The Financial and Operational Benefits of Zscaler MDR

Survey and interview data from 23 Zscaler MDR customers, analyzed by AimPoint Group



©2026 Zscaler, Inc. All rights reserved.

WHITEPAPER

Executive Summary & Overview

Key Findings of This Study

72%

The average reduction in the number of alerts that security teams triage and investigate weekly.

81%

The average reduction in time spent investigating and responding to alerts.

$600K+

The average cost reduction attributable to these time savings.

BROADER BENEFITS

Data demonstrating other financial and operational benefits, including tool consolidation, team upskilling, and lower cyber insurance premiums.

Overview of the Research

A managed detection and response (MDR) service helps organizations detect, investigate, and respond to cyberthreats. It also enables them to hunt for indicators of attacks, remediate security issues, and understand the current threat landscape.

MDR services leverage advanced technologies that monitor and analyze endpoint telemetry and identity and cloud logs, as well as alerts from a wide variety of cybersecurity tools. In addition, they enrich that data with threat intelligence and help security teams to triage alerts and respond to threats effectively. They also provide on-demand engagement with technical experts to help security teams contain attacks rapidly, plan for emerging threats, and implement best practices for efficient security operations.

But do MDR services actually produce measurable results? How large are those results, and what causes them? And what effect do they have on cybersecurity team members?

To answer these questions, Zscaler commissioned AimPoint Group, a leading industry research and marketing agency for the cybersecurity industry, to conduct a survey of Zscaler customers, interview a panel of their chief information security officers (CISOs), and analyze the results.

©2026 Zscaler, Inc. All rights reserved.

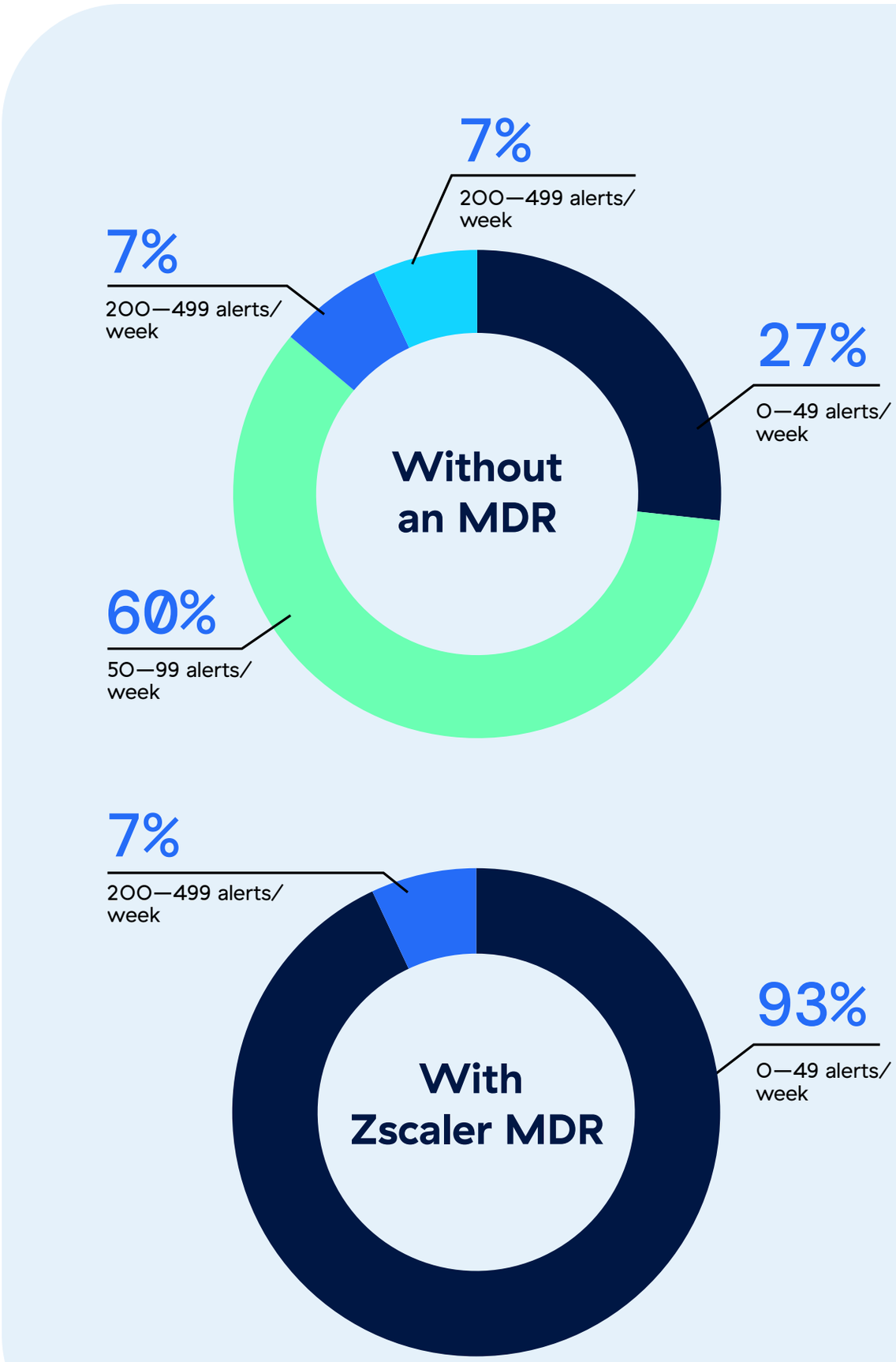
Reduction of False Positive Alerts

Eliminating Alert Fatigue

Alert fatigue is one of the most pressing challenges facing cybersecurity professionals. The volume of security alerts and incident tickets bombarding security operations centers (SOCs) and other security teams is growing rapidly. Among the factors driving the flood are expanding attack surfaces (particularly in the cloud), proliferating cybersecurity tools, and more intensive campaigns by threat actors. Impacts include real threats lost in the tumult, long queues of alerts and tickets that slow response times, and burnout of analysts and other security professionals.

Yet most of the alerts that plague security teams today are false positives. These include alerts that are duplicates (e.g., notifications about a single event from multiple security tools), trivial or irrelevant (such as low-impact threats and those targeting applications and systems not present in the organization), and flagging attacks for which the organization has effective security controls in place.

Filtering out false positive alerts could allow cybersecurity teams to spend much more time following up on genuine, relevant, high-priority alerts and on other key security tasks that prevent their business from being disrupted by cyber attacks.



How Much Can an MDR Service Reduce False Positives?

Can an MDR service play a significant role in reducing false positives? According to the participants in our survey, it can.

The survey respondents estimated that the number of alerts and tickets their organization has to investigate and triage per week has been reduced between 35% and 85% from what it would be without an MDR. The average organization is experiencing a 72% reduction in alerts triaged and investigated weekly.

With Zscaler MDR, the vast majority of organizations (93%) only need to investigate 49 or fewer tickets a week.

©2026 Zscaler, Inc. All rights reserved.

