Making Security an Enabler by Delivering Business Outcomes

May 2019

Author:
Dominic Trott

IDC #EUR145016919

An IDC InfoBrief sponsored by

Orange
Cyberdefense

Executive Summary

CHANGING PERCEPTIONS

The perception of security in the business has shifted; it is now recognized as an enabler rather than a blocker.

- Deperimeterization, driven by trends such as digital transformation, IoT, and extended ecosystems, is forcing security teams to operate in new ways.
- These trends expose the business to added risk, so traditionally security has aimed to mitigate or even stop them, yet they are central to business strategies.
- Security teams have therefore been driven to find ways to enable these trends, because if they don't, they will find themselves in conflict with or even side-stepped by the business.

PRESENTING TO THE BUSINESS

The way security teams present themselves is changing as a result; security leaders need to act much more like business leaders.

- Security teams need to position themselves as partners for creating business value, not as custodians of specialist technologies.
- Security needs to collaborate with lines of business more, and get involved in new business initiatives from a much earlier stage.
- CISOs need to engage at a more senior level — reporting to a board member or even sitting on the board themselves.
- These characteristics cause security to focus on metrics that are understood by the business and the board — particularly risk — to quantify impact, generate buy-in, and build influence.

FOCUSING RESOURCES

To achieve this, security teams must focus their resources on value-add activities — and demonstrate that value.

- They must back up the impact of their strategic programs to demonstrate a quantifiable outcome in areas such as cost reduction, operational efficiency, risk mitigation, brand protection, operational resilience, digital trust, and return on investment.
- They must release resources (human and financial) to focus on higher-value activities through techniques such as automation, orchestration, and integration.
- They must find the right blend of in-house capability and third-party support to deliver the security capabilities demanded by the enterprise.
- They must optimize their use of threat intelligence to provide context that helps prioritize threat management activities, finding the right blend of sources to generate that intelligence, bearing in mind the reach and insight offered by third parties.

By 2023, the automation and orchestration arms race in security operations will empower 40% of tier 1 SOC analysts in Europe to up-skill and perform higher-value activities, attacking the security skills shortage.

Source: IDC European Predictions and IT Trends 2019

Repositioning Security for Success

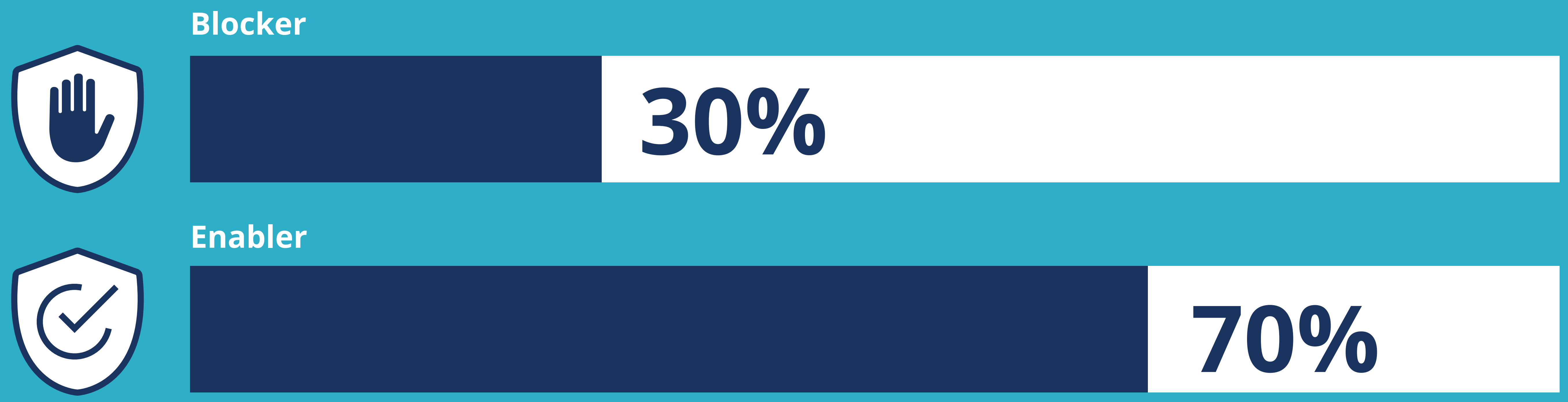
Security teams have struggled with a “brand reputation” issue. They have often been perceived as inhibiting or even actively blocking business innovation, rather than enabling partners.

> **You’re the security guy? You’re the person who says NO!**
>
> **Chief Digital Officer**, Major European Retail Bank

However, this position is shifting. IDC research shows that 70% of businesses now perceive security as a business enabler. From a separate study, further IDC research showed that in 2016/17 this level stood at 51%, showing a 21 point improvement over the past two to three years.

But this is tempered by the fact that there are systemic issues that prevent security teams from maximizing their positive business impact.

Security environments and operations tend to be fragmented and manual, weighing down scarce resources with menial tasks. Security teams must find better ways to demonstrate value, and to collaborate with/embed security into other business areas.



