KROLL

The State of Cyber Defense:

Diagnosing Cyber Threats in Healthcare

Table of Contents

Key Findings

This report offers new insights and analysis on the specific security challenges in the healthcare sector. Taking Kroll frontline data from its experience with over 3,000 incidents per year, this research provides an overview of the cybersecurity threat landscape the healthcare industry currently faces.

Our previous report, **The State of Cyber Defense 2023: Detection and Response Maturity Model**, surveyed 1,000 global security decision-makers and shone a light on the biggest inconsistencies that plague cybersecurity teams. It demonstrated a clear disparity between organizations' level of trust in their own cybersecurity status and their readiness to achieve true cyber resilience.

By combining the detection and response maturity model research with Kroll data, this report finds that senior leaders in healthcare are among the most confident respondents. They are resolute in believing they can defend their networks and choose to do so in-house rather than outsource.

However, the data also shows that healthcare scores poorly on more objective measures of security maturity. It is also among the **most commonly breached industries**.

Above-average confidence—Healthcare is the most likely industry to self-report as having very mature security. Only a tiny fraction of healthcare respondents **(3%)** said that they do not trust their organization's ability to defend against most cyberattacks.

Below-average capabilities—Unfortunately, the real-world security capabilities of healthcare organizations are below average. Of healthcare businesses, **26%** rank as having low cyber maturity, and healthcare performs badly in comparison to other sectors that scored highly for self-reported security.

In-house security services—Healthcare organizations are **65%** less likely to outsource their cybersecurity services than other sectors due to the dynamic nature of these work environments. However, nearly two-thirds **(62%)** of healthcare companies that currently handle everything in-house plan to outsource some services in the next 12 months.

Credential access fears—Of all the threats posed to organizations, healthcare respondents selected credential access as their number one fear—more than ransomware, BEC, and phishing. Interestingly, credential access was the least significant threat according to all other industries.

Email compromise and ransomware—Despite the fears of the healthcare industry, Kroll Threat Intelligence finds that they are consistently targeted by ransomware groups, which use a combination of valid credentials theft and exploiting vulnerabilities.

Top target for breaches—The healthcare industry is one of the most breached industries, ranking first in 2022 and second in 2023 in Kroll data. Further, the industry has had **YoY increases** in the number of inquiries and identified monitoring activations.

KROLL

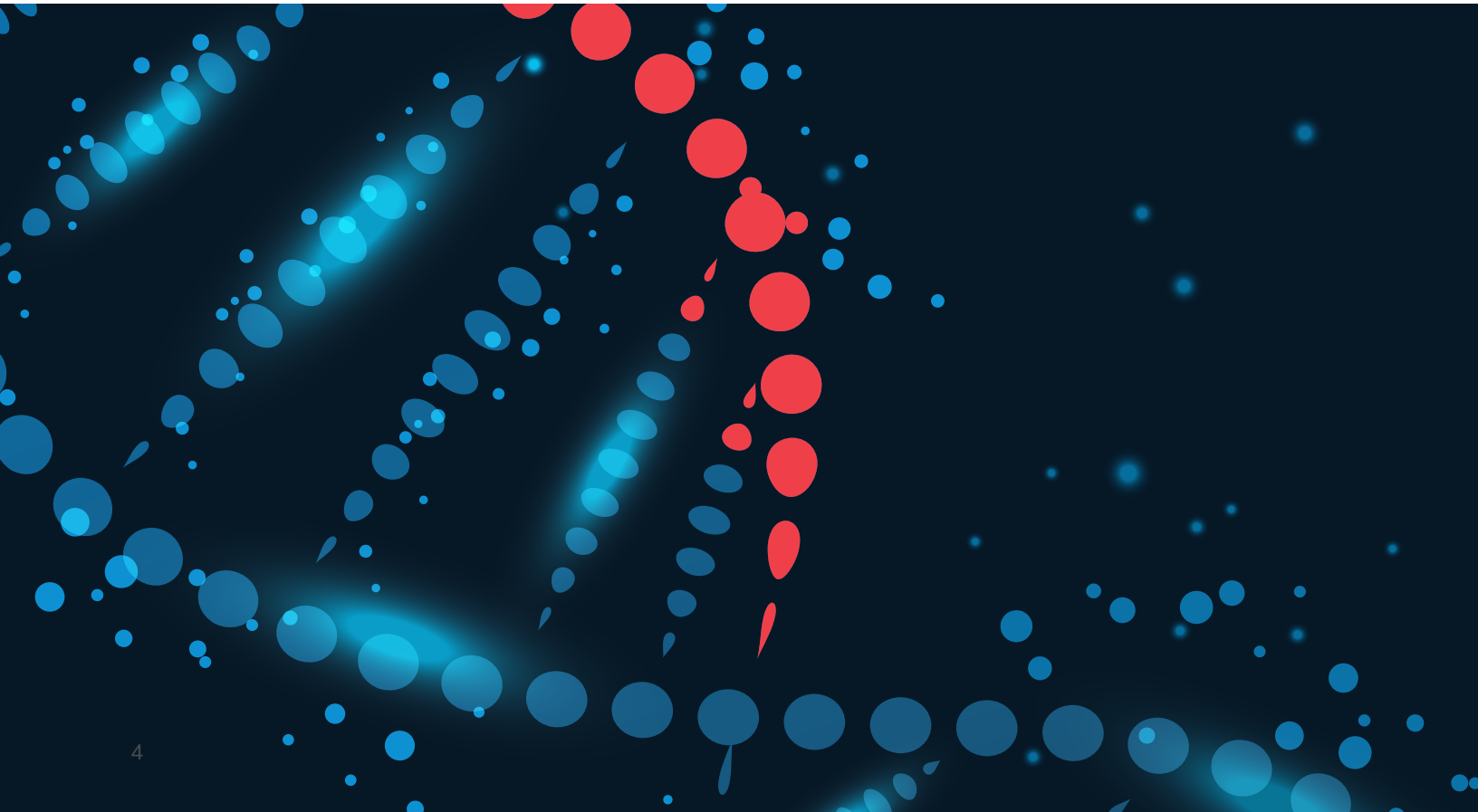
A Critical Self-Diagnosis Gap

When considering cyber maturity in the healthcare sector, we should note the scale and severity of threats posed to hospitals and other healthcare providers. If a cyber incident disrupts hospital operations, it can have terrible outcomes for patient care and treatment and even put human lives at risk. It is for precisely this reason that critical infrastructure, including healthcare organizations, is such a high-priority target for threat actors looking to cause as much disruption as possible to their targets.