Behind the Improvements

Customers surveyed pointed to several causes of the substantial reduction in alerts that need to be triaged and investigated, including:

- Extremely high accuracy in discriminating between false positives and genuine, relevant alerts
- Effective integration of AI to enhance detection and analysis capabilities
- The ability to ingest and correlate data from a very wide range of platforms, environments, security tools, and network devices
- Technology to identify and eliminate duplicate alerts for the same event
- Intelligence that adapts to new threats without the need for analysts to continually create and tune complex detection and response rules
- Processes to automatically respond to simple threats (e.g., isolating compromised endpoints and identities) without human intervention

Operational Impact

One large pharmaceutical customer stated that the Zscaler MDR solution allowed his organization to replace a team of 20 contractors performing tier 1 triage with an in-house team of four.

(Estimates of the financial savings from reducing the number of false positives is included in the "Financial impacts" section later in this report.)

KEY TAKEAWAY

With an MDR service, the average organization is experiencing a **72% reduction in alerts** triaged and investigated weekly.

Comments from Zscaler MDR Customers

> Switching over to Zscaler MDR helped us reduce the number of incidents we investigate each week significantly. Now we're focusing strictly on what is deemed a threat. It's been great."

> Not having to investigate false positives is one of the biggest benefits for sure. That's how you can run a really small internal team, because so much of that work is done for you."

> The manager of my SOC team has said…'Now I don't have to check a lot of work. When Zscaler MDR says it's real, it's real.'"

©2026 Zscaler, Inc. All rights reserved.

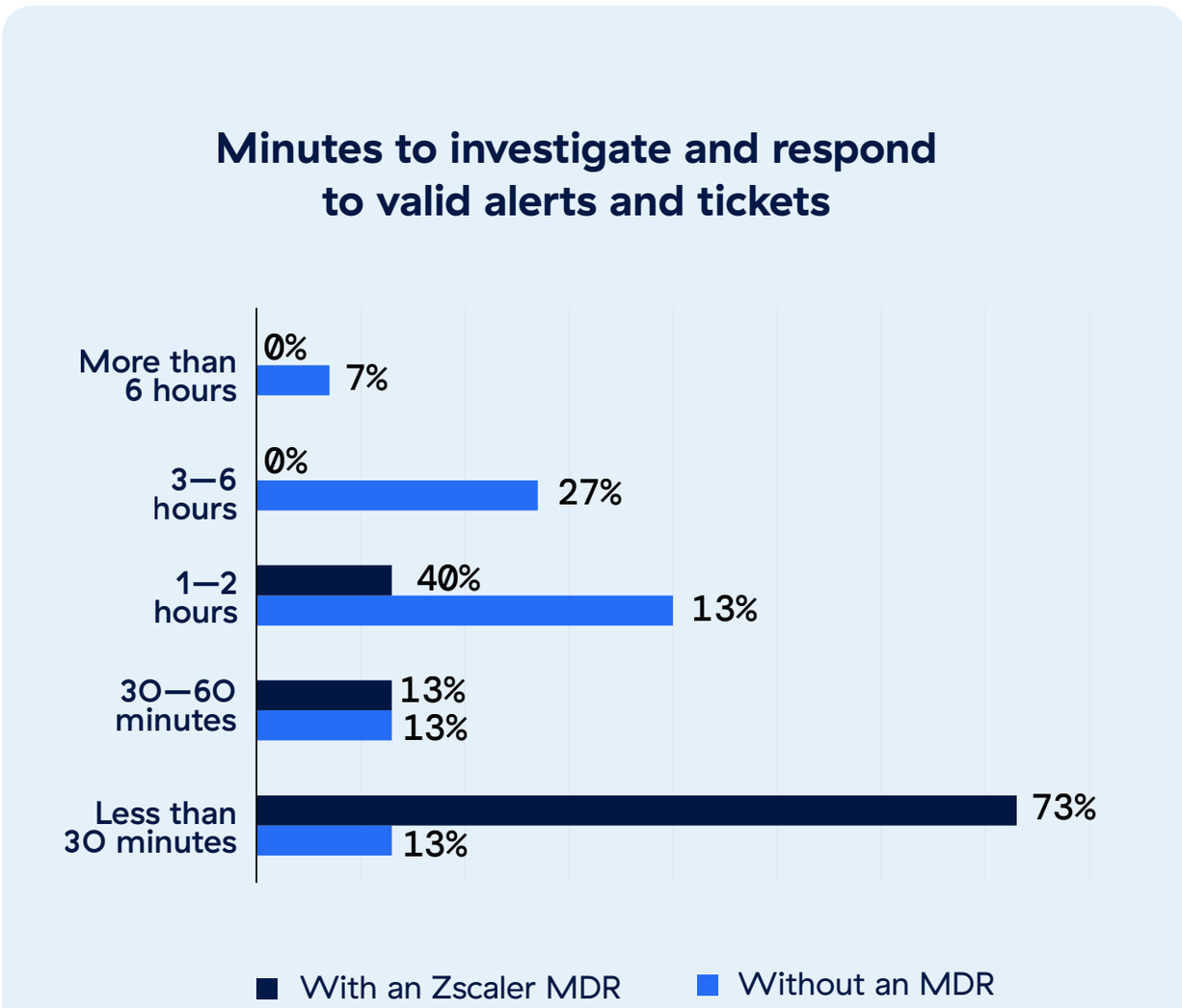
Reduction in Time to Investigate Alerts

Automating Manual Work

Investigating alerts can be an extremely tiring and time-consuming assignment. Senior SOC analysts and incident responders can spend hours on activities such as:

- Gathering context about the indicator of compromise (IOC) or vulnerability highlighted in the alert or incident ticket, such as the location and time of its detection and user accounts associated with it
- Searching logs to find if the same indicators have been seen in other systems or applications
- Creating a timeline of events prior to and after the initial detection that may be part of a related attack or campaign
- Checking vulnerability databases and other sources of threat intelligence to determine the nature and criticality of the threat
- If possible, identifying the threat actors behind the attack and learning about their tactics, techniques, and procedures (TTPs)
- Formulating plans to contain the attack
- Notifying stakeholders of the attack so they can take appropriate measures

With Zscaler MDR, the average organization reduced the time to **investigate each alert by 81%**.



How Much Faster Can You Investigate Alerts with MDR?

MDR services not only filter out false positive alerts and incident tickets, they also dramatically reduce the time required to investigate and respond to valid alerts.

The survey respondents estimated that without an MDR service their security teams would spend an average of 144 minutes (almost two and a half hours) investigating each alert or ticket. With Zscaler MDR, the average organization reduced the time to investigate each alert by 81%.

