Gartner
Peer Community™

Cybersecurity Mesh Architecture (CSMA)

Cybersecurity mesh architecture (CSMA) offers a centralized approach to security operations and can help organizations cope with increasingly complex point solutions. What do IT and security leaders think of this emerging strategy so far?

One-Minute Insights:

- The majority of respondents have an understanding of CSMA and foresee it becoming standard
- Over half of leaders are building CSMA at their org and among this group, most are satisfied with it
- Among those not currently building or planning to build CSMA, the majority feel they should be
- Key factors driving adoption include the increasing complexity of both attack methods and security tools
- CSMA being an emergent strategy presents major barriers to adoption such as the absence of tactical best practices and lack of vendors offering complete solutions

One-Minute Insights on timely topics are available to Gartner Peer Community members. Sign up for access to over 100 more, and new insights each week.

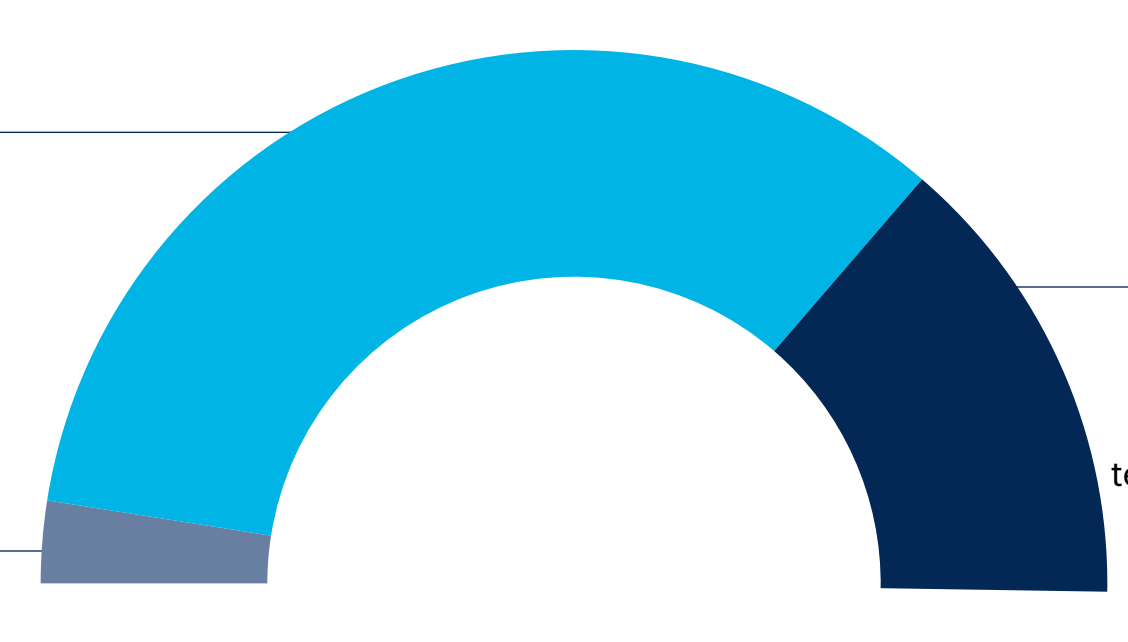
Data collection: Nov 2, 2022 - Jan 16, 2023

Respondents: 200 IT and information security leaders

Most leaders understand CSMA and believe it will likely become standard for security operations

Over two-thirds (68%) of respondents **understand** how CSMA works but only **5%** consider themselves to be **experts** on it.

How informed are you about cybersecurity mesh architecture (CSMA)?



