FORRESTER®

Identity Controls Are Central To Enterprise Plans For Cloud Security

To Scale Cloud, Companies Are Looking At CIG/CIEM, AI Monitoring And Investigation, Automation, Access Reviews, And Remediation

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY SONRAI SECURITY AND AWS | APRIL 2022

Cloud Is Accelerating, Can Security Keep Up?

Modern enterprises in highly competitive markets can no longer ignore the cloud's significant benefits for operations, staffing, and security. However, as cloud migration of business-critical applications and workloads continues to increase, so too do security threats to increasingly complex public cloud environments. IT decision-makers (ITDMs) facing breaches and security incidents are also struggling with access control policies, manual processes, and challenges managing cloud identities. To keep up with cloud acceleration, firms are looking to AI-powered solutions, smarter cloud identity governance (CIG), and cloud infrastructure entitlements management (CIEM) tools.

In January of 2022, Sonrai Security and Amazon Web Services (AWS) commissioned Forrester Consulting to explore the current state of cloud security, surveying 154 North American IT and security decision-makers about their current solutions and future expectations.

Key Findings

ITDMs recognize the need to implement security solutions that scale alongside cloud acceleration but struggle to keep up, especially in identity and permissions management.

Running several separate security solutions in the cloud is not getting the job done; firms are still experiencing security incidents and breaches.

Security solutions that incorporate CIG/CIEM, utilize AI to automate processes, and integrate into all major cloud platforms will enable firms to continue scaling in the cloud safely and securely.

Cloud Is Continuing to Grow In Importance

Cloud is increasingly important to business-critical workloads and applications. From customer-facing web and mobile applications to internal software creation platforms and tools, firms are currently running an average of six diverse applications and/or workloads on cloud platforms.

More than three-quarters of ITDMs surveyed agree that rightsizing and scaling in the cloud are critical drivers of success. The cloud is only continuing to grow in importance, as nearly a quarter of respondents note that they are accelerating the execution of their cloud migrations.

76%
of respondents agree that rightsizing and scaling in the cloud are critical to success.

"Which of the following applications or workloads is your organization currently running in a cloud platform?"

66%
Customer-facing web and mobile applications

62%
Internet-of-things applications

62%
Database applications/ systems of record

60%
Middleware and infrastructure

60%
Containers/serverless development platforms

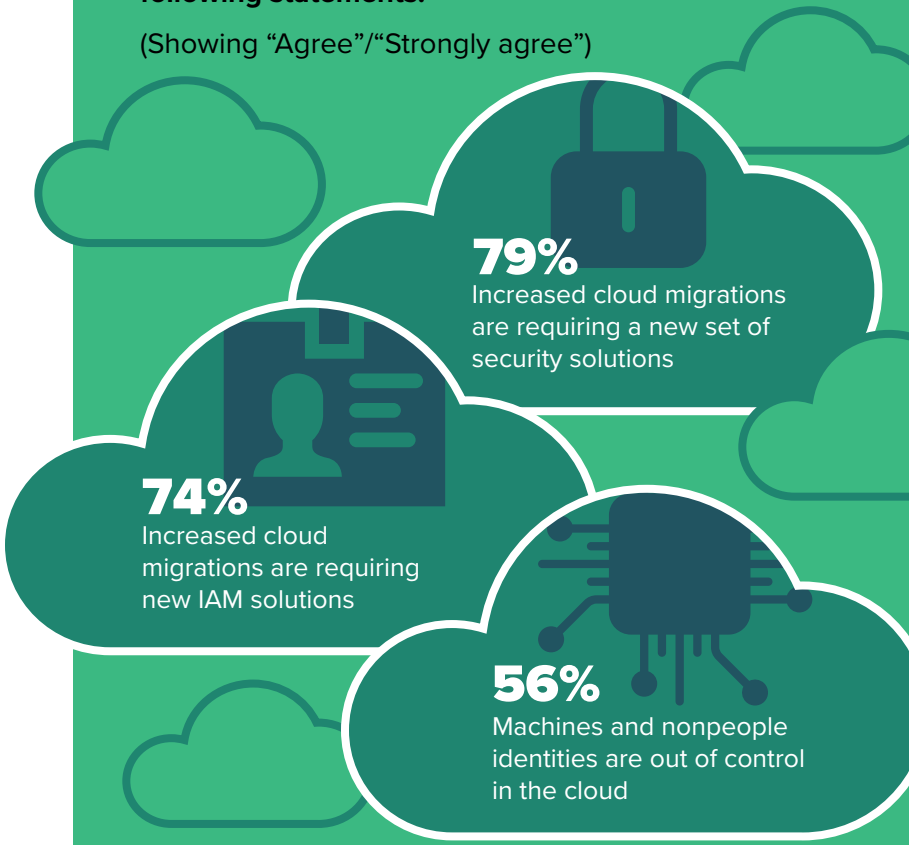
Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