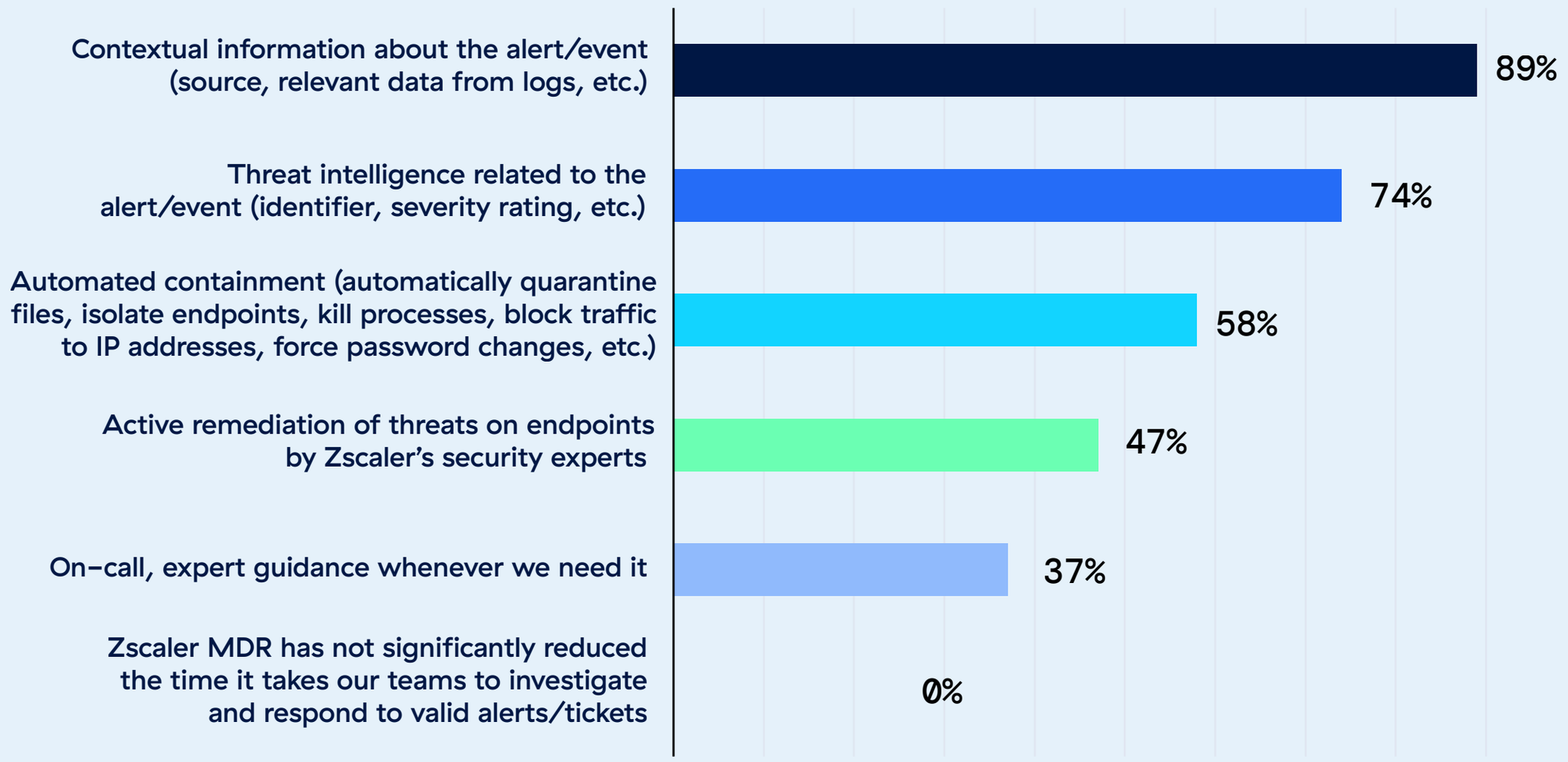
Figure 2 illustrates the impact of that reduction. About a third of survey participants (34%) estimated that without MDR, each investigation would require three hours or more. Another 40% require one-to-two hours. In contrast, with Zscaler MDR, 73% average less than 30 minutes to investigate each alert, and only 13% average more than one hour.

©2026 Zscaler, Inc. All rights reserved.

Capabilities That Reduce Investigation Times

We asked survey participants to select MDR capabilities that have significantly reduced the time it takes for their teams to investigate and respond to valid alerts and tickets. Their responses are shown in Figure 3.

Capabilities that have significantly reduced time to investigate and respond to valid alerts



Eighty-nine percent of survey participants highlighted the value of the contextual information Zscaler MDR provides, saving analysts time scanning networks, searching logs, and performing other time-consuming activities required to understand the scope of potential attacks.

About three-quarters pointed to time saved from not having to scour threat feeds, vulnerability databases, and threat intelligence blogs to attribute attacks to threat actors and learn about their TTPs. In addition, 58% cited the value of automatically blocking malicious activities in the early stages of attack.

89% of survey participants highlighted the value of the contextual information Zscaler MDR provides.

©2026 Zscaler, Inc. All rights reserved.

Comments from Zscaler MDR Customers

> It's almost like it's a senior person telling our junior people, 'You should look at this, and here are all the things you need to know.' We are getting an incredible advantage."

> The platform's output is like a paralegal prepping a file for a lawyer."

> There's AI built into the platform. It generates a lot of stuff the Zscaler MDR analysts can already have, and then their analysts add to that, and by the time it gets to us there is so much in there that our team pretty much knows exactly where to go to, instead of us having to research and figure out what's what."

For most of the organizations in our survey, the total **annual savings fell between $50,000 and $1.8 million**.