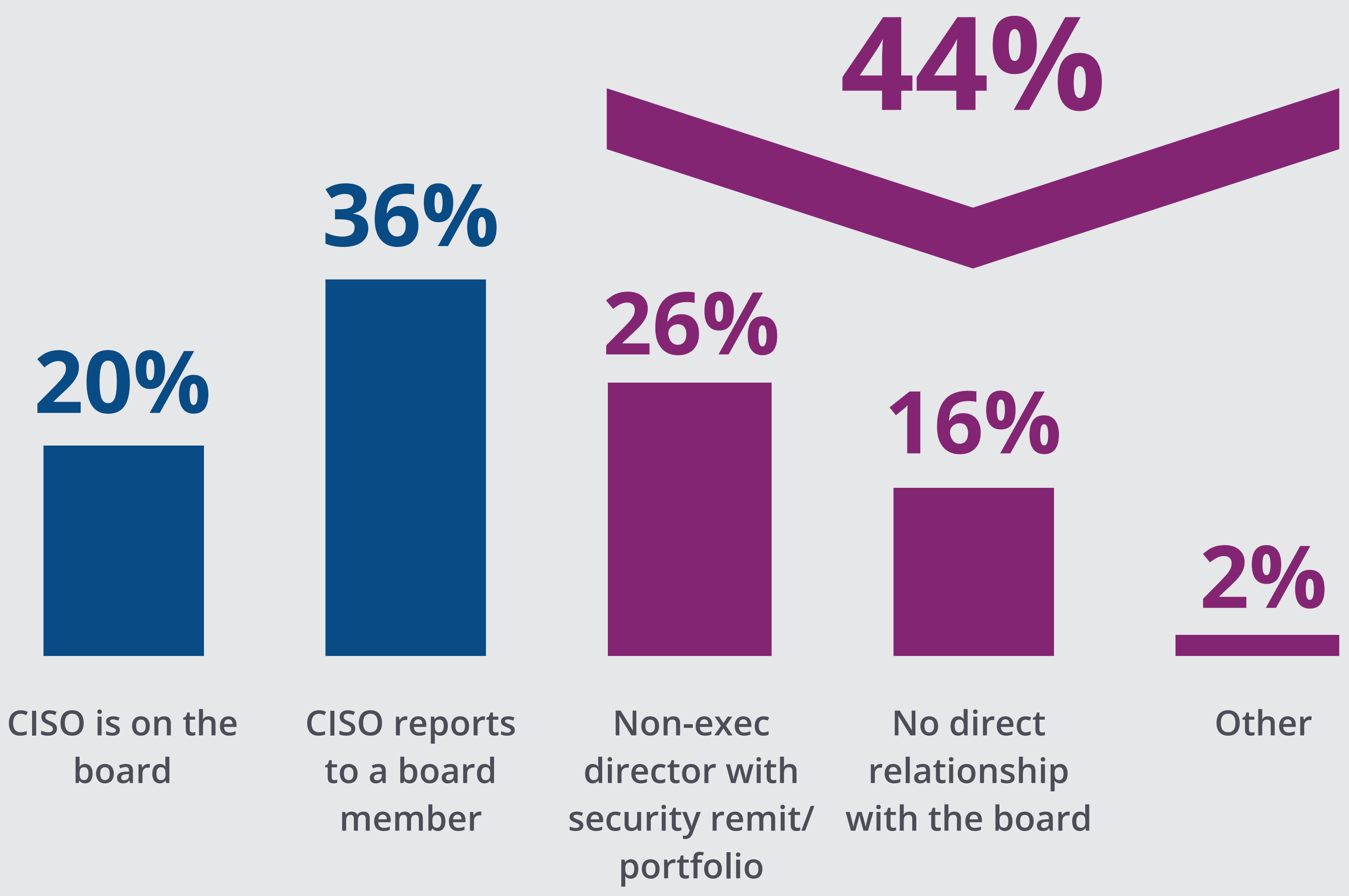
To do this, security teams need to help business leaders take decisions grounded in security reality. After all, security is not a “nice to have”; rather, it is foundational to any organization’s ability to operate.

So, what barriers must be broken down to achieve this goal?

Source: IDC Security Management, February 2019, n = 283

Engage the Board to Get Security's Voice Heard

How is security represented at board level?



Source: IDC Security Management, February 2019, n = 283

There is a clear need for business-enabling security. Risk is entering the language of security teams to demonstrate relevance to the business and the board.

However, simply referring to risk management is not enough. It must first be quantified and then tied to business outcomes.

> **How do I drive effective communication with the business and the board? It is all about risk!**
>
> **CISO,**
> Major European Public Body

> **Every interaction between security and the board is framed in terms of risk. It informs every decision we make, including vendor selection.**
>
> **CISO,**
> Global Pharmaceutical Company

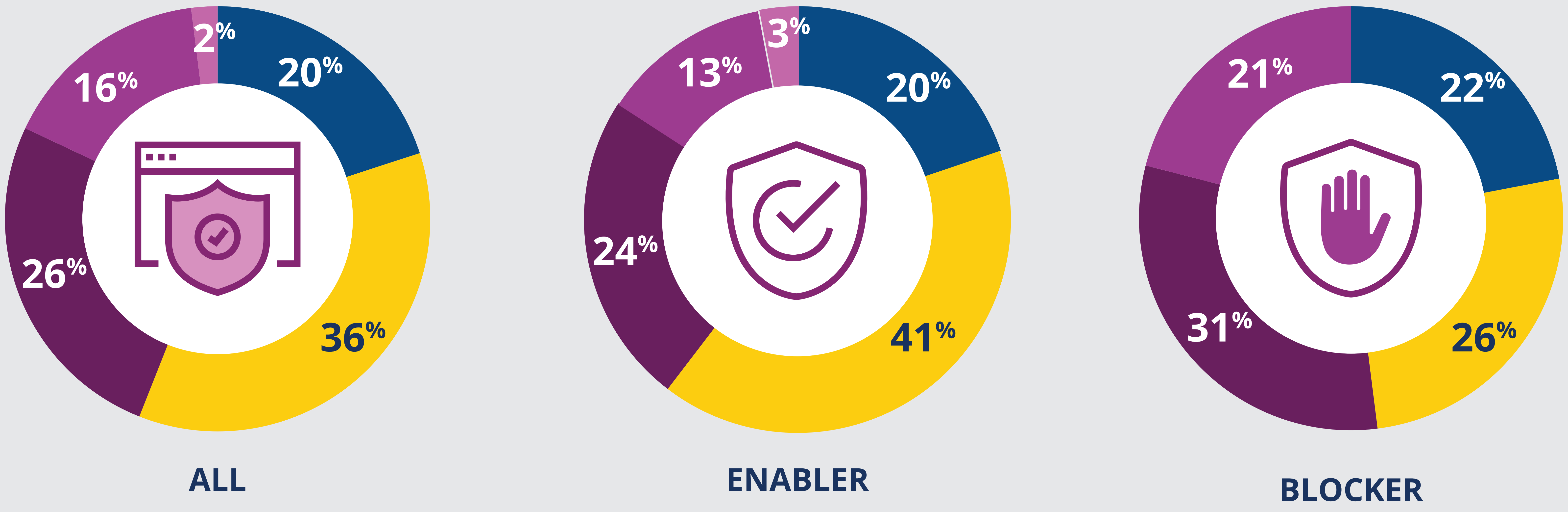
This situation is not helped by a lack of direct communication between security leaders and the rest of the business. In almost half (44%) of organizations, the CISO is neither a member of the board nor attends on an ad hoc basis.

But how can security leaders make the connection with the board to ensure security is being properly considered by business decision makers?

Engage the Board to Get Security's Voice Heard

How is security represented at board level?

- ● CISO is on the board
- ● CISO reports to a board member
- ● Non-exec director with security remit/portfolio
- ● No direct relationship with the board
- ● Other



Source: IDC, Security Survey, February 2019, n = 283

This picture is particularly stark when comparing the representation of security at board level between organizations where security is viewed as an "enabler" and those in which it is seen as a "blocker."

