## CloudBolt Industry Insights Report:

# “Sometimes, Somewhat” Security – A Disconcerting Look at the Reality of Hybrid Cloud/Multi-Cloud Vulnerabilities

# SETTING THE STAGE

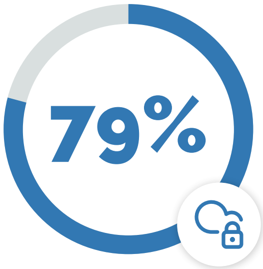
On the list of things that keep executives up at night, cybersecurity always appears at or near the top. As the corporate perimeter increasingly becomes virtual and decentralized, keeping the company safe from attack or exposure remains a highly funded priority.

One would think that as organizations increasingly move to hybrid cloud/multi-cloud, this vigilance would be even greater. However, this most recent CloudBolt Industry Insights report paints a perplexing picture of how cloud security may not be as consistent or fool-proof as one might expect.

For this CII report, 350 IT experts (Director-level and above) from primarily large enterprises with more than 5,000 employees from around the globe were surveyed using the Pulse research platform from Gartner (see Appendix for complete audience details). Respondents' answers provide a fascinating look into the beliefs, challenges, and misconceptions associated with securing their clouds.

# KEY FINDINGS

If you're looking for the Cliffs' Notes version of these new CII findings, here's the highlight reel. Welcome to the Good, the Bad, and the Head Scratch-Worthy.



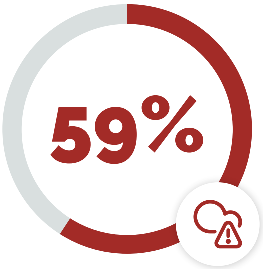
**79% believe their board members will do whatever is necessary for security**

## THE GOOD

Cloud Security looks like it's being addressed appropriately at the highest levels. **79% of respondents believe that their companies' Board of Directors and executive teams have demonstrated that they are willing to do whatever is necessary to ensure that cloud-related computing is secure.** And they believe they have the right Chief Information Security Officer (CISO) for the job (83%).

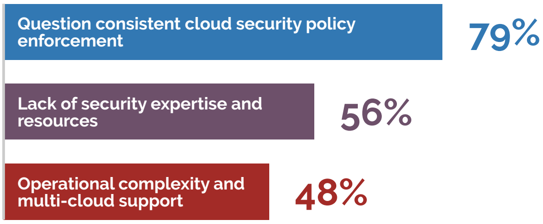
## THE BAD

75% of respondents say that cloud computing is the single greatest expansion of the enterprise attack surface in the last 20 years. More sobering still? **Fully 59% believe that moving to the cloud has made their enterprises less secure.**



**59% believe moving to the cloud has made their enterprises less secure**

Relative to specific cloud security concerns, respondents cited the following –



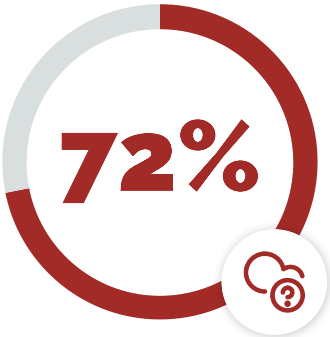
- 79% question whether their companies apply consistent cloud security policy enforcement
- 56% point to a lack of multi-cloud and cloud security expertise and resources; and
- 48% count operational complexity and multi-cloud support as key concerns.

And if that weren't enough, 69% of respondents say their developers spend less than a single hour per week ensuring the cloud resources they provision are secure.

## THE HEAD SCRATCH-WORTHY

Then, there were a multitude of answers that did little to instill confidence in the urgency and vigilance associated with making cloud infrastructure secure.

**68%** of respondents said their **companies' security skill sets across all clouds was only "Somewhat Mature"**; another 20% were "Neutral" – not exactly resounding assurance.



**72% admit their companies moved to the cloud without proper understanding**

- A mere 8% of respondents say they have implemented highly operationalized cloud security practices when spinning up new compute resources and environments
- Only 6% of respondents say that their companies automatically build security into every workload up front and orchestrate processes across every cloud so that developers don't have to worry about remembering to build security in themselves
- Only 3% of respondents consistently leverage "immutable infrastructure" as a security measure, whereby cloud resources are automatically destroyed and rebuilt every set number of days

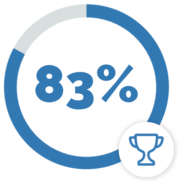
And if all of that wasn't enough, **72% of respondents admit their companies moved to the cloud and multi-cloud without properly understanding the skills, maturity curve, and complexities of making it all work securely**.

Clearly, there is work to be done to shore up cloud security in the hybrid cloud/multi-cloud world in which most companies now operate.

