FORRESTER®

Wise XDR Choices Lead To More Benefits Than Expected

Selecting The Right XDR Solution Positions Firms For Accelerated Security And More

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY SECUREWORKS | JUNE 2022

XDR Is Changing The IT Security Landscape

Cybersecurity environments are becoming increasingly complex and security teams are navigating a multitude of security threats.[1] Security operations centers (SOCs) must adapt strategically and modernize technology foundations to repel these evolving dangers. Firms require greater visibility across enterprise networks, identity, endpoints, and the cloud to detect and prevent cybersecurity threats to aid the business and improve customer experience.

Extended detection and response (XDR) technology provides this and more, powered by machine learning, analytics, and automation. However, many IT and security professionals need to be made aware of the benefits of XDR.

Secureworks commissioned Forrester Consulting to survey 406 security strategy decision-makers with insights into security solutions to explore this market.

Key Findings

XDR is top of mind for firms. Though not widely used yet, XDR technology is the top solution decision-makers plan to implement over the next year.

Companies know they need to keep pace. Security threats are increasingly complex and overwhelming, which burdens operations teams, weakens efficiency, and risks company security.

XDR benefits exceed expectations. XDR provides more value than anticipated for users, including better threat investigation, prioritization, and overall response, improving company risk and customer trust.

Overview
Situation
Challenges
Opportunity
Conclusion

Firms Are Prioritizing XDR Solutions

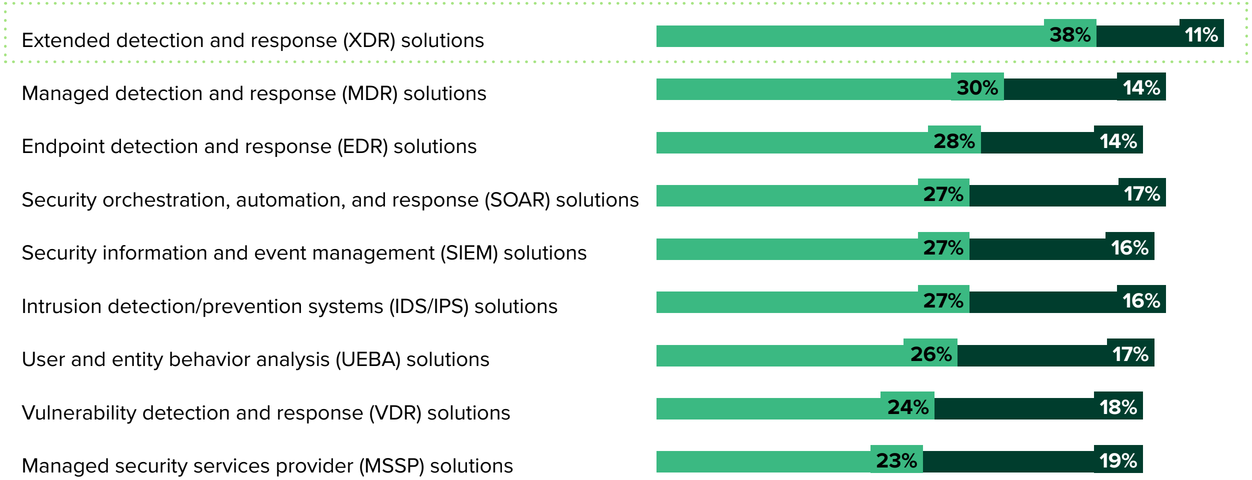
As cyberthreats proliferate, decision-makers are turning to XDR solutions. Respondents said XDR solutions (30%) are the top security priority for their organizations over the next 12 months.

Decision-makers are ready to back this priority with action. Though many haven't implemented XDR technology yet, respondents ranked XDR solutions as the top tool or service that they plan to implement in the next 12 months. Additionally, six in 10 (60%) of respondents noted their organizations plan to either implement or further expand their usage of XDR over the next 12 months.

XDR technology is the top security priority for firms over the next 12 months.

"Which of the following security operations tools or services is your organization currently evaluating/using?"

- ● Planning to implement in the next 12 months
- ● Interested, but no plans to implement



Base: 406 security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Secureworks, April 2022

Overview
Situation
Challenges
Opportunity
Conclusion

Decision-Makers Seek An Integrated XDR Partner

The evolution toward XDR comes as organizations seek more effective security, faster workflows, and better incident management. Thirty-nine percent of respondents considered or are currently considering XDR solutions to improve the speed and accuracy of their organizations' threat detection. Meanwhile, 35% said a need for faster incident and event response workflows is a key driver for consideration.