For the former group, the CISO either sits directly on the board or reports to a board member in **62%** of cases.

For the latter group, just **48%** are represented in this way.

This suggests that board access is a critical success factor for security becoming a business enabler.

Business Value to Gain Board-Level Attention

To raise the interest of the board, security teams need to demonstrate how they can generate an impact that is meaningful in business terms.

> **More established business influencers come to the board armed with basic business metrics like investment growth and risk vs. return.**
> **We must be ready to provide security equivalents to demonstrate business value.**
>
> **CISO,**
> European Insurance Group

To do so, security leaders are focusing on the business outcomes they can support in order to generate board-level attention. There are two key themes to this end:

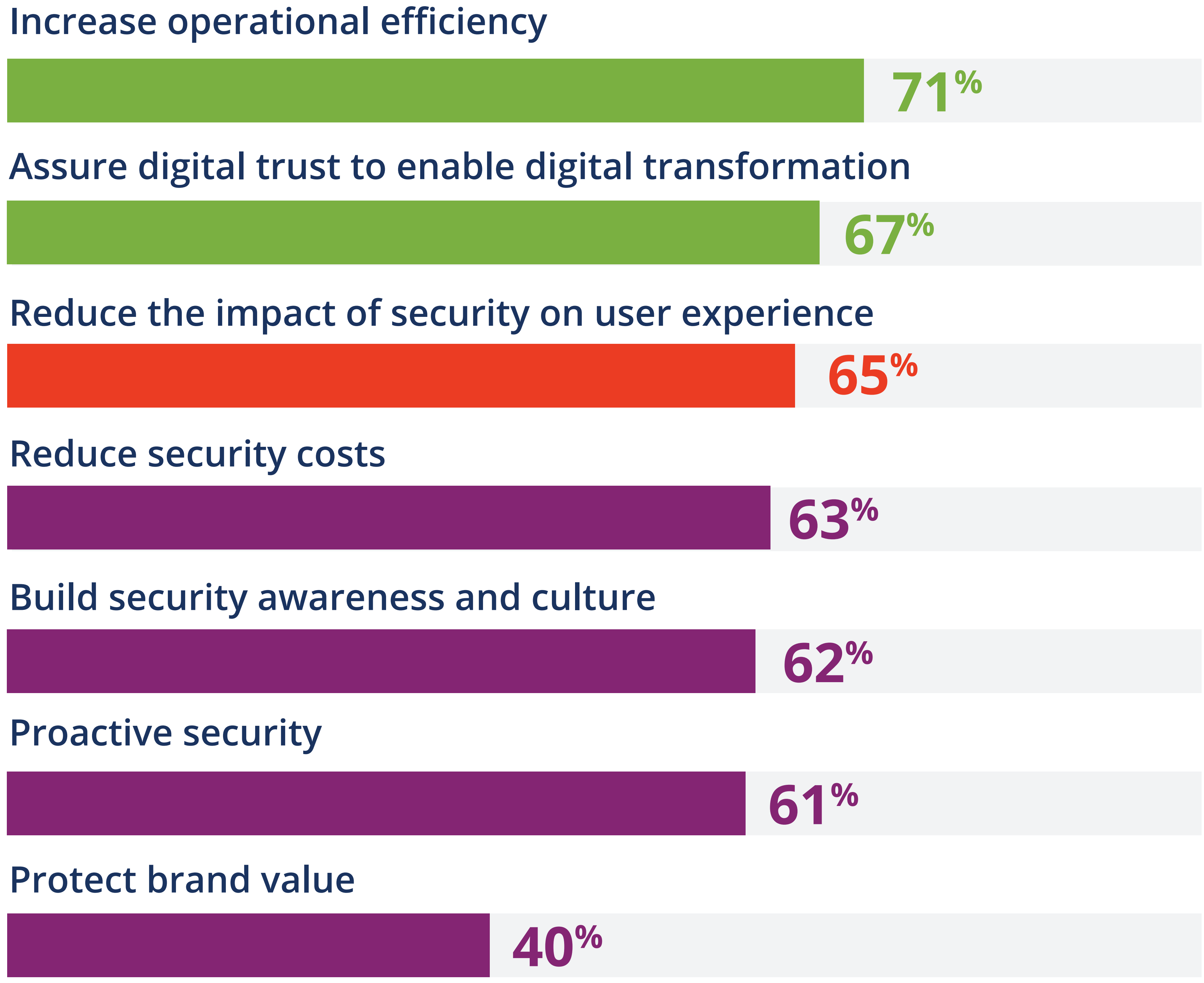
Demonstrating "operational excellence": i.e., reducing costs, improving efficiency, and maximizing effectiveness (such as moving towards "proactive security" approaches that identify and ameliorate unknown threats).

Augmenting business strategies: e.g., providing the digital trust that enables digital transformation, or building security awareness as an element of corporate culture.

In Asia, there is a strong focus on operational efficiency (**74%**). While still important for Europe (**68%**), there is equal emphasis on enabling digital transformation.

For organizations where security is seen as a **blocker**, the focus is to reduce the impact on user experience (**69%**). This is more of a "negative ambition," suggesting that security represents a burden for enterprise users in these organizations. For **enablers**, there is a much stronger focus on efficiency (**78%**), digital trust (**70%**), and security awareness (**70%**), showing how security can help to drive positive change.

What does the business expect of the security team?