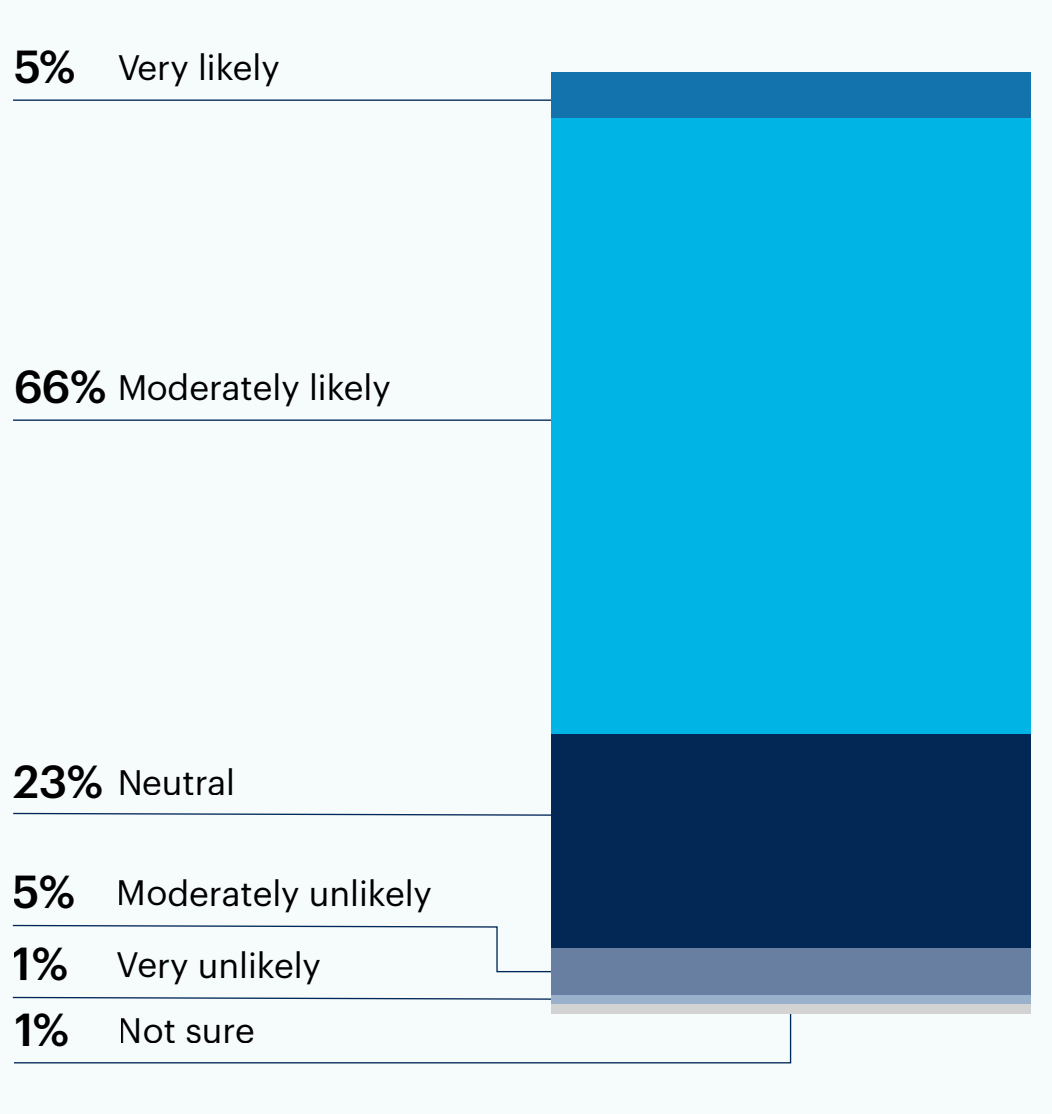
n = 200

71%

consider it **likely** that CSMA will eventually be a **standard component of security operations.**

How likely is it that CSMA will become a standard part of security operations?

n = 200



> "The concept is a perfect evolution in cybersecurity and the adoption speed will depend on how quickly things solidify across the market (definition, standards, etc.)."
>
> - Director, manufacturing industry, <1,000 employees

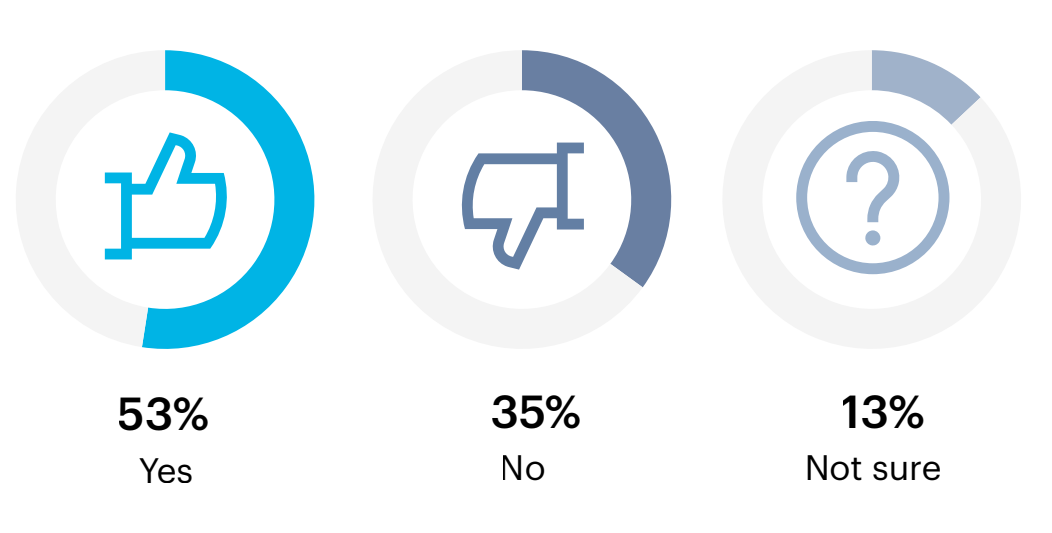
> "Cybersecurity mesh architecture (CSMA) is going to be the common buzzword in the cybersecurity industry if it isn't already. As risks to the public and private sectors increase, more organizations will be compelled to investigate deeper and/or implement CSMA."
>
> - Director, educational services industry, 5,000 - 10,000 employees