Once procured, nearly three in four (73%) decision-makers want XDR providers to be involved and integrated as a service into their security operations in some way. This shows that firms, especially smaller ones, need help from XDR providers. It also signals that XDR solutions with an integrated service may replace other service offerings like managed security services providers (MSSPs).

"What is driving or has driven your organization to consider using an XDR solution?"

39%
Improved speed/accuracy of threat detection

35%
More effective security with better incident management

29%
Optimizing existing security toolsets

32%
Need for better security visibility across our entire IT infrastructure

27%
Improving productivity of existing security staff

35%
Need for faster incident/event response workflows

29%
We've heard that XDR has benefits from peers/competitors in the industry.

26%
Consolidation of security tools

Base: 352 security strategy decision-makers, that are planning to implement, expand or upgrade XDR
Source: A commissioned study conducted by Forrester Consulting on behalf of Secureworks, April 2022

A Multitude Of Challenges Offer XDR Opportunities

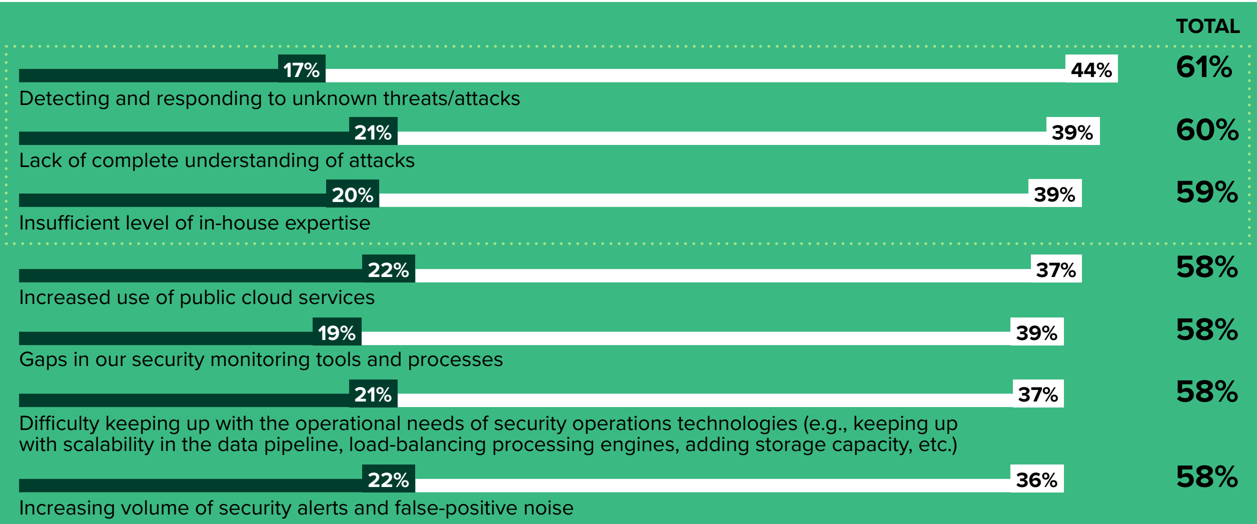
Firms face many security challenges including detecting and responding to unknown threats and attacks. Respondents said a lack of complete understanding of attacks (60%) and an insufficient level of in-house expertise (59%) are hampering security within their organizations.

Further, nearly one-quarter of decision-makers (23%) said security operations rely on a significant number of manual processes, which leads to scalability issues. This signals a need for more automation and efficient operations as firms with manual processes find themselves crunched for time and short on the skills required to do the job.

“How challenging are the following security issues for your organization?”

