misconfigurations occur is a lack of education and/or training for staff members, and an inadequate number of IT and/or security staff members. Even unexplained human error is believed to account for nearly three in 10 (29%) of misconfigurations. While agile and cloud investments are on the rise, the level of cybersecurity professionals' skills is not – leaving a gaping hole in security strategy that needs to be filled. In fact, executives report needing to increase their security staff to adequately manage their organization's cloud security. The absence of adequately trained professionals can leave holes in many aspects of modern-day security infrastructure, with one of the widest specifically involving cloud security as evidenced by misconfigurations and concerns from Figure 10.

Put two and two together, and these breaches make one thing apparent: organizations are lacking sufficient cloud security skills, which ultimately puts them more at risk of continued misconfigurations.

One analysis found that for the two-year period that ended December 31, 2019, there were 196 data breaches caused primarily by cloud misconfig-urations resulting in the breach of more than 33 billion records.

Figure 10
Reasons That Misconfigurations Occur
Percentage responding a "likely" or "major" reason



Source: Osterman Research
Cause of misconfigurations in enterprise organizations

Employees include those who are highly productive to those who are well-intentioned but careless, to those who are reckless … or even malicious in some cases. Many of these employees operate under daily pressure to be productive, meet deadlines, and deliver their work on time, a problem made worse by the pandemic in 2020. In these types of organizational cultures, getting quick and convenient access to cloud services is a great boon to productivity, although doing so might violate corporate security policies and often is outside of IT's oversight. In many cases, employees will migrate much of their day-to-day content away from authorized IT services and will store and share customer and organizational data freely on cloud services with a questionable security posture.

Moreover, there are some other identity security challenges that need consideration. For example, if an identity (people or non-people) is over-privileged, it can directly or indirectly promote itself to the ownership level of a resource. With this level of privilege, the identity has the authority to make administrative changes that could compromise an entire cloud operation.

If an identity (people or non-people) is over-privileged, it can directly or indirectly promote itself to the ownership level of a resource.

Another identity security risk example is giving widespread access to service accounts in the organization that need only limited permissions to perform their jobs. This creates a weak link in overall security. Allowing service account identities too much access opens the organization to risks. Apply the principle of least privilege by giving identities only the minimum set of permissions to perform their needed tasks.

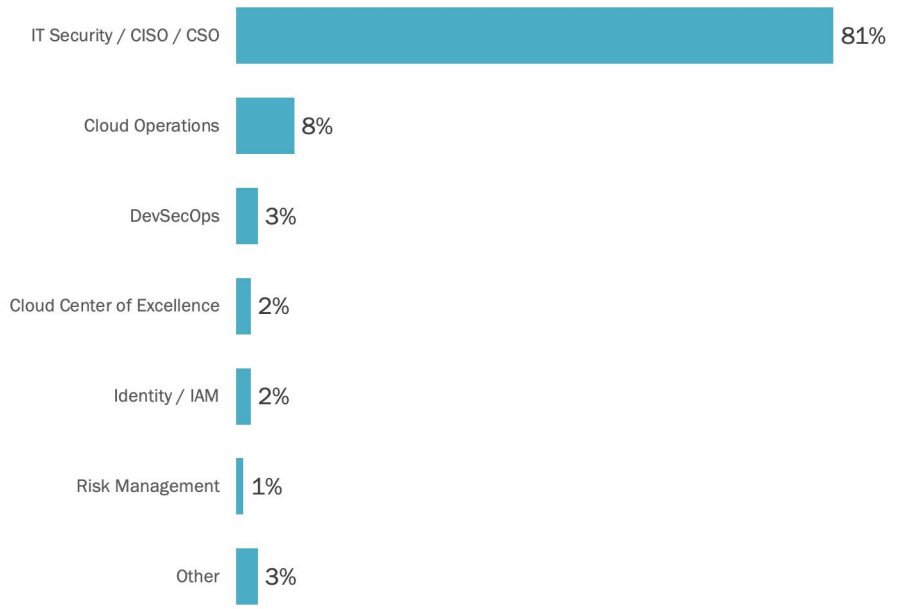
The truth is that misconfigurations are not always easy to detect. Indeed, another

industry survey cited that just 1% of misconfigurations are reported. This suggests that many cloud identities, people and non-people, could be leaking data without even knowing it.

IT SECURITY TYPICALLY OWNS CLOUD SECURITY

Not surprisingly, as shown in Figure 11, in more than four in five organizations the IT security function (or, by extension, the office of the CISO or CSO) is primarily responsible for cloud security. However, in eight percent of organizations a cloud operations team is responsible for cloud security, while DevSecOps and other groups are responsible for cloud security in only a small proportion of organizations.

