digital hands®

2025 State of Cybersecurity Report

Insights on What's Ahead — and Why the Future is Unified Security

2025

Table of Contents

Introduction

This past year has been a whirlwind of activity for our team at Digital Hands — and for SOC teams everywhere. From major, wide-reaching events impacting many customers, to new, sophisticated tactics trying to bypass even the most robust defenses, familiar and new threats kept defenders knee-deep in challenges.

Throughout the year, we deliver strategic insights and tactical advice to our customers on how to evolve their security in step with the shifting landscape. But, as 2025 unfolded, we wanted to look back at the big themes of past year to understand how the trends are changing — and share thoughts on what organizations should be ready for in the next 12 months.

This report brings together our SOC's observations, patterns noted by other leading security organizations, and our internal experts' thoughts on what's in store for the near future. We created the report with the intent of helping security leaders and practitioners better understand how the new evolution of the threat landscape may impact their business.

We are also seeing more organizations place a critical importance on outside expertise like managed detection and response (MDR). At Digital Hands, our motto is to "get their first" with real-world MDR. But, as we note in our report, traditional MDR solutions may not truly protect you in real-world scenarios. Just like the threat landscape, the MDR marketplace is evolving — so, we also included our take on the market and insights on what to consider as you navigate it.

No one has a crystal ball to truly know where another year will take us. But, with a team like Digital Hands — with hundreds of years of combined experience in threat detection, remediation, and response, and deployments across thousands of customer environments — it's as close as one can get.

Charlotte Baker
CEO, Digital Hands

Section
01

A Look at the Security Landscape in the Past Year

01

The Current State: Increased Board Visibility, Scrutiny, and Compliance Requirements

Over the past 12 months, the topic of cybersecurity has received increased visibility in the boardroom — and the results look promising. Data shows a correlation between an organization's resilience and the board's engagement in staying informed about cybersecurity incidents, vulnerabilities, trends, and risk predictions.[1]

Much of the pressure to bring security conversations into the boardroom is external, with regulatory scrutiny leading the way. Among new developments that are top of mind for directors are the U.S. Securities and Exchange Commission's new rules on cybersecurity risk management, strategy, and governance.

By requiring boards to engage actively in risk oversight, these rules have forced the directors' hand to become better educated about cybersecurity. To comply, they need to understand what counts as a "material" incident and how it could impact business operations, brand reputation, and financial strength. But an analysis of the 2024 filings shows that many organizations have struggled with compliance, including their interpretation of material incidents.

The past year brought plenty of other challenges in navigating compliance as new requirements emerged.

To name a few examples:

DORA

Financial institutions across the globe had to prepare for the Digital Operational Resilience Act (DORA), which became effective in January 2025 in the European Union. DORA aims to improve operational resiliency of financial entities by establishing a new risk-management framework, including for third parties.

NIS 2 Directive

The EU enacted the Network and Information Security Directive 2 (NIS 2) in 2023, and member states had until October 2024 to translate it into their national legislation. The directive aims to strengthen supply chain security, affecting 18 sectors ranging from critical infrastructure to digital providers like social networks.

State privacy laws

Many states have followed California's example in 2023 to enact comprehensive data privacy laws, and the flurry of activity continued in 2024. To date, more than a dozen states have signed privacy legislation into law, and several others have either introduced it or moved it through committees. The sheer diversity of requirements could create a compliance nightmare.

[1] World Economic Forum

As complex as the regulatory environment has become, a still tougher road lies ahead, as we note later in our predictions. And the matters are even more complicated for CISOs, following several high-profile cases that showed their risk of personal liability in security incidents. According to one survey, 66% of CISOs were concerned about personal, financial, and legal liability in their role last year, up from 62% in 2023.[2]

NIST Cybersecurity Framework (CSF 2.0)

Financial institutions across the globe had to prepare for the Digital Operational Resilience Act (DORA), which became effective in January 2025 in the European Union. DORA aims to improve operational resiliency of financial entities by establishing a new risk-management framework, including for third parties.

2024 Change

NIST

Updated its CSF

An additional incentive to improve security posture comes from cyber risk insurance underwriters. Nearly 70% of surveyed risk managers say their organization carries a cyber insurance policy. But premiums have been going up by double digits every year, and expected to rise again by 15-20% in 2025. The desire to get the most value from policies, including lower premiums and better coverage, is a driver for organizations to improve their security controls.

97% of organizations that purchased insurance boosted their defenses to improve their insurance position, with positive results:[3]

- 76% qualified for coverage
- 67% got better priced coverage
- 30% got better priced policy terms

97%

Boosted their defenses to improve their insurance position

[2] Proofpoint, "2024 Voice of the CISO," May 2024
[3] Nationwide, "Nationwide Cybersecurity Survey Report," September 2024

The Dynamic Threat Landscape: A Year in Review

Critical infrastructure vulnerabilities. Geopolitical tensions. Record-breaking breaches. It has been another defining year for cybersecurity as threat actors continued to push the envelope — making bolder demands, adopting advanced and cutting-age tools, and increasing in sophistication.

The threat landscape was a collision of the old and the new. Existing threats escalated and evolved while emerging threats made the landscape more precarious. Both nation-state actors and organized crime groups escalated activities while AI democratized cybercrime, boosting the odds of success for even the lowliest, low-skilled cybercriminal.

AI has significantly increased the scope, quality, and reach of what cybercriminals can produce. Generative AI enables them to conduct high-quality research and easily personalize attacks to specific individuals. And their reach is wider because they can now connect digital footprints across social profiles and personal and professional emails to target a person from multiple angles.

