ermetic

Osterman Research

WHITE PAPER

State of Cloud Security Maturity 2022

Survey Findings

White Paper by Osterman Research
Published **August 2022**
Commissioned by **Ermetic**

Contents

SECTION 1

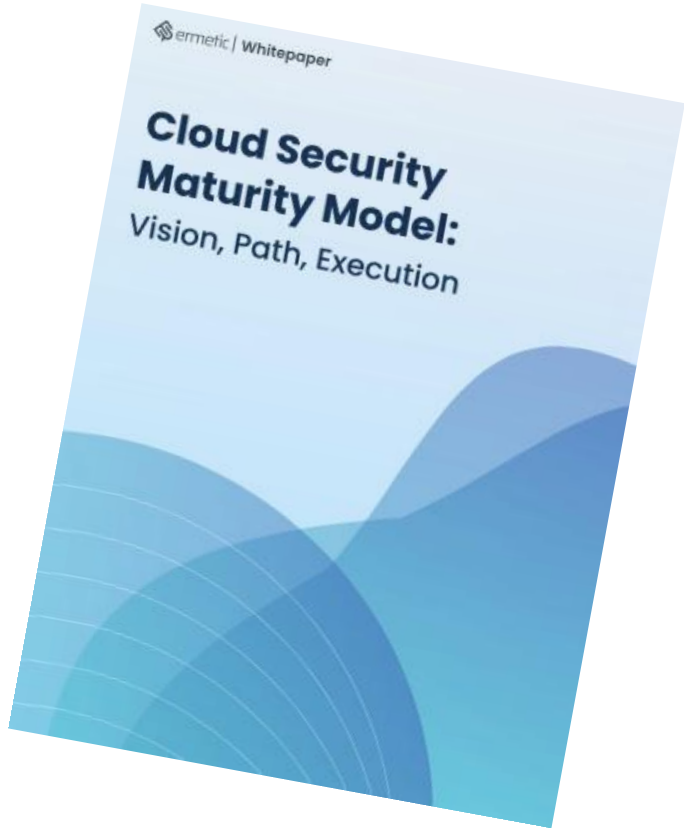
Research goal and method

Research goal

Ermetic recently published its Cloud Security Maturity Model, which provides organizations with a viable map for assessing status and progress in securing their cloud infrastructure. The model offers a lightweight framework for determining an organization's maturity level across multiple domains of cloud security.

Ermetic then commissioned Osterman Research to build a baseline of maturity against the model. Osterman Research surveyed 326 organizations in North America with 500 or more employees and that spend a minimum of $1 million each year on cloud infrastructure.

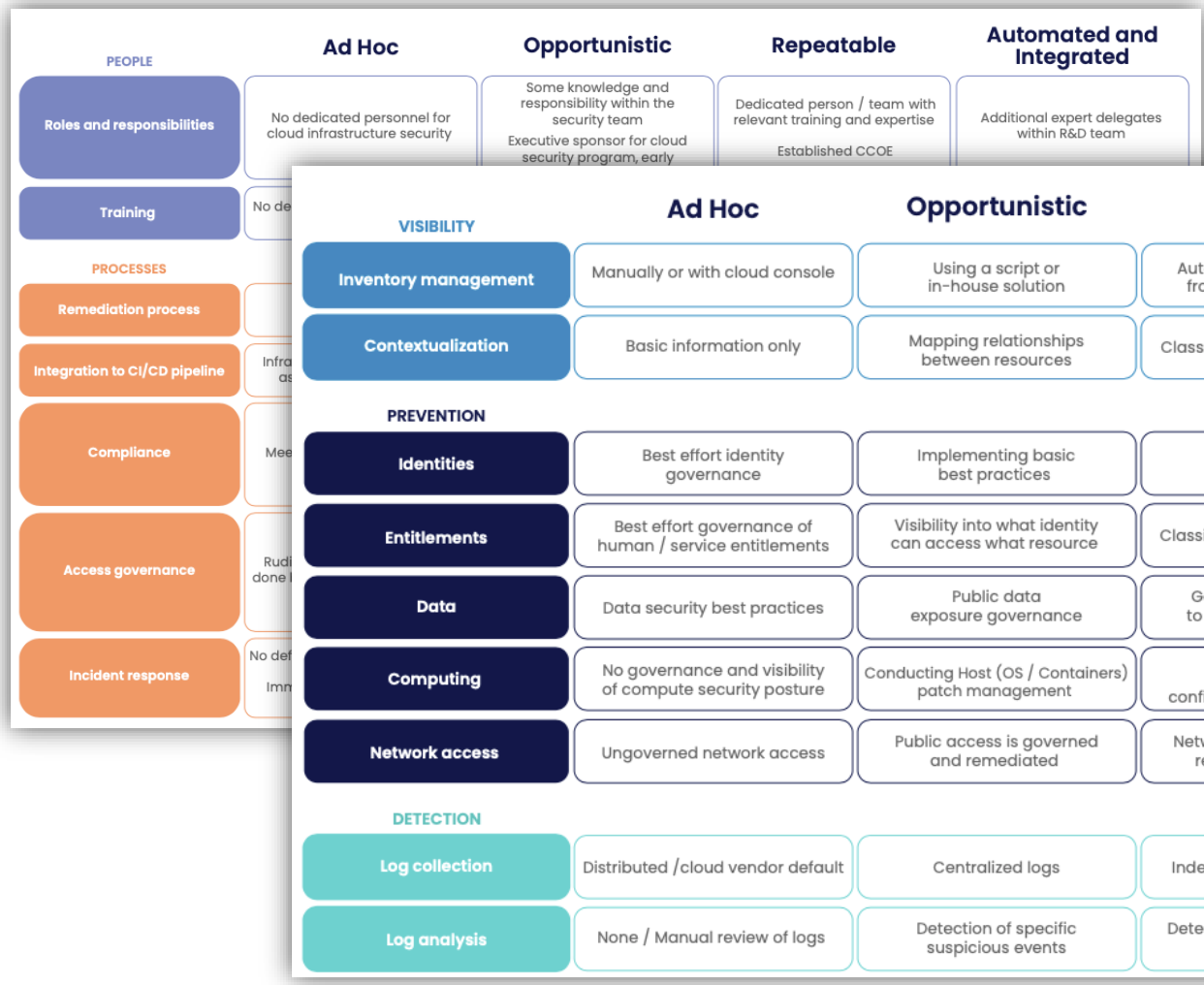
This report summarizes the survey's key findings—and the implications for cloud security stakeholders.



Ermetic Cloud Security Maturity Model

The Ermetic Cloud Security Maturity Model groups 16 separate domains of cloud security into organizational and technology issues. The organizational grouping has two areas—people and processes; together, these areas cover seven domains. The technology grouping has three areas — visibility, prevention, and detection; together, these areas cover nine domains.

For each domain, an organization is assessed as meeting the standards for one of four maturity levels: ad hoc, opportunistic, repeatable, and automated and integrated. Once all the domains are assessed, an organization is assigned to one overall maturity level in the model.



Research method—by Osterman Research

1

Develop questions to test maturity in each domain
Osterman Research developed a set of questions, based on the framework presented in the Ermetic Cloud Security Maturity Model, to assess each domain of cloud security in the model. The questions were finalized in collaboration with Ermetic. The question set is also used in Ermetic's online self-assessment tool.

2

Collect the maturity data
Osterman Research surveyed 326 organizations in North America that met the qualifying criteria of 500 or more employees and $1 million or more annual spend on cloud infrastructure. The survey respondent also had to work in an appropriate security role as a decision-maker, architect, engineer, or head of cloud security or cloud operations.

3

Analyze and group by maturity
Osterman Research analyzed the survey data against the standards required in each domain of cloud security to claim one of the four levels in the maturity model.

A cross-domain aggregation was used to assign each organization to a single overall maturity level.

The benefits of a maturity model

In recent years, Ermetic has published an annual *State of Cloud Security* report that looks at attacks against IaaS platforms and offers general insights into how organizations should respond.