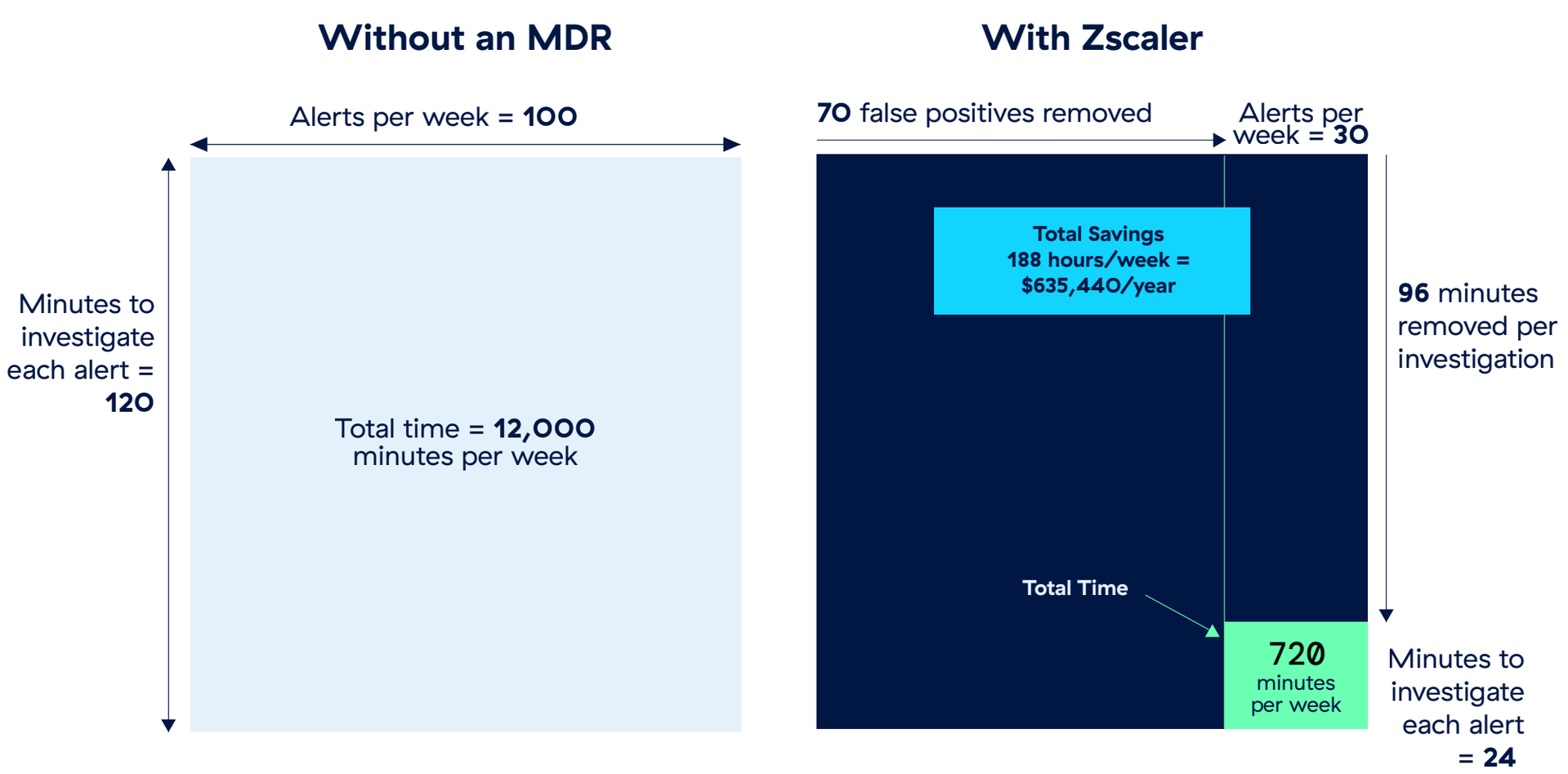
Financial Impacts

MDR Service Savings in Dollars

So far in this report we have been describing survey results in terms of minutes saved by reducing the volume of false positive alerts and shortening the time required to investigate and respond to valid alerts. By making a few reasonable assumptions, we can translate those estimates into dollars (and other currencies). We can also help you visualize the savings with a simple diagram and estimate potential savings for your organization.

Figure 4 illustrates how the estimates we have been talking about so far can be calculated based on a few simple inputs, which are described in the appendix. This calculation uses $65 as the fully loaded cost of an hour of a security analyst's time. All cost estimates are in U.S. dollars.

The total area of the rectangle on the left side of Figure 4 represents the time security teams at one organization spend investigating and responding to alerts: 100 alerts per week times 120 minutes per alert, equaling 12,000 minutes a week.



©2026 Zscaler, Inc. All rights reserved.

The rectangle on the right side of Figure 4 shows the time this organization would save with Zscaler. It is divided into three sections:

a. The time this organization saves with an MDR service by not having to spend any time investigating false positive alerts (the left half of the rectangle)

b. The total time an MDR service saves investigating and responding to valid alerts (the upper right corner)

c. The time needed with Zscaler to investigate and respond to valid alerts (the lower right corner)

The total savings from using the MDR service are listed in the blue box. The equations used to calculate those savings are described in the appendix.

For most of the organizations in our survey, the total annual savings fell between $50,000 and $1.8 million. To do a calculation for your own organization, see the equations in the appendix.

Economical and Effective After-Hours SOC Augmentation

Quantifiable Savings on 24x7 Staffing

Using MDR services for after-hours security coverage is not an issue for organizations that already have full-time 24x7 staffing. However, a few customers stressed that MDR services can provide excellent security at a far lower cost for organizations currently looking to add after-hours coverage and SOC augmentation.

For example, one survey respondent commented that going to 24x7 coverage would require his organization to add four or five full-time equivalents (FTEs). A CISO estimated that if he needed to staff a third shift, he would probably have to hire eight team members with salaries in the $150,000 range. Another CISO, working at a large global company that already has 24x7 coverage, estimated that an MDR service might have been able to save them from having to hire 13—14 SOC analysts and managers.

MDR Service Support for 24x7 Coverage

Figure 5 demonstrates how an MDR service can play supporting as well as starring roles in after-hours security.

Of the organizations in the survey, 32% rely primarily on Zscaler MDR for after-hours coverage. Almost two-thirds (63%) have members of their own security teams on call. However, most of those make frequent use of Zscaler MDR services to support them.

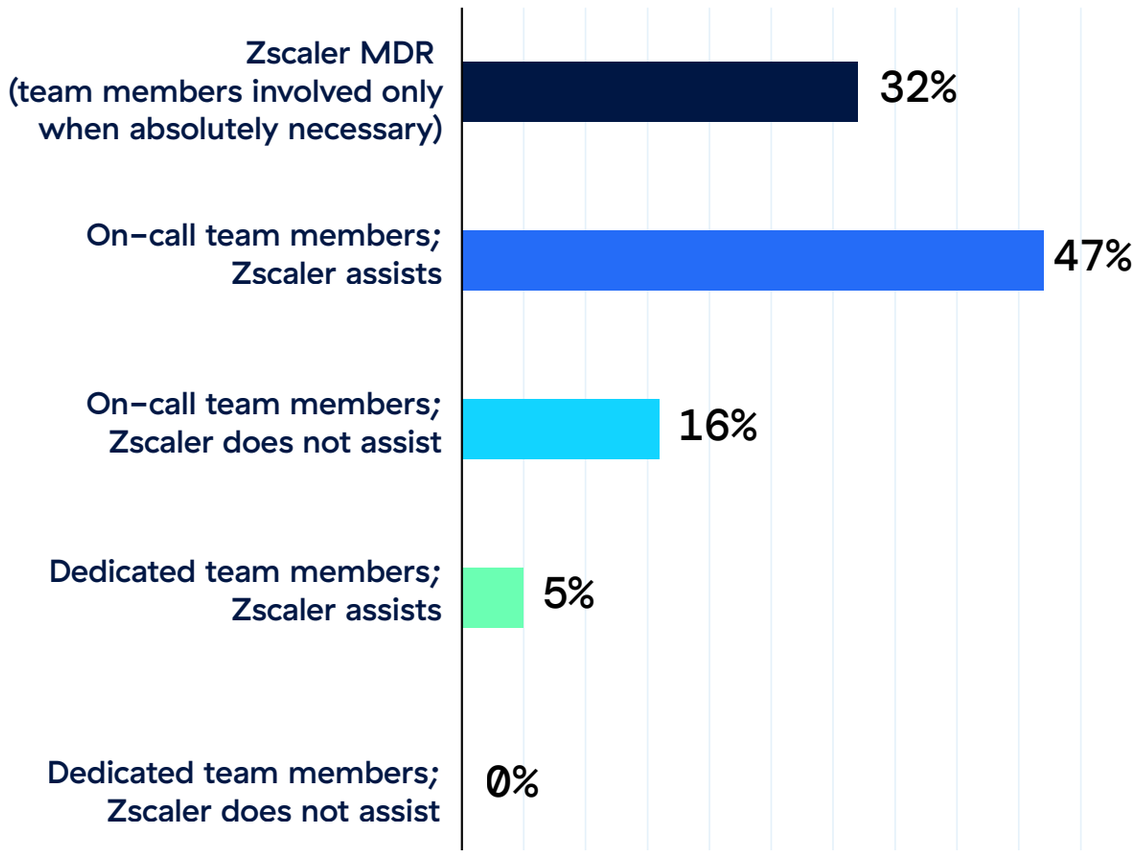
©2026 Zscaler, Inc. All rights reserved.