● Very challenging

○ Challenging



Base: 406 security strategy decision-makers
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Secureworks, April 202

Overview
Situation
Challenges
Opportunity
Conclusion

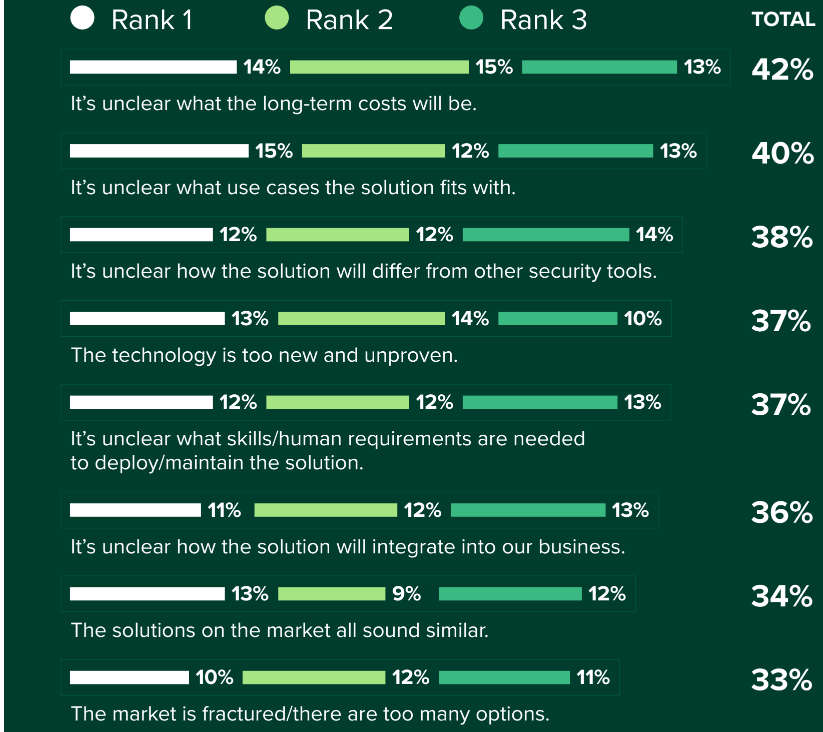
Choosing Security Solutions Means Addressing Tough Questions

Though solutions exist to combat the myriad challenges firms face, justifying spend on security providers (e.g., vendors of MDR, XDR, SIEM) can prove an additional hurdle. Respondents said a lack of clarity around long-term costs (42%) and the use cases the solution fits with (40%) ranked as one of their top three challenges when justifying provider value. The many pricing models on the market contribute to these hurdles, adding to uncertainty over long-term costs and to the novelty of the technology that's still in its infant stages.

For 38% of decision-makers, it isn't clear how the solution will differ from other security tools on the market. They naturally question why they should update their security stack when solutions sound similar to one another and day-to-day activities already take up so much of their time.

CONSIDER SECURITY THREAT SOLUTION PROVIDERS (E.G., VENDORS OF MDR, XDR, SIEM).

"Which of the following considerations make it challenging to justify spend on such providers?"



Base: 406 security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Secureworks, April 2022

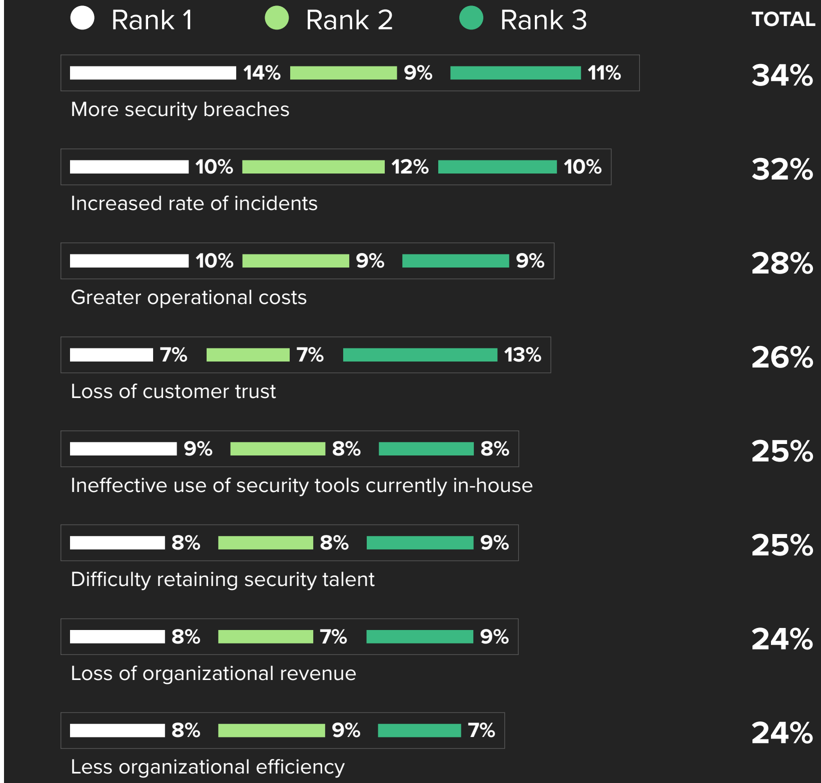
Overview
Situation
Challenges
Opportunity
Conclusion