Figure 11
Department that Owns Cloud Security



Source: Osterman Research
Cloud security ownership is with IT Security and the executive team

As a greater proportion of IT functionality is migrated away from the corporate data center and into various public clouds, the challenge of security is ever-present and increasing. Many of the current security concerns that face organizational decision makers using on-prem IT capabilities are in many ways amplified with cloud services, and a new set of challenges are introduced.

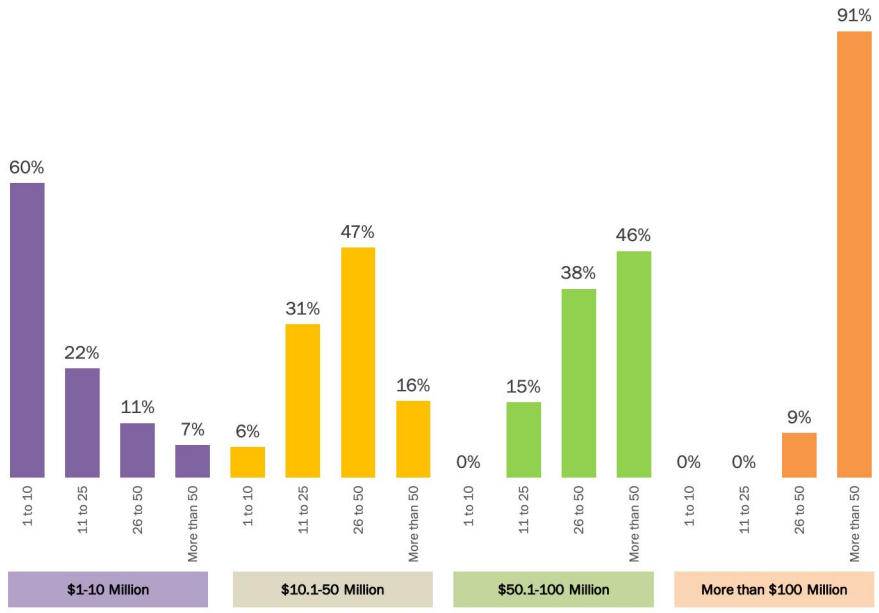
The ideal scenario is that every organization must be responsible for its own security and not rely on cloud providers to manage security for them. However, cloud services introduce a different security operating model with shared responsibility between the organization and the cloud provider – the Shared Responsibility Model – something with which many security managers may not be completely familiar. The different types of cloud services – SaaS, PaaS, and IaaS – have somewhat different lines of security demarcation. Decision makers must understand where those lines of demarcation fall, as they will need to competently deliver on the security requirements for which they are responsible.

As a greater proportion of IT functionality is migrated away from the corporate data center and into various public clouds, the challenge of security is ever-present and increasing.

EMPLOYEES ON THE CLOUD TEAM ARE GROWING

Not surprisingly, the number of full-time equivalent (FTE) employees on the typical organization's cloud team increases along with their investments in cloud. As shown in Figure 12, organizations that have spent the least on public cloud investments over the past three years generally have fewer FTE staff members – 60% have no more than 10 FTE staffers. However, at the other end of the scale, the vast majority of those that have spent more than $100 million have more than 50 staffers managing their cloud operations.

Figure 12
Full-Time Equivalent Employees on the Cloud Team



Source: Osterman Research
Cloud team resources are increasing with cloud investments

An organizations' employees and other users who operate independently or in small, informal workgroups comprise one issue inside the organization that drives the use of cloud services. A more organized driver involves the various business groups that sometimes pressure IT security teams to allow fast and convenient access to data and applications. Many employees want quick access to the public cloud.

SaaS offerings that don't get tied up in what's perceived as irrelevant "security red tape" can slow the deployment of services that these employees need to do their work. When IT security teams don't respond with demands for speed, business groups go off and do their own thing. The proliferation of shadow IT creates security visibility problems and can increase the threat landscape for data breaches and non-compliance.