Today, most organizations recognize the importance of cloud security but have trouble understanding where their efforts position them.

With this in mind, for 2022, Ermetic focused its attention on offering more prescriptive guidance on the steps a specific organization needs to take to improve its cloud security. This actionable approach is the key driver behind the Ermetic maturity model and the assessment of current organizational maturity in this research.

Read Ermetic's blog post on the State of Cloud Security in 2021

SECTION 2

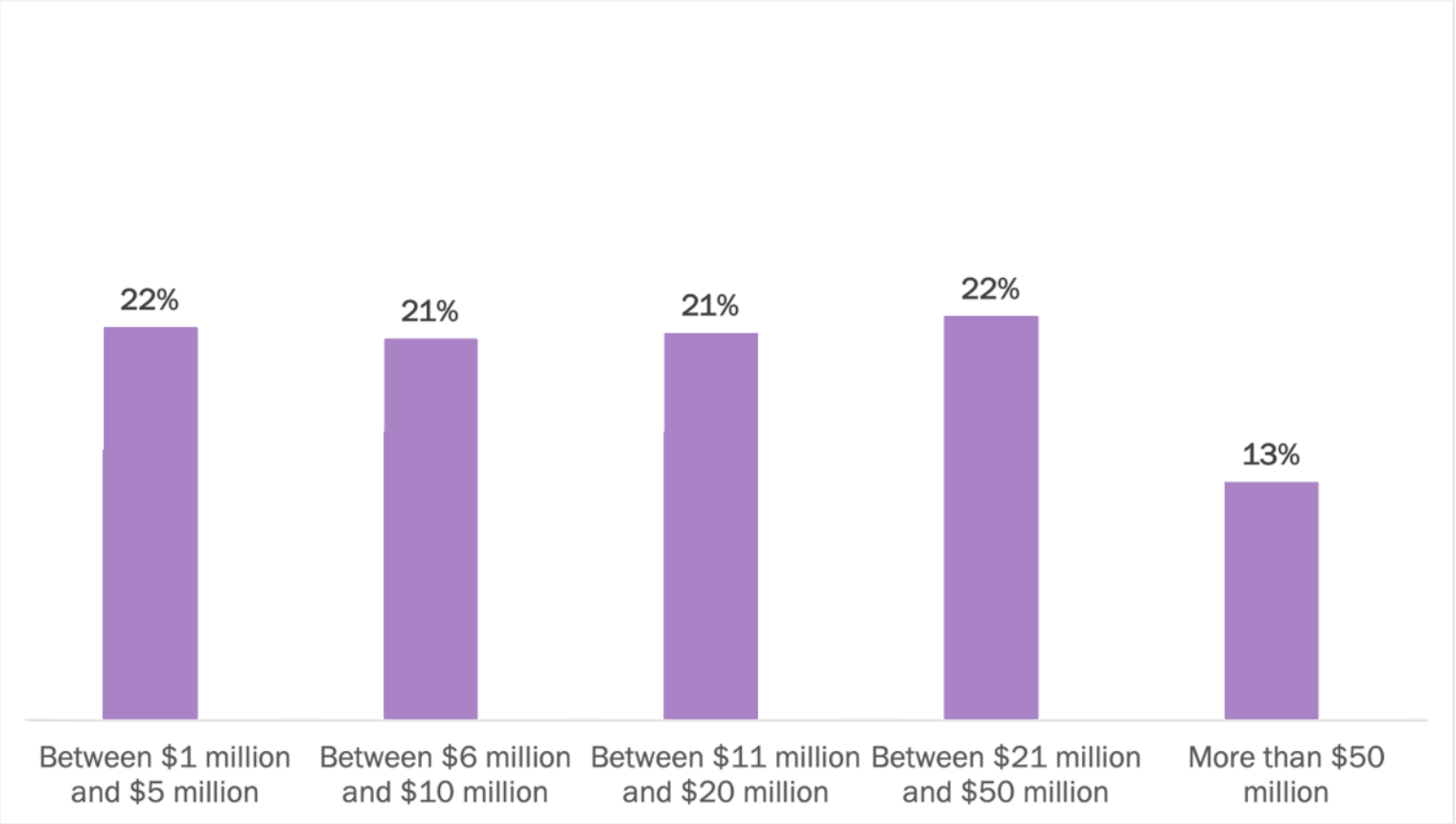
General insights

Organizations continue to invest in cloud infrastructure

Cloud infrastructure is a key part of how organizations serve customers, drive transformation and engage the world. Organizations are putting significant financial resources into supporting their ability to do business in the cloud.

56%

of organizations are spending at least $10M each year on cloud infrastructure.

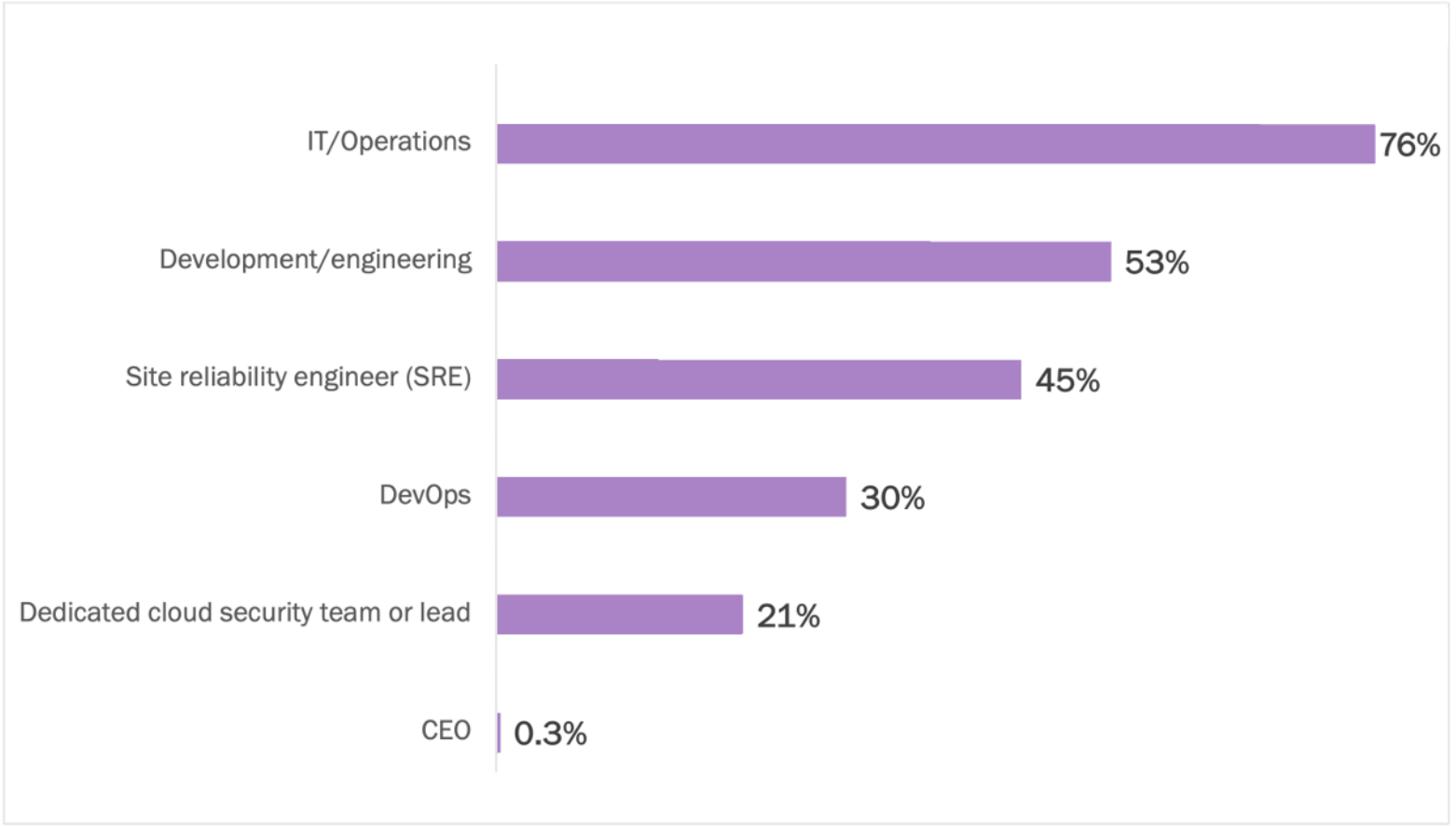


Percentage of respondents

80%

of organizations do not have a dedicated cloud security team/lead.