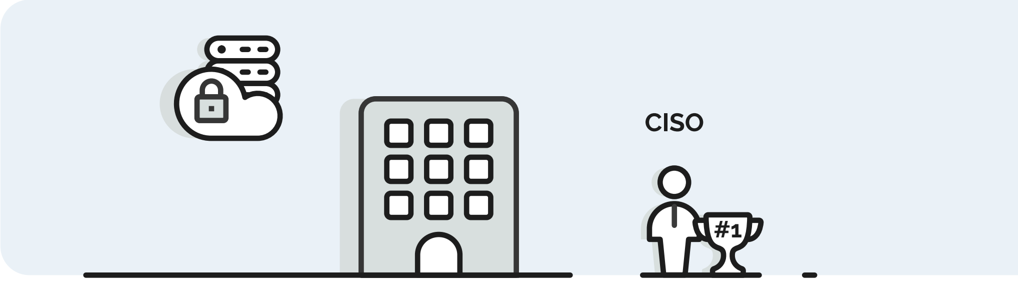
# DIGGING IN:
## Cloud Security – The View From The Top

Given the risks and dangers of cyberattacks and breaches, it's not surprising that the highest levels within organization are perceived as strongly embracing cloud security. 79% of survey respondents indicate the board of directors and executive team at their companies have demonstrated that they are willing to do whatever is necessary to ensure that cloud-related computing is secure.

The person most responsible for cybersecurity within most enterprises is the Chief Information Security Officer (CISO). Cloud security has become another set of attack vectors that the CISO must defend against. By a large majority, **83% of companies gave their CISO high marks for being adept at Cloud Security**.



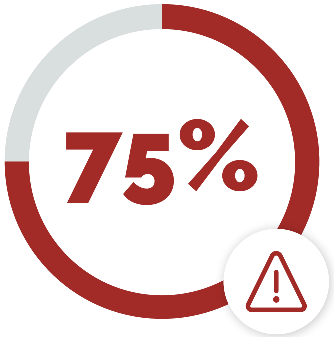
83% gave their CISO high marks for being adept at Cloud Security



So given strong executive and board support, as well as competent CISOs, one would expect consistent and effective cloud security for most enterprises. Unfortunately, the reality appears to be looser and less consistent.

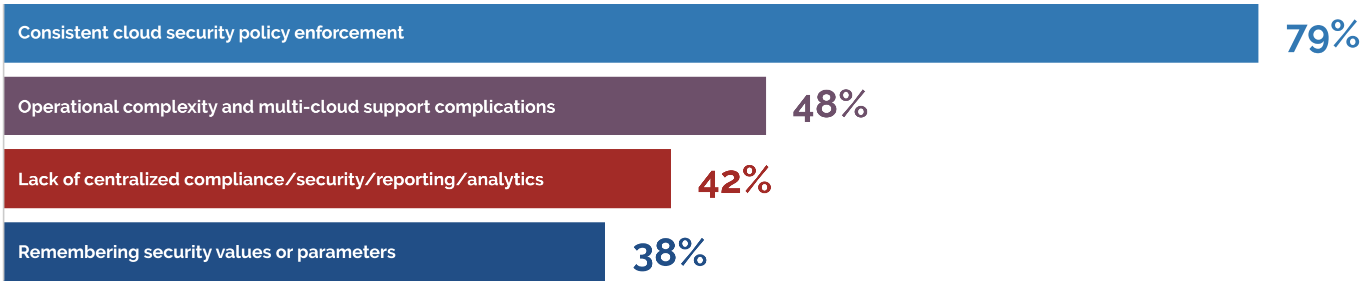
# THE REALITY

The move to cloud wasn't just another evolutionary event. **Fully 75% of respondents say that cloud computing represents the single greatest expansion of the enterprise attack surface in the last 20 years!** And nearly **3 out of 5 respondents agree that moving to the cloud has made their enterprises less secure.**

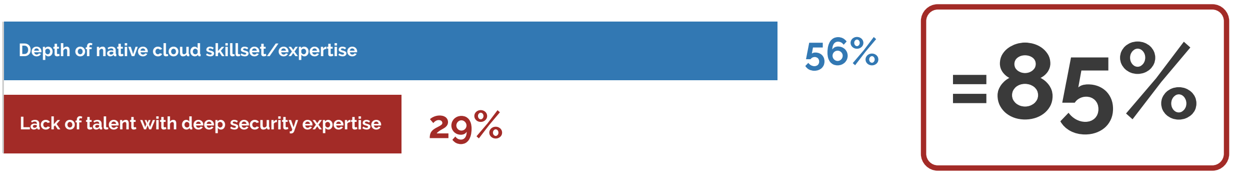


**79% believe cloud computing represents the greatest expansion on the enterprise attack surface**

When asked where their companies struggled most and what their biggest concerns were, 4 out of 5 (79%) questioned whether their organizations employed consistent cloud security policy enforcement. Nearly half (48%) also cited operational complexity and the complications of multi-cloud support as key areas of concern, followed by lack of centralized compliance/security/reporting/analytics (42%) and needing to remember security values or parameters unique to each cloud platform (38%).