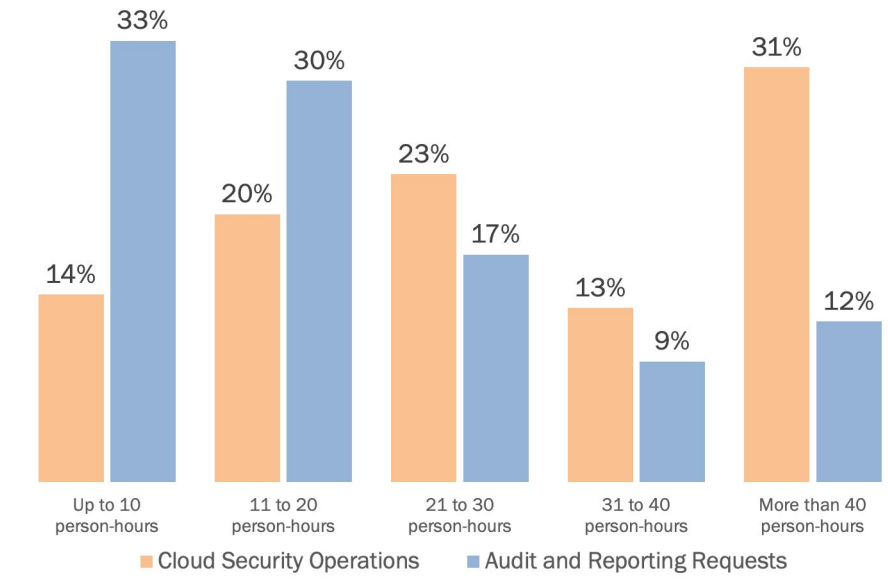
When IT security teams don't respond with demands for speed, business groups go off and do their own thing.

LABOR INVOLVED IN MANAGING SECURITY OPERATIONS, AUDITING AND REPORTING IS DISPROPORTIONATE TO NEEDS

As shown in Figure 13, the majority (63%) of organizations surveyed spend no more than 20 person-hours per week managing auditing and report requests in their cloud environments, while the remaining 37% spend more than 20 person-hours

per week on this activity. By contrast, only 34% of organizations spent no more than 20 person-hours on cloud security operations, while the remaining 66% spend more than 20 person-hours per week. What this tells us is that cloud security operations are more time consuming and labor-intensive than are auditing and report requirements for the majority of organizations.

Figure 13
Total Person-Hours Spent by Teams During a Typical Week Managing Cloud Security Operations and Managing Audit and Reporting Requests



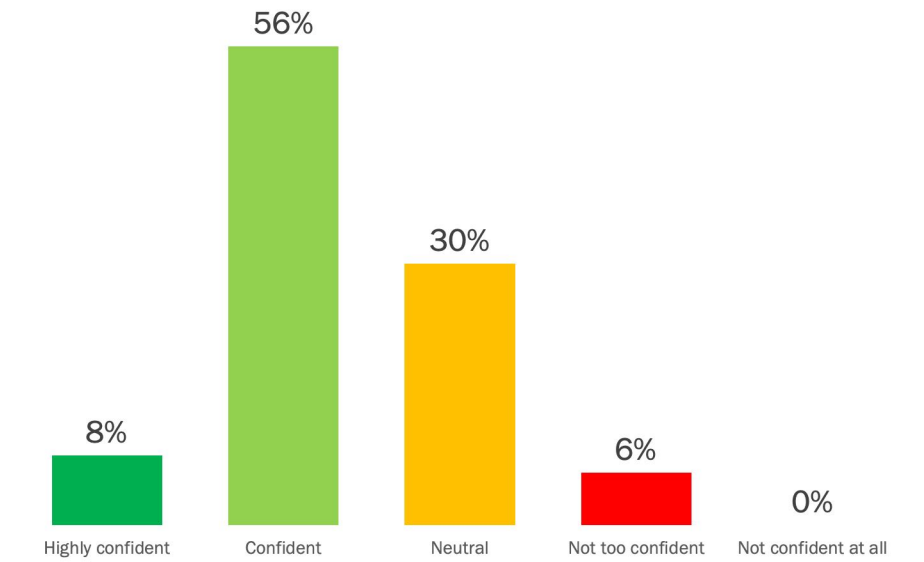
Source: Osterman Research
Majority (63%) of organizations spend no more than 20 person-hours per week managing auditing and report requests in their cloud environment

MOST ENTERPRISES ARE NOT HIGHLY CONFIDENT IN THEIR AUDITING AND REPORTING CAPABILITIES

As shown in Figure 14, only 8% percent of those surveyed are "highly confident" in their auditing and reporting capabilities, while another 56% are "confident." However, more than one-third (36%) of respondents are less than confident in these capabilities.

Only 8% percent of those surveyed are "highly confident" in their auditing and reporting capabilities.