Who is at the helm of the security ship? As per the maturity model, distributed security is an indicator of higher maturity levels. However, the model also makes clear that security efforts require supervision by a specialized team. While heartening to see that organizations are increasingly spreading the work of security among other roles, the lack of a dedicated security team will likely prevent them from reaching higher maturity.



Percentage of respondents

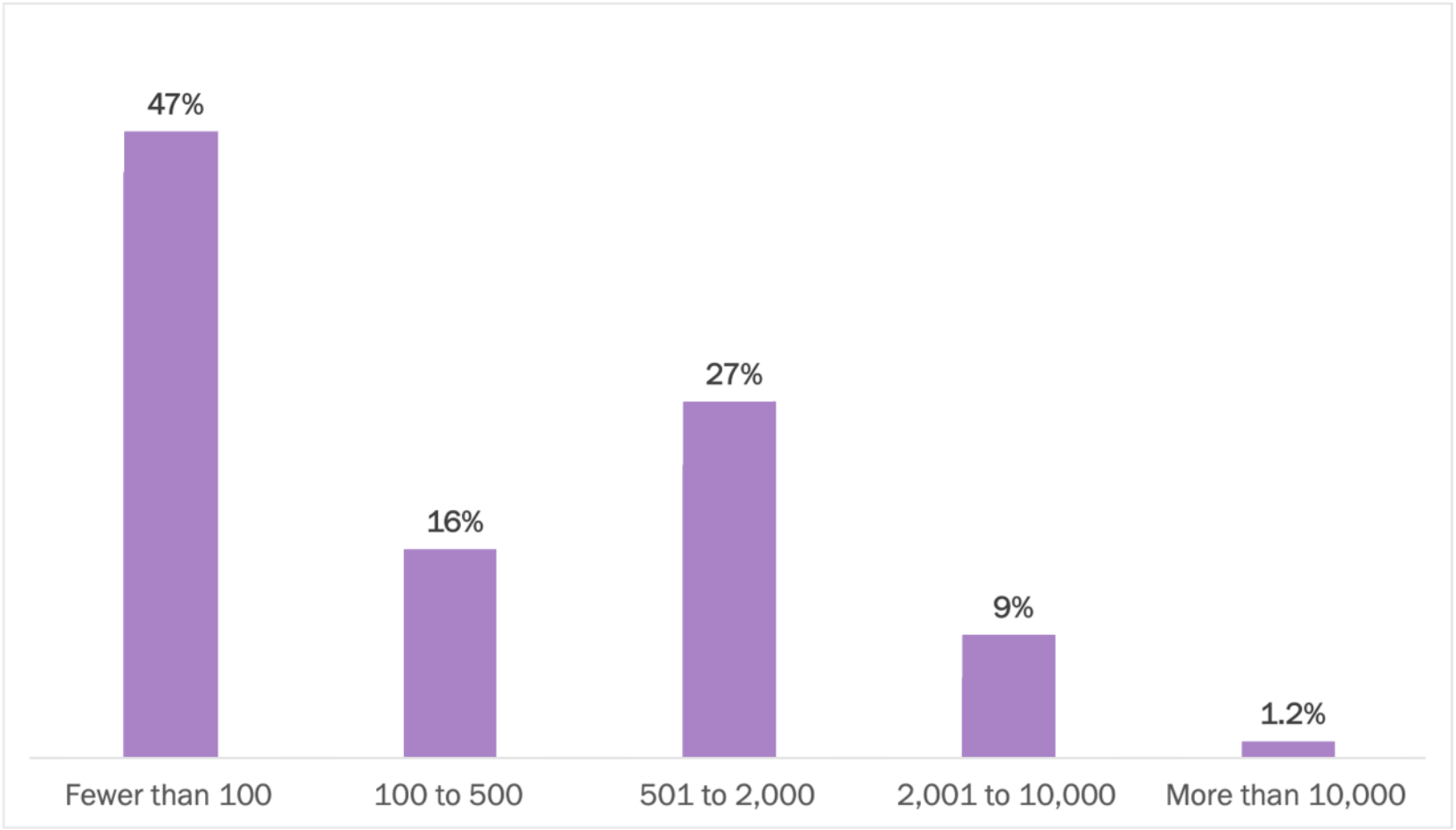
Almost

40%

of organizations have more than 500 developers or DevOps engineers.

Development teams are getting larger, increasing cloud security risks

Many organizations have substantial development and DevOps teams, resulting in many more privileged users which, in turn, elevates cloud security risks.