Source: IDC, Security Survey, February 2019, n = 283

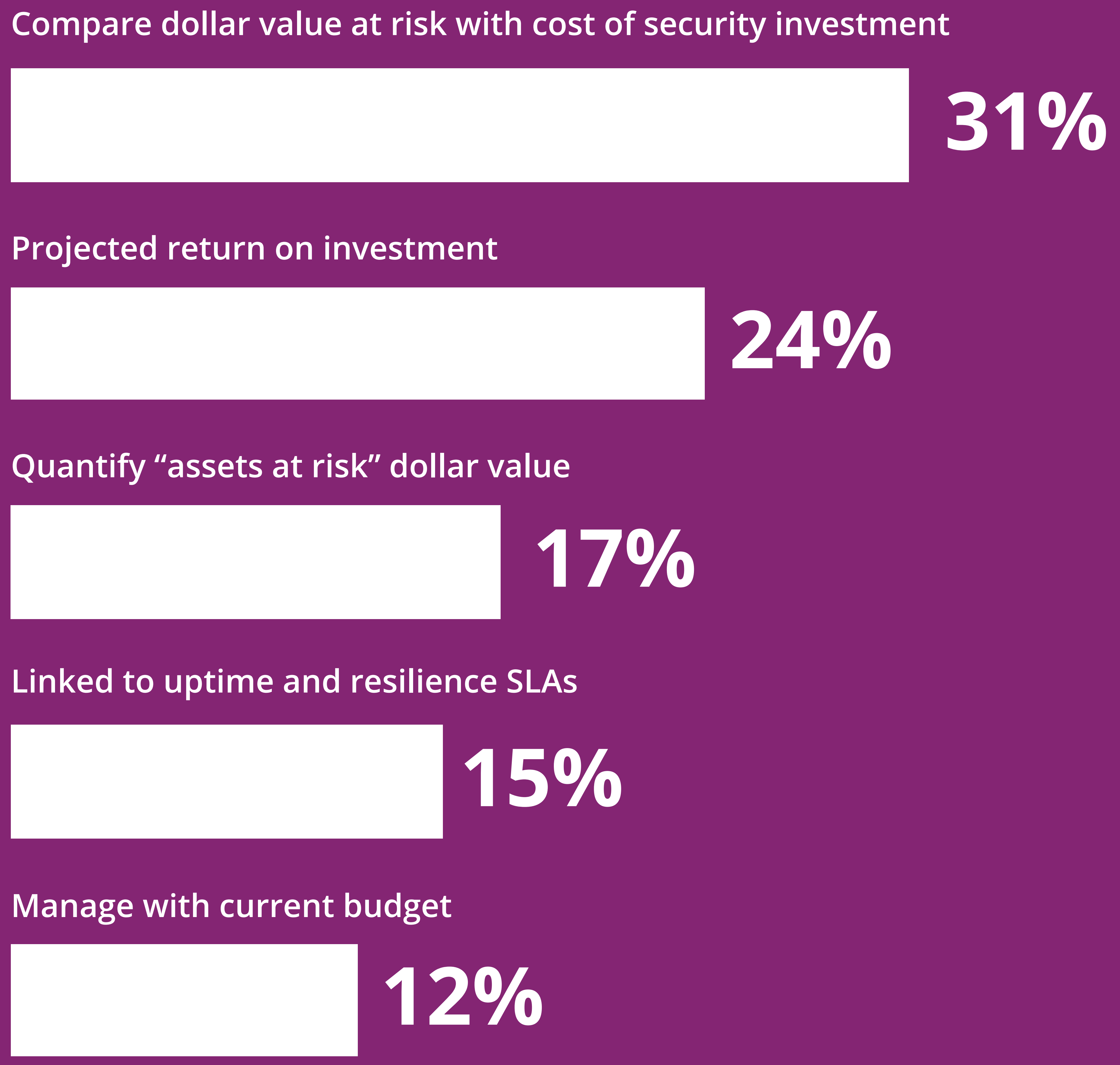
Business Benefits to Demonstrate Business Value

Having identified the key business outcomes that security can enable, there remains a question: how can security teams show their impact?

12% of organizations simply aim to cope with the security budget that they have been allocated. However, that means 88% of enterprises are finding ways to demonstrate the value security has in achieving business goals.

Interestingly, there is a complete polarization between business enablers and blockers. For blockers, the primary focus (32%) is on quantifying the dollar value of assets at risk (the weakest focus for enablers, at 11%).

For enablers, the strongest focus (41%) takes the same approach initially — establishing the value at risk — but then comparing it with the cost of security investment to close that risk. This is the weakest focus for blockers (9%), suggesting a lack of maturity in considering risk among this group.



Source: IDC, Security Survey, February 2019, n = 283

Roadblocks to Security Reform

Enabling business outcomes and demonstrating business value are top priorities for security teams. However, there are structural issues inhibiting their effectiveness.

The primary limitations to improving cybersecurity capabilities are linked to resources and visibility. In order, the top 3 inhibitors are:

1. Security teams being too busy with routine operations
2. Budget constraints
3. Lack of insight into secure/sensitive activities

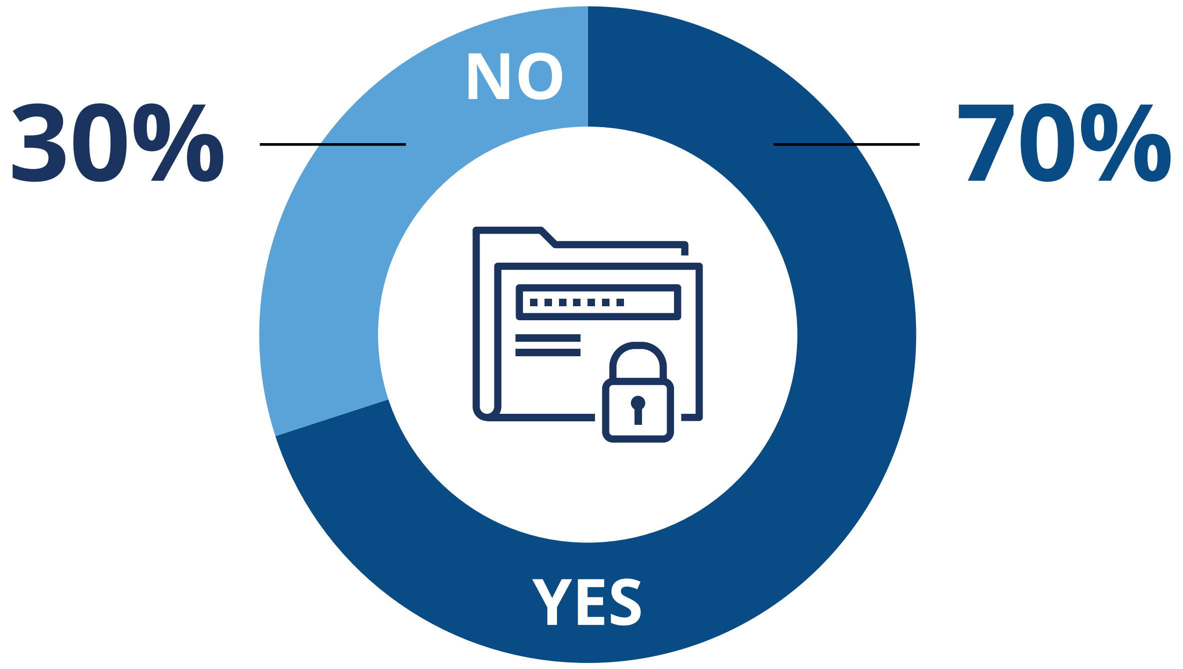
These challenges are exacerbated by the complexity of security provider ecosystems. The majority of enterprises have four or more security providers to deal with.