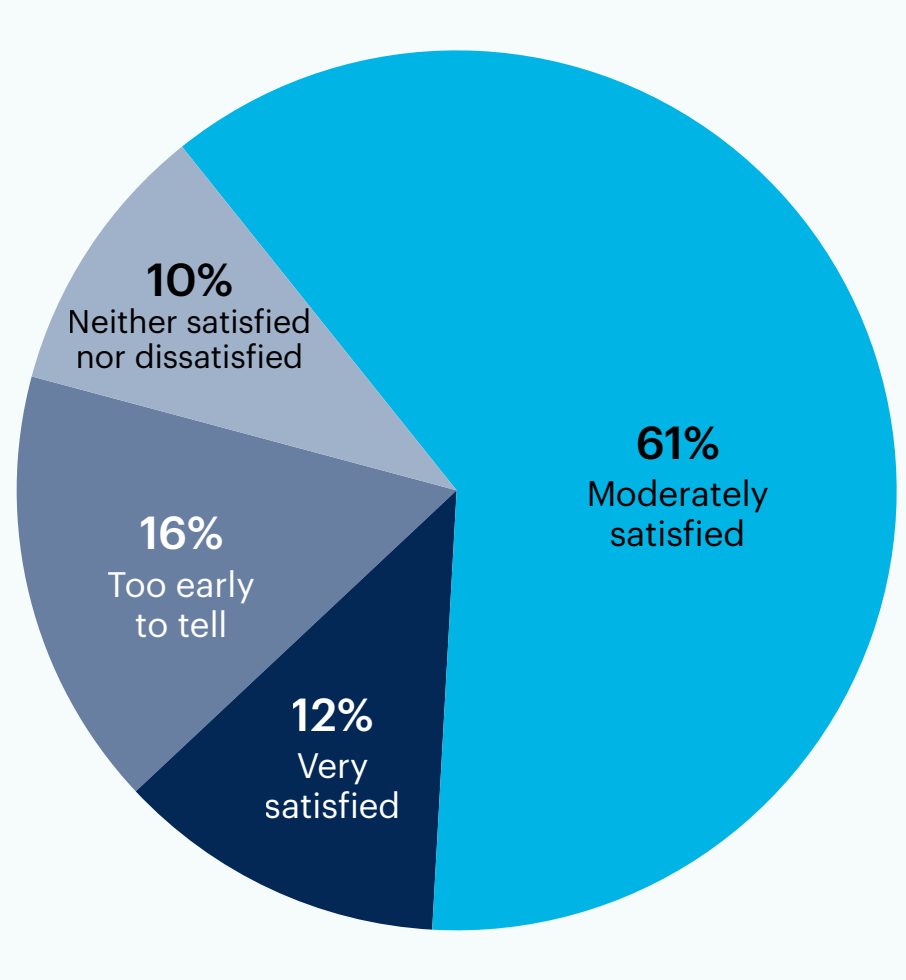
The majority are satisfied with the CSMA their orgs are building

Over half (53%) of leaders are **building** CSMA at their organization.

Is your organization currently building CSMA?

n = 200





And **almost three-quarters (73%)** of those building CSMA feel **satisfied** with their organization's progress.

Are you satisfied with your organization's CSMA?

Moderately dissatisfied **0%**, Very dissatisfied **0%**

n = 105

> "The initiatives from business regarding digital transformation of business operations have direct impact on cybersecurity needs which often can't keep up or are seen as impediments to progress. The [cybersecurity] industry has a major problem in making a business case and methodology for how to implement CSMA comprehensively and in a way that makes sense to business leaders."
>
> - Director, healthcare industry, 1,000 - 5,000 employees

> "We have several vendors working together on [CSMA]."
>
> - C-suite, construction industry, 5,000 - 10,000 employees

> "We are looking for trusted vendors."
>
> - Director, government, 10,000+ employees