Percentage of respondents

SECTION 3

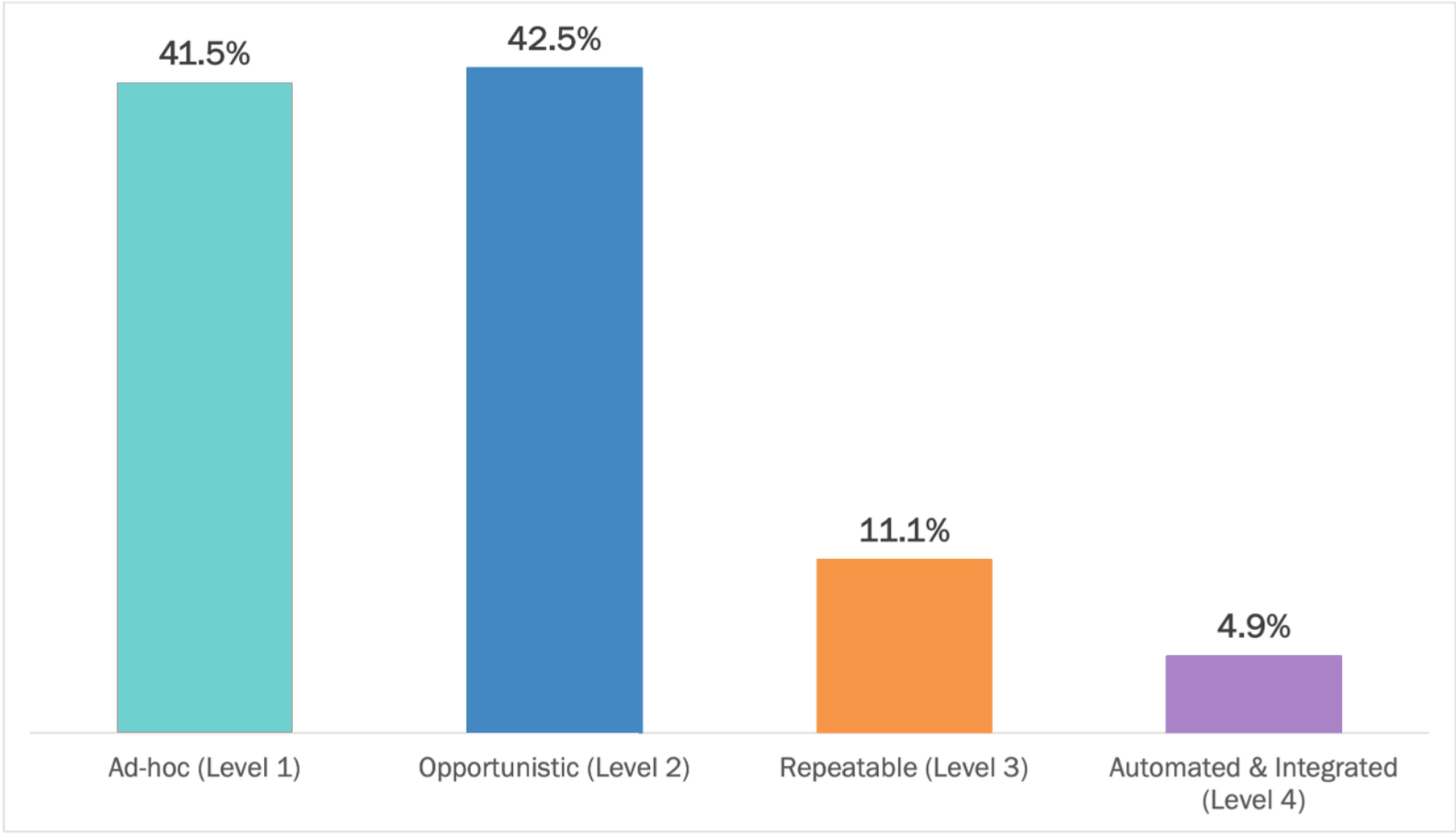
Key survey findings

Overall cloud security maturity level

More than four out of five organizations are situated at the Ad-hoc or Opportunistic level on the Ermetic Cloud Security Maturity Model. Only 5% currently meet the standards of the highest level - Automated & Integrated.

84%

of organizations are at low levels of maturity—and less than 5% have achieved the highest maturity level.



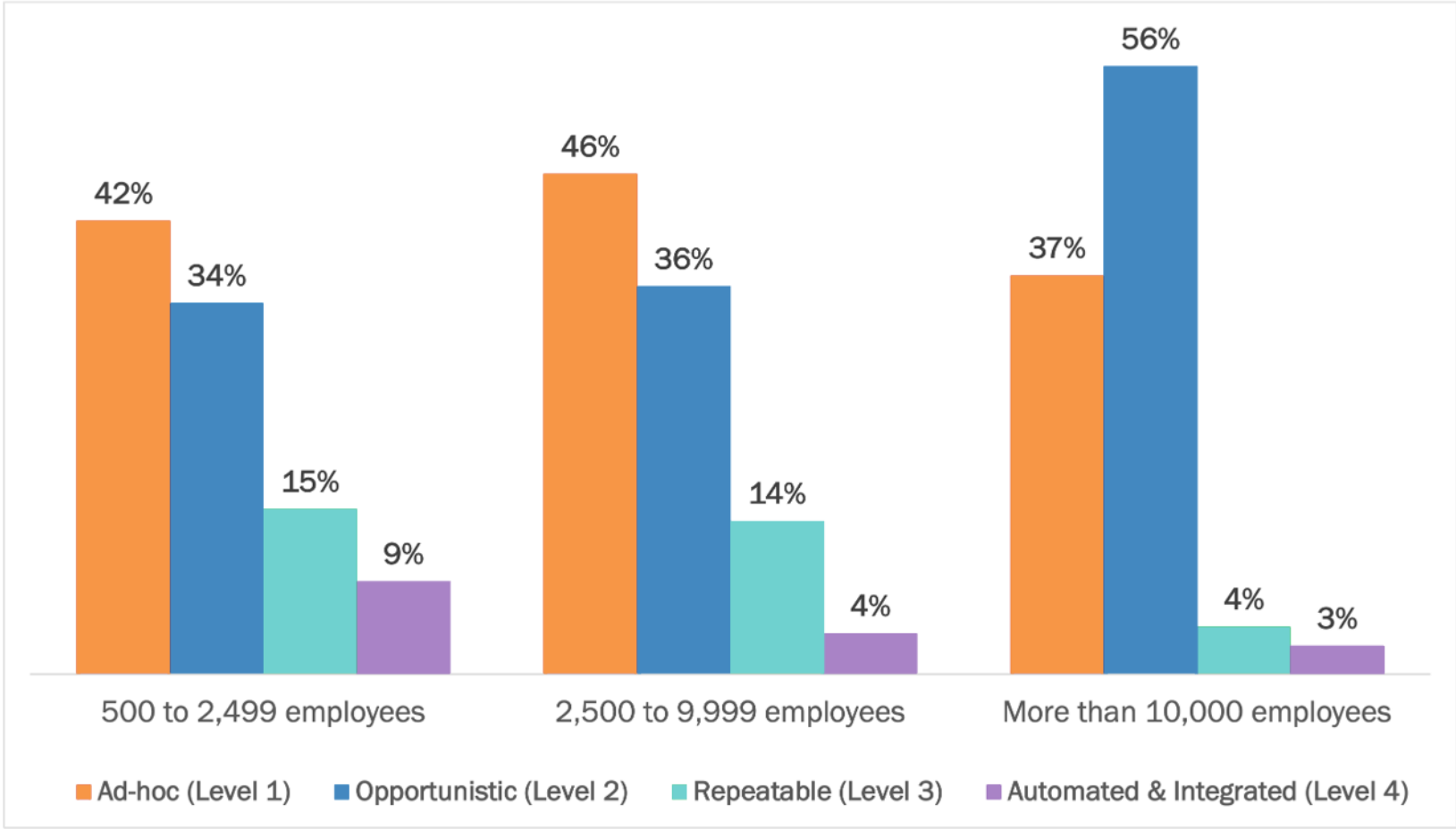
Percentage of respondents

Cloud security maturity by organization size

Smaller organizations are 3x more likely to reach the highest maturity level (Automated & Integrated stage) than very large organizations.

93%

of large organizations are only at the low levels of cloud security maturity.



Percentage of respondents

Tech

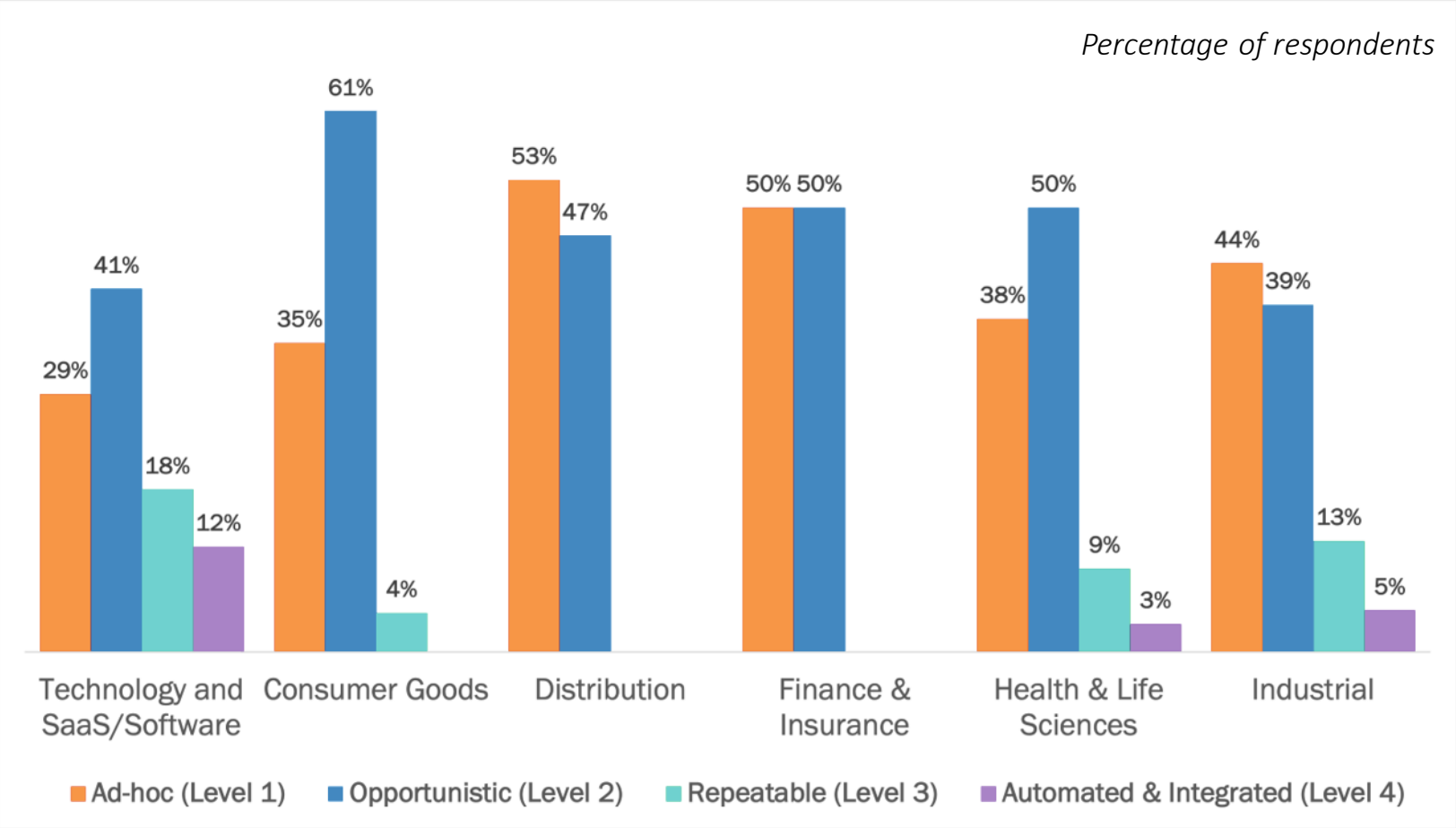
and SaaS/Software are the most mature industry sector.