The critical nature of healthcare is also why ransomware gangs target the sector.

They cannot tolerate downtime in the same way that a private sector services business can. Attackers know that healthcare providers may, therefore, be disproportionately likely to pay a ransom to ensure they remain operational. This is why we have seen gangs like Lockbit mass exploiting Citrix Bleed and other vulnerabilities to hit healthcare targets. Other operations, such as Rhysida Ransomware, have been purposely built to target hospitals, as well as other high-profile targets like the British Library. More recently, the UnitedHealth Group's Change Healthcare cyberattack by the ALPHV/BlackCat ransomware gang demonstrates that, unfortunately, the sector will continue to be an attractive target.

The self-diagnosis gap between healthcare's confidence in its security and its real-world security capabilities is not an abstract issue. It is deeply alarming to discover that hospitals and healthcare organizations are not as secure as they believe they are. These kinds of gaps can lead to dire real-world consequences.



Self-Reported Security

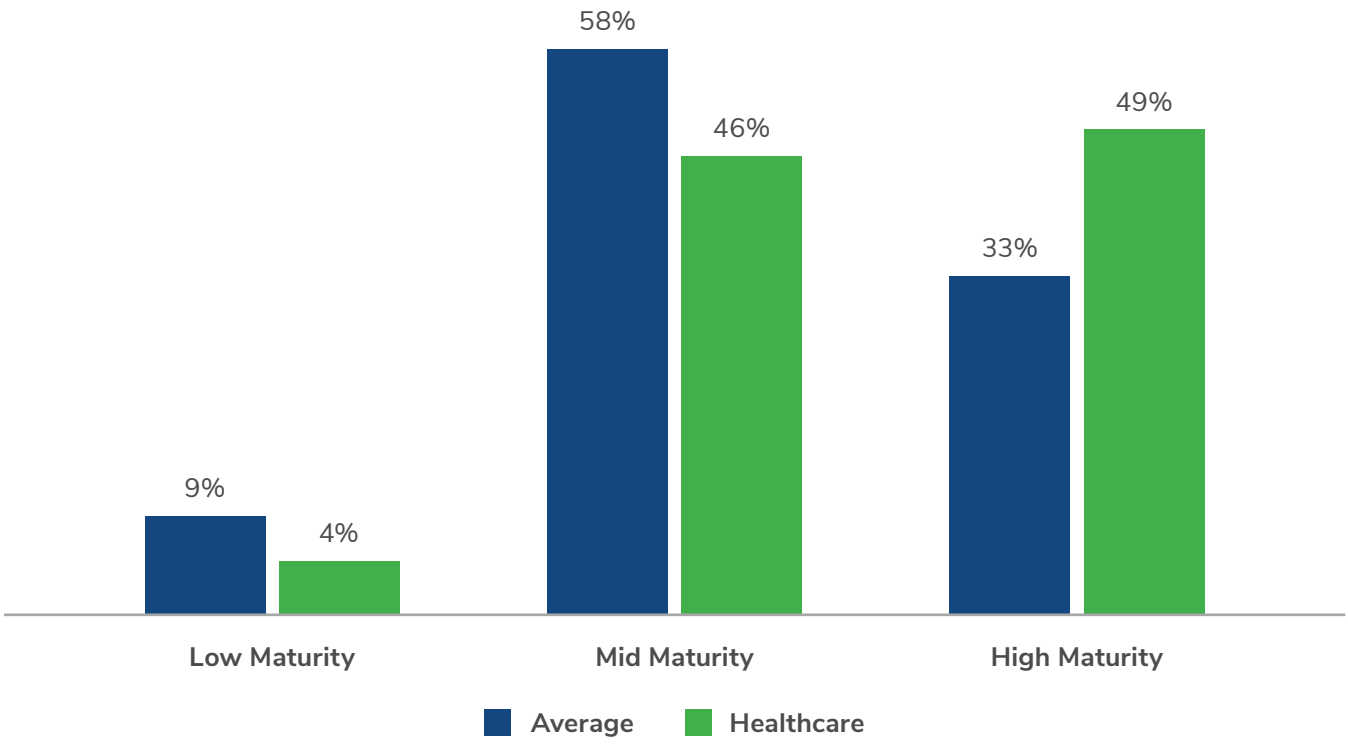
As we discovered in the **State of Cyber Defense: Detection and Response Maturity Model**, there is a worrying disconnect between how mature organizations believe they are and how mature they really are.

Alongside manufacturing and finance, healthcare was the most bullish sector in our research.

Nearly 50% of healthcare respondents rated their overall cybersecurity as “very mature,” more than any other sector, and 16 percentage points higher than the survey average.

It was also among the most likely to believe that absolutely zero improvements are needed to its security.