But the one area that bubbled up to the top is a familiar refrain in multi-cloud: the skills gap. As first revealed in a previous CII study ("Filling The Gap: Service Providers' Increasingly Important Role in Multi-cloud/Multi-Tool Success"), there are not enough people with the necessary skills across all major cloud platforms and private cloud to effectively address the biggest cloud challenges – including cloud security. 56% of respondents cite "depth of native cloud skillset/expertise" as a top concern. Additionally, another 29% point to a "lack of talent with deep security expertise" as an issue. **Both point to the skills gap issue which if combined would point to a concern noted by 85% of respondents.**



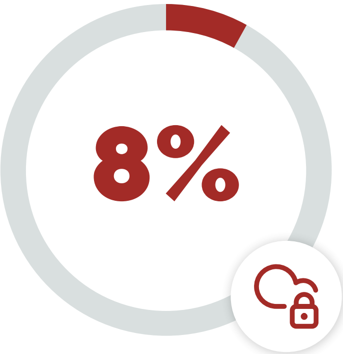
Further adding to the troubling trends: 69% of responding companies' developers spend less than a single hour per week ensuring the cloud resources they provision are secure.

# HAND GRENADES AND HORSESHOES

Cybersecurity requires absolute vigilance. CISOs have known for decades now that it just takes one lapse or vulnerability to expose the company to all kinds of damage via a breach. "Almost secure" is the same as not secure at all. Similarly, so are answers like ***"Somewhat"*** or ***"Sometimes"***. And unfortunately, there were quite a few of those types of answers to important questions in this CII Report.

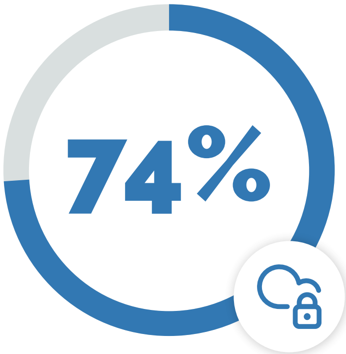
When asked about the skillset maturity across all clouds, respondents chose ***"Somewhat Mature"*** 68% of the time; another 20% said they were "Neutral" in terms of level of maturity. Considering the amount of rogue provisioning through Shadow IT and lack of process for cloud security best practices, it's amazing that more detrimental events have yet to be reported.

Even worse, **only 8% of respondents say they have implemented highly operationalized cloud security practices when spinning up new compute resources and environments**; 83% say they have ***"Somewhat"*** done so.



**8% have implemented highly operationalized cloud security practices**

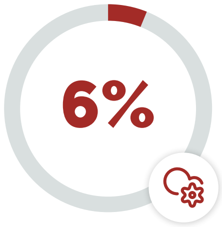
Every Cloud provider offers security tools (often at considerable incremental expense) that companies can utilize to secure each Cloud type. But in a multi-cloud world, the unique nuances of settings and requirements between each of the major clouds create plenty of opportunities for errors, omissions, or mistakes. **Yet, most respondents seem enamored with these native cloud security tools - 74% say they are relying on them to provide "adequate security."**



**74% are relying on native cloud security tools**

For teams that embrace Hashicorp's Terraform, 64% believe it can solve their cloud security concerns. And nearly everyone (84%) indicated that simply using a monitoring tool like Prisma is the best way to deal with cloud security.

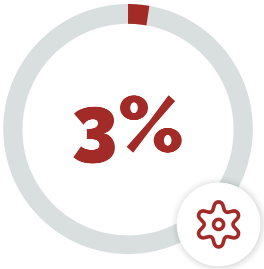
Whether cloud-native, Terraform, or Prisma, the data strongly suggest that people want to believe the tools they use will simply take care of security for them. Unfortunately, there are no panaceas.



**6% automatically build cloud security into workloads up front**

Emerging best practice would indicate that the most effective and logical way to ensure cloud security is to automatically build it into workloads up front so that developers don't have to worry about adding it in later. **Unfortunately, only 6% of respondents indicate that they do this regularly.** 51% say they do it ***"Sometimes*.***"*

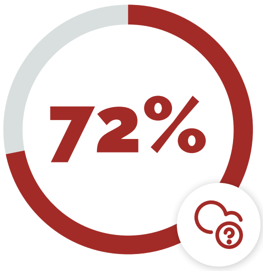
Even the practice of leveraging "immutable infrastructure", whereby a server automatically destructs after a pre-determined number of days and is then reconstituted as a clean new build, has yet to become anywhere near ubiquitous. **Only 3% of respondents actually do it,** while 53% say they incorporate it ***"Sometimes*.***"*