Uncontrollable Cloud Identities Are Causing IT Headaches

Nearly 80% of decision-makers surveyed note that the increase in cloud migrations is requiring a new set of security solutions. As the cloud's presence grows across workloads, the complexity of cloud workload configurations grows as well. This results in firms being more susceptible to security incidents. Over half of all surveyed decision-makers note that they are struggling with machine and nonpeople identities running rampant in the cloud. Decision-makers are also keenly aware that keeping cloud environments secure and permissions up to date requires integrating new identity and access management (IAM) tools.

"Please state your level of agreement with the following statements."

(Showing "Agree"/"Strongly agree")



Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

Security Solutions Are Not Unified

ITDMs are running an average of six different tools or features to secure their public cloud environments. Forrester expects that this large variety of tools indicates that no single solution can cover all security, functional, and multi-cloud coverage requirements. This variety of security tools and features signifies that firms are struggling to keep up with the evolving security needs of public cloud environments, adding new solutions as concerns arise and attempting to manually integrate tools together to form an ad hoc security suite. Over half of respondents' firms are currently using CIG/CIEM solutions as part of their security strategy, indicating that governance and identity entitlement management, mapping permission paths, and access control are known solutions for securing public cloud environments.

"What tools/features do you currently use to keep your public cloud environment secure?"

- Security analytics and threat intelligence
- Cloud identity governance/cloud identity entitlement management (CIG/CIEM) solution
- Key management, encryption, and tokenization of data
- Cloud threat monitoring and management with AI-driven response
- Cloud platform service provider's native security controls
- Cloud access security broker (CASB)

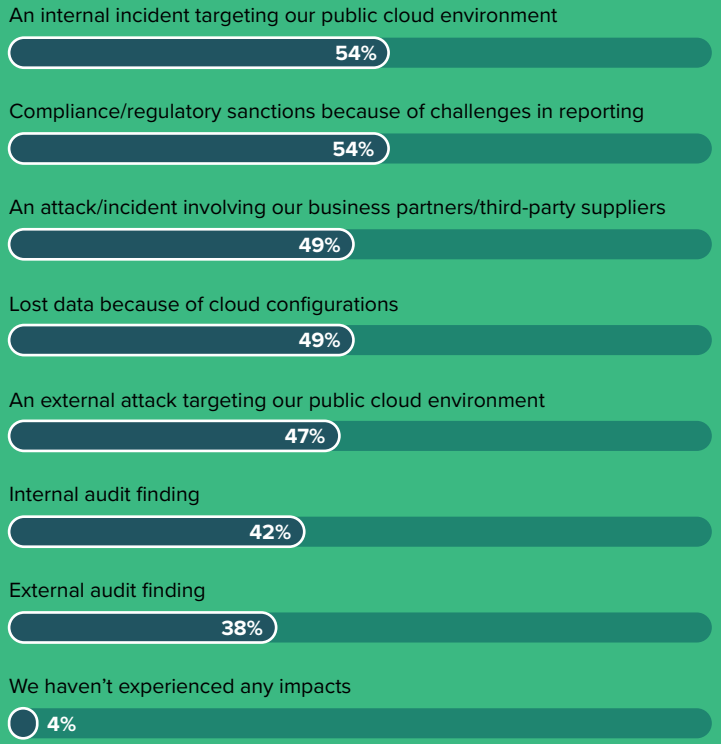
Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

More Security Tools Do Not Equal A More Secure Cloud

Despite the multiple tools currently in use to secure their public cloud environments, 96% of decision-makers report that their organizations faced security incidents in the last 12 months. Compliance and regulatory sanctions due to reporting challenges and internal incidents are the most common issues reported by survey respondents, but they also note experiencing data loss, external attacks, and third-party incidents. Incidents across so many diverse types of cloud-hosted workloads and applications indicates that something is missing from firms' current data security operations. Stacking one tool on top of the other can only get security so far, with incidents slipping through the cracks in the pile.