Getting Security Solutions Wrong Increases Risk And Impacts Customer Trust

The top consequences of failing to implement the right security solutions are both critical and extensive. Decision-makers noted more security breaches and an increased rate of incidents as the top consequences, which can be the result of siloed solutions and poor management of a far-reaching attack surface.

Additionally, 28% ranked greater operational costs as a top consequence of failing to implement the right security threat solution, while one in four said a loss of customer trust (26%) and ineffective use of security tools in-house (25%) also ranked as top consequences.

"What do you envision are the consequences of not implementing the right security threat solutions at your organization?"



Base: 406 security strategy decision-makers
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Secureworks, April 2022

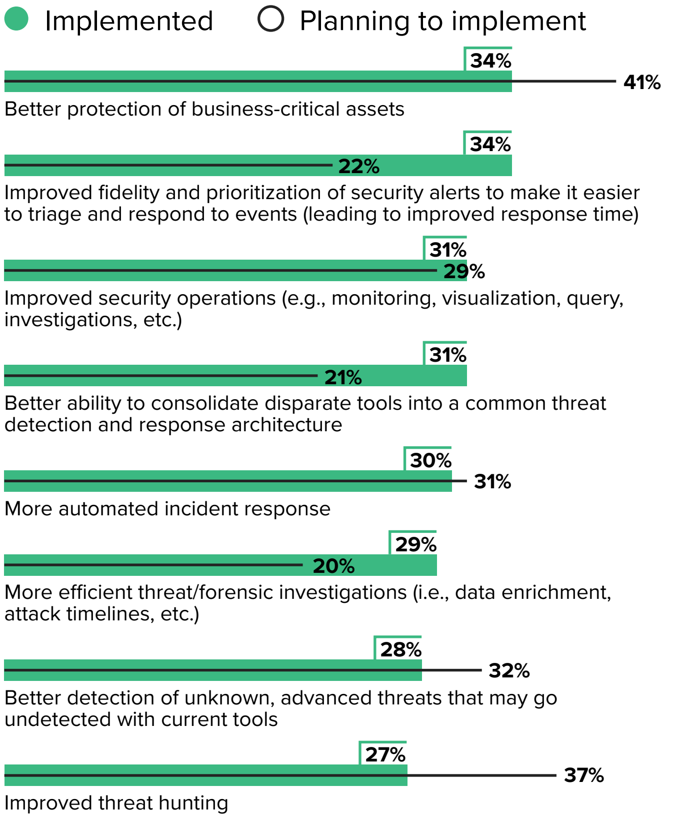
Benefits From XDR Go Beyond The Expected

Decision-makers anticipated the benefits of XDR to include better protection of critical assets and improved threat hunting. However, expectations around XDR benefits vary depending on experience. This reveals a knowledge gap between the true value that XDR offers and how it differs from other tools.

Those planning to implement XDR expect more benefits related to threat hunting, protection, and detection. Yet those who have already implemented XDR find they have better threat response than expected (e.g., improved fidelity and prioritization of security alerts, better ability to consolidate disparate tools, more efficient investigations). Experienced users signal that XDR solutions go beyond the expected toward improving visibility and measurement, reducing alert fatigue, enhancing automated processes, and decreasing response time within their organizations.

> “[XDR] helps analysts avoid risk by speeding up the investigation procedure.”
>
> **C-level executive, US**

“What do you anticipate the benefits are of implementing XDR solutions at your organization?”