Consequently, organizations are looking towards security aggregators to help reduce this complexity. 70% of enterprises agreed that a security aggregator to manage supplier complexity would be of value.

> **The biggest threat I face is my own security environment. It is too fragmented, meaning I can't understand my holistic security posture.**
>
> **CISO,**
> Major European Bank

> **If someone came in and said they could look at supplier management across multiple vendors, taking away the complexity I don't have time or resource to handle, that would be attractive.**
>
> **CISO,** Digital Agency

Would you value a security aggregator partner to reduce the number of vendors and simplify supplier and contract management?



Source: IDC Security Management, February 2019, n = 283

Lightening the Load

Third-party security service providers can help to address the limitations that prevent security teams from maximizing their capabilities. They can also help to deliver some of the business outcomes that are expected of security.

- 97% of organizations already work with security service providers to some extent
- Plans for expenditure on security service providers are net positive (proportion that plan to increase spending less proportion that intend to decrease = 28%)
- Sentiment towards security service providers is net positive (proportion that are pro-externalization less proportion that are against = 23%)

The primary driver for engaging third-party providers (69% of respondents) is to gain access to “state of the art technologies and techniques,” indicating the role that providers play for their customers in driving technical and operational excellence.

Beyond that, though, the top drivers for third-party security service provider engagements are much more business-outcome oriented:

65% Predictable costs

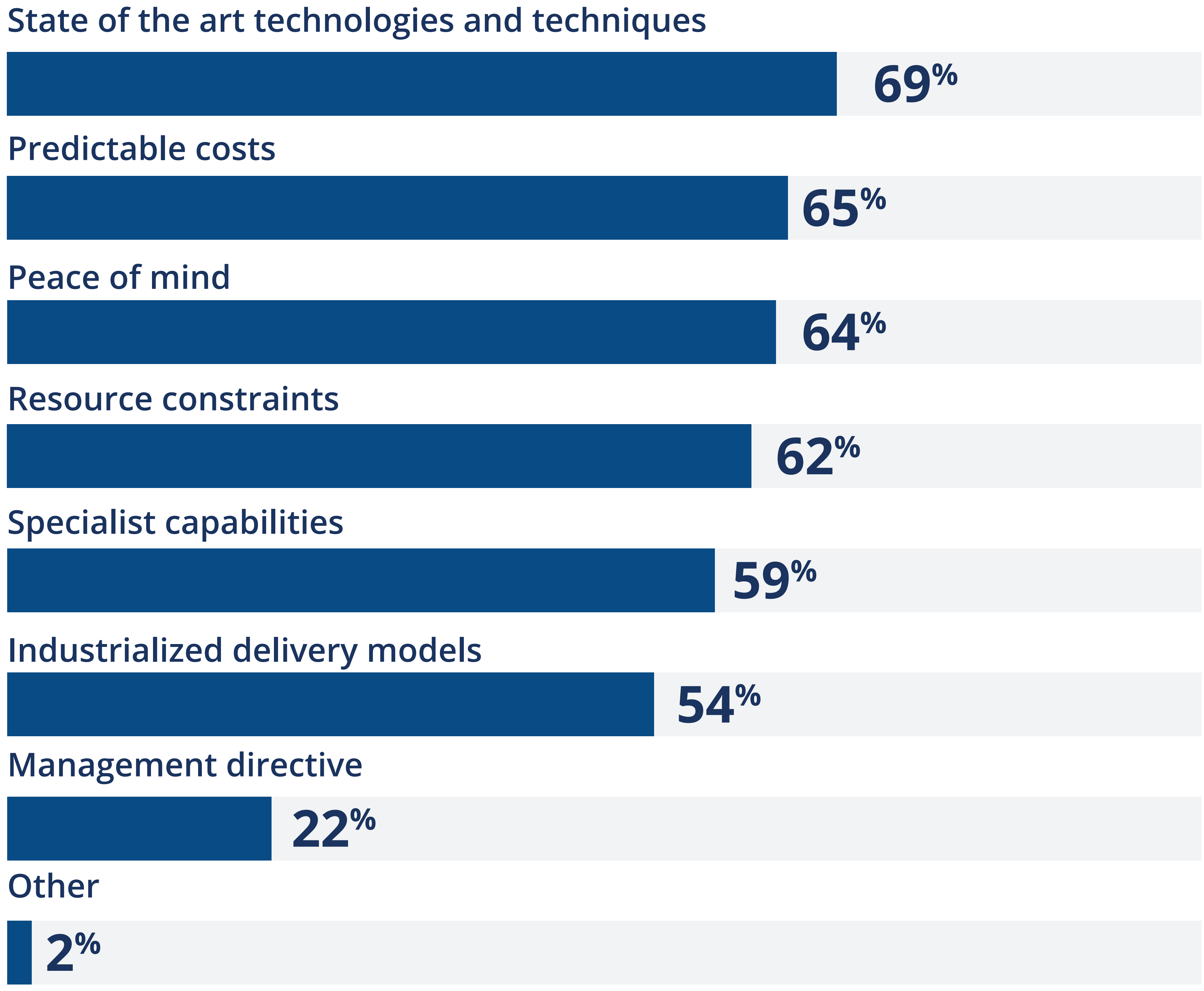
64% Peace of mind

62% Resource constraints

59% Specialist capabilities

Clearly, security service providers provide a dual role for their customers: on one hand, providing them with the scale, technologies, and capabilities that do not exist in-house; on the other, supporting business goals such as financial planning, trust, resilience, and resource optimization.

What are/would be your motivations for using a third-party security services provider?