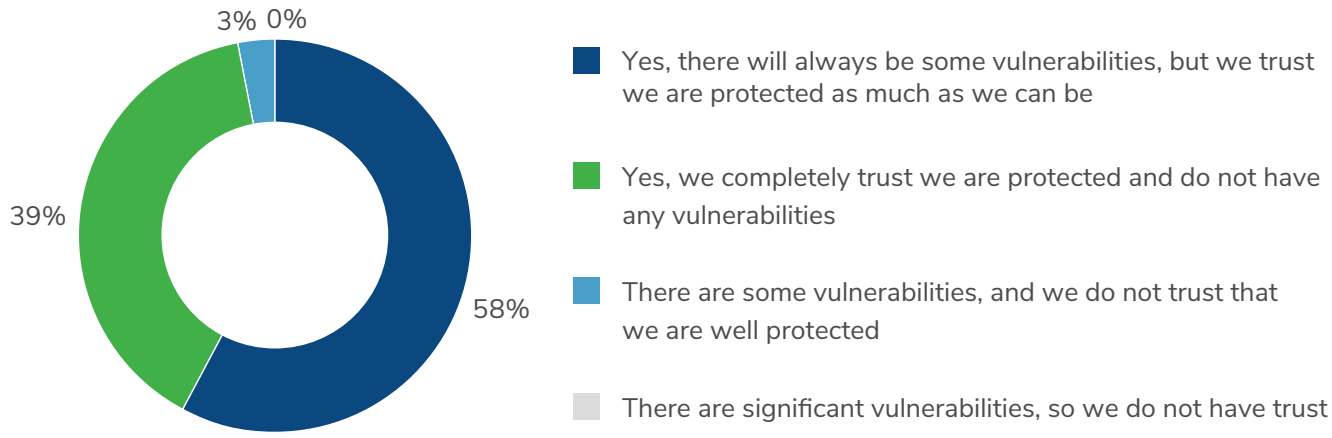
Perceived Cybersecurity Maturity, Overall vs. Healthcare



Only a tiny fraction of healthcare respondents (3%) said that they do not trust their organization's ability to defend against most cyberattacks. The vast majority have no such doubts.

More than a third (39%) said that they "completely" trust their protection and that they have no vulnerabilities whatsoever. Considering the rate at which threats continue to evolve and the high number of data breaches reported in every sector, this figure feels incredibly high.

Do You Trust Your Organization's Cybersecurity Defenses to Successfully Defend Against Most/All Cyber Attacks?



Unfortunately, our other survey questions which indicate the cyber maturity of these same organizations, would suggest that this confidence is wildly overzealous.

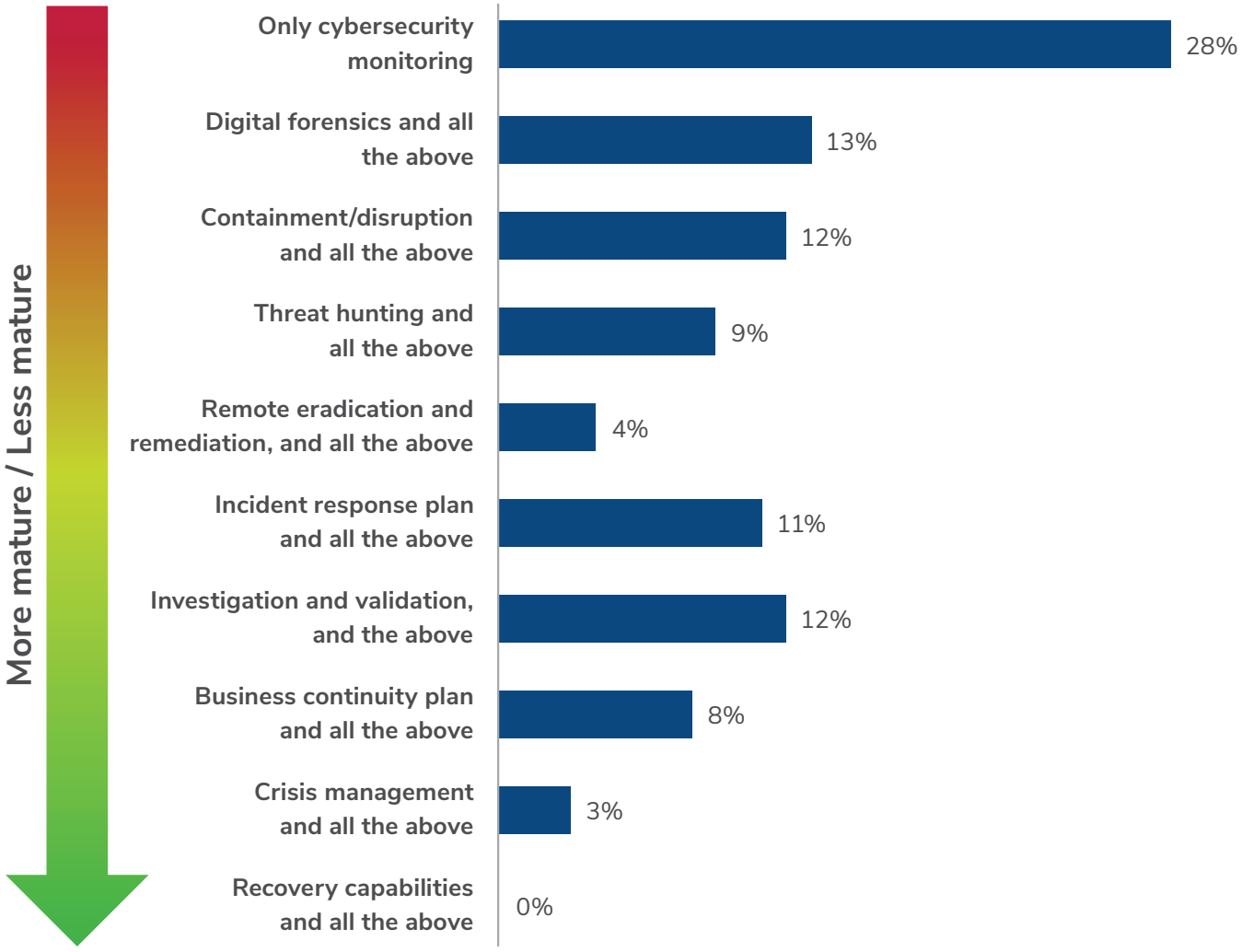
Real-World Security Capabilities

Given healthcare respondents' confidence and overwhelming belief that they have "very mature" cybersecurity provisions in place, we would expect to see that reflected in their real-world technical capabilities. However, there is a significant disconnect between healthcare's self-reported maturity scores and healthcare organization's actual ability to detect and respond to cyber incidents.