Base: 397 security strategy decision-makers, who are implementing or plan to implement.
Source: A commissioned study conducted by Forrester Consulting on behalf of Secureworks, April 2022

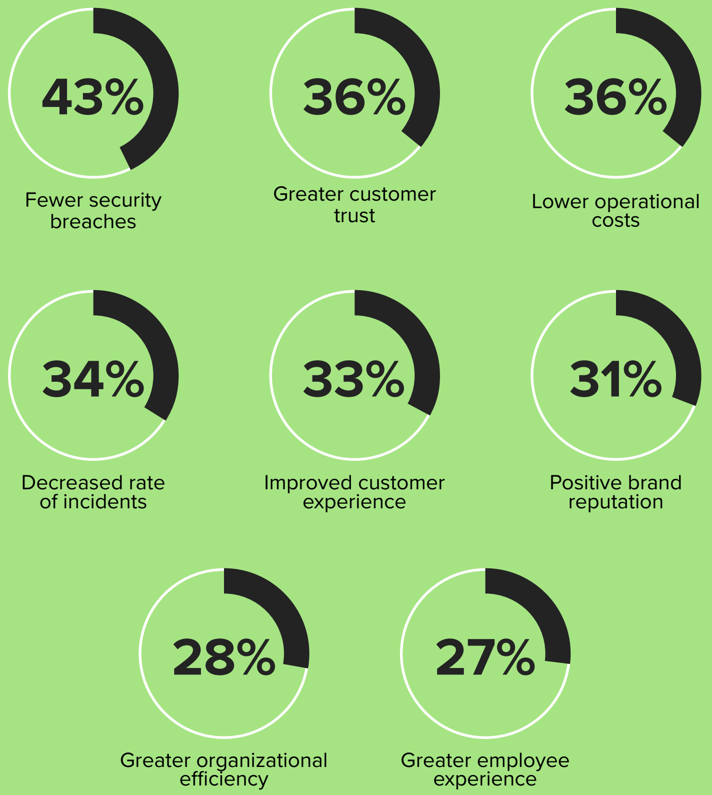
XDR Lowers Risk, Improves Customer Trust, And Strengthens Security

Firms have much to gain by improving their security operation solutions. From implementing XDR, surveyed decision-makers envisioned fewer security breaches and incidents. Thirty-six percent of respondents also expect greater customer trust, due to safer interactions and customer experiences.

Finally, more than one in three (36%) respondents expected lower operational costs from implementing XDR solutions. Shifting toward XDR will take away costs currently going toward other solutions, while additional costs may decrease given reduced workloads and the better use of employee time amidst ongoing labor shortages.

> “[XDR is] cyber-threat management without increasing staff.”
>
> **Vice president, Canada**

“What do you envision are the outcomes of XDR benefits?”



Base: 406 security strategy decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Secureworks, April 2022

Overview
Situation
Challenges
Opportunity
Conclusion

Conclusion

To lower risk and drive better customer outcomes, firms must continue modernizing their security solutions. Decision-makers adapting to the evolving nature of threats will prioritize XDR solutions that:

- Improve speed and accuracy of threat detection and offer faster incident and event-response workflows. XDR will be tasked to reduce manual time and effort, increase automation capabilities, and provide greater visibility of threats.
- Integrate XDR providers who can guide, support, and bolster company security operations for fewer siloed solutions and better risk management now as well as in the future.
- Reduce risk and improve customer trust. XDR offers greater understanding of the firm's security landscape and improved threat response, ultimately benefitting both the organization and the customer experience.

Project Director:

Jason Daniels,
Market Impact Consultant

Contributing Research:

Forrester's Security & Risk research group

Overview
Situation
Challenges
Opportunity
Conclusion

Methodology

This Opportunity Snapshot was commissioned by Secureworks. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 406 security strategy decision-makers. The custom survey began in March 2022 and was completed in April 2022.

ENDNOTES

[1] Source: March 30, 2022, "The State Of The XDR Market," Webinar (https://www.forrester.com/webinar/The+State+Of+The+XDR+Market/WEB37782).

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Demographics

COUNTRIES	
United States (44%)	**44%**
Canada (30%)	**30%**
United Kingdom (26%)	**26%**

COMPANY SIZE (EMPLOYEES)	
5,000 to 19,999	**28%**
1,000 to 4,999	**50%**
500 to 999	**22%**

TOP 4 INDUSTRIES	
Technology	**10%**
Healthcare	**9%**
Agriculture/food	**8%**
Retail	**7%**

RESPONDENT LEVEL	
C-level	**14%**
Vice president	**47%**
Director	**31%**
Manager	**8%**

FORRESTER®