72%

of surveyed security leaders reported a rise in cyber risk in 2024[4]

[4] Economic World Forum

2024 Threat Landscape at a Glance

Identity-Centric Threats the Biggest Challenge for Organizations

#1

Initial entry vector:
stolen or compromised credentials[5]

This vector surpassed phishing as the initial entry in 2024. Breaches involving stolen credentials also take longer to identify and contain: 292 days on average *(vs. 258 across the board)*

Security Teams Are Waking Up Every Day to 100 New Vulnerabilities

+40k

new CVEs published,[6] the equivalent of more than 100 a day

On the most prolific day (May 3), the number of published vulnerabilities was 845. **For comparison, the number of CVEs was 28,818 in 2023** *(38% fewer than in 2024)*

Ransomware Activity Not Showing Signs of Slowing Down

5,414

published ransomware attacks, an 11% increase over previous year[7]

The number of active ransomware groups also grew — **to 95 in 2024 from 68 in 2023** *(40% increase)*

Misconfigurations a Common Entry Vector in the Cloud

34%

of incidents in the cloud caused by misconfigurations[8]

In the second half of 2024, misconfigurations were the second most-common initial access vector in cloud environments *(credential-related vulns were #1)*

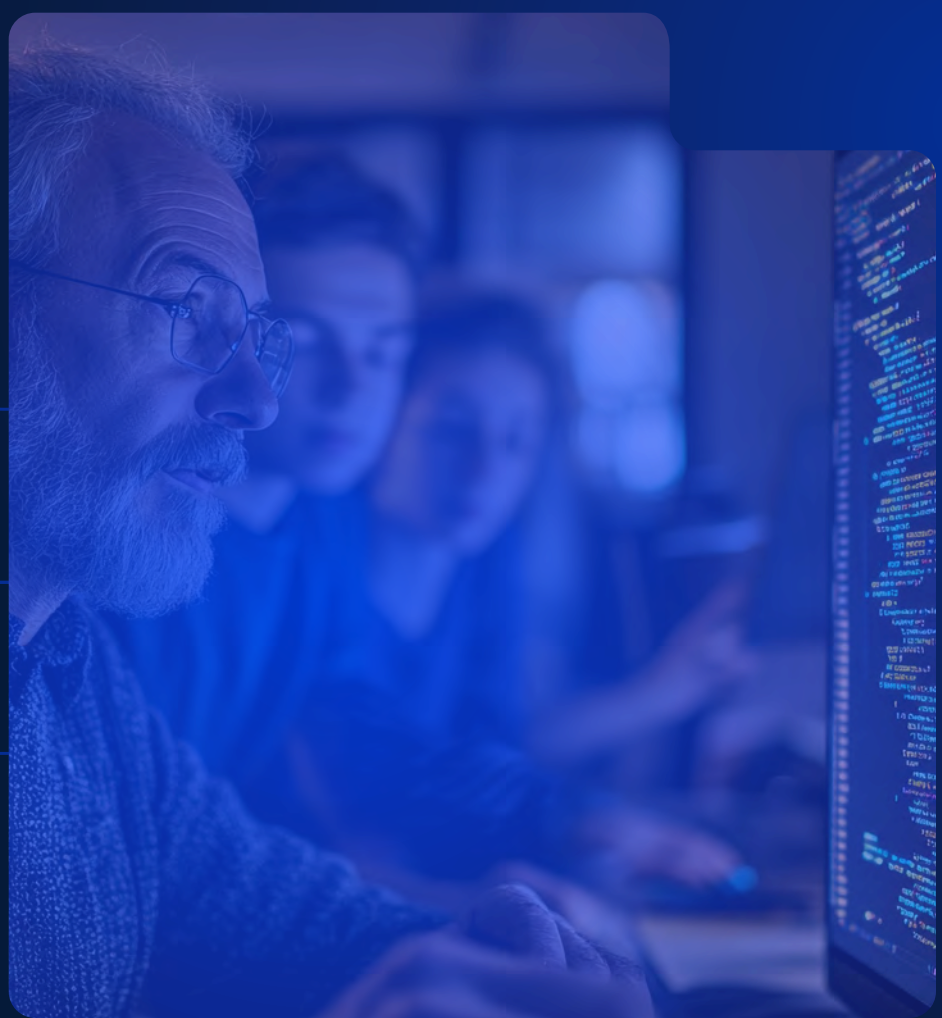
Multiple Breaches and Negative Impact Now a Fact of Life for Most Businesses

93%

of organizations were breached at least twice[9]

Among the breached organizations, **99% said they experienced negative business impacts as a result**

[5] IBM Security, "Cost of a Data Breach Report 2024," 2024
[6] Cyber Press, "Over 40,000 CVEs Published in 2024, Marking a 38% Increase from 2023," January 2025
[7] Cyberint, "Ransomware Annual Report 2024," January 2025
[8] Google Cloud Security, "H1 2025 Threat Horizons Report," January 2025
[9] CyberArk, "2024 Identity Security Threat Landscape Infographic," May 2024