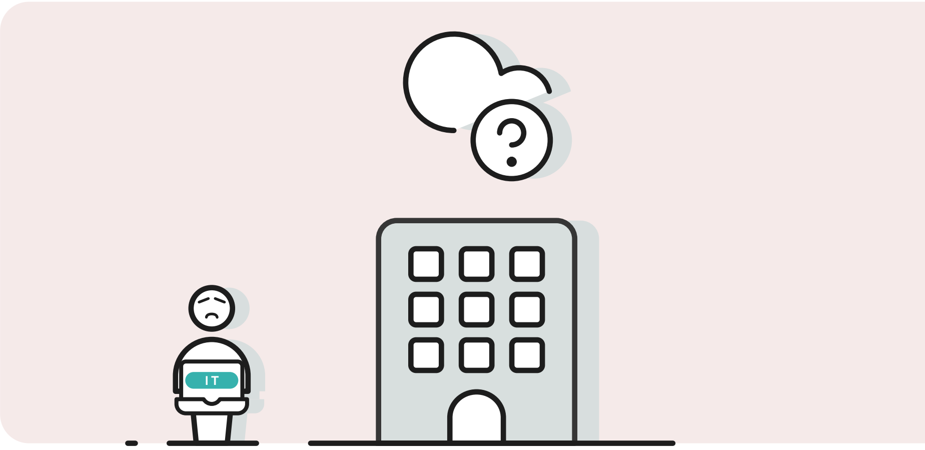
**3% leverage immutable infrastructure**

If you are surprised by the number of questions where the majority answer came back ***"Somewhat and Sometimes"***, you wouldn't be alone. For an issue as vital as security, there certainly appears to be a gap in vigilance. It's hard to imagine an answer of ***"Somewhat"*** or ***"Sometimes"*** ever being acceptable in traditional perimeter or cybersecurity. Yet, these answers seem to be chosen unapologetically when applied to cloud security. And in that light, the following then makes perfect sense:

**72% of respondents admit their companies moved to the cloud and multi-cloud without properly understanding the skills, maturity curve, and complexities of making it all work securely.**



**72% admit their companies moved to the cloud without proper understanding**



# CONCLUSION:

What is the real state of cloud security? Our study shows that it's somewhat and sometimes good, which by any measure can't be good enough when compared to any other type of enterprise security. In the exuberance to move everything to the Cloud and be CloudFirst, true cloud security appears to have been marginalized and, in its place, "good enough security" suffices in day to day practice. While corporations feel like their executives and boards have done whatever is necessary to ensure secure clouds, the actual practice of cloud security appears to be falling short. Time will tell if companies will be able to shore things up as their hybrid cloud/multi-cloud practices mature.

CloudBolt® software

CloudBolt helps companies automate easily, optimize continuously, and govern at scale in hybrid and multi-cloud, multi-tool environments. Pulling together islands of automation, our framework helps unify disparate capabilities for DevOps, ITOps, FinOps, and SecOps. Backed by Insight Partners, CloudBolt has won numerous awards and has repeatedly been recognized as one of the fastest-growing private companies on the Deloitte Fast 500 and the Inc. 5000 lists. For more information, visit www.cloudbolt.io.

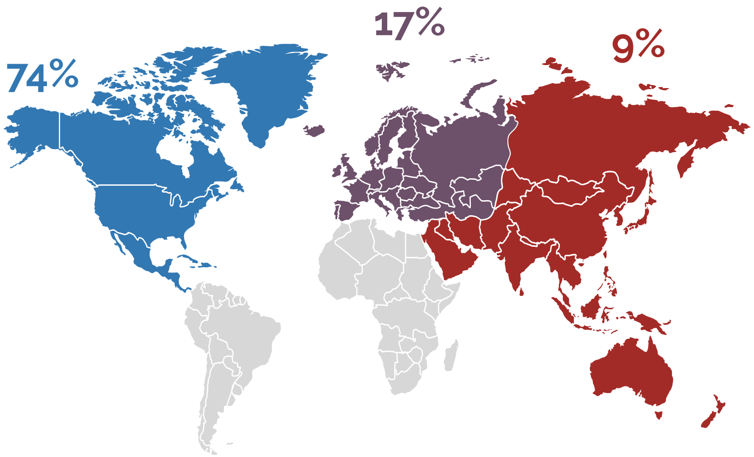
WWW.CLOUDBOLT.IO    INFO@CLOUDBOLT.IO    703.665.1060

JOIN THE CONVERSATION

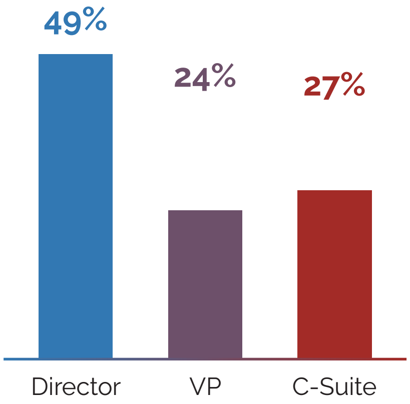
# Appendix:

## Methodology

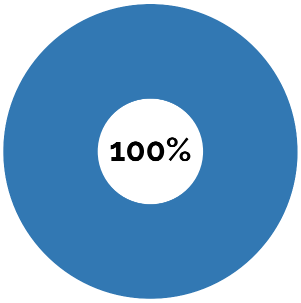
### REGION



### ROLE IN ORGANIZATION



### COMPANY SIZE



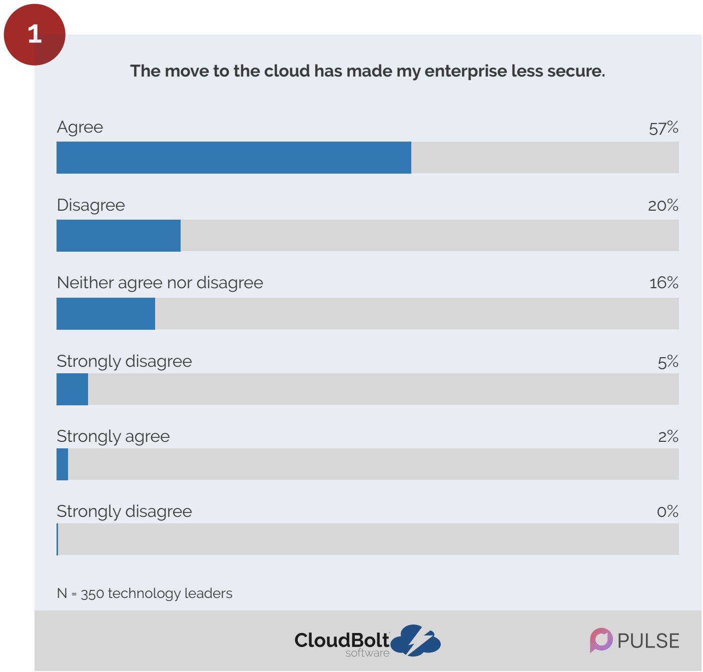
**100% large enterprises**
1,000-5,000 employees = 11%
5,000-10,000 employees = 40%
10,000+ employees = 49%

### RESPONDENT BREAKDOWN

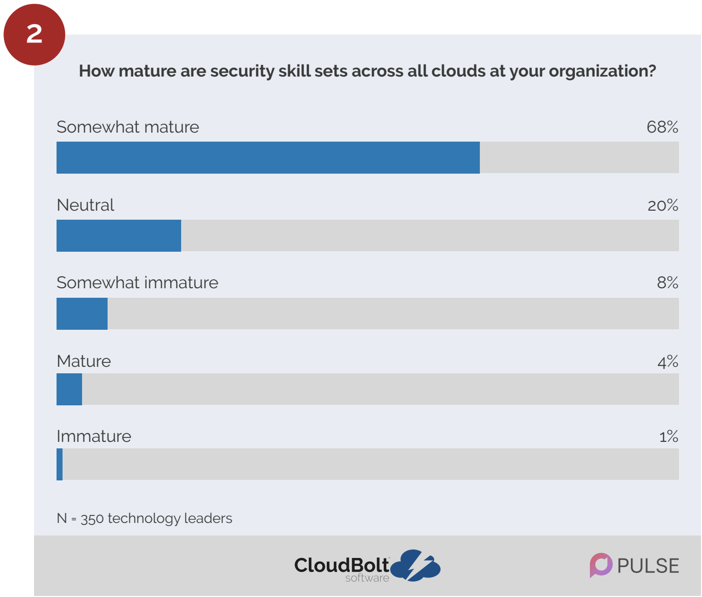
350 Respondents

# Appendix:

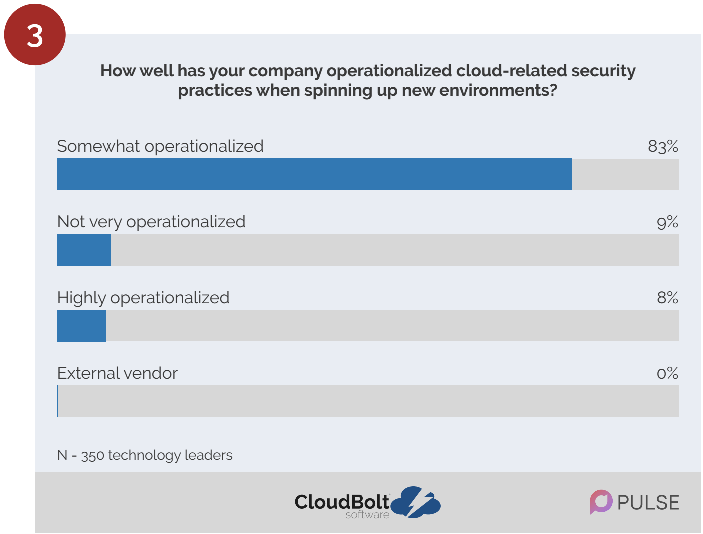
## Survey Data:


1

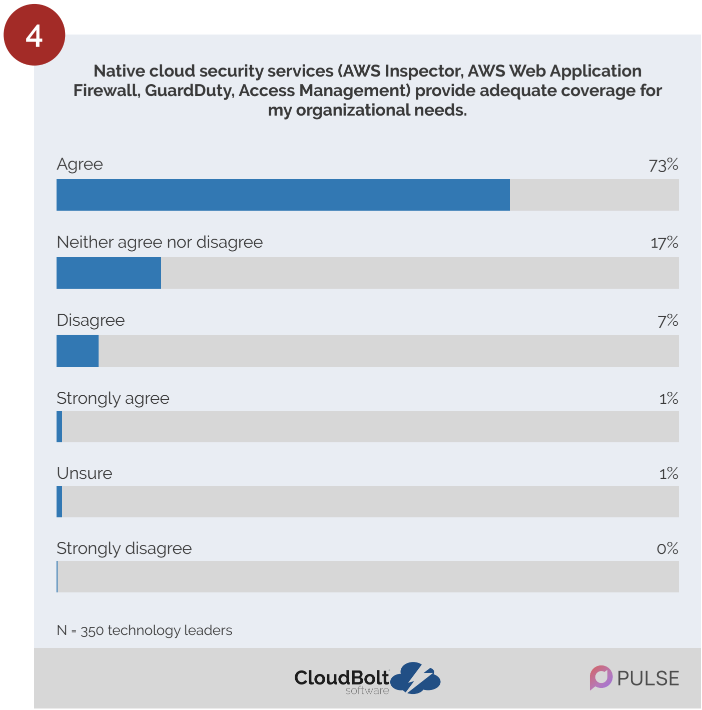
The move to the cloud has made my enterprise less secure.


2

How mature are security skill sets across all clouds at your organization?


3

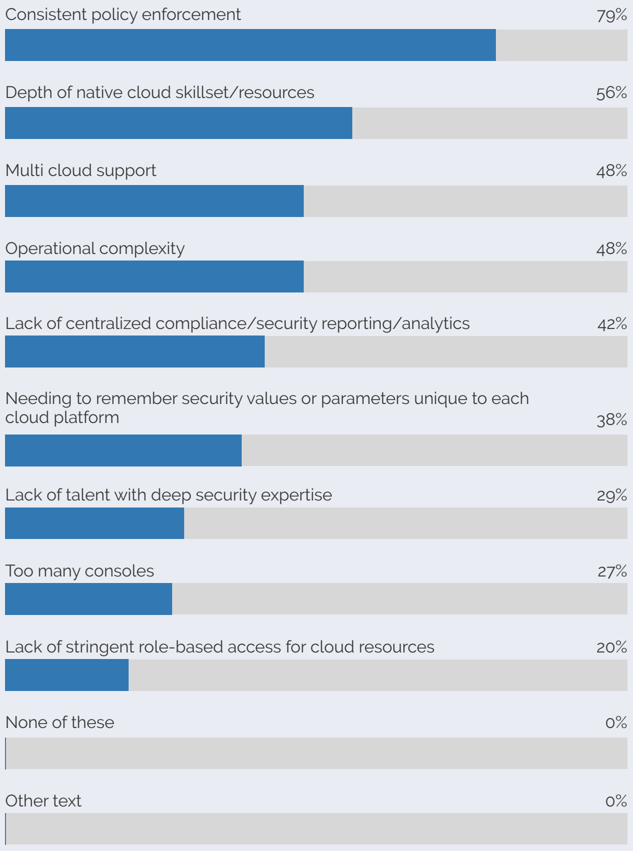
How well has your company operationalized cloud-related security practices when spinning up new environments?


4

Native cloud security services (AWS Inspector, AWS Web Application Firewall, GuardDuty, Access Management) provide adequate coverage for my organizational needs.

5

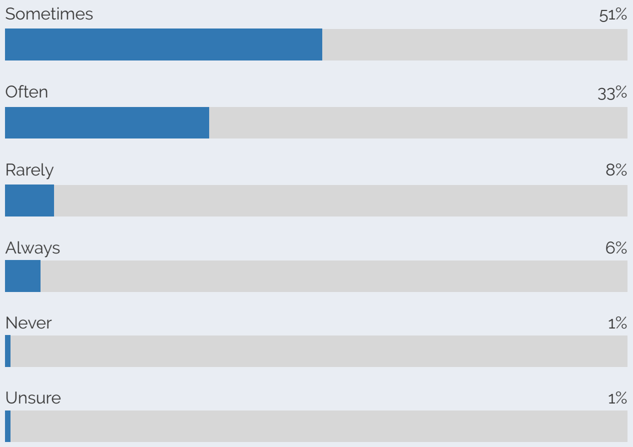
**What are your top native cloud security services concerns? Select all that apply.**