When it comes to threat detection and response capabilities, the healthcare industry is more likely to employ more basic or immature processes.

Indeed, many only employ the most basic security capabilities, such as cybersecurity monitoring, and none of the healthcare industry respondents surveyed had all threat and detection capabilities in place.

Threat and Detection Response Capabilities Used by Healthcare



Maturity Splits

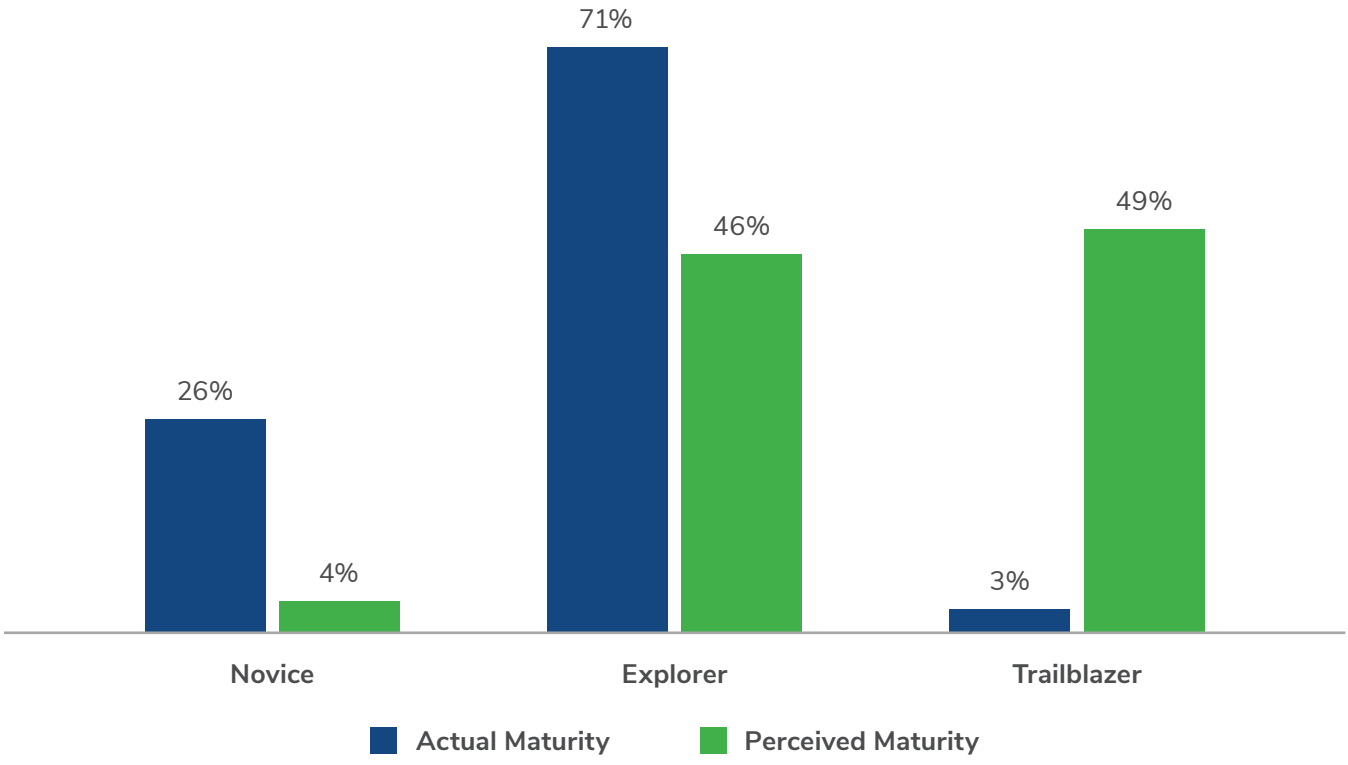
Our previous report analyzed and placed the global respondents into one of three categories—Novice, Explorer, or Trailblazer—depending on what stage they were at in their detection and response maturity journey, thus developing the **Detection and Response Maturity Model**.

The graph here demonstrates that the majority of respondents fall into the Novice or Explorer maturity groups, and only a small percentage of businesses are Trailblazers.

However, a large portion of the healthcare industry (49%) believe that they belong in the Trailblazer group. Unfortunately, based on the research, the majority (71%) belong in the Explorer category and over a quarter (26%) of businesses in the healthcare industry belong in the least mature, Novice, maturity group. The characteristics of the Novice, Explorer and Trailblazer maturity groups can be found in our **Maturity Model report**.

Compared to all industries, healthcare organizations are slightly more likely to be featured in the Novice category and slightly less likely to be featured in the Trailblazer category.

