
# XDR: Redefining the future of cybersecurity

New survey highlights key SecOps challenges—and how to overcome them

The threat landscape is always expanding and evolving. But many organizations still rely on disconnected and inefficient security solutions to protect from dynamic attacks.

That was one of the key takeaways in our latest research. To find out more about the present and future of cybersecurity, we partnered with Coleman Parkes Research to survey 9,000 security professionals across 15 countries.

Our respondents included a range of experts, from CISOs and SOC managers to security analysts and engineers. They work for organizations of various sizes—from small and midsize businesses to large enterprises. And they cover many industries, including manufacturing, financial services, healthcare, and more.

What they told us was eye-opening. Our research highlighted just how much companies are struggling to keep up with threat actors that never stop evolving. And it points to a future of security that's moving away from disjointed solutions toward **extended detection and response (XDR), a single intelligent and integrated ecosystem that's always learning and adapting.**

Dive in now to discover what else our research revealed.

# Understanding the current state of cybersecurity

Year after year, the number of cyberthreats continues to grow, turning the everyday challenge of protecting a business into a daunting task. In our survey, more than a third of respondents (34%) said they had to deal with 25 to 50 security incidents daily, with 25% handling twice that amount. And that's just the incidents they worked on. It doesn't include the countless alerts they received, sorted through, and analyzed.

Not only is the volume of threats expanding, but what they look like is always shifting. They can take many shapes—from phishing and ransomware attacks to risks like insider data theft. And the global increase in remote work only adds more potential for breaches.

According to our research, the top five greatest cyberthreats their organizations face are:

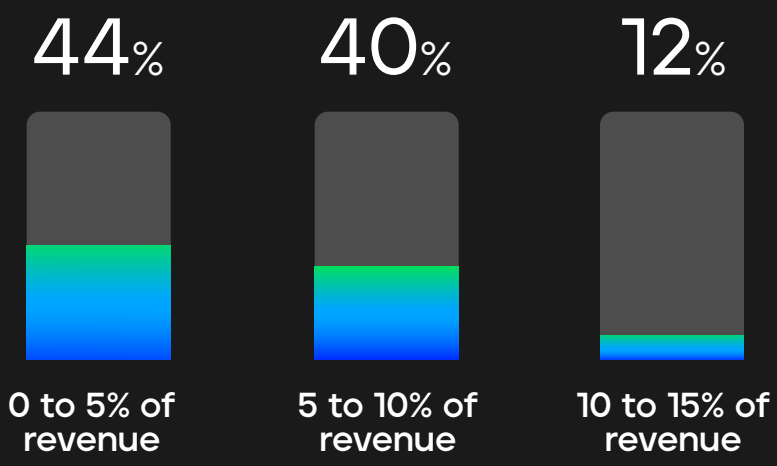
# The impact of today's security challenges

Faced with continuous dynamic attacks from across vectors, SecOps employees are feeling the strain—in the form of longer hours and heavier workloads.

Organizations are also seeing an impact to their bottom lines. Nearly half (40%) of our survey respondents reported losing up to 10% of revenue from security breaches in the last 12 months. For a small or midsize business generating $50 million a year, that's as much as $5 million lost.

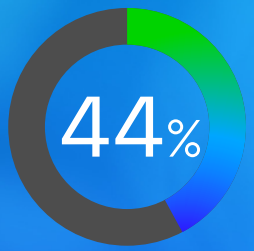
The challenges are clear: threats are constantly changing, the cyber skills gap is growing, organizations are losing money, and current security tools and strategies aren't cutting it.

## Revenue lost due to security breaches in the last 12 months

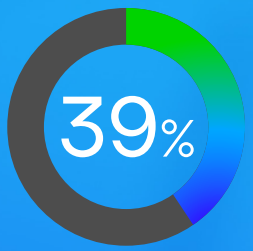


# Top 5 cybersecurity challenges

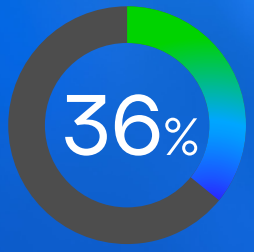
Organizations struggle with a variety of security issues, from internal constraints like budget and staffing to external pressures like a never-ending barrage of attacks. In our survey, respondents ranked their primary cybersecurity concerns. Here's what topped their lists:



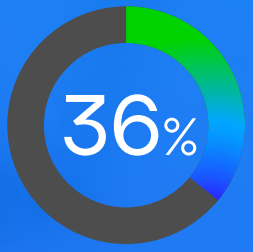

High cost of cybersecurity solutions and services



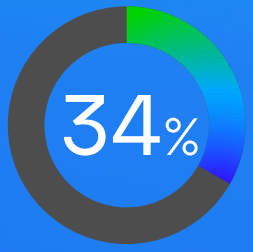

Difficulty detecting and responding to advanced threats




Shortage of skilled resources




Limited threat intelligence and insights




Inability to manage the overwhelming volume of threats

# Moving on from security approaches of the past

Today's attackers continue to grow more sophisticated, and organizations must keep pace to stay safe. But many aren't equipped to meet the challenge: 60% of our survey respondents agreed that security threats are evolving so rapidly that they're struggling to keep up. And only 36% were "very confident" in their organization's ability to quickly adapt to new threats.