N = 350 technology leaders

7

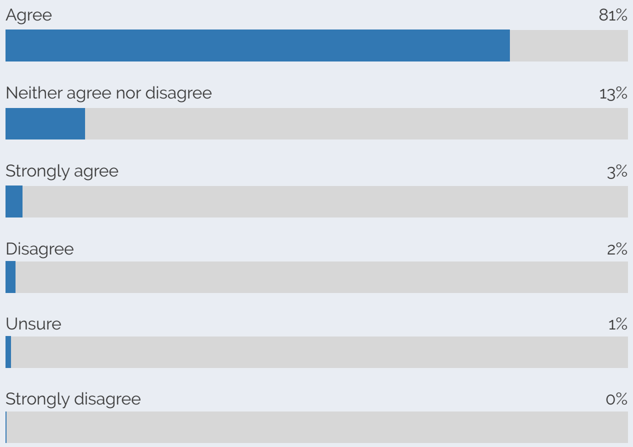
**My company automatically builds security into every workload up front and orchestrates processes across every cloud so that developers don't have to worry about remembering to build in security themselves.**



N = 350 technology leaders

6

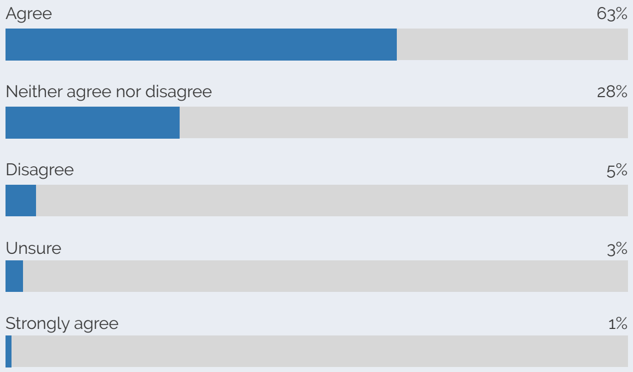
**The best way to deal with cloud security is to layer in a monitoring tool (e.g. Prisma) to identify issues and create alerts as they occur.**



N = 350 technology leaders

8

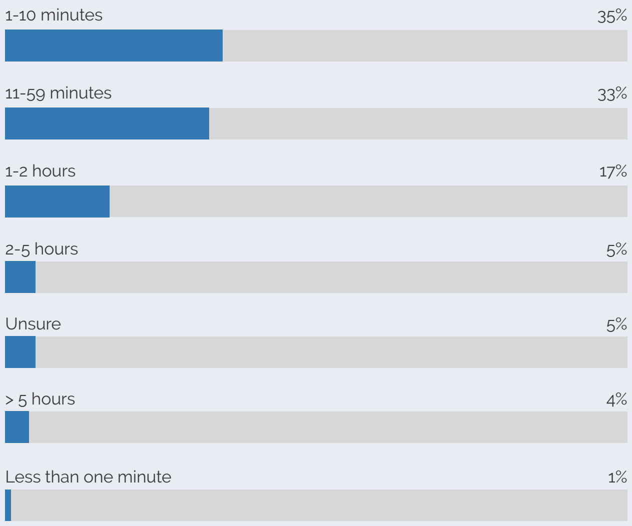
**Using Terraform solves cloud security concerns.**



N = 350 technology leaders

9

**How much time per week do developers spend to ensure the cloud resources they provision are secure?**

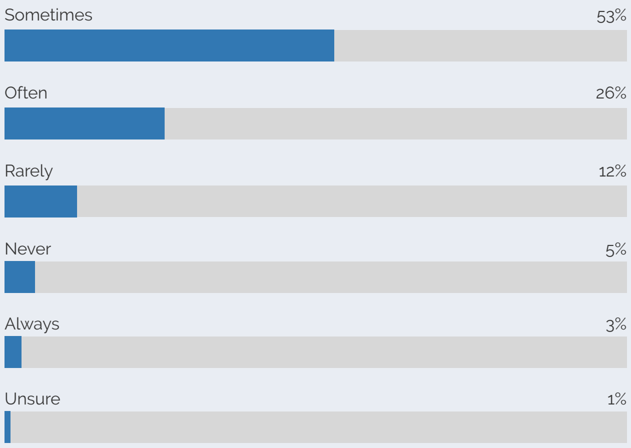


N = 350 technology leaders

CloudBolt software PULSE

10

**How often does your company leverage "immutable infrastructure" as a security measure, whereby cloud resources are automatically destroyed every X number of days?**