Finance

is, surprisingly, lagging behind other industries.

Cloud security maturity by industry grouping

We correlated maturity with six industry groupings. Not surprisingly, the Technology and software grouping has the highest maturity. Quite surprisingly, Finance & Insurance—an industry most targeted by cyber attacks—are by and large at the low levels of maturity.



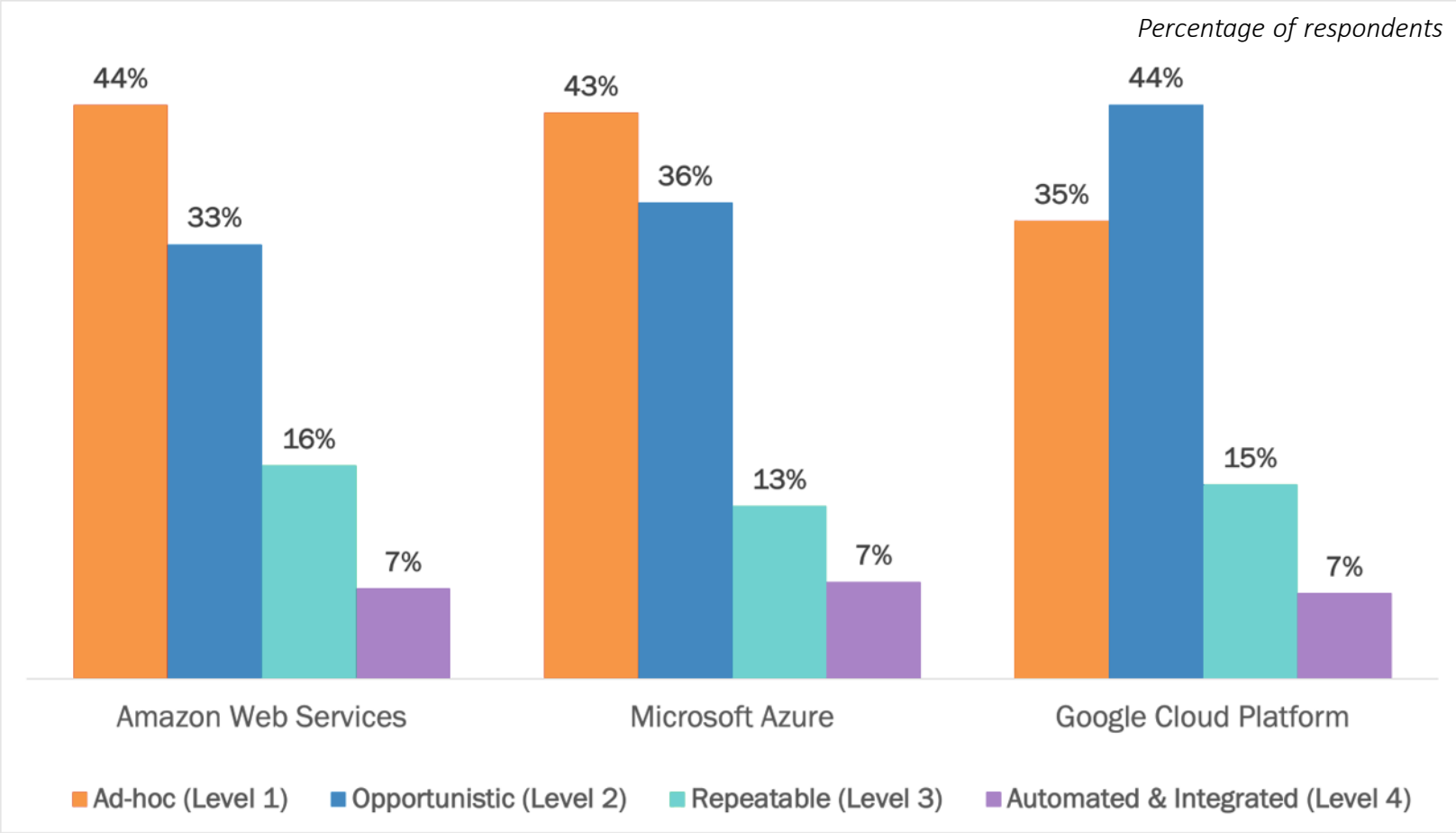
Industry compositions of the six groupings above: Technology and SaaS/Software (technology n=71, SaaS/Software n=22), Consumer Goods (consumer products n=13, food/beverage n=10), Distribution (retail/distribution n=23, logistics/transportation n=9), Finance and Insurance (financial services/banking n=20, insurance n=8), Health & Life Sciences (healthcare n=21, life sciences n=11), Industrial (manufacturing n=26, construction/architecture/engineering n=22, chemicals n=5, aerospace/defense n=2).

Overall maturity levels by cloud provider are quite similar

Many of the organizations use two or more providers; when compared per platform, maturity level is strikingly similar regardless of level. Organizations using Google Cloud (alone or among other platforms) stand out as having more security practices at the Opportunistic level and fewer at the Ad-hoc level than for AWS or Azure.

40%

of organizations on average have not moved beyond the lowest level of cloud security maturity regardless of cloud provider.