Actual vs. Perceived Maturity in the Healthcare Industry



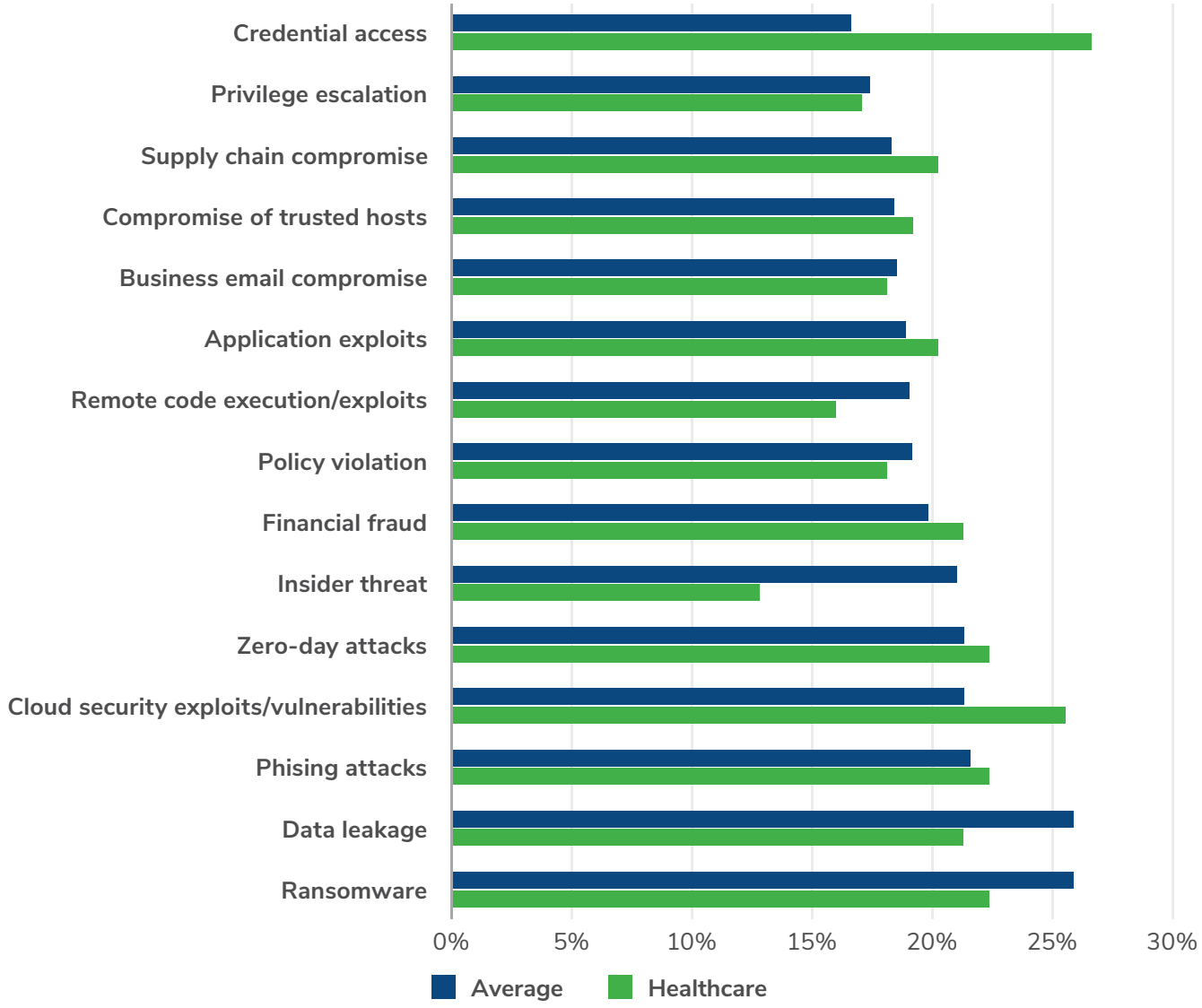
Security Priorities

The chart here shows that security priorities and threats facing healthcare organizations are broadly aligned with other industries. Healthcare companies are just as concerned with ransomware, BEC and phishing as other industries. However, there are a couple of notable anomalies. Healthcare organizations are considerably less concerned by insider threats, which was chosen by just 13% of healthcare respondents vs. 21% of all respondents.

Meanwhile, healthcare organizations appear to be far more concerned by credential access threats than any other industry.

Credential access was cited as most concerning threat type by only 16% of all 1000 respondents, making it the least concerning threat across all sectors. However, it was chosen by more than a quarter (26%) of healthcare professionals—more than ransomware, zero-day attacks and supply chain compromise.

Threat Types of Most Concern to the Healthcare Industry

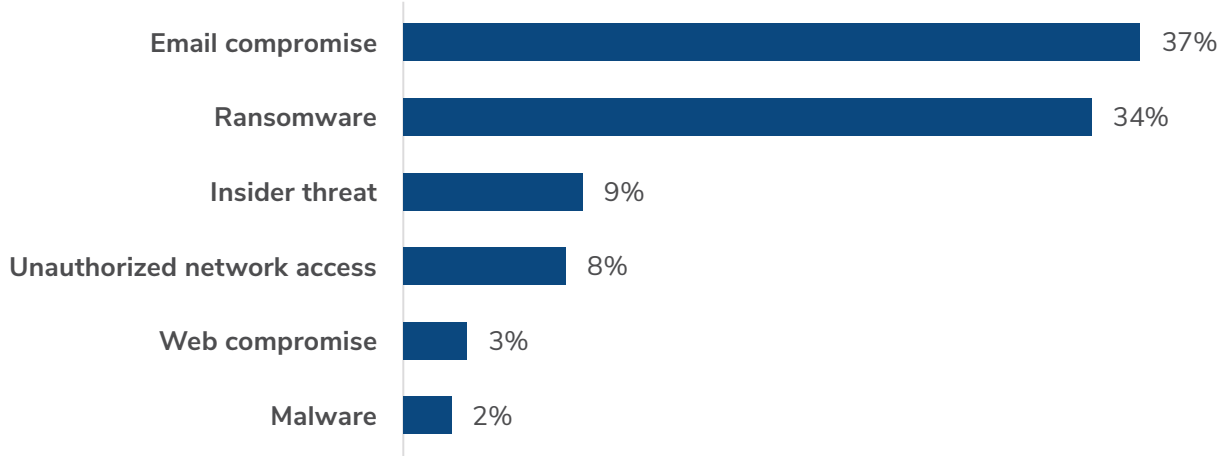


The Threats the Healthcare Industry Faces

As mentioned in the previous section, the healthcare industry appears to be more concerned with credential access threats than ransomware, zero-day attacks and supply chain compromise.