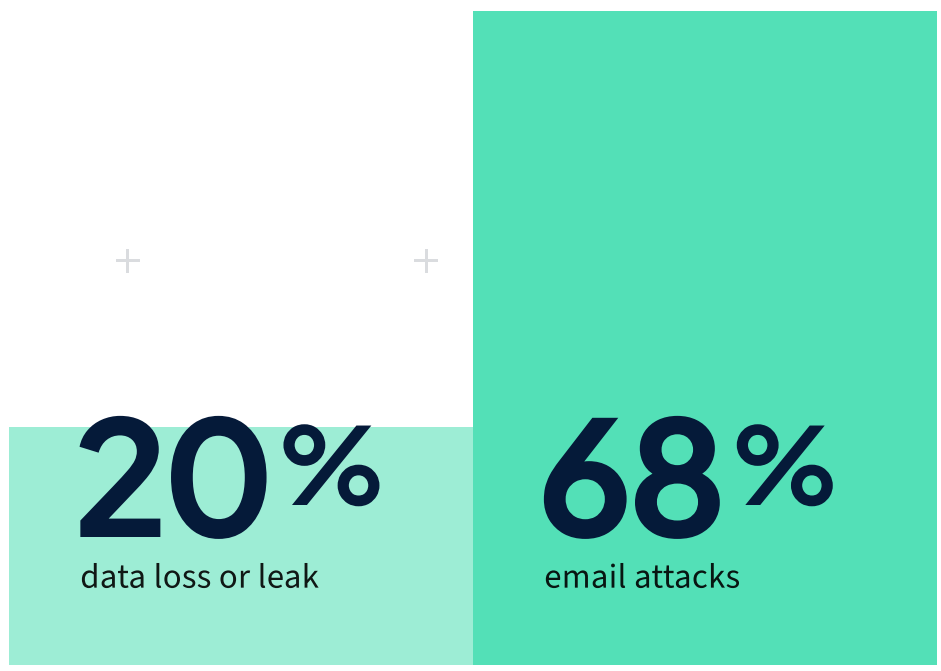


How Secure Is Your Email Layer?

Email is a top entry vector because most compromises related to phishing and credentials are using this channel. Hence, the importance of email security can't be emphasized enough. Many organizations rely on controls that are built into their email apps like Office365 or Google. **But Digital Hands data shows we are detecting a large number of threats that would have evaded legacy email security tools — an average of nearly 28,000 each month for an organization with 5,000 employees.**

Security research shows that 68% of attacks originate from email.[10] This data aligns with observations from our inline email security solutions. Even for customers who have leading email security platforms, we detect and block an average of about 200 legitimate phishing and malware emails every week.

About **20% of our detections are related to data loss or leak** — the most common attack type behind spam. The risk can be tremendous as attackers continue to move toward credential harvesting rather than hacking in.



[10] Checkpoint, "The State of Cyber Security," 2025

The State of the SOC

Against the backdrop of this changing threat landscape, the SOC continued to struggle with talent shortages and tooling complexities while looking to balance its approach to AI and automation.

01

Talent and skills shortages

The global gap in the cybersecurity workforce is estimated at 5.46 million.[11] The skills shortage is an even bigger problem than inadequate staffing — 64% of surveyed practitioners believe that the skills gap can have "a more significant negative impact than a staffing shortage." The good news is that the trend toward automating low-level and mundane task is freeing up the SOC for more meaningful or complex work.

02

Tooling complexities

The majority of IT security pros (89%) spend at least three hours a day managing their cybersecurity tools (an average of 4 hours, 43 minutes).[12] But less than a third of that time is spent responding to high-priority alerts — and the bulk of the time (52%) goes to monitoring security platforms. Perhaps that explains why 90% of teams report that their backlog continues to grow and 87% say they always feel behind, despite their best efforts.[13]

03

Striking a balance with AI and automation

Security practitioners are eager to embrace AI and automation. AI-enabled technology is the biggest spending category on security decision-makers' lists in the next 12 months.[14] While AI will become a critical tool for defenders, there are many implications for the workforce. For instance, if all baseline tasks are automated, how are human experts getting experience? And if they don't have that experience, how can they verify AI's decisions, knowing its propensity to hallucinate? The other side of the coin is that AI automations are based on known threats while cybercriminals are using creative tactics to circumvent defenses. Human analysts are still an important part of the SOC, and their expertise must be balanced with AI efficiencies.

[11] ISC2, "Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World," October 2024

[12] Coro, "2024 SME Security Workload Impact Report," April 2024

[13] Osterman Research, "Making the SOC More Efficient," October 2024

[14] Foundry, "Security Priorities Study 2024: The state of the security situation," October 2024

Security Teams' Performance Shows Improvement

258d

mean time to identify and mean time to contain a breach[15]

MTTI and MTTC dropped in 2024 to a seven-year low, perhaps a positive sign that security teams' performance is improving thanks to AI and automated response actions

Talen and Skills Shortage Magnifies the Risk

58%

of cybersecurity professionals say skill gaps put their organization at significant risk[16]

Additionally, 67% of surveyed pros say they had a staffing shortage, which was the most challenging aspect of their jobs in the past 12 months

Organizations Not Getting Full Value from Tooling

18%

of SIEM rules are broken due to issues like misconfigurations[17]

To make matters worse, enterprise SIEMs are configured for only 19% of MITRE ATT&CK's techniques

Alerts Are Overwhelming the SOC

22,111

security alerts per week are received by organizations on average[18]

Of those alerts, 9,854 are false positives. And an average of 12,009 unknown threats aren't even investigated

Security Teams Are Embracing AI

45%

of security teams have used generative AI in cybersecurity tools[19]

Top use cases include augmenting common operational tasks, streamlining incident reporting, simplifying threat intelligence, and accelerating threat hunting