96%
of decision-makers' organizations have faced a security incident in the past 12 months.

"Which of the following, if any, has your organization experienced in your cloud environment in the last 12 months?"



Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

Confronting CIG/CIEM Challenges

An astounding 98% of ITDMs report that they are facing CIG/CIEM-adjacent security challenges. Some of the most reported issues stem from overly complex access control policies, which make configuring fewer privileges among cloud identities nearly impossible to accomplish. Legacy tools that cannot integrate well, or at all, in the public cloud environment enable the persistence of short-lived identities and the proliferation of unrecognized nonpeople and machine identities. At the same time, firms are experiencing difficulties seeing a single view of cloud platform identities. This is a space in need of big changes to meet the evolving needs of firms as they scale in the cloud.

"Which of the following, if any, CIG/CIEM challenges is your organization facing?"

Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

AI Is Emerging As The Way Forward

As ITDMs pinpoint the objectives of their cloud security programs, AI-driven solutions are emerging as a top priority. Half of our survey respondents note the necessity of AI-driven investigation or behavioral detection programs to better their current security programs. Decision-makers also want to empower faster innovation for development teams and automate security processes. These priorities point to a similar goal: ITDMs want to get ahead of issues and respond to them quickly.

"What are the top objectives of your organization's cloud security program?"

(Ranked in top 5)

50%
Employ better AI-driven investigation or behavioral detection

47%
Create a faster path to innovation for development teams

45%
Effectively automate cloud security processes

45%
Develop better employee experience with seamless access and sign-on

44%
Secure container and server workload infrastructure

41%
Create a concise ecosystem of security tools and technologies to manage our cloud

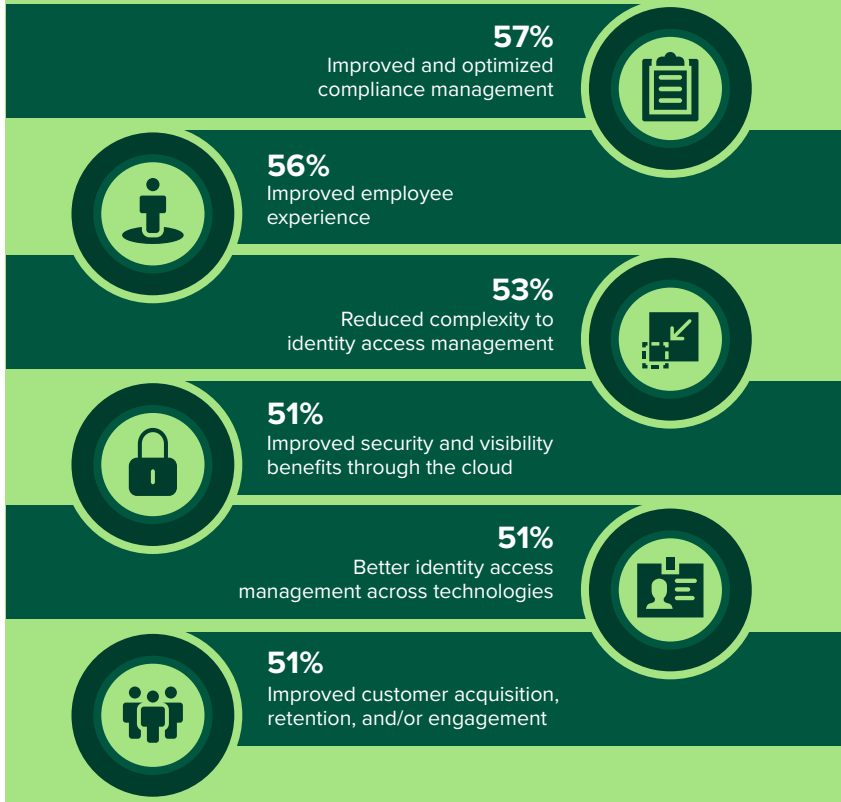
Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

ITDMs Have Great Expectations for CIG/CIEM Solutions

Over half of ITDMs' firms are already investing in a CIG/CIEM solution, and by 2023, 82% are planning to do the same. They expect a CIG/CIEM solution to help with their compliance difficulties, improve employee experience, and reduce complexities to IAM — many of the same top security goals they note earlier in the survey.