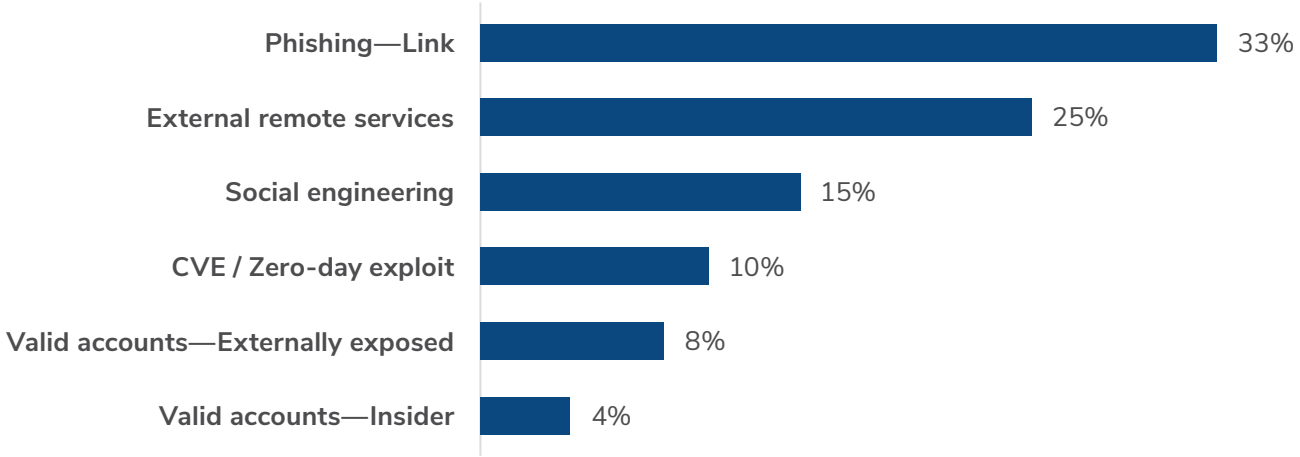
However, Kroll's Cyber Threat Intelligence team has seen the healthcare industry consistently targeted by ransomware groups using a combination of valid credentials theft and exploiting vulnerabilities.

Most Common Threat Incident Type Targeting the Healthcare Industry in 2023



As demonstrated in the above graph, email compromise and ransomware are the two most common incident types.

Most Common Initial Access Method for the Healthcare Industry in 2023



According to Kroll data, a third (33%) of attacks on the healthcare industry used phishing as the initial access method.

Lessons from Offensive Security

The Environment Is Sprawling: Healthcare is a wide-reaching environment and includes everything from clinics to hospitals, doctor's offices, medical labs and more. The level of investment available for cybersecurity will also range greatly depending on the size of the operation. A small rural clinic will not have the same budget for cybersecurity as a cutting-edge hospital. However, many healthcare institutions might use the same billing, insurance or third-party suppliers, linking them in a network a threat actor could exploit.

Regulation up to Interpretation: Regulations like the Health Insurance Portability and Accountability Act (HIPAA) are incredibly important to help protect patient privacy through the use of security controls. However, the disparate nature of the industry means that these regulations could be more stringent and specific in their language. Determining what is or isn't appropriate or adequate protection could vary significantly, especially as we've discovered in the previous section that a large proportion of the industry is only employing the least mature detection and response capabilities.

Time Poor and High Risk: As expected, professionals within the medical industry are incredibly time-poor and are dealing with far graver consequences compared to other sectors. Trying to find time to train medical professionals on new security measures or adding additional security steps to a doctor's sign-in process is often met with backlash. When losing time can mean the difference between life and death, this industry is in a uniquely difficult position and, thus, has a slower pace when it comes to upgrading its security practices.

Legacy Systems: When testing a hospital, it is common to encounter legacy systems within the network. However, often, these legacy systems are crucial and can be involved in operating medical equipment, such as an MRI machine. Replacing these legacy systems is not straightforward, replacing the PC could also mean replacing the entirety of the medical equipment, making the changes incredibly costly.

Top Considerations for the Industry:

- Businesses must complete risk assessments, such as the HIPAA risk assessment, to identify vulnerabilities and protect patient information on, at minimum, an annual basis.
- Conducting external and internal pen testing every year is critical to fully stress test security provisions and give insight into the risks a business faces, especially as threats evolve continuously.
- Making sure the basics are in place and doing the "simple stuff" often. While it might sound rudimentary, good password management, multi-factor authentication, and system updates are akin to washing hands in the medical profession. They are crucial first steps to making it harder for bad actors to infiltrate a network.

Data Breach

Of course, it's not a surprise that the healthcare industry is one of the most targeted sectors by threat actors. Indeed, unauthorized access by threat actors are one possible cause of data breaches.