Comments from Zscaler Customers

> There is the sleep at night kind of thing, the 24x7 coverage. I don't have to worry about my one or two guys catching something in the middle of the night."

> I'm a huge believer in having the kind of hybrid setup where you have a small cyber team and Zscaler MDR does all that 24x7 coverage with all their people in the seats."

Who monitors and investigate alerts and events after business hours?

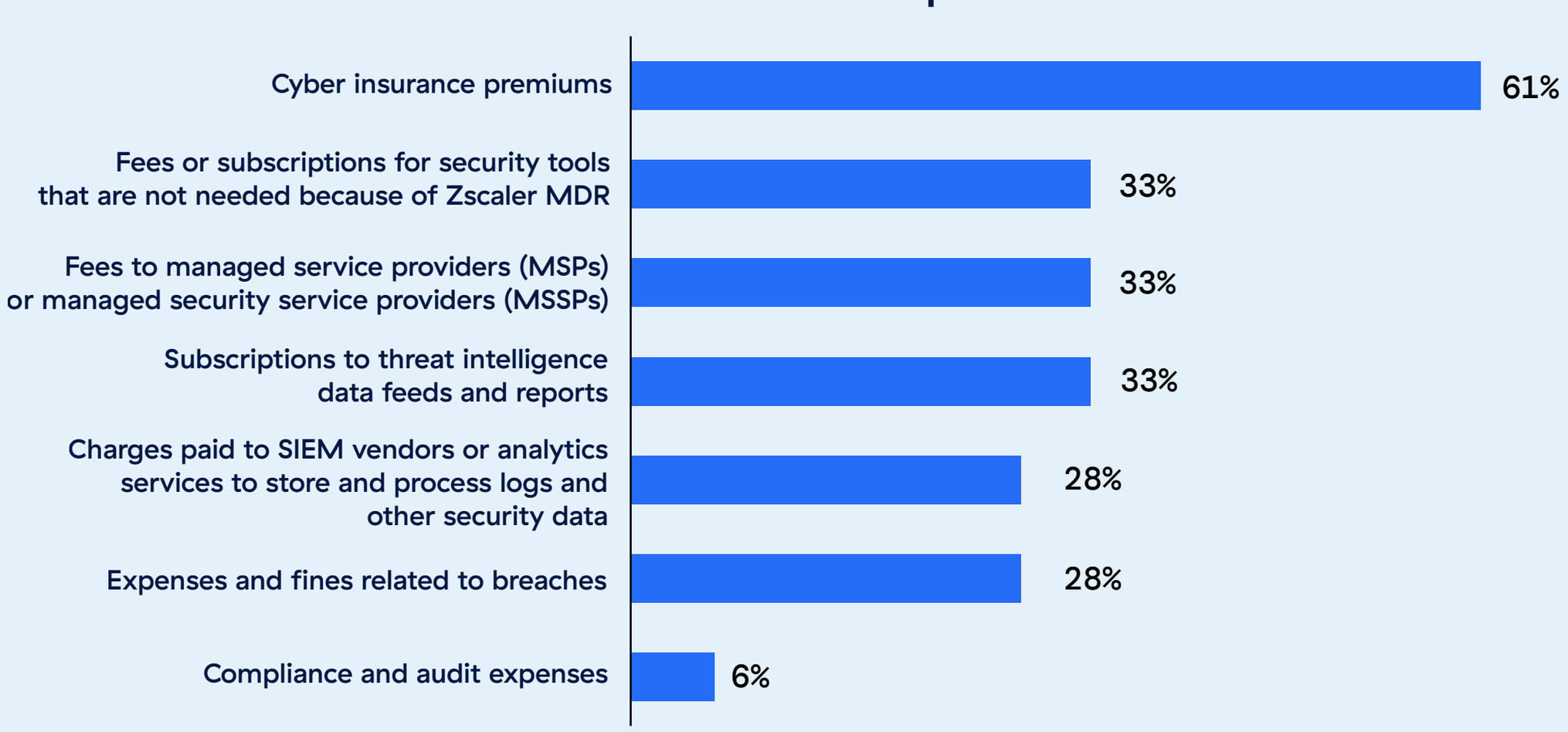


Other Opportunities to Reduce Expenses

MDR Services and Cyber Insurance

Until now this report has focused on freeing cybersecurity professionals from time-consuming threat detection and response tasks so they can provide value in other ways. But most organizations are finding additional opportunities to reduce expenses with MDR services, as shown in Figure 6.

Areas where Zscaler MDR services allowed organizations to reduce or avoid expenses



©2026 Zscaler, Inc. All rights reserved.

The most striking insight from this data is that a majority of organizations are finding that an MDR service reduces their cyber insurance premiums. This is because cyber insurance underwriters look favorably on organizations that are deploying leading-edge security tools and can demonstrate reliable 24x7 monitoring and response capabilities.

Consolidating Security Tools and Service Providers

Some organizations have found significant savings by cutting back subscriptions for duplicative detection and threat hunting tools, terminating contracts with MSPs and MSSPs that did not perform as well as Zscaler MDR, and controlling skyrocketing costs for storing security log data.

In fact, a few customers pointed to savings from these areas that totaled approximately $40, $70, and $83 per employee of the organization. One security executive stated, "We don't have to send all of our EDR telemetry to our SIEM because of Zscaler MDR."