ITDMs want their ideal CIG/CIEM solution to understand and detect changes across a minimum of five different scenarios — most commonly cloud-native encryption key management, cloud-native access key management, data stores deployed on top of cloud platform-as-a-service (PaaS) solutions, data stores deployed on cloud infrastructure, and infrastructure-as-a-service (IaaS) serverless functions.

"What benefits do you anticipate from a CIG/CIEM solution?"



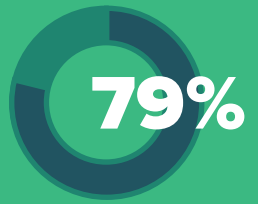
Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

Integration, Automatic Right Revoking Are The Top Features ITDMs Look For In A CIG/CIEM Solution

ITDMs expect their CIG/CIEM solutions to integrate with all the major cloud platforms and perform automatic rights revoking and monitoring tasks.

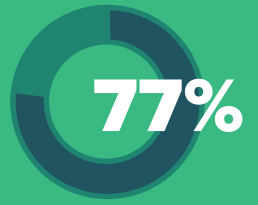
As the cloud becomes an evermore central part of their growth strategies, organizations are recognizing that consistent, automatic monitoring and revoking of rights across all the cloud platforms they use with a single-pane-of-glass tool is critical to keep their clouds secure and tamp down on sprawl. Additionally, AI-based anomaly detection and in-depth integration with all public cloud platforms are critical features of a CIG/CIEM solution.

"How important are each of the following features/ functions in a CIG/CIEM solution?"

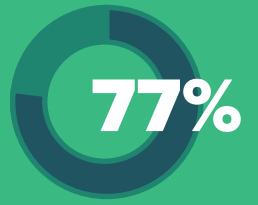


Automatic rights revoking when a user performs a risky activity

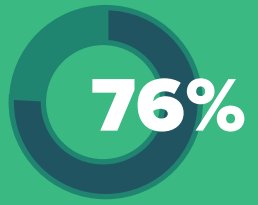
In-depth integration with all major public cloud platforms



Automatic monitoring of breadth of cloud deployment



Continuously updated access rights for the latest cloud services



AI-based anomaly detection

Automatically revoking excessive privileges

Base: 154 Cloud security decision-markers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Sonrai, January 2022

Conclusion

As organizations continue to increase their usage of the public cloud, ITDMs face increased challenges managing the security of their cloud instances, including applying the correct settings and/or configurations at scale. With the growing number of cloud services, roles, and policies written in code, there is exponential growth in potential permission controls. To better meet these needs, ITDMs are looking toward CIG/CIEM solutions, AI-powered monitoring and investigation, and better automation of time-consuming manual workflows for investigation, access reviews, and remediation. With the majority of respondents either using or planning to use CIG/CIEM solutions in the near future, it is clear that ITDMs view cloud identity management as an essential component of a cloud security program that enables firms to continue successfully and securely scaling in the cloud.

Project Director:

Ana Brzezinska,
Market Impact Senior Consultant

Contributing Research:

Forrester's security & risk research group

Methodology

This Opportunity Snapshot was commissioned by Sonrai Security and Amazon Web Services (AWS). To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 154 cloud security decision-makers in North America at organizations that were using public cloud deployments at the time. The custom survey began and was completed in January 2022.

Demographics

REGION	
United States	**82%**
Canada	**18%**

RESPONDENT LEVEL	
C-level executive	**5%**
Vice president	**12%**
Director	**82%**

COMPANY SIZE	
1,000 to 4,999 employees	**42%**
5,000 to 19,999 employees	**55%**
20,000 or more	**3%**

CURRENT CLOUD SECURITY STRATEGY	
We have implemented various cloud security point solutions or controls, but we lack a holistic strategy	**65%**
We have a clear, documented, and periodically updated cloud security strategy	**35%**

Note: Percentages may not total 100 because of rounding.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®