Disconnected and cumbersome solutions are holding many businesses back. With 61% using more than 10 different security tools, it's no surprise that this is a point of frustration.

Constrained by solutions that don't work together, SecOps teams can't communicate efficiently, manage security, and keep companies protected. And they recognize the limitations of their existing systems: 60% agreed that they're hampered by a patchwork of solutions that don't integrate seamlessly.

# Too many tools, not enough protection

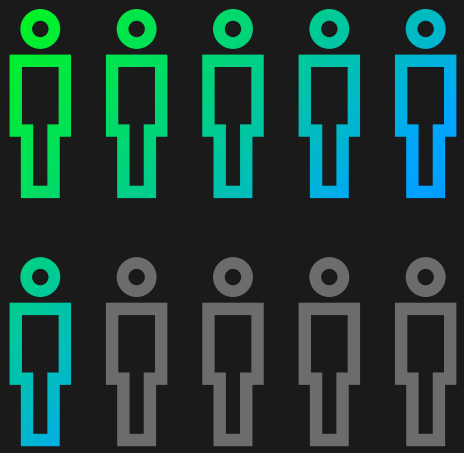
Hindered by an excessive number of disjointed solutions, organizations can't:

1. **Get the visibility they need** to detect and predict attacks, creating blind spots that prevent them from gaining a better understanding of threats and accurately assessing their impacts

2. **Respond to incidents quickly** because they lack effective processes consisting of high-quality alerts, a streamlined queue, accurate analysis, and seamless management

3. **Gain the efficiency and savings** of an integrated approach, which would help streamline financial costs, minimize impact costs, control operational costs, and lower total cost of ownership

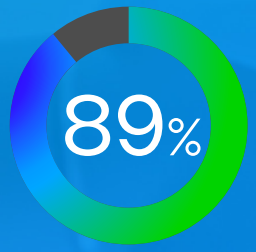
With threats constantly evolving, static security doesn't deliver the protection organizations need. In our survey, 60% agreed that it can feel like they're fighting a losing battle against cybercriminals.



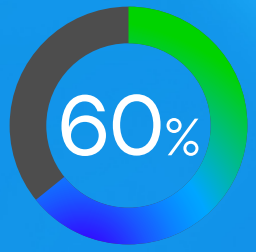
**6 in 10**

respondents agreed that security threats are evolving so rapidly that they're struggling to keep up

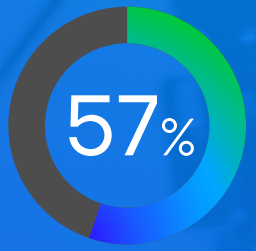
# Siloed security by the numbers



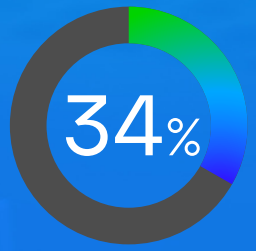

of respondents described their current security model as **"siloed"**



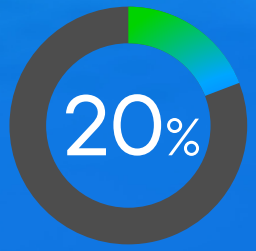

said their current tools don't enable SecOps teams to **work efficiently**




admitted that their current security model needs to be **updated** to predict, detect, and respond to attacks in real time




recognized that they have **blind spots** in their current approaches




are **working to change** their siloed solutions

# Reshaping your security operations with XDR

For many organizations, the key to solving the "siloed solutions" challenge rests on one thing: bringing their tools together in a unified XDR platform. But there's a problem with that. Many people within the cybersecurity industry still don't fully grasp what XDR is all about. In fact, 63% of survey respondents said they either don't know what XDR means or only have a partial understanding of it.

This uncertainty has created confusion about what exactly XDR is—32% called it a solution, 19% called it a feature, and 15% called it a product.

The truth is, XDR isn't a product or a solution.