Threat Hunting Delivers Measurable Results

62%

of surveyed organizations report measurable improvements from threat hunting

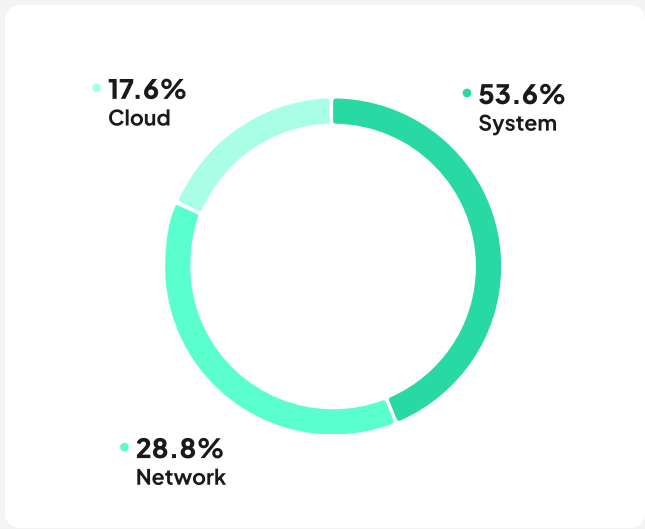
Top outcomes from threat hunting include smaller attack surface exposure and hardened network and endpoints, more accurate detections and fewer false negatives, and shifting of resources to remediation.

[15] IBM Security, "Cost of a Data Breach Report 2024," 2024
[16] ISC2, "Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World," October 2024
[17] CardinalOps, "State of SIEM Detection Risk," 2024
[18] Ponemon Institute/MixMode, "State of AI in Cybersecurity Report 2024," February 2024
[19] ISC2, "Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World," October 2024

Although attackers are homing in on the human layer more, securing systems and the perimeter should remain a top priority, Digital Hands detections indicate. Our robust detections, based on specific observed behavior, pattern, or anomaly, augment what our customers' technologies miss. These detections are unique because they're customized to each customer's environment, which greatly increases the likelihood of our SOC detecting anomalous behavior.

Last year, **54% of our detections were at system level, followed by the network** (29%) — indicating that these areas are the most commonly targeted. It should be noted that our data may differ from other industry sources since these detections are based on the technologies deployed within our customer base.

Digital Hands Detections in the Past 12 Months



Making Cyber Insurance Work for You

Cyber risk insurance has gained popularity as a risk-management tool. But 52% of IT and cybersecurity practitioners say that purchasing a policy is highly difficult because of underwriters' requirements like regular vulnerability scanning, and patching and adequate staffing to support security policies and programs.[20] And, as noted earlier, many organizations that are insured are looking to get the best value from their policy by improving security posture and implementing more robust controls.

Many of these organizations recognize that they need help from outside experts to achieve those goals. Among surveyed organizations that had gone through a cyber insurance claim, 26% are seeking third-party advisory services to improve future outcomes and 34% plan to engage with a cybersecurity services provider to address their shortage of resources and gaps in controls.[21]

If you're considering cyber insurance, it's important to ensure it's right-sized to your organization. The more assets you have, the higher your risk. If you're experiencing high growth, going through mergers or acquisitions, or undergoing other big changes, reevaluate your policy to determine if you need a higher premium.

[20] Ponemon Institute/Optiv, "2024 Cybersecurity Threat and Risk Management Report," June 2024
[21] TELUS, "The TELUS Canadian Cyber Insurance Study," December 2024

Section
02

What to Expect in the Coming Year

02

10 Predictions for the Next 12 Months

1. As AI tools get cheaper and more accessible to attackers, threat actors will grow even more efficient, accurate, and effective — with little investment required.

Cheap, easily accessible AI tools will democratize cybercrime. The “as-a-service” economy in the criminal underground has already removed many barriers to entry for new waves of cybercriminals. AI tools will further enable anyone to exploit weaknesses (especially the human factor) more effectively with little or no infrastructure required.

Remember the proliferation of script-kiddies in the mid ‘90s, when premade hacking scripts and tools became readily available? Much the same way, the ranks of malicious actors will grow — and thrive — thanks to generative AI. **In fact, AI can now turn anyone into a proverbial script-kiddy because it enables any average person to design, tweak, and customize a script without any programming knowledge.**

> **These tools can improve efficiencies at scale — summarizing reconnaissance data in seconds, writing or improving code, and providing unlimited iterations for fine-tuning phishing emails. Not only can malicious actors automate the generic aspects of a phishing attack, they can also quickly glean comprehensive details online about high-value targets to craft a perfectly customized spear-phishing message. And it’s not difficult to fool these tools into sidestepping built-in safeguards for preventing prohibited use.**

AI will also help attackers exploit stolen data more efficiently and find new ways of monetizing it. They could simply download data after a breach into a large language model (LLM) and quickly query it to get tactical insights. What took hours or days can now take just a few minutes.

2. AI-driven tactics will give rise to next-generation attacks and force organizations to reconsider defense strategies.

A November 2024 Gartner survey found that malicious attacks enhanced by AI emerged as the top overall risk for enterprises for the third consecutive quarter. In the next 12 months, these attacks will become commonplace — and top of mind for every SOC and CISO.

In addition to using AI for crafting flawless phishing emails, malicious actors will scale impersonation attacks using AI-generated deepfakes. We have already seen some of these capabilities in the wild, including an evolution of business email compromise into a next-generation attack using deepfakes.