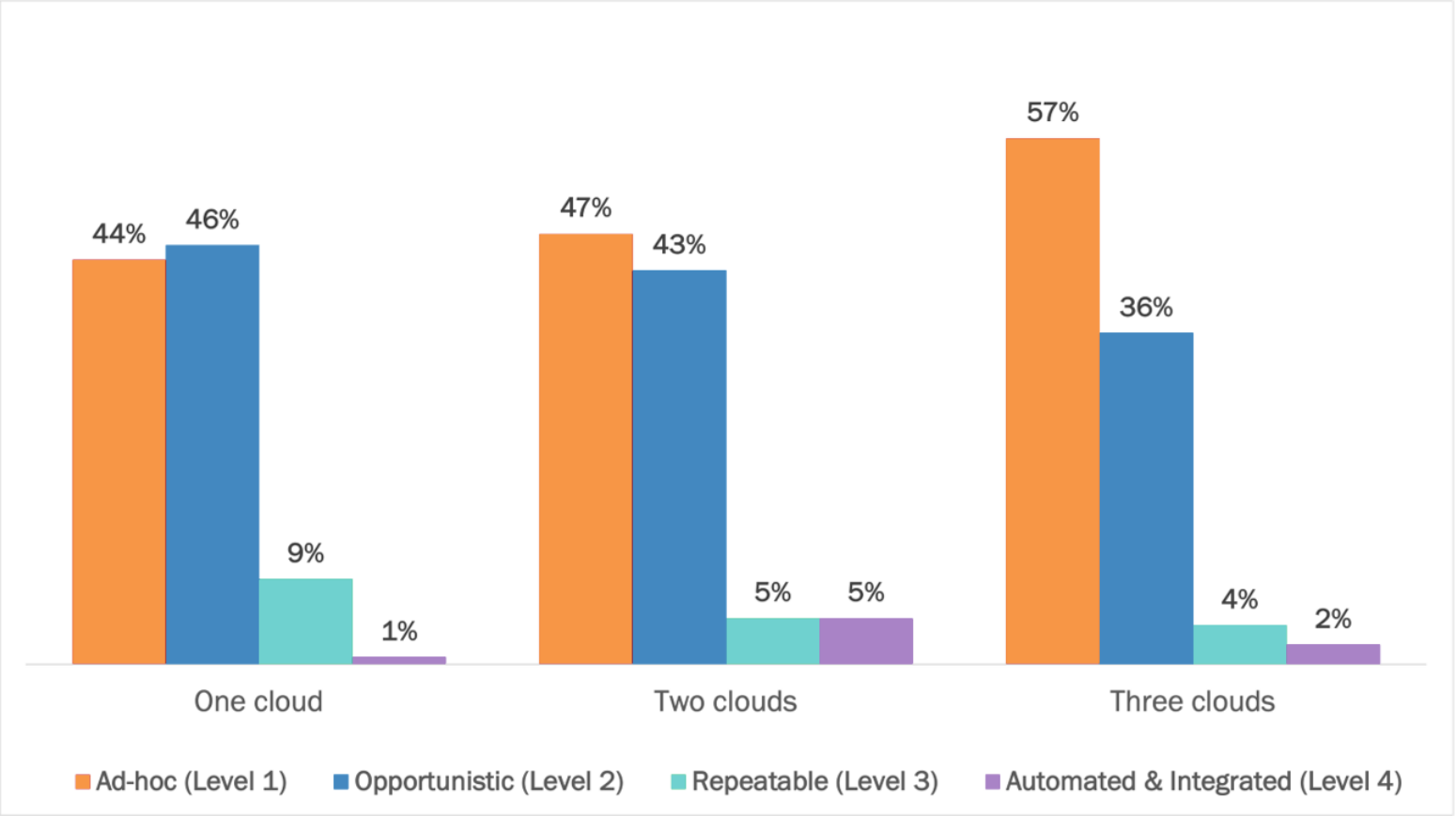


57%

of organizations adopting multicloud strategy are operating at the lowest level of cloud security maturity.

More clouds, less maturity

With each additional cloud, maturity of cloud security practices seems to get increasingly stuck at the Ad-hoc level. Whatever the reason—multicloud complexity, a shortage in specific cloud knowledge, a lack of cross-cloud common practices or other—this finding suggests the challenge of scaling security as the cloud environment grows more diverse.



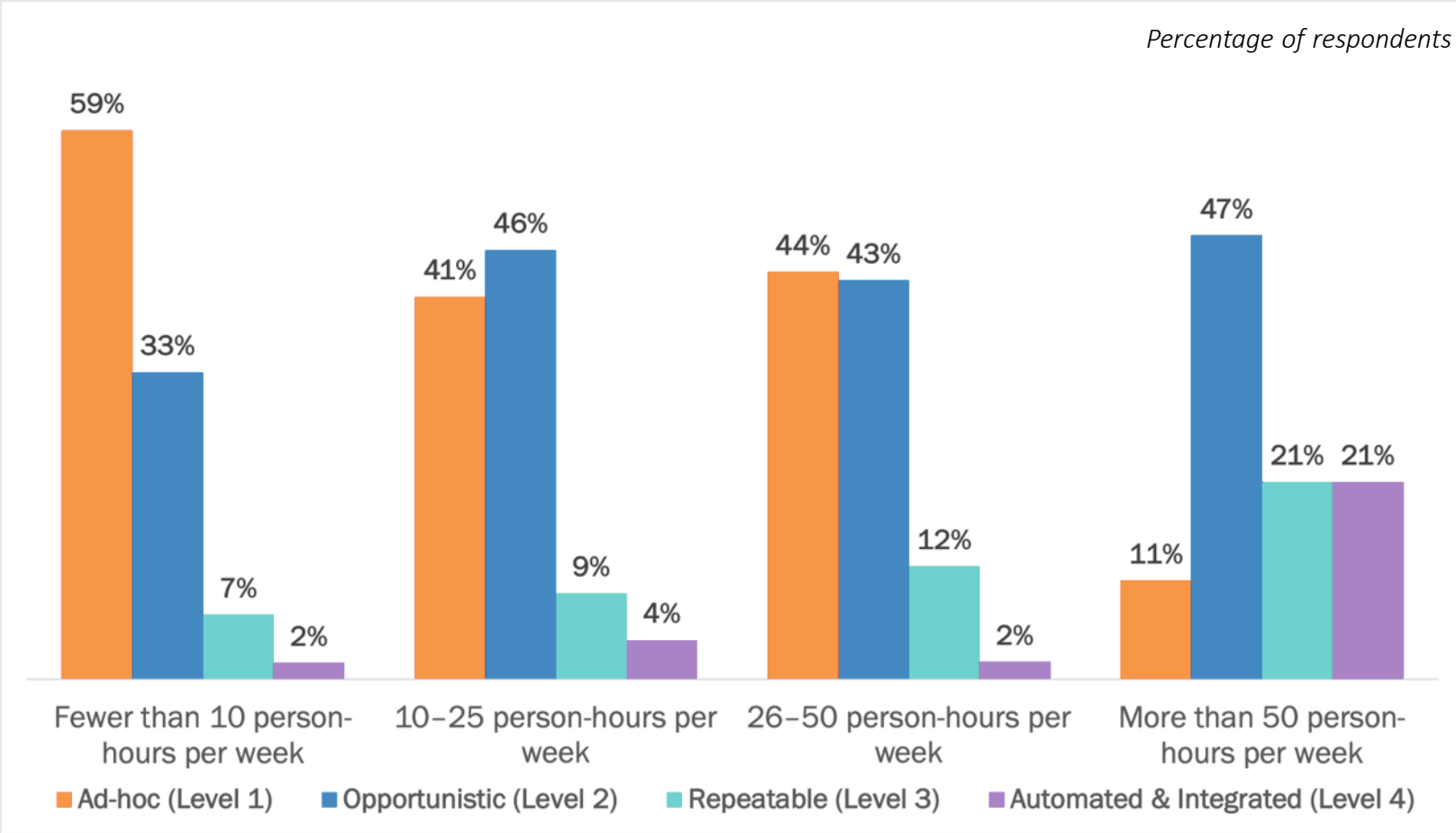
Percentage of respondents

Maturity increases when organizations invest time in cloud security

Time spent on cloud security is correlated with organizations reaching the higher maturity levels (4x higher). However, this is not the only factor driving maturity.