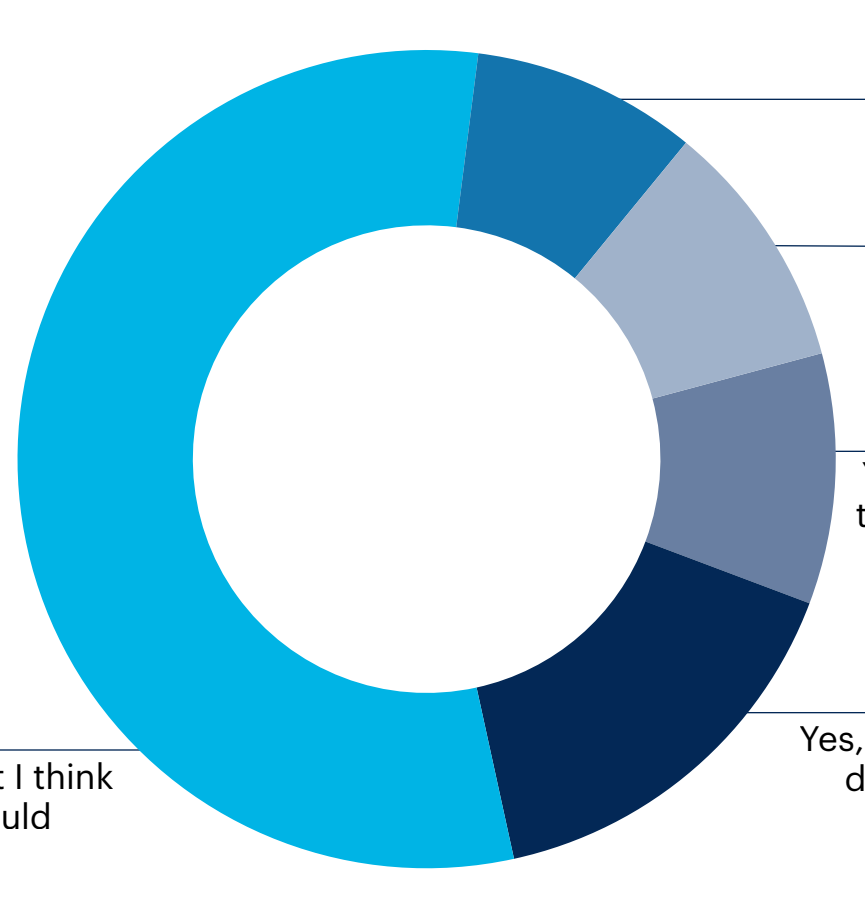
Organizations adopt CSMA to cope with the increasing complexity of threats, attack methods and security tools

26%

of those who are **not yet** building CSMA **plan to adopt it**. Over half of leaders (56%) say they **don't have such plans** in place but believe they should.

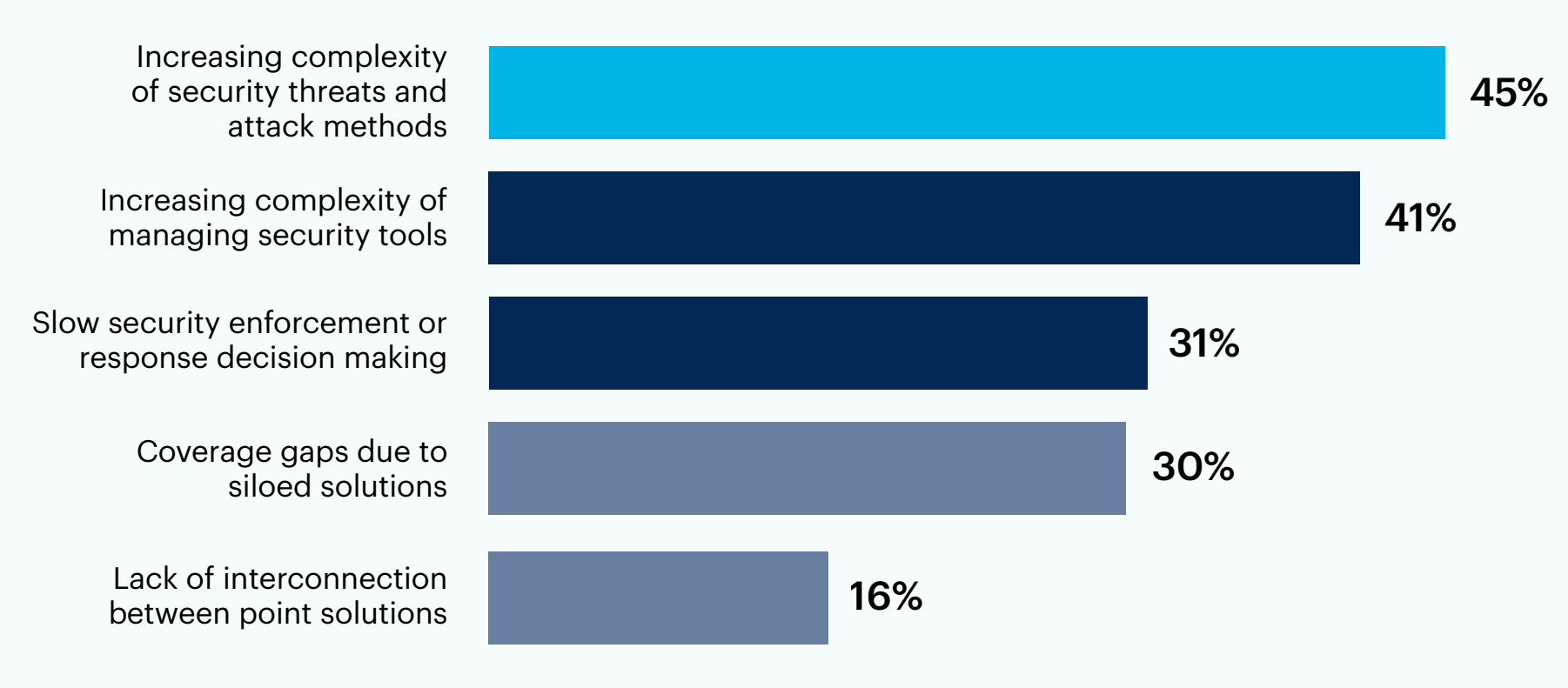
Is your organization planning to adopt CSMA?