> **For instance, malicious actors carried out a $25 million fraud scheme last year by impersonating a company executive in a live video call with a company's finance employee. In another scheme, fraudsters reportedly used deepfake technology to create an AI hologram impersonating a crypto company executive in meetings with clients.**

We expect to see these kinds of deepfake attacks and other sophisticated impersonation schemes to become prevalent. They're only limited by the cybercriminals' imagination, whether they use a fake voicemail to an employee from the CEO with a fraudulent request, or a fake, embarrassing photo they threaten to post on social media.

To combat the knowledge and speed of AI-based attacks, defenses need to employ AI that has more extensive knowledge than attackers and can match their speed. For example, an advanced, AI-driven email security solution trained on millions of emails could identify even the subtlest indicators of compromise and intercept malicious emails before they reach a user's inbox.

In addition to rethinking their security stack, organizations will need to overhaul their security training — both for employees and IT teams. The existing, old-school programs don't teach employees how to detect deepfakes. Even getting on a phone or video call is no longer a trustworthy way to verify the authenticity of a suspicious email message. And to start with, phishing emails written by AI will be extremely difficult to detect. The evolution of these threats requires a new approach to user awareness as well as IT and security practitioner training.

3. Nation-states will continue to weaponize trust, compromising IT vendors to get access to their customers — accelerating the move to zero-trust security.

Supply chain attacks have been on the rise for several years, but more recently nation-state affiliated actors have doubled down on targeting technology and cybersecurity companies. Globally, IT was the most-targeted sector by Russia, China, Iran, and North Korea in 2024, according to Microsoft security data.[22] This trend will continue because attacks on IT products and services can give threat actors access to a large number of the vendor's customers, greatly increasing their return on investment.

> Digital Hands is observing a lot of activity targeting security companies like firewall vendors, and zero-day attacks are often a preferred tactic. Threat actors are especially interested in those that provide centralized management tools or SaaS platforms. One example of this threat was the December incident that allegedly gave Chinese state-sponsored attackers access to the U.S. Treasury Department workstations by compromising a privileged access management vendor.

The escalation of supply chain attacks will compel organizations to scrutinize their trusted partners more and do their due diligence. Unfortunately, cybercriminals are also adapting. One growing tactic is vendor hopping, where attackers compromise the smaller, weaker vendors to move laterally within their trusted network and get to their primary target.

One of the most effective ways to negate attacks like zero days and defend against weaponization of trust is through a zero-trust model. While the conversation about zero trust has been happening for several years, the marketing hype surrounding it makes this approach sound much more complicated than it needs to be. However, zero-trust security is now a critical piece of a multi-layered defense strategy, and organizations will be doubling down to figure out how to implement it.

[22] Microsoft, "Microsoft Digital Defense Report 2024," October 2024

4. The digital supply chain will be as fragile as ever, pushing organizations toward better resilience.

Nation-sponsored actors are not the only ones weaponizing trust — and it's not just security vendors that organizations have to worry about. An estimated 90% of companies are undergoing digital transformation[23], expanding their digital interconnectivity. This interdependency contributes to the sprawling attack surface, introducing vulnerabilities across the entire supply chain.

The compromise of the Linux XZ Utils tool last year is a recent example of the enormous impact that one compromised link in the supply chain can cause. The compromise could have affected millions of computers around the world. Fortunately, it was only a close call and Linux "narrowly escaped a massive cyberattack" — but we've seen plenty of other examples of vendors (and their customers) not being as fortunate.

> **Not surprisingly, the World Economic Forum's recent security outlook survey found that 54% of large organizations view supply chain challenges as their "greatest barrier to achieving cyber resilience.[24]" The biggest challenge is that compromises in the digital supply chain are one of the most difficult threats to detect and mitigate. These threats pass traditional perimeter defenses, and the SOC has no visibility into the vulnerabilities of their organization's partners and suppliers.**

With such an obscure view of supply chain vulnerabilities, risk becomes more unpredictable. Add to that the emerging problem of AI — both AI adoption and AI-driven threats — and it's easy to foresee that boosting resilience will be on every security leader's mind.

The Third-Party Problem That Can Become Your $12 Million Problem: How MDR Defends Against Supply Chain Exploits

Read our insights into why supply chain vulnerabilities are one of the more difficult threats to mitigate and how managed detection and response can help you combat it.

Read Now

[23] McKinsey & Co., "What is digital transformation?" August 2024
[24] World Economic Forum, "Global Cybersecurity Outlook 2025," January 2025

5. Ransomware, extortion-based, and sophisticated malware attacks will continue to cause major disruption, and attackers will target new vectors.

Ransomware has gone through ebbs and flows over the last few years. In 2024, ransomware operators may have had their best year yet, with ransom payouts and the number of attacks breaking records. The convergence of AI tools, rise in double and triple extortion tactics, increased ROI, growing number of ransomware groups, and booming ransomware-as-a-service economy will continue to escalate the frequency of large-scale ransomware attacks.

> **Based on our observations, email is the most successful initial access vector in ransomware attacks, another sign that malicious actors are exploiting the human factor. And while humans will continue to be the attackers' preferred weak link, we also expect to see them double down on circumventing security technology with tactics like zero-days.**
>
> **We also expect threat actors to target new vectors with malware. One of them is collaboration tools like Slack, Teams, and other messaging apps. These apps don't have robust security tools, making them an attractive channel for phishing attacks. The other increased area of focus for malicious actors will be operational technology (OT), with more attacks targeting industrial control systems (ICS) or SCADA hardware.**

Regardless of what the adversary's tactic of the day or targeted vector is, defenders will have a much more difficult time if they don't integrate advanced AI in their security stack.