42%

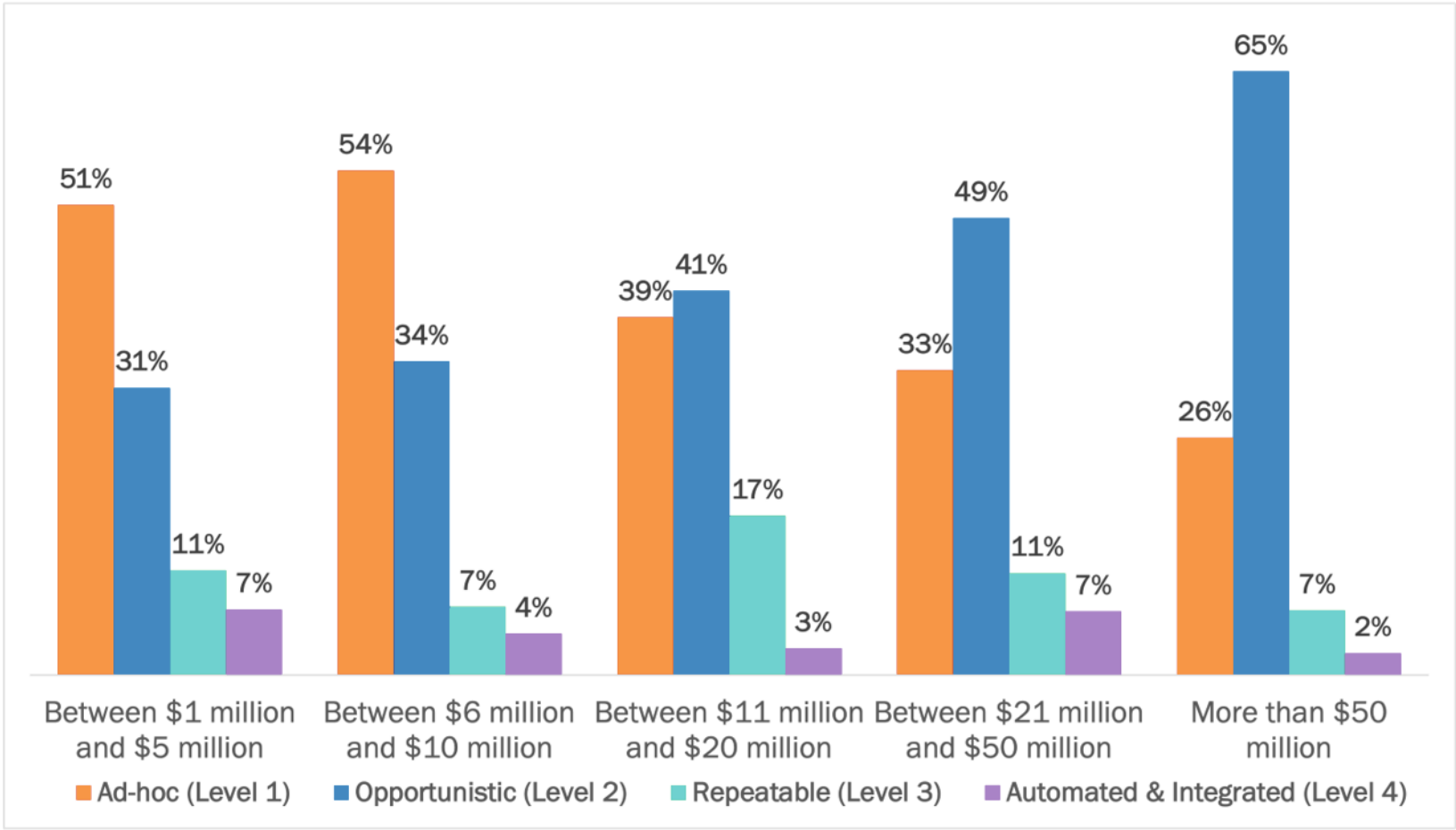
of organizations investing more than 50 hours per week on cloud security are achieving the high levels of maturity.



Maturity increases when organization spend more on cloud infrastructure
Organizations spending the most on cloud infrastructure shift to improved maturity levels. Though in the right direction, this shift appears to be capped. Maturity is not about investing more; rather, about prioritizing and investing wisely.

74%

of organizations spending more than $50M annually on cloud infrastructure achieve higher levels -- but only 9% get past the Opportunistic level.



Percentage of respondents

Top 5

cloud security priorities that correspond with higher maturity levels

Security priorities that align with higher maturity levels
Organizations surveyed that had the highest maturity levels told us that these are their top five priorities:

1. Detecting general cloud misconfigurations (e.g., unencrypted resources, MFA)
2. Achieving the ability to track and investigate activities performed by human users and applications/service accounts across the cloud infrastructure
3. Establishing Just-in-Time (JIT) access for developers / DevOps / Cloud operations teams to cloud infrastructure environments
4. Evaluating and reporting on alignment with security best practices (e.g., AWS well-architected, CIS) and compliance standards (e.g., NIST, ISO, SOC2, PCI-DSS)
5. Achieving least-privilege for identities in the cloud (both human identities and service accounts)

Fundamental controls are starting to be used, more advanced security is lagging
Some organizations are implementing basic controls for managing access permissions. Yet full visibility into access entitlements and the ability to ensure least privilege are less well-established.

52%

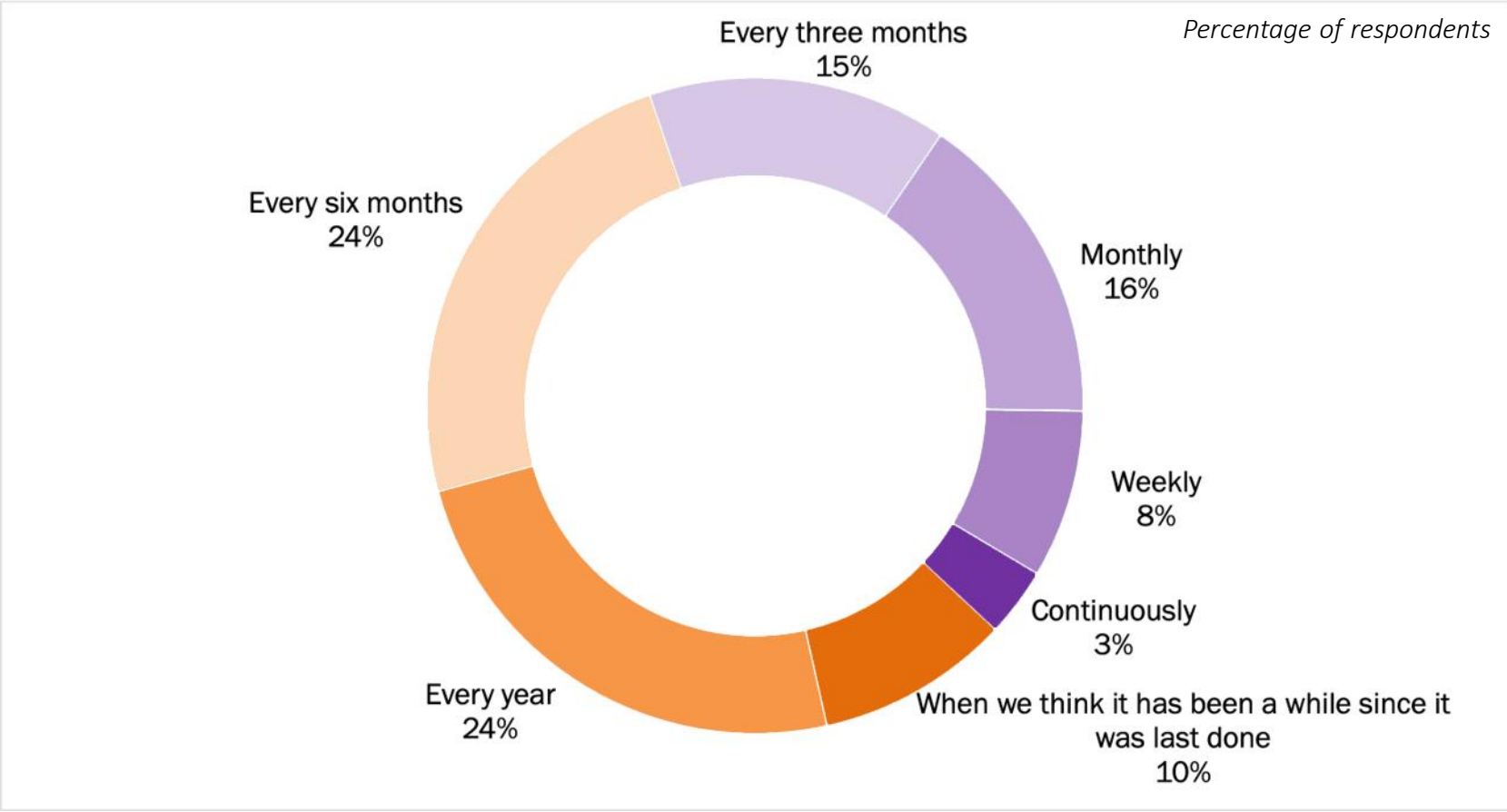
of organizations lack full visibility into the resources an identity can access, and the permission level granted.