n = 70



The **most reported factor** driving CSMA adoption is the **increasing complexity of security threats and attack methods (45%)**, followed by the growing difficulty of managing security tools (41%).

What were the reasons your team decided to adopt or is planning to adopt CSMA?

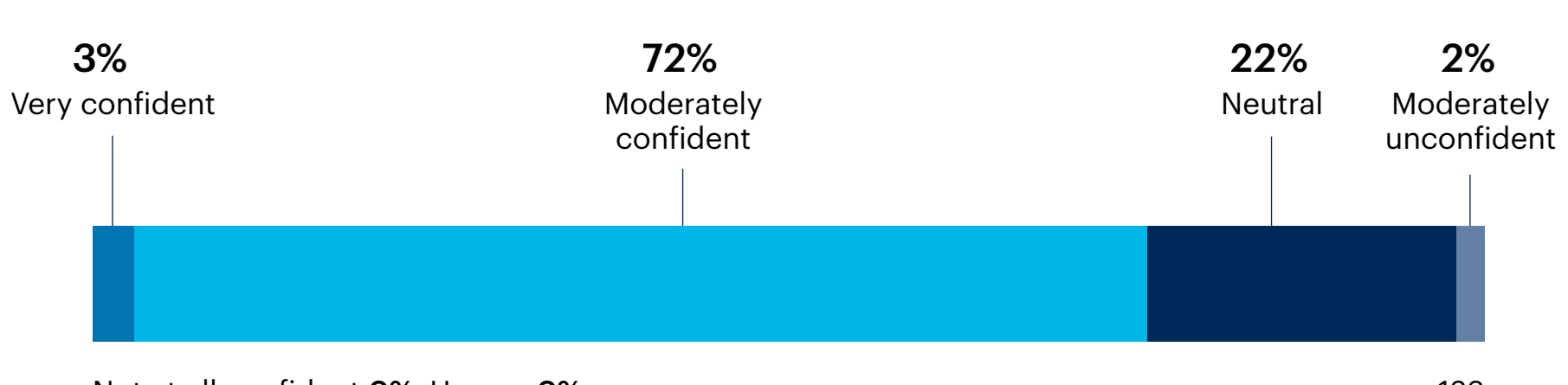


Lack of centralized policy management **10%**, Inconsistent visibility **9%**, Lack of centralized threat databases **8%**, Uncoordinated detection methodology, threat correlation and response **7%**, Inability to apply protections based on asset value **5%**, Difficulty stopping spyware **4%**, None of these **0%**, Other **0%**

n = 123

Three-quarters (75%) feel **confident** that their team is capable of building CSMA.

How confident are you in your team's ability to build CSMA?