6. Industries providing critical infrastructure and services will remain at the top of the hit list.

Healthcare organizations have been pummeled by ransomware in the last few years, with 2024 reaching an all-time high.[25] One of the breaches of the year across all sectors was the ransomware attack on Change Healthcare, which reportedly paid a $22 million ransom. The attack, which impacted more than 100 critical software solutions and disrupted thousands of healthcare providers, has so far cost parent company United Healthcare more than $3 billion.

> **Healthcare is one of the top-targeted sectors because of the criticality of the services that could be impacted. With patients' lives and wellbeing at stake, hospitals and other medical providers are much more likely than others to pay a ransom to restore operations.**

A healthcare executive told the United Nations recently that ransomware attacks on hospitals and healthcare systems "pose a serious threat to international security." Attacks on other sectors that serve critical functions — including energy and utilities, government, transportation, and industrial manufacturing — pose just as big a threat around the globe. Critical infrastructure organizations overall will remain major targets because of the disruptive nature of attacks on those functions. So will other types of organizations that serve as a conduit to numerous businesses, such as managed security providers., such as managed security providers.

7. The rapid adoption of generative AI will expose companies to more data privacy and data loss risk.

GenAI and LLMs have disrupted the business world. Organizations are adopting these game-changing technologies at an unprecedented pace. A McKinsey survey found that 65% of organizations were using genAI regularly in 2024, nearly doubling in 10 months. But the rapidly growing reliance on LLMs and genAI models — especially when provided by third-party vendors — has outpaced organizations' understanding of security risks.

AI systems integrated into daily business functions are also processing large amounts of sensitive data like confidential customer information or intellectual property. On top of that, they're connecting to more systems, apps, and other data sources. Consequently, unauthorized access creates a big risk of data breaches and leaks that could be caused either by unwitting employees or attackers targeting the organization.

> **Incidents like Samsung's sensitive leak of source code have illustrated how employees inadvertently can cause huge exposure for their organization. And even if the organization bans specific tools in their workplace, the exploding market means that employees will easily find other options.**

Emerging AI-specific threats like prompt injections and model theft can also compromise sensitive data. These threats compound the other risks related to AI adoption, including cloud vulnerabilities and supply chain attacks.

[25] Sophos, "Two-Thirds of Healthcare Organizations Hit by Ransomware – A Four-Year High, Sophos Survey Finds," September 2024

8. Complying with evolving requirements will ratchet up the pressure on CISOs, risk leaders, and boards, with resilience rising as a priority.

The evolving nature of regulatory frameworks and mandates makes it ever challenging to keep up with compliance. And this landscape continues to shift. In the next 12 months, we expect to see a bigger focus on resilience, similar to what EU aims to achieve with DORA.

AI's broad access to vast amounts of data, along with the technologies' data collection and processing capabilities, will also get more attention of government and industry regulatory bodies. Last year, the U.S. Department of Homeland Security introduced a new framework for regulating use of AI in critical infrastructure, NIST released new guidance related to AI development, and various states enacted or considered AI privacy regulations.

As the implications of AI to data privacy and security become better understood, expect the scrutiny to increase. For CISOs, CIOs, risk leaders, and boards of directors, this means even more pressure to keep up with new developments while they also prepare for looming PCI DSS 4.0 compliance deadlines, adapt to significantly stepped-up requirements of frameworks like ISO 27001, and more.

> **Additional pressure will come from cyber insurance companies. Underwriters will maintain rigorous requirements and further tighten terms to improve the stability of the market. To obtain and maintain a policy, as well as get the best value from insurance, organizations will need to keep a sharp focus on complying with policy requirements and evolving their controls as their environment changes. They will also need to ensure that their incident response plans align with their changing environment, including new risks introduced by their adoption of AI.**

To keep up with these changes, organizations need to create AI security policies, as well as consider adding ISO 42001 to their security programs. This new ISO/EIC standard is designed to implement, manage, and improve AI management systems to ensure secure, responsible, and ethical use of AI.

9. The increased role of AI in defense will redefine security roles while raising liability questions.

With both attackers and defenders leveraging AI for speed and efficiency, the AI arms race will intensify. On the defense side, the outcomes will include better response playbooks as AI helps cut back on the noise, enables analysts to derive faster insights, and frees up time for humans to focus on threat hunting.

In the next 12 months, most Tier 1 jobs will go away because AI will be trained to take over tasks like low-level, simple data analysis. In the process, as more basic and repetitive tasks are automated, the SOC will have to rethink job descriptions. What used to be more advanced tasks that require human oversight will move down to Tier 1 or Tier 2. That said, we don't see AI replacing humans altogether any time soon, although it may relieve the pressure from the entry-level talent gap.

The growing role of AI in defense will raise new questions for organizations. If your security technology or service provider is relying 100% on AI for things like data analysis and playbooks, who's liable for the decisions? If the AI makes the wrong conclusion due to hallucinations (a common AI issue), and this leads to a costly incident or another negative outcome, whom do you hold accountable? Who's "policing" the AI? If there's no human in the loop to review the AI analysis, what gives you the confidence that the outcomes are always positive?

AI's Impact on Cybersecurity Skills

51% of surveyed security practitioners believe genAI will make certain cybersecurity skills obsolete, but most view AI as a positive — two-thirds are confident that their expertise and the technology are complementary[26]

51%

of security practitioners believe GenAI will make some cybersecurity skills obsolete

2 out of 3

AI complements their expertise and view it as a positive force in security

10. More organizations will seek unified security models to combat the proliferation, sophistication, and speed of attacks.