Percentage of respondents indicating "agree" or "strongly agree"

Access reviews are a good first step toward least privilege but not done enough
Access reviews are a structured engagement to ensure access rights held by people and other identities are scoped appropriately. Only ~40% of organizations perform an access review of their cloud infrastructure at least quarterly—the bare-minimum accepted timeframe.

60%

of organizations are failing to do an access review at the minimal security practice of a quarterly review.

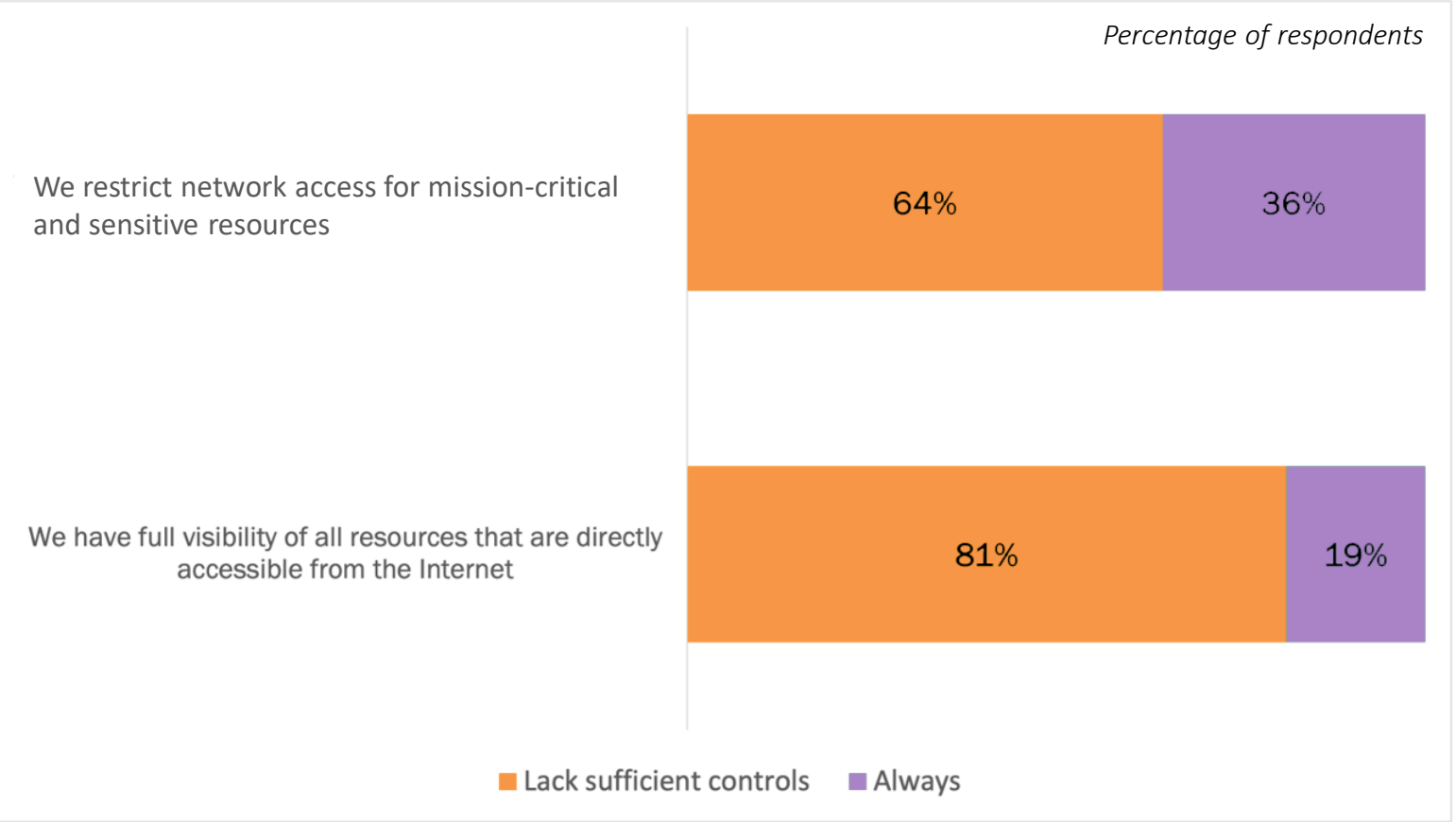


Few organizations are doing enough to restrict unwarranted network access, even from the Internet

Only 36% of organizations restrict network access for mission-critical and sensitive resources, and only 19% have full visibility into all resources directly accessible from the Internet.

81%

of organizations lack full visibility of all resources that are directly accessible from the Internet.



SECTION 4

Applying the Ermetic maturity model

Assessing your maturity level

There are two ways you can assess the maturity level of your organization against the Ermetic Cloud Security Maturity Model.

1

Review Ermetic's maturity model whitepaper and develop your own set of questions
Ermetic's whitepaper includes all the details needed to assess your maturity. Grab a copy of the whitepaper, review the standards applicable to each domain, and prepare a set of assessment questions. Answer the questions for your organization and see where you land.

Next action: Get your copy of the whitepaper.

2

Complete the self-assessment on Ermetic's web site
Ermetic has released a free (and product-neutral) self-assessment for organizations wanting to benchmark themselves against the maturity model and the organizations that participated in this survey. Head over to Ermetic's web site and answer the questions to see how your organization measures up.

Next action: Take the self-assessment.

Plan for getting better

Congratulations! You have assessed your organization's maturity level according to the Ermetic Cloud Security Maturity Model. Whatever your result, the clarity gained gives you the data needed to move forward and improve. A maturity assessment is only ever a point-in-time view of where you are currently. This visibility and insight provide a dynamic opportunity for continual improvement over time. Plan for getting better, by which we mean addressing the limitations and gaps that are holding you back from reaching the standards of the next level up.

Next steps are:

Remember: A maturity level is a **commitment**, not a certification. You will slip backward if you don't keep improving.

SECTION 5

Methodology and About Ermetic

Research methodology and survey demographics

Osterman Research surveyed 326 organizations in North America in June 2022 with 500 or more employees and that spend a minimum of $1 million each year on cloud infrastructure.

Annual spend on cloud infrastructure	
Between $1 million and $5 million	22%
Between $6 million and $10 million	21%
Between $11 million and $20 million	21%
Between $21 million and $50 million	22%
More than $50 million	13%

Organizational role of respondent	
Director of Information Security	27%
VP of Information Security	19%
Manager of Information Security	19%
CISO (or role with this responsibility)	15%
Cloud security architect or engineer	6%
Senior security engineer	6%
Head of cloud security	4%
Head of cloud operations	3%
Head of DevOps/DevSecOps	2%

Industry of organization	
Technology (other than SaaS/Software)	23%
Manufacturing	8%
Retail/Distribution	7%
Construction/Architecture/Engineering	7%
SaaS/Software	7%
Healthcare	7%
Financial Services/Banking	6%
Professional Services	5%
Education	5%
Consumer Products	4%
Life sciences (Pharma, medical, biotech)	4%
Energy, Utilities, Oil/Gas, Minerals, Mining	3%
Food/Beverage	3%
Logistics/Transportation	3%
Insurance	3%
Chemicals	2%
Government	1.3%
Other	1.0%
Aerospace/Defense	0.6%

About Ermetic

Ermetic's identity-first comprehensive cloud infrastructure security platform provides holistic, multi-cloud protection in an easy-to-deploy SaaS solution.

With offices in Tel Aviv, Palo Alto and Boston, Ermetic is led by industry veterans and backed by prominent cyber security investors. Around the world, organizations of all sizes are using Ermetic to mitigate access risk, secure cloud data, and ensure compliance.

Learn more at www.ermetic.com.