Figure 14
Level of Confidence in Auditing and Reporting Capabilities



Source: Osterman Research
Executive confidence in managing audits and reporting is high

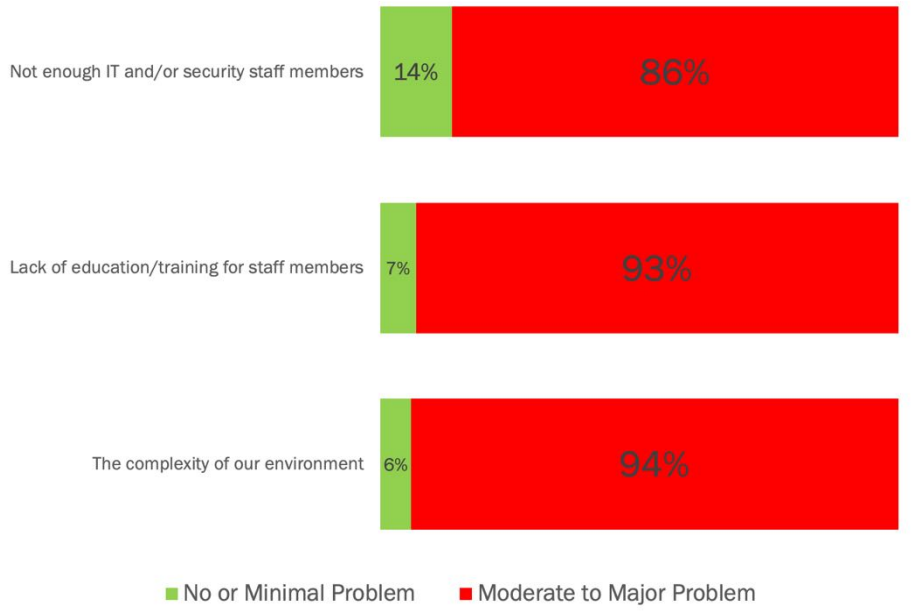
Having a false sense of confidence in the security of the cloud from auditing means decision makers are falsely confident in security and operational parts of their cloud.

GAPS IN STAFF, SECURITY TRAINING, AND EDUCATION

As noted in Figure 4, a significant proportion of organizations are not investing adequately in cloud security, and as shown in Figure 9, misconfiguration problems are not improving or are getting more serious for the vast majority of organizations. Reasons for this are varied, but in many cases are the result of understaffing in IT and security, lack of education and training for staff, and the overall complexity of public cloud management environments. As shown in Figure 15, only a very small percentage of the public cloud security specialists responding to this survey consider these to be non-issues in their organizations – the vast majority consider them to be quite serious issues that contribute to their misconfiguration problems.

A significant proportion of organizations are not investing adequately in cloud security misconfig-uration problems are not improving or are getting more serious for the vast majority of organizations.

Figure 15
Problems That Contribute to Misconfigurations



Source: Osterman Research
Complexity of cloud environment is biggest factor to misconfigurations

Summary and Conclusions

The cloud is the future, and the future is now, and the cloud is garnering a growing share of identities, workloads, business data, compute, and critical applications. The cloud can also be a potentially dangerous place because a lack of security training and skills are leading to misconfigurations, poor auditing practices, and/or poor identity management, allowing records to be breached. Consequently, decision makers must make the appropriate investments to secure their cloud infrastructure in order to provide the necessary level of security, as well as to enable the organization to remain in compliance with the various requirements to protect identities and data.

Executives have a false sense of security when it comes to cloud. Security teams are out of touch with the number of identities in their clouds and the resulting complexity.

To avoid suffering the fate of a data breach, enterprise organizations need to take proactive measures, dig deep, and understand their identities' effective end-to-end permissions to protect data and ensure operational stability. All organizations should prioritize protecting the new identity perimeter in their technology ecosystem in 2021, which will reduce risk to the business, increase security, and enforce compliance.

Executives have a false sense of security when it comes to cloud.

About Sonrai Security

Sonrai Security delivers an enterprise identity and data security platform for AWS, Azure, Google Cloud, and Kubernetes. The Sonrai Dig platform is built on a sophisticated graph that identifies and monitors every possible relationship between identities and data that exists inside an organization's public cloud. Dig's Governance Automation Engine automates workflow, remediation, and prevention capabilities across cloud and security teams to ensure end-to-end security.

Identity and data access complexity are exploding in your public cloud. Tens of thousands of pieces of compute, thousands of roles, and a dizzying array of interdependencies and inheritances. First-generation security tools miss this as evidenced by so many breaches. Sonrai Dig, our enterprise identity and data governance platform, de-risks your cloud by finding these holes, helping you fix them, and preventing those problems from occurring in the first place.

The company has offices in New York and New Brunswick, Canada and is backed by Menlo Ventures, Polaris Partners and TenEleven Ventures. For more information, visit https://sonraisecurity.com.

REFERENCES

[i] https://www.gartner.com/en/documents/3986121/managing-privileged-access-in-cloud-infrastructure

[ii] https://www.gartner.com/en/documents/3899373/innovation-insight-for-cloud-security-posture-management