The bulk of IT security pros' time goes to monitoring security platforms. The SOC simply has too many data portals, too many places to find answers, too many settings to worry about.

Whether they're outsourcing security or handling it in-house, more organizations will be implementing unified security in the next 12 months. And they will have many more platforms to choose from than in the past. While tool consolidation has been a growing trend for several years, we're now seeing security vendors' race to offer unified platforms reaching a fever pitch.

> **Although this trend is positive, it does bring downsides. Many platforms offer simple "drag-and-drop" functionality. In theory, organizations no longer need skillful, experienced professionals to manage the technology — or at the very least, they don't need an entire team. The tradeoff is that the organizations lose 24/7 "eyes on glass" coverage. Additionally, they could feel locked into their vendors because they no longer have the staffing or the skilled experts to stand up and configure something else.**

[26] ISC2, "Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World," October 2024

The Evolution of the MDR Space

The trifecta of growing cyber threats, complexity of the security landscape, and expanding regulations is driving organizations to seek strategic guidance and tactical assistance from third-party security experts.

Managed security offers a viable solution for augmenting or extending in-house SOC teams. **The managed detection and response (MDR) market has been growing dynamically as more organizations seek a holistic approach that can address complicated security challenges.**

Market analysts (Markets and Markets, Grand View Research) forecast the MDR market to expand at a 23.5% compound annual growth rate between 2024 and 2029-2030.

MDR market

23.5%

Compound annual growth rate between 2024 and 2029-2030

A 2024 survey of security decision-makers found that 82% of organizations planned to outsource security functions to a third party like a managed service provider in the next 12 months.[27] **The primary functions being outsourced are:**

- **Threat detection and response**
- **Security awareness training**
- **Security operations center**

[27] Foundry, "Security Priorities Study 2024: The state of the security situation," October 2024

What is MDR?

MDR combines advanced, state-of-the-art technologies, and advanced behavioral analytics with remotely delivered human expertise that includes proactive threat hunting and 24/7, real-time threat detection and response. Building on the adoption of new security platforms like SIEM and SOAR as well as outsourced security models, MDR is a modern approach to detecting, analyzing, and neutralizing threats and responding to cyberattacks.

A comprehensive MDR solution should provide:

- ✓ Advanced threat detection **and real-time response** to actively identify, disrupt, and contain attacks.
- ✓ **Human expertise** to take response actions against emerging threats or based on nuances like context, industry-specific threats, and the customer's distinct network architecture and user base.
- ✓ **Proactive threat hunting** that combines AI and human expertise to comb your environment for unknown threats.
- ✓ **A flexible and customized approach** adapting solutions to your existing IT infrastructure and security stack, starting with areas like the data sources you ingest and all the way down to custom parsers, detections, and response playbooks.
- ✓ **Real-time, unified visibility,** with clear dashboards that present a real-time view of your security posture.
- ✓ **Curated, aggregated threat intelligence feeds** to power detections and response capabilities.

What MDR typically doesn't include:

- ✕ Advanced threat hunting
- ✕ Active alerts and tickets
- ✕ Security posture benchmarking
- ✕ Activity logs of attacks

MDR providers' offerings continue to expand. Many are forging partnerships with companies providing incident response, forensics, cyber insurance, and other services to offer their customers a broader range of security solutions.

Read our blog post, "MDR, MSSP, or Something Else?" to understand how to choose the best solution for your SOC.

Misconceptions and Limitations in the Market

The growing trend toward automation and AI has brought new players to the MDR market, but many solutions have limitations. **Here are common misconceptions about MDR:**

You can rely entirely on an automated platform and a predefined framework without any human intervention.

In reality, you need both. Machine response can be very effective for known-bads or enriching alerts — for example, instantly quarantining endpoints, blocking malicious connections, and correlating data from multiple sources. But human expertise is still critical for nuanced investigation and to customize and properly configure your tools, select the right data sources, manage threat intelligence, lead threat hunts, and more.

Additionally, standard MDR services are built on rigid frameworks based on common use cases and are not adapted to the unique needs of your environment and business goals. These frameworks excel at detecting and responding to common threats but lack the flexibility to address your specific organizational requirements, business processes, or custom infrastructure setups. You can't rely on a one-size-fits-all solution — whether it's an automated platform or a rigid framework — in an environment that rapidly changes every day.

> **Without human expertise, MDR leaves critical gaps in protection and limits the effectiveness of MDR services in truly mitigating risks within your operational context. Additionally, vendors who don't offer customization only push updates that apply to their entire customer base rather than your specific situation.**

Your MDR vendor doesn't need to manage your entire stack.

There's a trend among organizations to simply use connectors rather than having the MDR vendor fully manage technology like firewalls and SIEM. While this option is better than nothing, you may have security gaps if the stack is not managed consistently and all your response actions are done through APIs. Your MDR experts cannot provide a full security solution when they're blind to major sections of your environment.

> **Some questions to ask yourself are, who's reviewing your firewall policies to ensure they're not outdated? Who's refreshing the equipment when you deploy new solutions? Who's backing up your team 24/7 or providing oversight? Vendors who only provide automated technology don't offer the human expertise when you need it. Additionally, the more technology your MDR partner manages, the more effective and comprehensive your security is.**

If your MDR vendor only provides a platform that requires manpower for you to manage, then you're simply getting yet another technology in your stack rather than solving security problems. And if you decide to switch vendors, you're back to square one because your MDR provider takes all the capabilities, rules, and automations that were built into the vendor's platform.