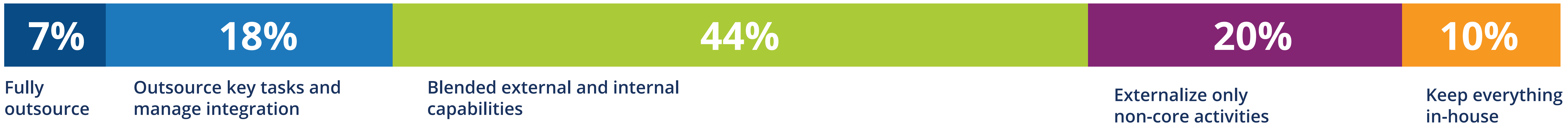


Source: IDC Security Management, February 2019, n = 283

Security Externalization — Best Practice

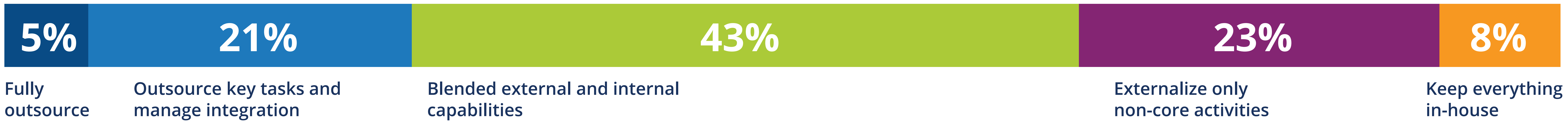
Looking at current approaches towards working with third-party security service providers, the clear focus is to work on a blended basis between internal and external delivery:

What is your current approach to the use of third-party security service providers?



There is a similar profile when it comes to views on best practice for the engagement of third-party security service providers:

What do you consider to be best practice for the use of third-party security service providers?



However, there are some key differences between current approaches and best practice:

Compared with current approaches, there is a stronger view that best practice is to work with specialists to outsource key tasks and manage integration

Yet there is also a stronger representation of those that believe best practice is to externalize only non-core activities

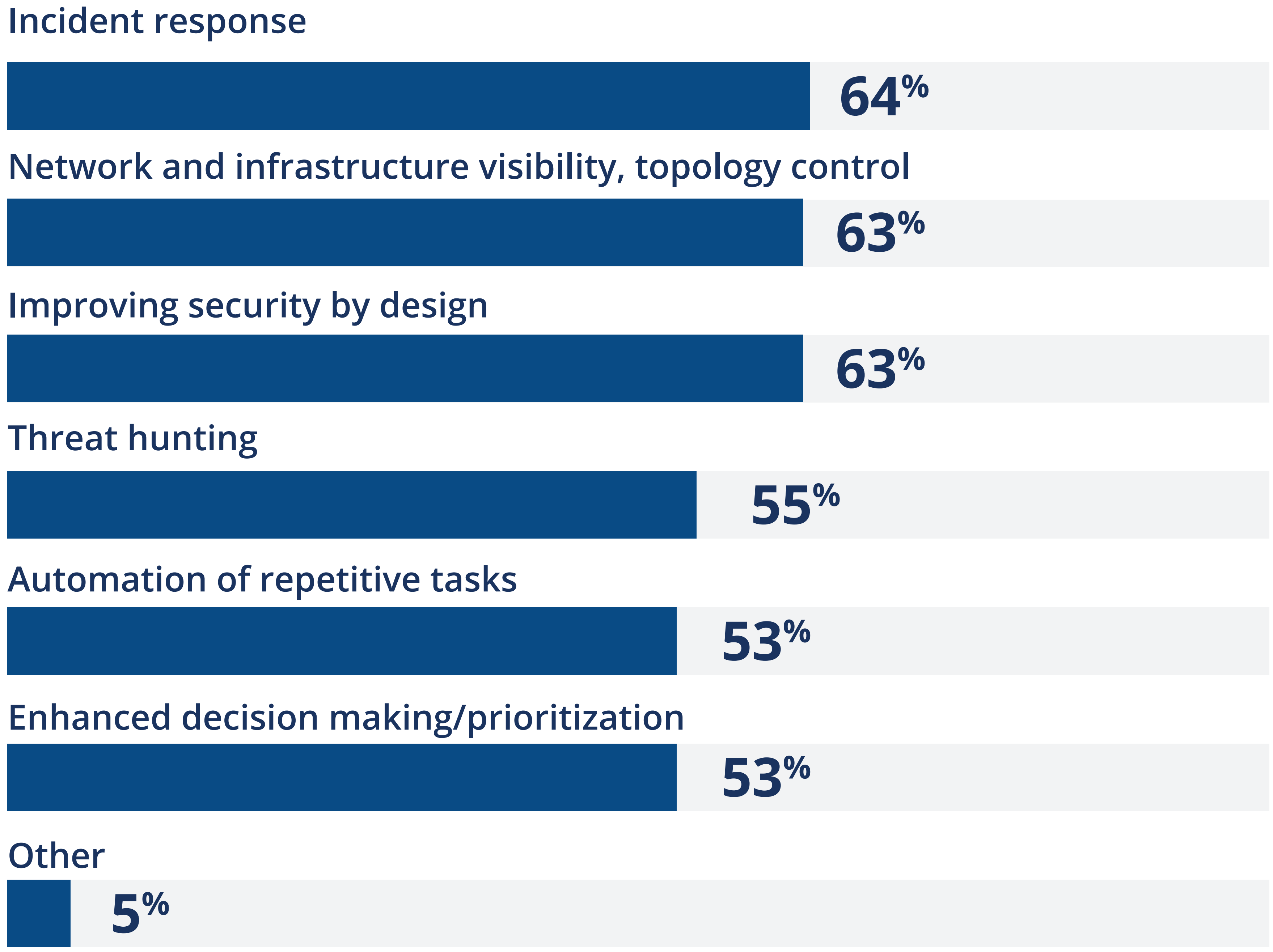
Fewer enterprises believe that best practice is to fully outsource than those that currently adopt this approach

However, there are also fewer enterprises that believe best practice is to keep everything in-house than currently adopt this approach

Functional Role of Security Externalization — Current Situation

Our research indicates the following levels of adoption for security service categories:

In which areas do you currently work with third-party security service providers?



