Akamai | PORTER RESEARCH

WHITE PAPER

Porter Research for Healthcare & Life Sciences

Severity and Frequency of Cyberattacks Drive Urgency, Investment

Executive summary

The healthcare and life sciences communities have been undergoing a massive digital transformation since the COVID-19 pandemic. Everything from healthcare consumer expectations to government regulations are driving providers, payers, and pharmaceutical organizations to move aggressively toward digital interactions and transactions.

These and many other dramatic shifts are putting more healthcare organizations at risk of cybersecurity vulnerabilities and ransomware attacks that can jeopardize both patient safety and financial resiliency. To better understand and measure the security gaps that now exist across a more digital-centric healthcare industry, Porter Research completed a study of more than 100 IT and business leaders across the provider, payer, and pharmaceutical/life sciences industries. The study was conducted from November 2022 through January 2023.

The results reveal an alarming concern among leaders about their preparedness to prevent and mitigate ransomware attacks, along with an enhanced focus on the medical ecosystem and sustainability.

Key findings

60%	of leaders are “less than fully confident” in the technologies they currently use to prevent and mitigate ransomware attacks
81%	of leaders are currently relying on basic methodologies, such as email filtering and firewalls, as their primary defense mechanisms against cyberattacks
85%	of leaders place mitigating cyberattacks as a “high” or “very high priority” in 2023
82%	of leaders are increasing their investments aimed at preventing and mitigating ransomware attacks in 2023
100%	of leaders noted “growing hacker sophistication” as the primary driver behind the increase in ransomware attacks

> "The primary goals of phishing and email compromise have evolved from basic malware to ransomware and credential harvesting, a prime example of the progressive sophistication of hackers targeting healthcare organizations."
>
> — Microsoft's Digital Defense Report

As the frequency and severity of ransomware attacks on healthcare organizations continues to rapidly increase, so does the pressure on IT leaders when it comes to minimizing cybersecurity risks and having mitigation strategies in place at their organizations.

> "Not only are cyber criminals more organized than they were in the past, they are often more skilled and sophisticated."
>
> — American Hospital Association

Why is the healthcare industry uniquely at risk?

Rapid change in recent years, including the addition of virtual care services and the expansion of the Internet of Medical Things, propelled innovation in healthcare at a dizzying pace. Accelerating digitization drove many healthcare organizations to modernize their technology faster than their traditional security protocols and practices, which left them more prone to cyberattacks. And what were previously nefarious attacks and breaches are now shifting toward more demands for ransom through highly targeted, highly coordinated activity.

In its industry tracker of 14 leading industries worldwide, IMD Global Center for Digital Transformation noted a rapid ascension of healthcare and pharmaceuticals from the outward, lagging perimeter, to the middle of its Digital Vortex in just two years.

At the same time that healthcare is rapidly pursuing its digital transformation, cybercriminals are identifying the industry's weaknesses. These include:

- The prevalence of legacy systems that are not equipped to handle today's sophisticated attack technologies
- The massive collection of digital health and financial data that healthcare organizations have collected via their use of and dependencies on electronic health record systems and mobile applications
- The proliferation of application program interfaces (APIs) in an attempt to meet government standards for interoperability and public pressure to support smoother transitions across the continuum of care
- The expansion of the traditional "four walls" into at-home and virtual modalities of care (such as home health, remote patient monitoring, and remote workforces) that stretch the traditional boundaries of IT protection

Unlike other leading industries, such as manufacturing, retail, and media, healthcare involves millions of workers performing manual tasks like patient intake, medical documentation, and medical billing with millions of patients' sensitive medical data. And that data that is becoming more valuable on the dark web than ever before.

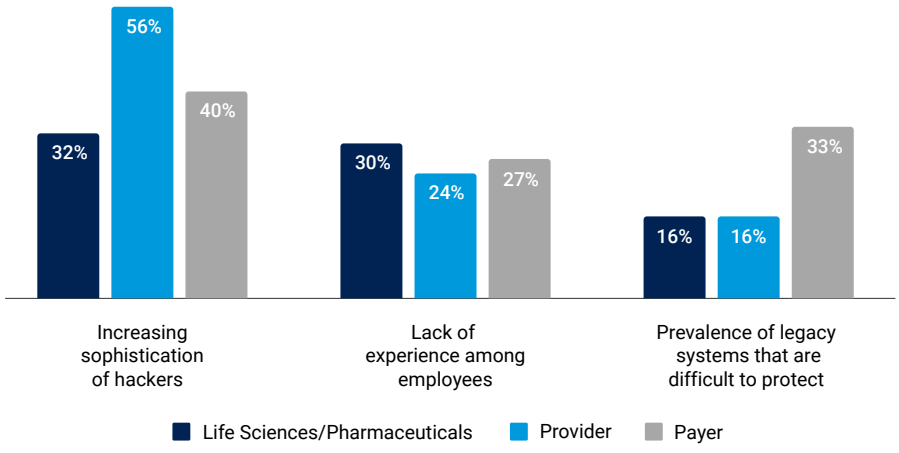
> **"Patient medical records sell on the dark web for as much as $1,000 per record compared with financial records, which are valued at $20 to $110, and Social Security numbers at $1."**
>
> **— Experian**