5,337,325 malicious inbound and outbound IPs (comprising multiple vectors and threat actors across 55 countries) blocked through Digital Hands proactive threat blocking curated threat intelligence feeds for just one customer in 2024.

Malicious IPs Blocked

5,337,325

Inbound and outbound threats from multiple vectors and actors across 55 countries.

Your MDR providers' prescribed security stack will solve your security problem.

Many MDR providers support a limited number of technology vendors, forcing you to adjust your strategy to their services. A true partner should be technology-agnostic and meet you where you are, working with your stack and customizing the solution to your use cases.

> **Depending on where you are on your security journey, your MDR partner should make recommendations for how to improve your security posture based on your requirements and your technology. And if an MDR vendor tells you that their platform can do it all, challenge that statement. True MDR partners will not position their solution as a "one-stop" shop but instead work together with you to find the best approach.**

Some MDR vendors will go so far as to say you don't need a SIEM if you're using their platform. While this is true in some cases, there are still many situations where a SIEM is a valuable and necessary technology. A true partner will recommend whether taking the SIEM out of the equation makes sense for your environment rather than making a wholesale decision.

The Impact of AI on MDR

As we noted in our predictions, AI plays a growing role in both offense and defense. The magnitude of the threat is still unfolding, but we're already seeing implications in the wild. For instance, OpenAI, developer of ChatGPT, confirmed last year that more than 20 attacks leveraged its genAI chatbot for spear-phishing attacks, malicious software development, and other activities. Security researchers also observed ChatGPT being used to exploit vulnerabilities and steal passwords.

76% of cybersecurity professionals surveyed by ISC2 named deepfakes as their biggest concern related to AI-related attacks (making it the top concern, followed by disinformation campaigns and social engineering)[28]

Viverra hendrerit

76%

Lorem ipsum dolor sit amet conse ctetur gravida nulla.

And it's not just genAI and LLMs — attackers are using other AI technologies like machine learning to automate and launch far-reaching attacks at scale, improve their evasion techniques, accelerate data gathering, and more.

On the defense side, AI is the topic of conversation among CISOs and SOC teams alike. Nearly half of surveyed IT security executives plan to increase spending on AI-enabled technology in the next 12 months.[29] A quarter of organizations are already using it and another 62% are considering or piloting AI.

The top three outcomes of using these tools include:

44%

Reducing security team's workload

43%

Remediating threats faster

43%

Identifying unknown threats faster

[28] ISC2, "The Real-World Impact of AI on Cybersecurity Professionals," February 2024
[29] Foundry, "Security Priorities Study 2024: The state of the security situation," October 2024

From an MDR perspective, there's a danger from overreliance on AI-driven tools and platforms. It's simply impossible to have 100% confidence in AI-powered results due to the technology's inherent shortcomings like hallucinations. **Your MDR provider needs humans to watch over the technology, as well as enhance it with the type of expertise that only skilled human analysts and incident responders can deliver.**

AI playbooks are also based on human actions and inputs, so you need experienced practitioners to write the AI rules and customize them to your needs and environment. You also need skilled analysts to respond to unknown and emerging threats using threat intelligence combined with their knowledge, experience, and intuition.

A hybrid approach that combines AI-driven technologies and an experienced team of highly skilled experts will give you the best value from your MDR solution. And a standalone, automated portal will simply not be there for you in a moment of crisis.

How are security teams using AI?[30]

26%
Malware detection

24%
Threat detection

23%
Automating alerts and triage

[30] Foundry, "Security Priorities Study 2024: The state of the security situation," October 2024

The Unified Future:
Beyond Cookie-Cutter Security

Unified security can help solve the problem of increasingly understaffed and overworked in-house security teams grappling with an increasingly complex threat environment and attack escalation. Cyber threats don't fit a standardized, traditional mold, and neither should security. That's where real-world MDR represents a critical shift in the cybersecurity market, offering a proactive, unified security that adapts to modern challenges and enables you to "get there first."

Out-of-the-box, predefined frameworks and tools sound great in theory. But they're not going to deliver on your expected outcomes in your unique environment. MDR that's missing critical pieces like custom detection and playbooks or firewall management — and that doesn't play nice with the rest of your tech stack — will likely bring more headaches that actual solutions. As you prepare for what the future threat landscape may hold, look beyond vendor claims that promise to solve all your security problems with automated platforms.

Unified security is a lot more than a unified tech stack. It means a unified, holistic approach that combines technology and automation with skilled people and effective processes. When your MDR partners uses this model to deliver a fully custom solution — from parsers and content to detection and playbooks — you can face the threats in the next 12 months and beyond with more confidence.

Learn how real-world MDR from Digital Hands delivers the speed and automation you expect from MDR — but with the customization, flexibility, and multidisciplinary expertise that a one-size-fits-all solution will never deliver. Download our MDR Buyer's Guide or Contact Digital Hands experts today.

About Digital Hands

Digital Hands is how you finally get MDR with the flexibility, fine-tuning, and support needed to make it work in your specific environment. We call it Real-World MDR.

Too many companies get excited about the promise of MDR, only to be disappointed by MDR's missing pieces. Where are the custom playbooks? The expert guidance? Firewall management? How do you handle the sheer volume of alerts? Why won't this play nice with your tech stack? And on and on it goes. Meanwhile, the bad actors are becoming more and more sophisticated with AI and automation.

So, you've got to think fast, act fast, and flex fast. That's why organizations with some of the most sensitive data of all – such as hospitals, financial institutions, law firms, and government agencies – continue to give us industry-leading satisfaction sentiments year after year after year.

Digital Hands. Get There First™.