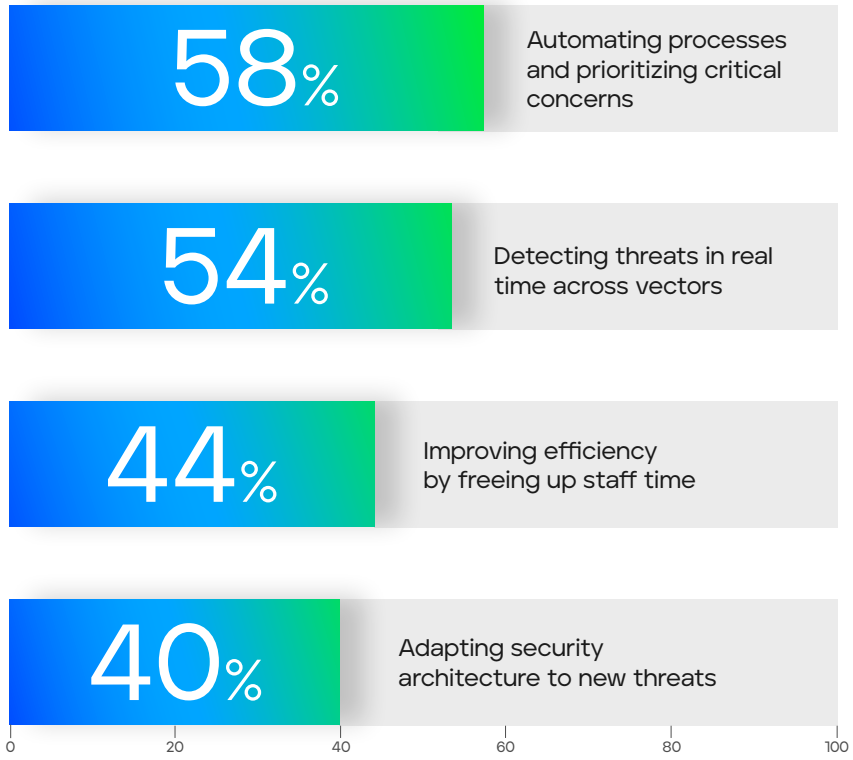
It's an ecosystem.

It's a way for your organization to simplify cybersecurity by integrating multiple tools into a single platform. The ecosystem brings together multiple threat vectors—including endpoint, email, network, and cloud—to deliver holistic visibility into your entire threat landscape.

> Attacks are becoming increasingly multivector, and linear security solutions that identify just one vector are no longer sufficient. This is where XDR technology can make a difference."
>
> — Aparna Rayasam, Chief Product Officer, Trellix

# Retooling the future

According to our survey findings, **the top four benefits for organizations that have already implemented XDR are:**




And with the right XDR ecosystem, this is just the beginning. Respondents also report the ability to reduce mean time to respond to incidents, boost visibility and insights across vectors, and realize significant cost savings.

# Bringing your security to life with Trellix XDR

Our survey findings were a revelation.

They validated the fact that cyberattacks continue to grow in both volume and sophistication—and they won't stop any time soon. They confirmed that organizations need to break free from disconnected tools to stay safe from dynamic threats. And they proved that the only way to stay safe is by **bringing your security to life.**

The Trellix XDR platform delivers the living security your organization needs to build resilience and confidence.

## Learning and adapting

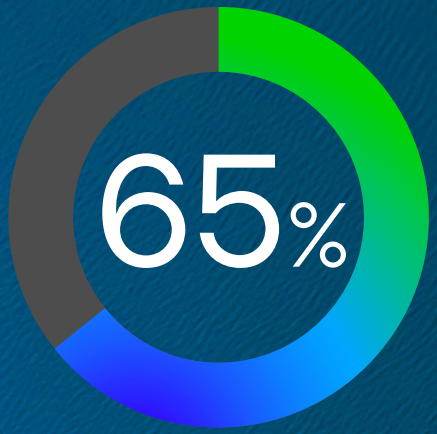
To help you thrive now and in the future, Trellix XDR generates and prioritizes threat insights from inside and outside the organization, constantly evolving to strengthen detection, response, and remediation. And the platform allows you to harness the power of machine learning to predict and detect attacks, identify root causes, and automate responses.

## Native and open

With the ability to ingest and correlate data from a wide range of tools, Trellix XDR can empower your organization with greater visibility and control. We can optimize telemetry data by combining our extensive native integrations with a broad network of open API partnerships so you can gather and analyze data from as many as 650 security tools.

## Expert and embedded

Our XDR platform comes jam-packed with insightful security tools and resources—like defensive playbooks, cultivated incident management, and a threat hunting workflow—that easily integrate with your existing apps. By tapping into the knowledge of our qualified professionals, you'll be able to increase the expertise of your security team. And with tools more readily at their disposal, they can automate security operations like never before.




of global respondents plan to implement XDR in the next 12–18 months

Visit our site to learn how to kick-start your XDR journey today.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at trellix.com.



**Trellix**
6220 American Center Drive
San Jose, CA 95002
www.trellix.com