Source: IDC Security Management, February 2019, n = 283

Looking at how security service providers are engaged at present, there are three “spikes” of focus:

Scarce and/or specialist capabilities
(e.g., incident response and threat hunting)

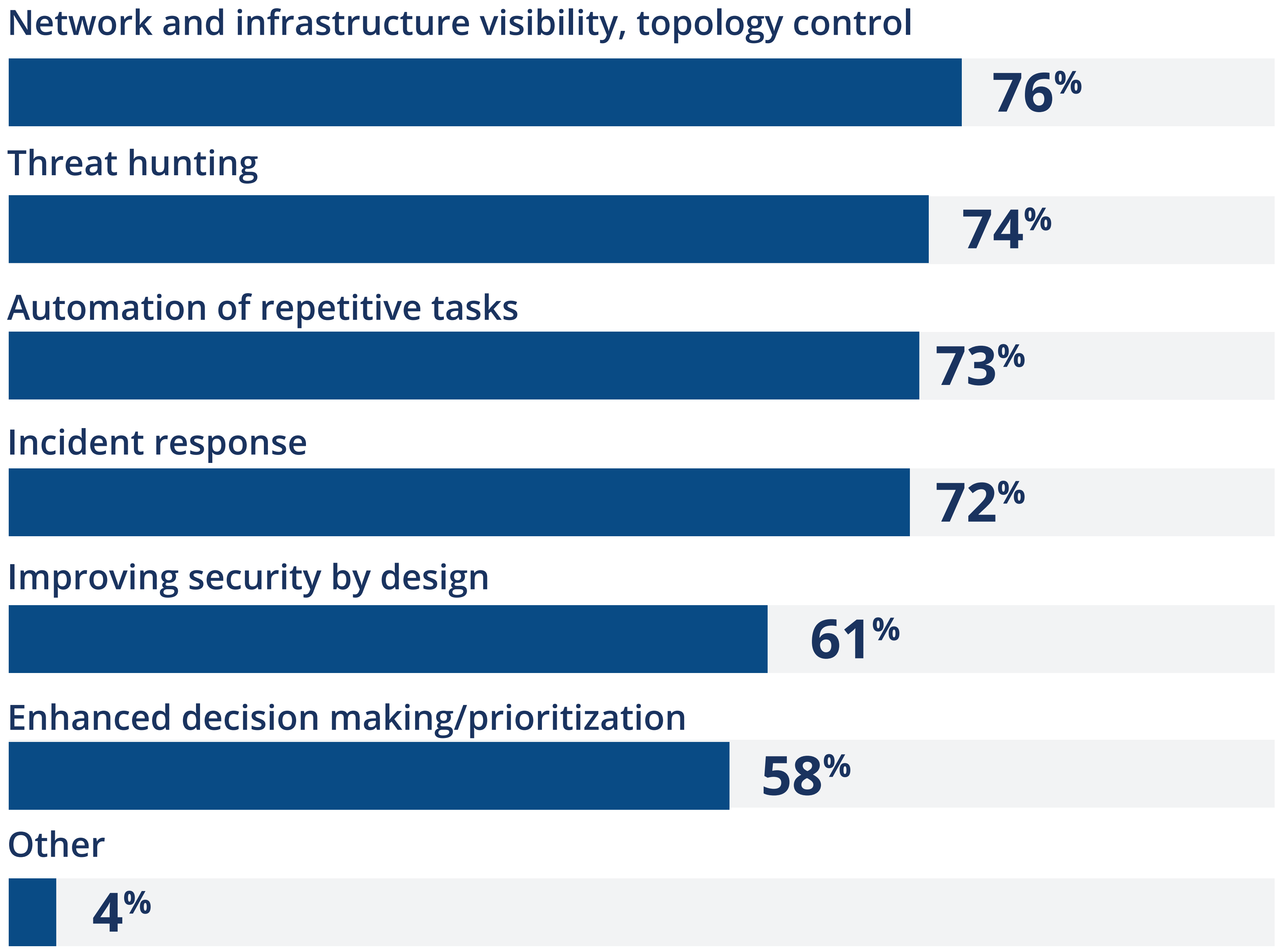
Making security central to new business initiatives
(i.e., improve security by design by embedding security into all technology initiatives, processes, etc.)

Delivery at scale
(e.g., network infrastructure visibility, automation of repetitive tasks)

Functional Role of Security Externalization — Future Guidance

Our research also considered how enterprises seek to make use of third-party security services providers in future:

What are the areas that you would consider or like to use a third-party security services provider for?



Source: IDC Security Management, February 2019, n = 283

All areas saw an increase in interest compared with current usage levels. However, there are particular peaks in interest for the following areas:

- **Automation of repetitive tasks**
- **Threat hunting**
- **Network and infrastructure visibility, topology control**

The presence of these themes at the top of respondents' wish-lists for working with third parties suggests a focus on threat life-cycle management:

- **Network visibility and control** correlates strongly with threat detection.
- **Incident response** and **threat hunting** speak for themselves. Their presence among the top focus areas shows the importance of not just seeking to block attacks as they occur, but also both seeking out threats proactively and dealing with incidents after they have occurred.
- **Automation of repetitive tasks** shows the opportunity to bring scale and capability to bear in order to improve security operations with robust and specialist platforms, taking advantage of capabilities such as artificial intelligence and machine learning.

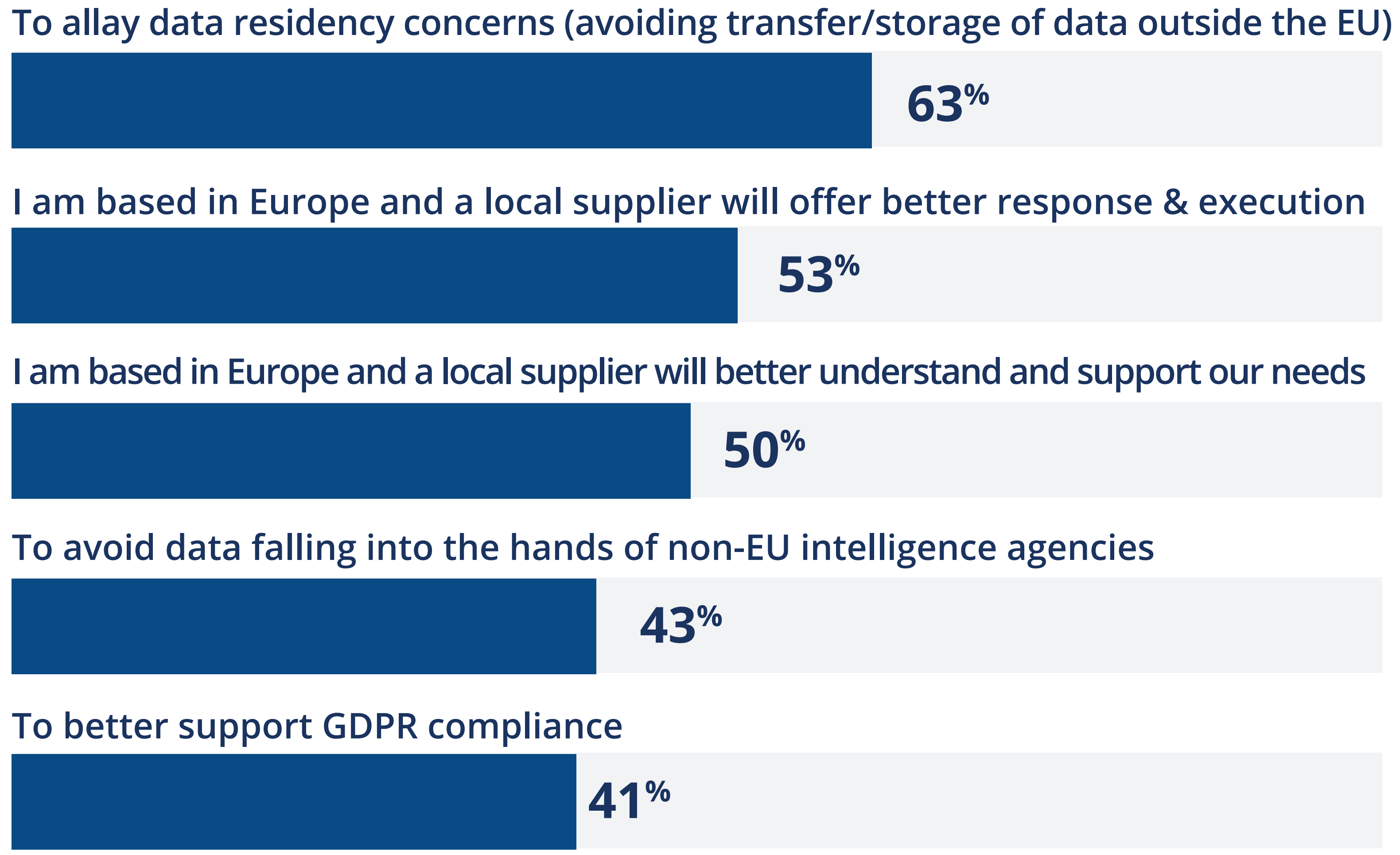
Data Residency and Security Externalization