Not at all confident **0%**, Unsure **0%**

n = 123

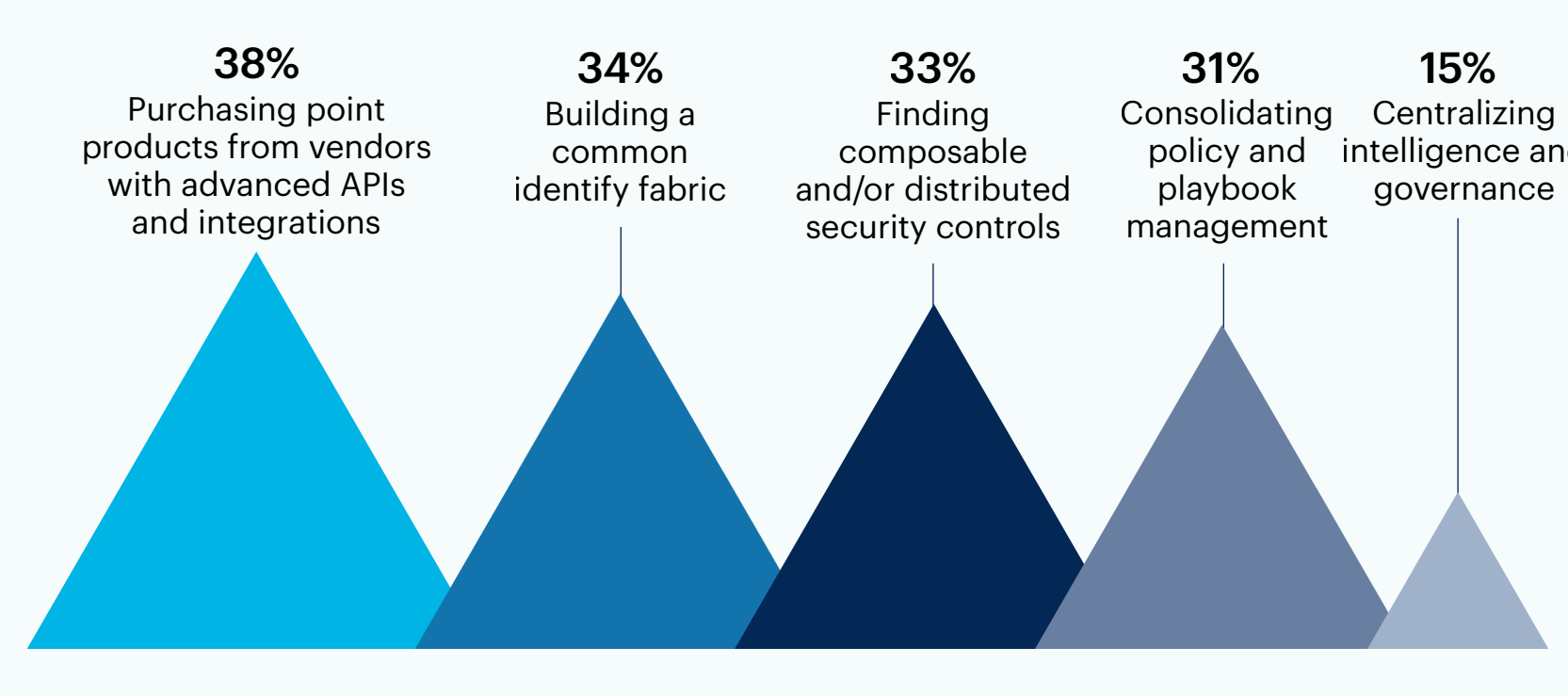
> "Threats may be identified in real-time with the use of CSMA, and assets like data and devices can be better safeguarded than with standard VPN passwords."
>
> - C-suite, software industry, <1,000 employees

> "We first need to increase our current skills in order to keep implementing CSMA in the company."
>
> - Director, government, 1,000 - 5,000 employees

Advanced APIs and integrations present a major challenge to building CSMA

38% report that one of the most **difficult** aspects of building CSMA is **purchasing point solutions** with advanced APIs and integrations. About a third also find that building a common identity fabric (34%) and sourcing composable/distributed security tools (33%) are major challenges.