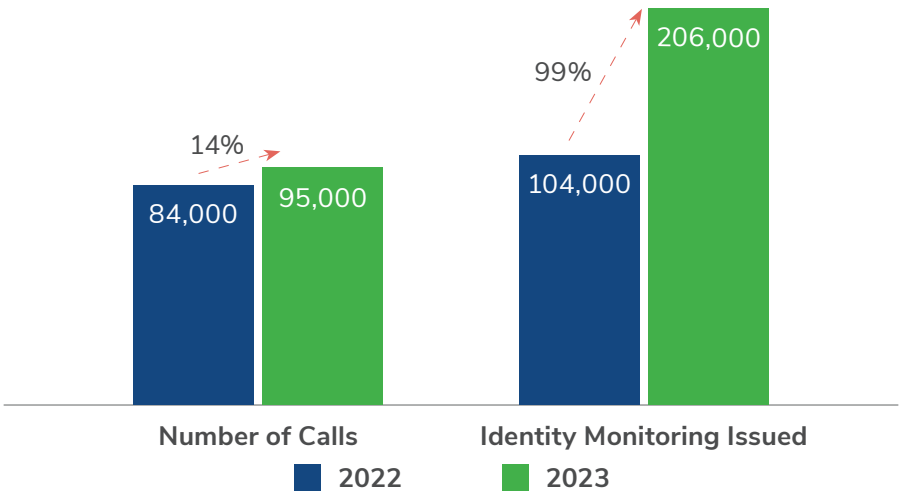
Kroll's last two Data Breach Outlook reports clearly demonstrate the vulnerability of the sector. Not only does it hold sensitive data which may be at risk of poor handling but threat actors with malicious intent may also be tempted to target and expose such data to cause disruption.

Most Breached Industries in 2022 and 2023

Sector	2022 Rank	2023 Rank
Healthcare	1	2
Finance	2	1
Professional Services	5	3
Retail	4	4
Industrial Services	3	5

Further investigation into the data unveils some insights into how concerned those in the healthcare sector are about the data breaches in question. The healthcare industry showed YoY increases in the number of inquiries following a breach (14%) and in the amount of credit or identity monitoring taken up (99%).

Kroll Engagement from the Healthcare Industry



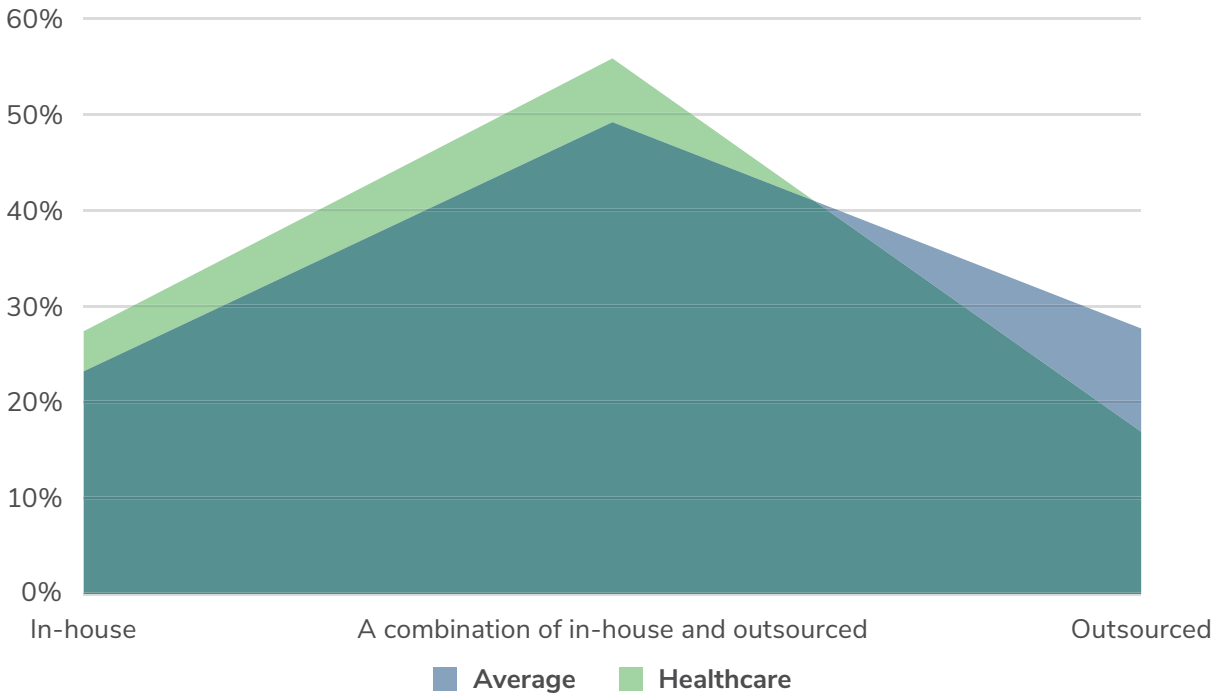
Kroll saw more engagement—in the form of calls and the number of identity monitoring services activated—from the healthcare sector than the financial sector in 2023, which is surprising given the finance sector was the most breached industry. Kroll provided a little more than 200,000 identity monitoring service activations.

Outsourcing Cybersecurity Services

Healthcare organizations are 65% less likely to fully outsource their cybersecurity services than the average organization (17% vs. 28%). They are also more likely to do everything in-house.

Again, this may be due to the differences between traditional office environments and more flexible sites like hospitals. Typically, healthcare organizations have internal IT and security teams to maintain control; it can be harder to run a remote or managed service for healthcare providers.

Cybersecurity Services Sourcing Model



However, this trend may be starting to shift. Of the healthcare respondents who currently manage all their cybersecurity services in-house, 62% confirmed that they have plans to outsource in the next 12 months.

Outsourcing may be becoming increasingly popular in healthcare due to a lack of in-house security resources and people, as well as the perceived benefits of leveraging the expertise of external cybersecurity teams.