of enterprises view it important to have a security provider headquartered and resident in the EU

A key factor when working with security service providers is to consider the data residency/data transfer needs of your organization.

69% of enterprises view it as important to some extent (slightly, moderately, or very important) to have a security services provider headquartered and resident in the EU.

In which areas do you currently work with third-party security service providers?



Source: IDC Security Management, February 2019, n = 283

The top reason identified by respondents is to avoid data residency concerns by ensuring that data is not transferred beyond the EU. This is a particularly strong concern for Asian respondents (70%), and not quite so much for Europeans (58%).

There are also strong perceptions held by European respondents (61%) in particular that working with EU-based providers will result in better and more rapid service delivery due to cultural affinity. This is a minor concern for Asian respondents (40%).

These issues are particularly relevant given the broader trend of enterprise cloud migration. Demonstrating the impact and pace of this trend, IDC's Cloud Server Tracker shows that while in 2018 the cloud represented 35% of the total market as measured by value in Europe, in 2023 it will have shifted to represent almost half the market (48%).

The top four public cloud vendors in 2018 according to IDC's cloud tracker — AWS, Microsoft, Salesforce.com, and Google — are all U.S.-based. This means that U.S. federal laws such as the Patriot Act and the CLOUD Act, pertaining to the accessibility of data by the U.S. government regardless of its residency, let alone concepts such as data sovereignty, are very much "in play" for European organizations.

With these four vendors alone controlling one-third of the European public cloud services market, there is considerable value to be found in working with a Europe-based security services provider as a counter-balance.

Threat Intelligence to Bring Focus and Context

Threat intelligence has already been adopted by the majority of enterprises, with our research showing that 67% of enterprises are using it.

Best practice is to avoid reliance on a single source or small group of sources, but rather to aggregate multiple feeds, especially from third-party sources. The top 5 most adopted are:

1. Third-party breach reports
2. Third-party threat intelligence specialists
3. Industry-aligned threat intelligence communities
4. Internal threat hunting
5. Law enforcement

There are multiple options for consuming threat intelligence. However, our research indicates that these are prioritized as follows (in order):

1. Fed directly into the SIEM
2. Through a dedicated threat intelligence platform tool
3. Through the portals provided by third-party sources
4. Internally developed automation solutions
5. Internally developed manual solutions

Source: IDC Security Management, February 2019, n = 283

However, with 23% of enterprises either not yet using threat intelligence, or using it only on an ad hoc basis, it is clear that there is room for improvement in terms of how its impact can be "operationalized":

- Particularly with 64% of enterprises planning to use threat intelligence to increase the influence of security within the business, enterprises are recommended to reconsider how threat intelligence can be escalated to play a more strategic role in security operations.
- The real value of threat intelligence lies not in its use as an "ad hoc" source of intelligence, but rather to help prioritize security operations based on threats that are contextually relevant.
- Consequently, this ties in with the top business outcomes that security teams seek to enable and thus raise their profile and influence within the organization: operational efficiency and operational effectiveness.

Essential Guidance

- **In the majority of cases, security is now recognized as an enabler by the business.**
- **In “security enabler” organizations, CISOs are likely to report to a board member, or even sit on the board themselves.**
- **“Enabling” security teams demonstrates business value by increasing operational efficiency and providing the digital trust to enable digital transformation.**
- **Security must convey its impact in terms of risk to win buy-in and increase its influence. Comparing the value of assets at risk with the security cost to close that risk is the preferred method for “security enablers.”**
- **To maximize security effectiveness, security teams must adopt the optimum blend of in-house and third-party resources.**
- **Security teams should expect to work more with third-party specialists in the future to meet their evolving needs — especially to benefit from automated delivery of large-scale activities and to access niche/scarce resources and capabilities.**
- **Organizations concerned about data residency and transfer in their security operations should consider working with EU-headquartered security service providers.**
- **Security teams should harness threat intelligence to focus threat management activities on contextually relevant challenges, driving efficiency and optimizing resource utilization.**

The Orange Group’s specialist cyber security division

Sales and support in 160 countries

Over 1,800

multiskilled cyber experts worldwide

16 SOCs
10 CyberSOCs
4 CERTs
3 DDoS scrubbing centers

More than 3,700

multinational and thousands of SME customers worldwide

End-to-End solutions

Anticipate, identify, protect, detect, and react to cyberattacks

24 x 7 x 365

follow the sun capabilities

Partnerships and Alliances

Orange Cyberdefense includes Orange Business Services, SecureLink, and Secure Data, top industry vendors TF-CSIRT, FIRST, Phishing Alliance, and Europol

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC is a subsidiary of IDG, the world's leading technology media, research, and events company. Further information is available on our websites at www.idc.com

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters

5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright Notice