According to the Porter Research study, healthcare executives agree that the primary reason ransomware attacks are increasing is the growing sophistication of hackers. In fact, 56% of life sciences/pharmaceutical executives, 40% of payer executives, and 32% of provider executives cited hacker sophistication as the top driver for the volume of attacks.

> **"I think digital protection in healthcare is more complex than other industries, such as digital media. That involves a younger market, and has deployed more modern technologies — so digital media can more easily adapt and respond."**
>
> **— Porter Research healthcare executive interview**

As the number of attacks has risen, many study participants indicated they had experienced cyberattacks in their organizations. Fifty-four percent of provider executives in the Porter Research study reported experiencing an attack in the past three years, a number that could likely be higher given the many attacks that go unreported. Thirty-six percent of life sciences/pharmaceutical participants and 27% of payer participants also noted having experienced an attack in the past three years.

Top drivers for the increased volume of cyberattacks



Source: Porter Research; Sample: provider, and life sciences respondents surveyed between November 2022 and January 2023

Without proper technologies and methodologies in place, healthcare organizations that experience a ransomware attack are left with few options other than paying the ransom. According to TechTarget, 61% of healthcare organizations pay the ransom, compared with the global average of 46% across other industries. This is likely due to the fact that patients' lives are at stake when operations are compromised, and healthcare organizations need to take the fastest route to system restoration.

> **"I think many healthcare organizations struggle to balance the resources they need to protect their organizations with the resources they need to support high-quality care and changing government regulations. When you couple this with the rigidity of legacy systems and a lack of focus on cybersecurity for several years, it is very hard to catch up to the level of sophistication that today's cyber criminals have."**
>
> **— Porter Research healthcare executive interview**

Many security industry analysts and innovators are also taking notice of emerging trends in healthcare ransomware attacks:

- "The core cybercrime method, which is phishing, hasn't changed, but the sophistication of [methods] has." — Chris Jenkins, Chief Digital Officer of the FBI
- "Targeted attacks are way more sophisticated and specific, and we have seen an increase in reports that indicate custom ransomware has been launched against an organization's specific technology stack." — Forbes

The real impacts of ransomware in healthcare

The impacts of a ransomware attack on healthcare organizations come in many different forms, including the loss of public trust, loss of revenue, backlogs in work, decreased patient satisfaction and loyalty, and legal repercussions and fines.

Executives report the most common negative impacts of ransomware

Healthcare providers

- Loss of public trust (76%)
- Financial loss (74%)
- Decreased patient satisfaction/loyalty (70%)

Life sciences/pharmaceuticals

- Financial loss (80%)
- Legal repercussions/fines (74%)
- Decreased patient satisfaction/loyalty (46%)
- Loss of public trust (43%)

Healthcare payers

- Legal repercussions (67%)
- Fines incurred (50%)
- Backlog of claims processed (33%)

In addition to the financial loss that occurs when systems are down, healthcare organizations are at risk of impacting patient lives. The AHA recently described a ransomware attack on a hospital as "crossing the line from an economic crime to a threat-to-life crime," a description that brings acute awareness to the potential repercussions of ransomware attacks in healthcare.

Current security mechanisms are not enough — strategic investment can bridge security gaps

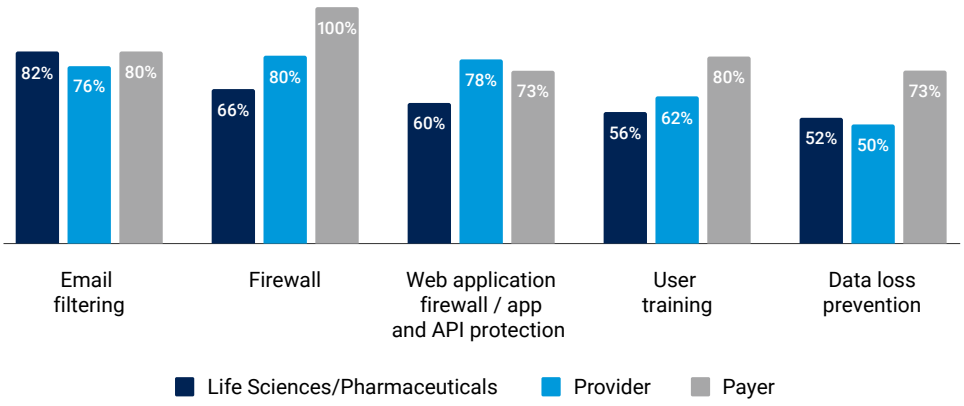
When evaluating what healthcare organizations are doing today, the landscape of approaches is broad but not deep. The Porter Research study reveals that the vast majority of organizations are using only the most basic methods, such as email filtering and firewalls, as their primary mechanisms to protect their entities.