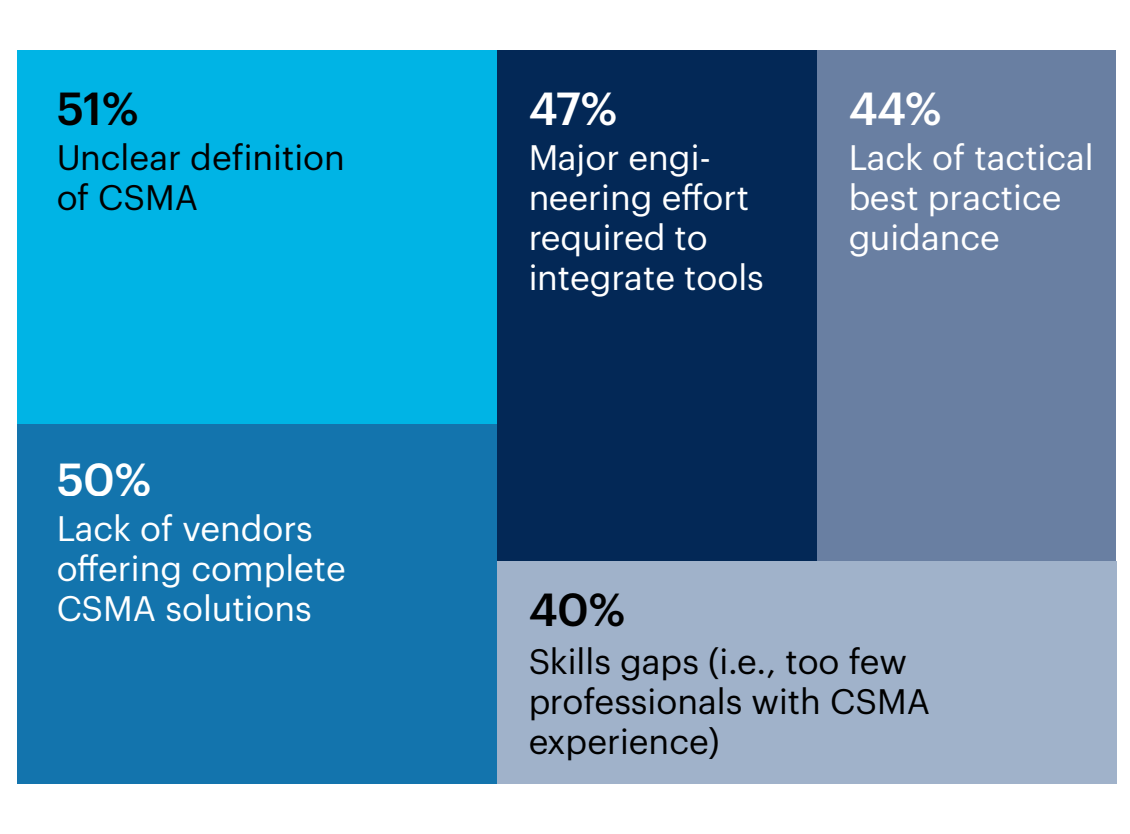
Which aspects of building CSMA have been most challenging?



Consolidating dashboards **11%**, Increasing enforcement capabilities **10%**, Increasing analytics capabilities **8%**, None of these **0%**, Other **0%**

n = 123

Half of leaders say **the unclear definition of CSMA (51%)** as well as a **lack of vendors offering complete solutions (50%)** both represent **key hurdles** to adoption. The engineering efforts needed to integrate tools (47%) and the absence of tactical best practices (44%) are also common barriers.



What are the main barriers to CSMA?

Investment risk (i.e., introduction of industry standards may drive up cost of org's proprietary CSMA approach) **36%**, Costs **18%**, Lack of executive interest **8%**, None of these **0%**, Other **0%**

n = 200

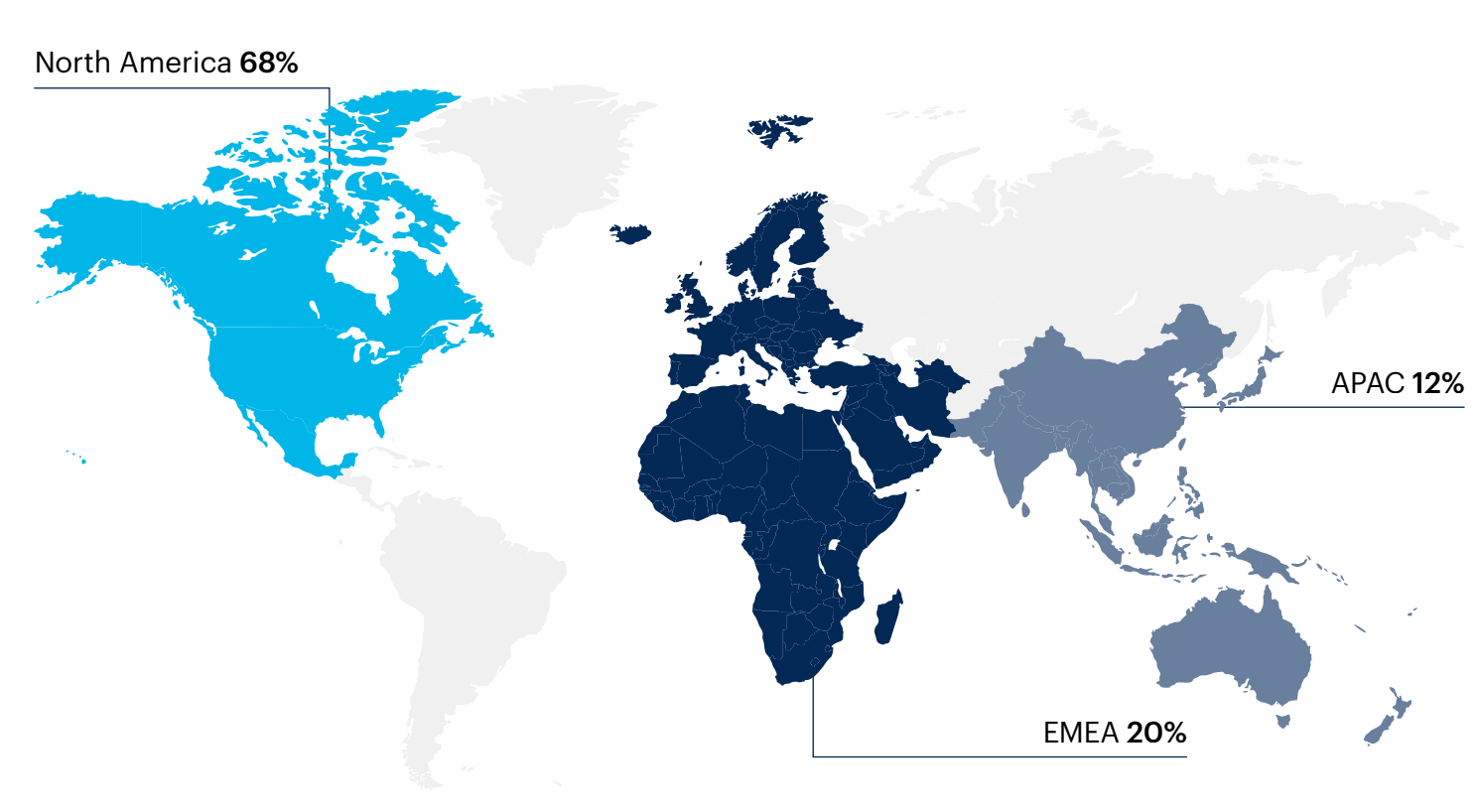
> "We need to find proper experts."
>
> - C-suite, utilities industry, 10,000+ employees