Partnering with Cybersecurity Experts

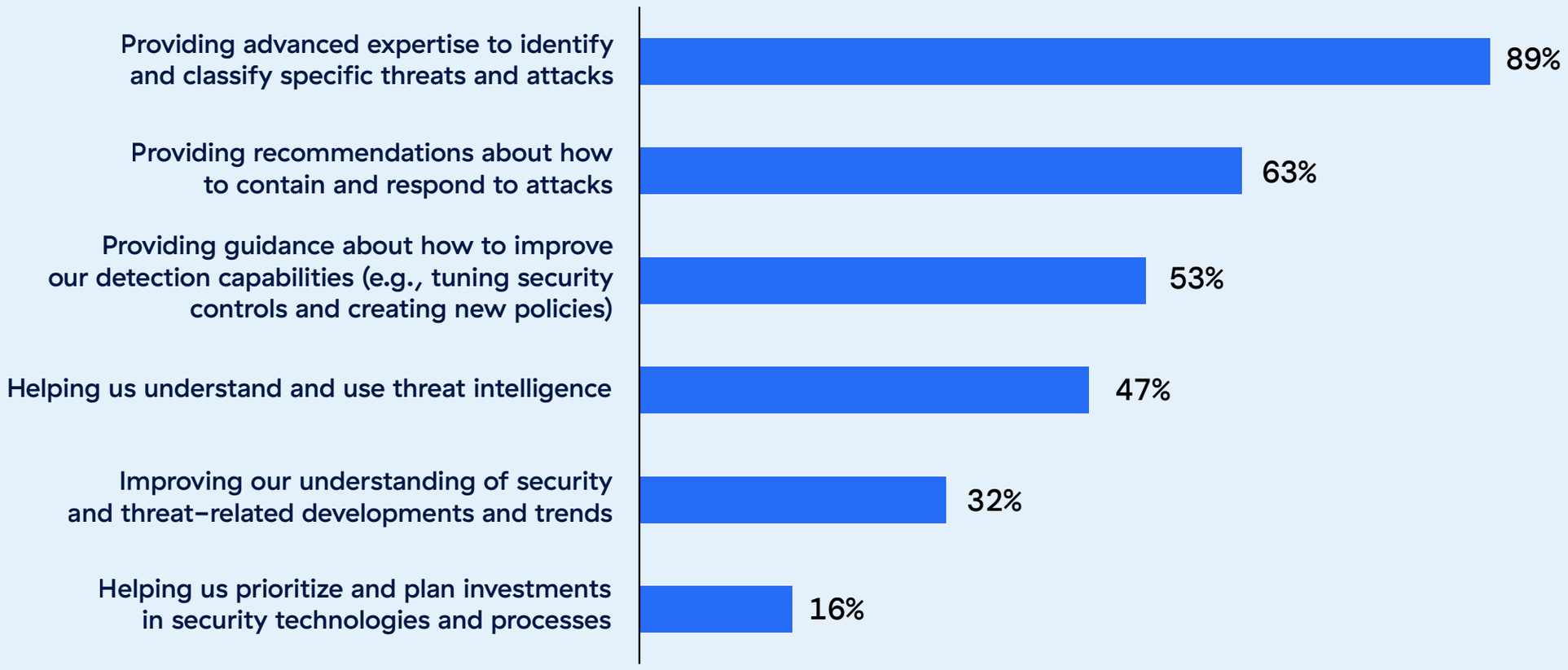
Advanced Expertise Is a Major Selling Point for MDR Services

The Zscaler MDR customers surveyed were almost unanimous in highlighting the tremendous value of the advanced expertise provided as part of Zscaler MDR services. Figure 7 shows the many ways organizations are leveraging that expertise.

One finding from this survey question is that almost all of the customers rely on Zscaler's experts for help analyzing and responding quickly to ongoing attacks. In addition, there is significant demand for medium-term objectives (improving detection and how to use threat intelligence) and long-term planning (understanding security and threat-related trends and prioritizing security investments).

89% of customers cite Zscaler's advanced threat detection expertise.

How customers are taking advantage of Zscaler experts



©2026 Zscaler, Inc. All rights reserved.

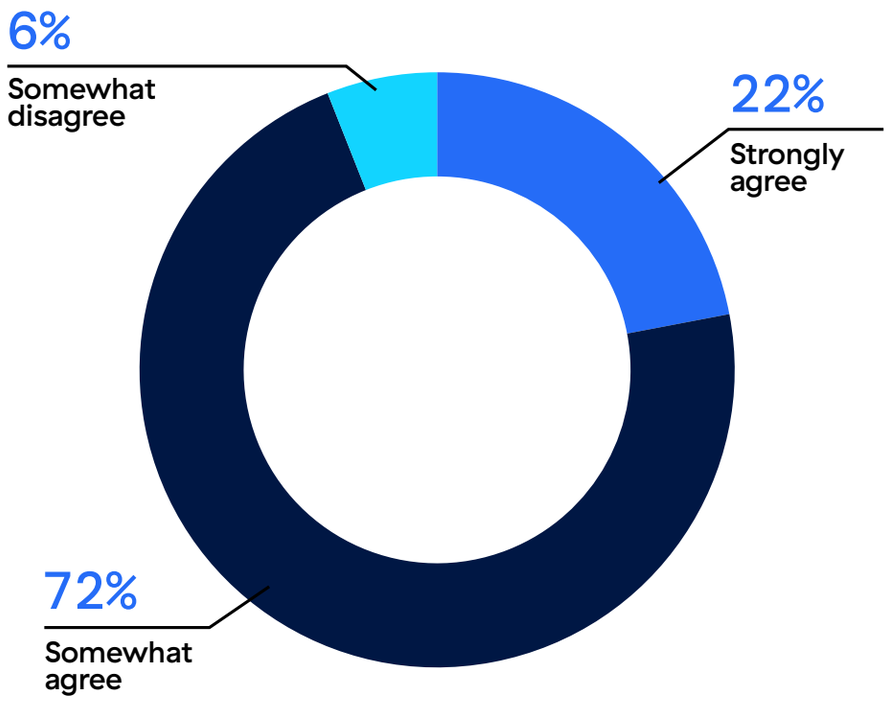
> “Zscaler MDR people are always top-notch. I have tried and fired almost every MSSP you can imagine, usually because of the uneven quality of the people. However, I have never had a weak analyst with Zscaler MDR.”

Team Performance and Security Posture

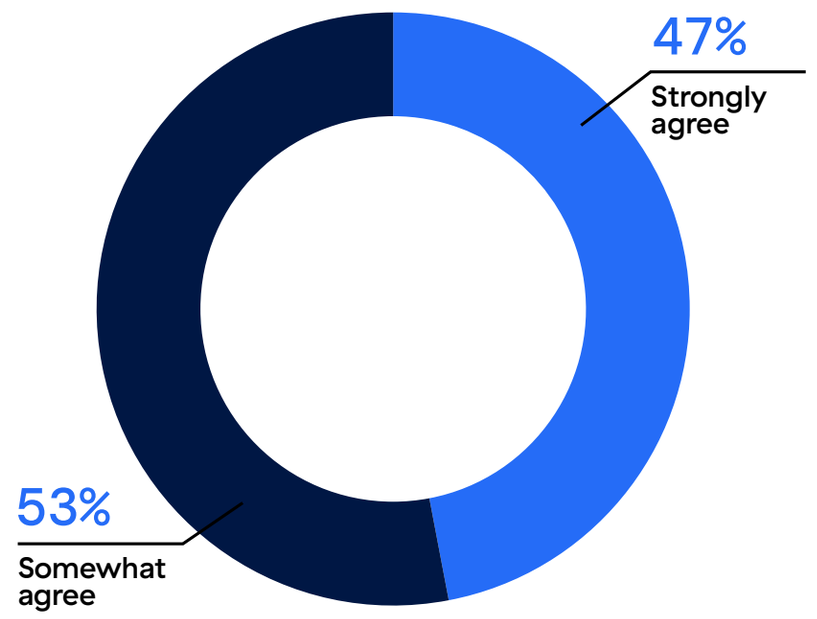
Supporting Junior and Senior Security Talent

There was also wide agreement among survey participants that MDR services can support and educate junior security team members (Figure 8) and enable senior security team members to focus on analytical and strategic tasks appropriate for their skill levels (Figure 9).