Ransomware protection methodologies

These basic tools are no match for today's sophisticated cybercriminals and, according to Porter Research, healthcare industry executives recognize the need for improvement. As a result, these executives are shifting their investment strategies.

> **The current cybersecurity protection landscape across healthcare providers, life sciences/pharmaceuticals, and providers focuses on mostly basic technology and training, limiting these organizations' ability to defend against ransomware threats.**
>
> **— Porter Research, 2023**

Yesterday's protections don't match today's capabilities



Source: Porter Research; Sample: provider, payer, and life sciences respondents surveyed between November 2022 and January 2023

The majority of respondents across all healthcare market segments said that their budgets to prevent ransomware have increased over the past 12 months, including:

- 78% of respondents from provider organizations
- 73% of respondents from payers
- 72% of respondents from life sciences/pharmaceutical organizations

The majority of respondents also said they expect cybersecurity investments at their organizations to continue to rise across all market segments over the next few years, including:

- 78% of respondents from provider organizations
- 87% of respondents from payers
- 80% of respondents from life sciences/pharmaceutical organizations

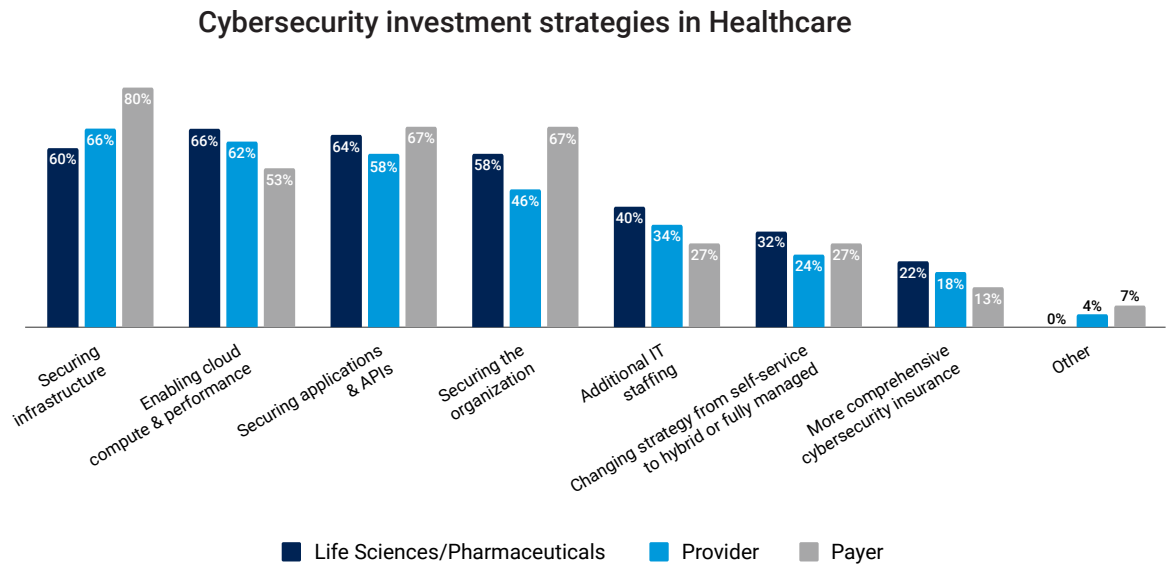
These findings are further supported by data from other industry sources, including Gartner's 2023 Healthcare Provider CIO and Technology Executive Survey, which notes 75% of respondents will spend more on cybersecurity and information security in 2023 than they did in 2022.

KLAS Research and Bain & Company also point to cybersecurity as a priority investment, with 95% of their provider study participants planning to make significant investments in technology in 2023, with primary areas of focus on cybersecurity, IoT security, and patient privacy monitoring, in addition to revenue cycle management.

Top priorities in cybersecurity investments

According to the Porter Research respondents, the foremost priorities for investment across all segments include securing infrastructure, enabling cloud compute, and securing applications and APIs.