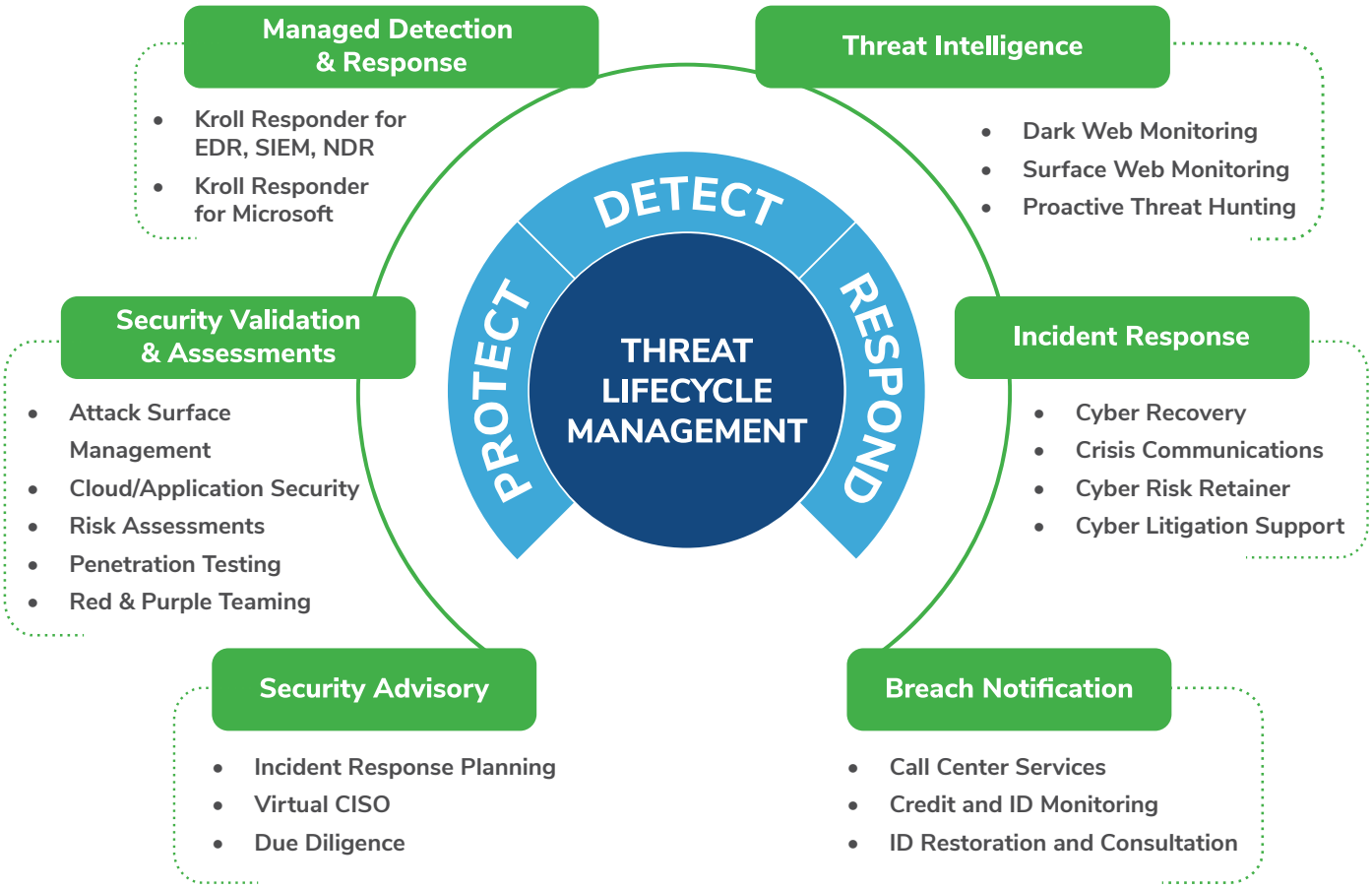
Outsourced managed security could help the healthcare industry close the self-diagnosis gap and better protect themselves in the future.

62% of healthcare providers with in-house security services are planning to outsource this year

KROLL

Kroll Capabilities

We are the incident response leaders. Merging complete response capabilities with frontline threat intelligence from over 3000 incidents handled per year and end-to-end expertise we protect, detect and respond against cyberattacks.



Kroll's proven cybersecurity capabilities enable organizations to progress their cyber maturity, whether they are in the Novice, Explorer, or Trailblazer group. Our elite cyber risk leaders are uniquely positioned to deliver end-to-end cybersecurity services worldwide.

Healthcare Cyber Expertise

Kroll helped 100s of healthcare organizations worldwide protect, detect, and respond to cyberattacks.

Protect

- Dozens of **penetration tests**, including web applications, network infrastructure, and cloud
- Nearly 100 **cyber risk assessments**, including HIPAA standards, cloud and email security, and remote work
- 10+ **vCISO engagements** to help with complex projects or overall strategy refinement

Detect

- 24x7 **Managed Detection and Response** to nearly 100 healthcare organizations worldwide, monitoring close to 100,000 endpoints and terabytes of data across SIEM instances

Respond

- 300+ **incident response** engagements where healthcare orgs were involved, including ransomware, business email compromise, IP theft, and insider threat among others
- **Breach notification**, call center services and identity monitoring for a population of 4M+ impacted by breaches in healthcare orgs

KROLL

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data, and technology to help clients stay ahead of complex demands. Kroll's team of over 6,500 professionals worldwide continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients with the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

For the latest insights, threat intelligence, and analysis from Kroll check out kroll.com/cyberblog

TALK TO A KROLL EXPERT TODAY

North America
T: 877 300 6816

UK
T: 808 101 2168

Brazil
T: 0800 761 2318

Additional hotlines at:
kroll.com/hotlines

Or via email:
CyberResponse@kroll.com

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.