Zscaler MDR services and support enable junior security team members to operate at a much higher level of effectiveness



Zscaler services enable senior security team members to avoid repetitive routine tasks and focus on analysis and strategy



Comments from Zscaler MDR Customers

> “I feel like the team operates a lot better and more focused, more methodical with an advanced MDR service…They’re operating more effectively…They have more ownership of the tickets coming in.”

> “Best-in-class cybersecurity people like to feel they are working with the best technology.”

©2026 Zscaler, Inc. All rights reserved.

Enhancing Security & Retaining Key Team Members

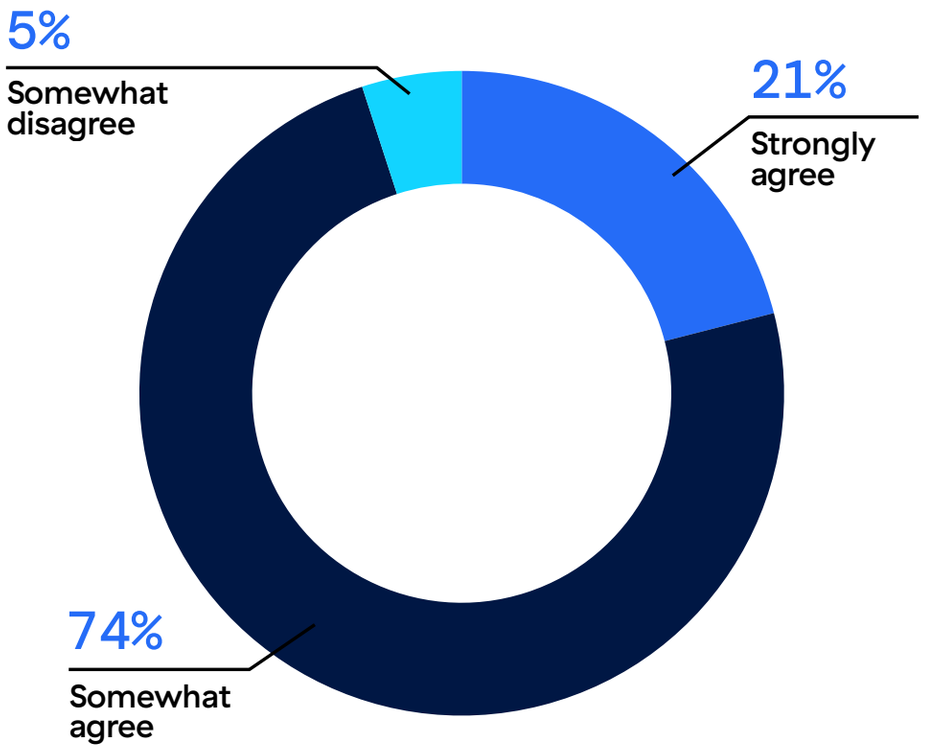
Enhancing Security

This report focuses on how MDR services provide financial and operational benefits. But they also have a positive effect on organizations' security postures, as shown in Figure 10. Ninety-five percent of survey respondents agree that MDR services provide unique threat detection capabilities.

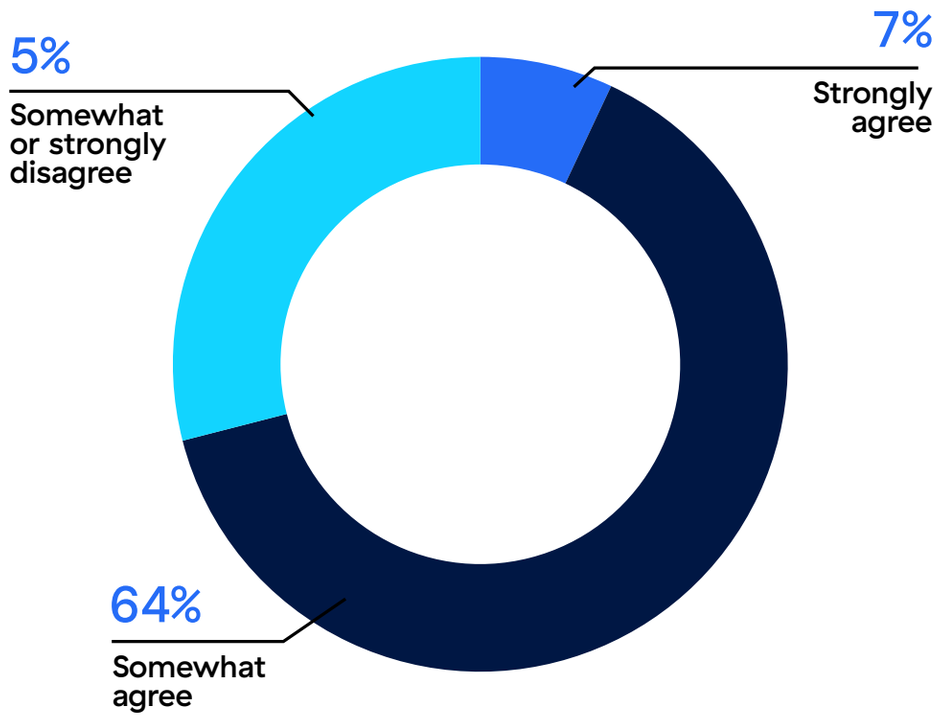
Retaining Key Cybersecurity Team Members

One of the toughest challenges in cybersecurity today is recruiting and retaining experienced team members. As shown in Figure 11, 71% of the survey participants believe that advanced MDR services help motivate cybersecurity professionals to join or stay with organizations.

Zscaler MDR routinely identifies threats that none of our other security tools detect



Zscaler helps us recruit and retain security team members because they value working with world-class technology.



Comments from Zscaler MDR Customers

> I don't have to sit there and watch all day long, because I know I have Zscaler MDR behind me that's on it...Also, if we find something internally, I've got this huge team that I can just call and say 'hey, let's look at this,' and they are there to do it, because we're partners."

> Every big company should look at Zscaler MDR. It can automate 80% of operations and offload the bottom 80% of threat alerts."