> **Study participants across all market segments indicated they are increasing investment in cybersecurity, with most planning to do so in the next 12 months.**
>
> **— Porter Research, 2023**



Source: Porter Research; Sample: provider, payer, and life sciences respondents surveyed between November 2022 and January 2023

Cybersecurity investment strategies in healthcare

If we look more specifically at the technologies involved in these major investment categories, we see the areas of focus are:

Securing infrastructure

- Segmentation
- DDoS protection
- Authoritative DNS
- Global server load balancing

Securing applications and APIs

- In-browser threat protection
- Web application and API protection
- Account takeover protection

Enabling cloud compute and performance

- Serverless edge computing
- Alternate cloud
- Content delivery network and edge logic solutions
- Load testing platform and real-time user monitoring
- Optimizing videos/images at the edge

Securing the organization

- Multi-factor authentication
- Secure web gateway
- Zero Trust Network Access
- Segmentation

When asked in the Porter Research study to rank their top security strategies for the next one to three years, healthcare provider organizations prioritized, in order, securing their infrastructure, enabling cloud transformation, followed by implementing a Zero Trust framework, and securing applications and APIs.

Life sciences/pharmaceutical organizations view cloud transformation, securing applications and APIs, and securing their infrastructure as top priorities, in that order.

Payers pointed to securing their infrastructure, securing applications and APIs, and securing their organizations.

Aligning with the right security partner

As leaders evaluate technology vendors to support their cybersecurity strategies, they are prioritizing factors that ensure long-term protection and breakthrough methods to protect against advancing hacker sophistication.

Study participants in the provider segment indicated that they are prioritizing the following factors when considering cybersecurity technology partners (listed in order of importance):

1. The ability to prevent hackers from going undetected for an extended period (rated 4.38/5)
2. The ability to prevent hackers from moving from one system to another (4.30/5)
3. Ease of use (4.22/5)

This prioritization points to the fact that healthcare leaders are focused on countering the advanced tactics hackers employ as they attack healthcare organizations.

Life sciences/pharmaceutical IT executive participants shared similar insights, with the following priorities:

1. The ability to prevent hackers from going undetected for an extended period (rated 4.42/5)
2. The ability to prevent hackers from moving from one system to another (4.38/5)
3. Cost-effective solutions (4.18/5)

Payer IT executive participants are seeking partners with similar capabilities:

1. The ability to prevent hackers from going undetected for an extended period (rated 4.6/5)
2. The ability to prevent hackers from moving from one system to another (4.0/5)
3. Cost-effective solutions (4.0/5)

Impediments to advancements in cybersecurity

Although healthcare industry executives know what needs to be done and are prioritizing investments to meet security needs, they face myriad other challenges, including the resource constraints that are also impacting other industries as they navigate labor shortages.

> **According to the 2021–2023 Emerging Technology Roadmap for Large Enterprises from Gartner, 64% of IT executives cite talent shortages as the most significant barrier to the adoption of emerging technology, compared with only 4% in 2020.**

Healthcare provider groups' top 3 barriers to meeting security needs

1. Lack of experience and resources on their IT teams (52%)
2. Lack of investment in modern technology (52%)
3. Lack of comprehensive cyberstrategy (32%)

Life sciences/pharmaceuticals top 3 challenges to meeting security needs

1. Securing personal devices (84%)
2. Securing access for remote/hybrid employees (78%)
3. Preventing access to systems via phishing (66%)

Healthcare payers' top 3 barriers to meeting security needs

1. Securing access for remote/hybrid employees (93%)
2. Securing personal devices (80%)
3. Preventing access to systems via phishing (80%)

Looking ahead

The first step to solving any challenge is acknowledging that it exists. The Porter Research study reveals that healthcare leaders across all segments are doing just that. The next step is identifying the partner that can help overcome those challenges.

Advancements are being made by many major security vendors, including Akamai, a leading provider of security, compute, and delivery solutions that help healthcare organizations prevent and mitigate ransomware attacks. Akamai works with healthcare organizations to implement advanced security strategies through technology and processes, including:

- Web application firewall/app and API protection
- Firewalls
- Microsegmentation
- Multi-factor authentication/two-factor authentication
- Endpoint protection/antivirus
- Secure web gateway/sandboxing
- Data loss prevention
- Email filtering
- Threat hunting/honeypots
- Patching/vulnerability management
- Backups
- User training

To assess your readiness and learn more about advanced protections for your organization, visit www.akamai.com/healthcare

PORTER RESEARCH

Porter Research works with healthcare and IT companies to develop and execute market research programs and create strategies using market intelligence uncovered. With 30 years of experience, Porter Research has worked with more than 300 IT companies, and completes thousands of interviews annually. This means Porter Research knows your industry. We know how you need to use the data, and we execute the right research program to uncover what you can't find on your own.

Akamai

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn. Published 02/23.