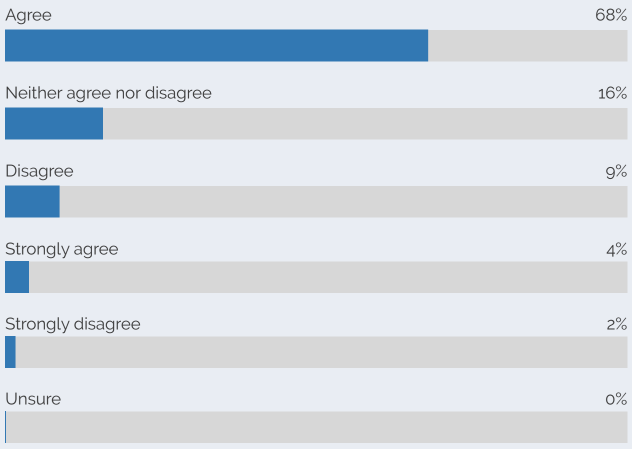


N = 350 technology leaders

CloudBolt software PULSE

11

**My company made the move to cloud and multi cloud without necessarily understanding the skills, maturity curve, and complexities necessary to make multi cloud work securely.**

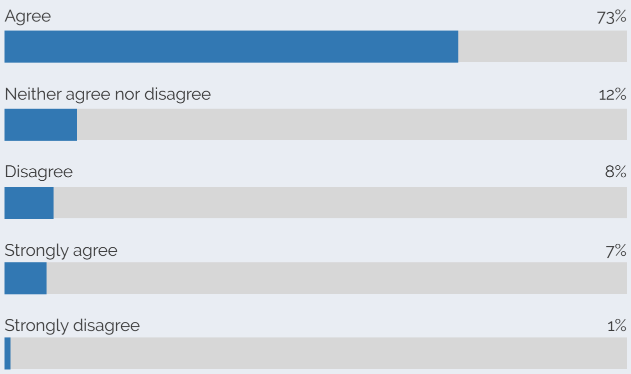


N = 350 technology leaders

CloudBolt software PULSE

12

**The difference between "cloud security" and "cloud compliance" is clearly understood at my company.**

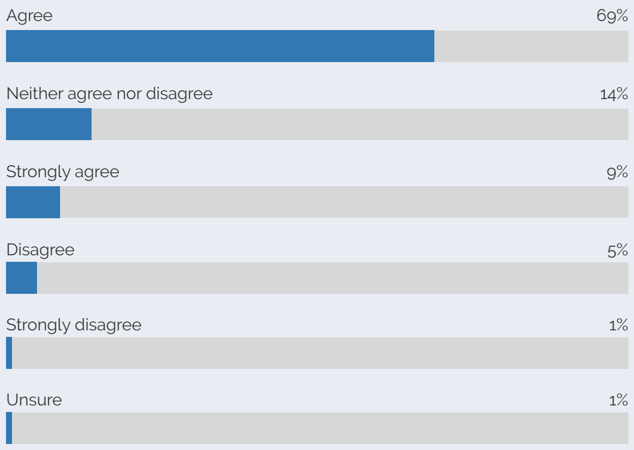


N = 350 technology leaders

CloudBolt software PULSE

13

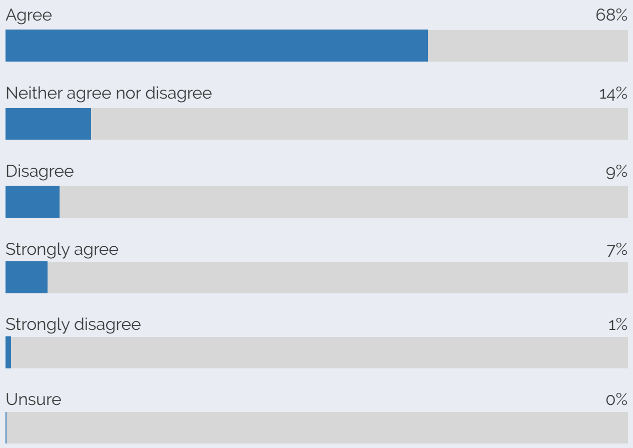
**My company's board and executive team have demonstrated that they are willing to do what is necessary to ensure cloud related computing is secure.**



N = 350 technology leaders

14

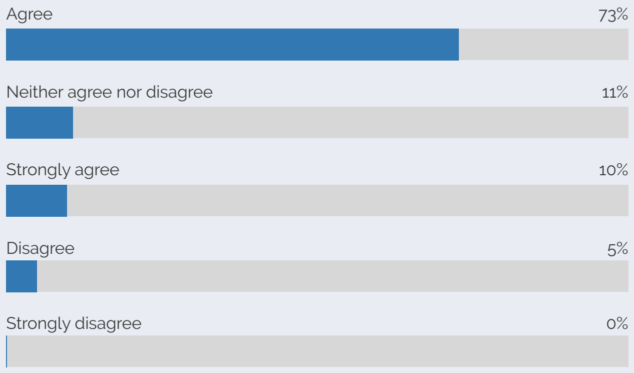
**Cloud computing is the single greatest expansion of the threat surface for enterprises in the last 20 years.**



N = 350 technology leaders

15

**Our company's CISO is highly adept at cloud security.**



N = 350 technology leaders