Conclusion

This study underscores the substantial financial and operational advantages Zscaler MDR delivers to organizations. It reduces alert volume by an average of 72% and accelerates investigations by 81%. In addition, the service enhances overall security effectiveness, facilitates tool consolidation, reduces cyber insurance premiums and other direct expenses, and strengthens organizational resilience. Finally, Zscaler MDR's expert analysts make the company a valuable partner in achieving long-term cybersecurity success.

©2026 Zscaler, Inc. All rights reserved.

Appendix: Calculations of Financial Impact

This appendix describes the calculations and diagrams used to quantify the monetary benefits of MDR services presented in the financial impact of the report. It also shows how you can make the same calculations for your organization.

1. TIME TO INVESTIGATE ALERTS WITHOUT AN MDR

The time to triage and investigate alerts without an MDR in a typical week is simply:

Estimated alerts investigated per week×average number of minutes to investigate an alert

For a typical organization like the one described in the financial impacts section, that can be represented as the width and height of the rectangles in Figure 4:

100×120=12,000 minutes per week

2. TIME SAVED ON ALERTS THAT DON'T NEED TO BE INVESTIGATED

Based on the survey data described in the reduction in false positives section of the report, a typical organization using Zscaler MDR services can reduce the number of false positives they investigate by 70%. Therefore, the number of minutes saved by not needing to investigate those false positives would be:

(100 alerts×0.7)×120 minutes=70×120=8,400 minutes

(That number is represented by the left side of the rectangle in Figure 4.)

3. TIME SAVED INVESTIGATING VALID ALERTS

Based on the survey data described in the reduction in time to investigate alerts section of the report, a typical organization using Zscaler MDR services can reduce the average investigation time for each valid alert by 80%. The savings might be:

(100 alerts×0.3)×(120 minutes×0.8)=30×96=2,880 minutes

(That number is represented by the upper right section of the rectangle in Figure 4.)

4. CONVERTING THE SAVINGS FROM MINUTES INTO DOLLARS

Based on the figures above, the total savings for the organization would be:

8,400+2,880=11,280 minutes saved per week

To convert that to an annual cost, divide that number by 60 to get hours saved per week, multiply by the cost per hour to get savings per week, and multiply that by 52 to get savings per year.

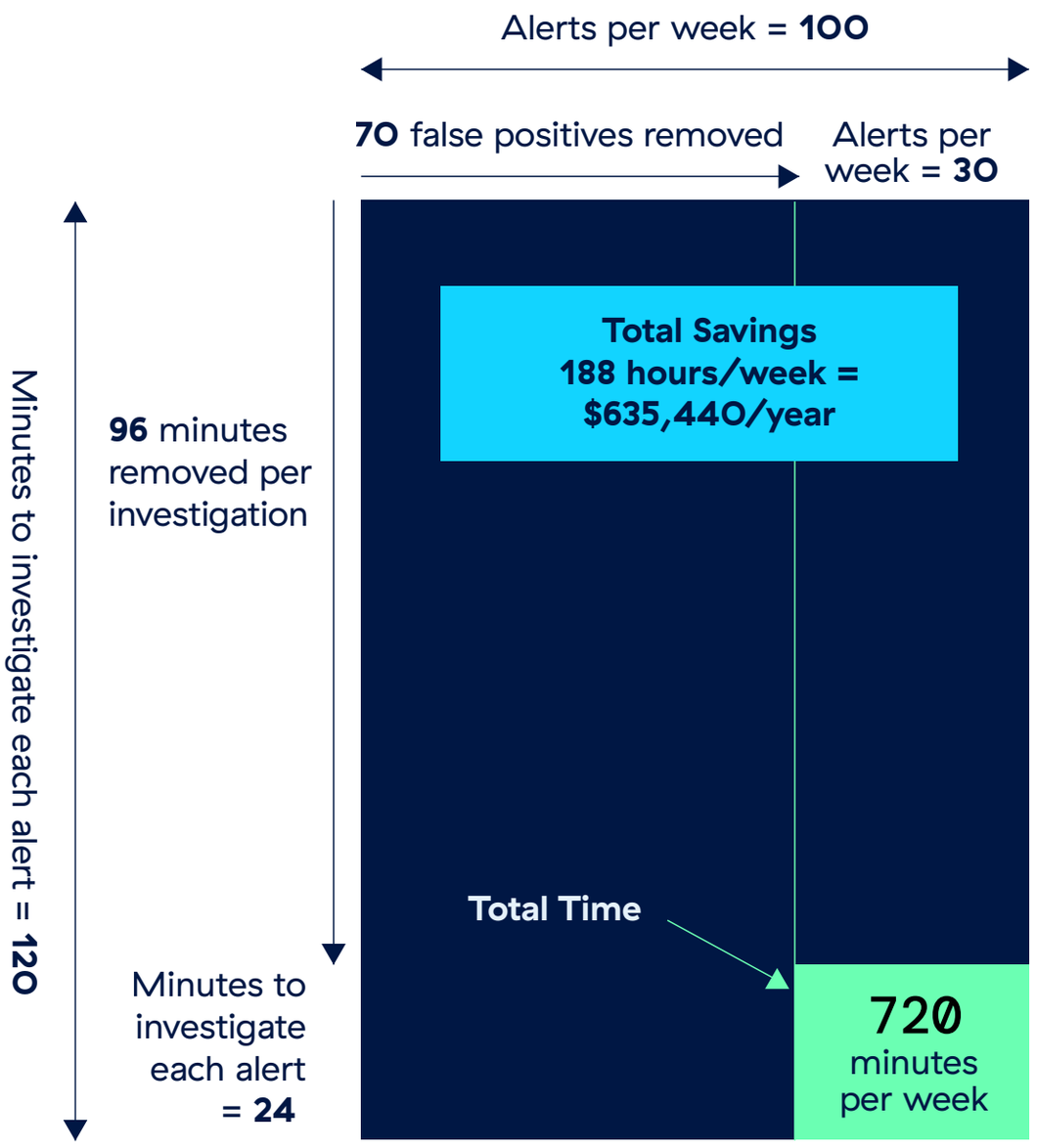
©2026 Zscaler, Inc. All rights reserved.

IF WE USE $65 PER HOUR AS THE COST*, THE EQUATION IS:

6011,280=188 hours per week

$188 hours×$65 per hour=
$12,220 savings per week$

$12,220×52=$635,440
savings per year



*Note on hourly rate: $65/hour is roughly equivalent to total compensation of $136,000 per year ($65/hour × 40 hours/week × 52 weeks/year). The Glassdoor website reports the median total pay for cybersecurity roles as $136,000/year (as of November 2025). e https://www.glassdoor.com/Salaries/cyber-security-salary-SRCH_KO0,14.htm.

See Zscaler MDR in Action

GET A DEMO

AimPoint Group
high-impact marketing

About AimPoint Group

AimPoint Group (APG) provides expert content and fractional marketing support for the world's leading cybersecurity companies. With decades of technology marketing, research, and writing experience, APG is committed to exceeding expectations and creating customer delight. For more information, visit the company's website at aimpointgroup.com.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

**Act Fast.
Stay Secure.**