> "We don't have enough talent and knowledge around CSMA, so we are thinking about hiring external consultants."
>
> - Director, government, 5,000 - 10,000 employees

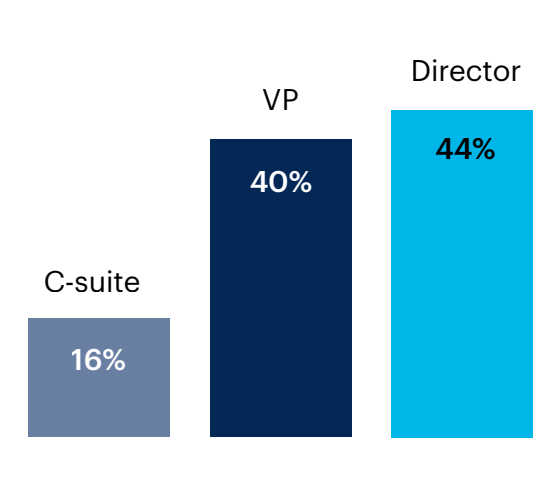
> "It's a beast but necessary for a growing company and an increased threat landscape."
>
> - VP, retail industry, 1,000 - 5,000 employees

Respondent Breakdown

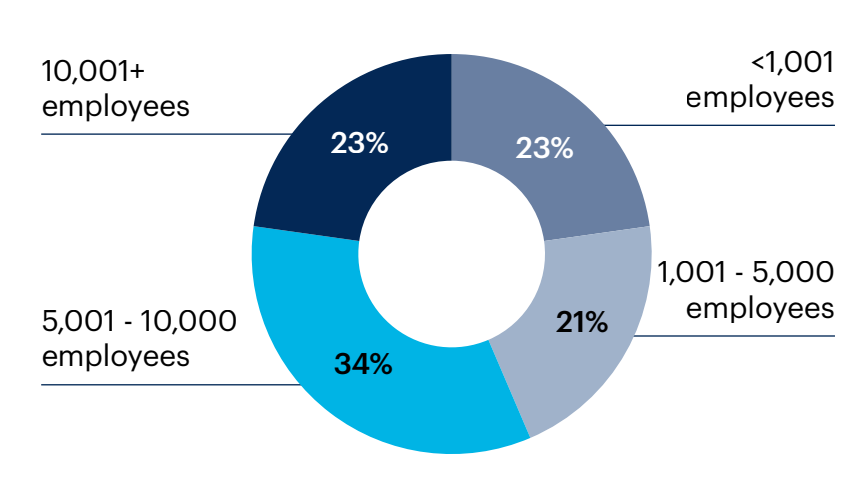
Region



Job Level



Company Size



Gartner

Source: Gartner Peer Community, Cybersecurity Mesh Architecture survey