

Importance of IT Security Amid Evolving Care Models in Healthcare and Life Sciences

February 2024: Complimentary Abstract / Table of Contents



Our research offerings

This report is included in the following research program(s):
[Cybersecurity, Life Sciences Information Technology, Payer and Provider Information Technology](#)

- ▶ Amazon Web Services (AWS)
- ▶ Application Services
- ▶ Artificial Intelligence (AI)
- ▶ Asset and Wealth Management
- ▶ Banking and Financial Services Business Process
- ▶ Banking and Financial Services Information Technology
- ▶ Catalyst™
- ▶ Clinical Development Technology
- ▶ Cloud and Infrastructure
- ▶ Contingent Staffing
- ▶ Contingent Workforce Management
- ▶ Customer Experience Management Services
- ▶ CX Excellence
- ▶ CXM Technology
- ▶ Cybersecurity
- ▶ Data and Analytics
- ▶ Digital Adoption Platforms
- ▶ Digital Services
- ▶ Digital Workplace
- ▶ Employee Experience Management (EXM) Platforms
- ▶ Employer of Record (EOR)
- ▶ Engineering Research and Development
- ▶ Enterprise Platform Services
- ▶ Exponential Technologies
- ▶ Finance and Accounting
- ▶ Financial Services Technology (FinTech)
- ▶ Forces & Foresight
- ▶ GBS Talent Excellence
- ▶ Global Business Services
- ▶ Google Cloud
- ▶ HealthTech
- ▶ Human Resources
- ▶ Insurance Business Process
- ▶ Insurance Information Technology
- ▶ Insurance Technology (InsurTech)
- ▶ Insurance Third-Party Administration (TPA) Services
- ▶ Intelligent Document Processing
- ▶ Interactive Experience (IX) Services
- ▶ IT Services Excellence
- ▶ IT Talent Excellence
- ▶ Life Sciences Business Process
- ▶ Life Sciences Commercial Technologies
- ▶ Life Sciences Information Technology
- ▶ Locations Insider™
- ▶ Marketing Services
- ▶ Market Vista™
- ▶ Microsoft Azure
- ▶ Microsoft Business Application Services
- ▶ Modern Application Development (MAD)
- ▶ Mortgage Operations
- ▶ Multi-country Payroll
- ▶ Network Services and 5G
- ▶ Oracle Services
- ▶ Outsourcing Excellence
- ▶ Payer and Provider Business Process
- ▶ Payer and Provider Information Technology
- ▶ Price Genius – AMS Solution and Pricing Tool
- ▶ Pricing Analytics as-a-Service
- ▶ Process Intelligence
- ▶ Process Orchestration
- ▶ Procurement and Supply Chain
- ▶ Recruitment
- ▶ Retail and CPG IT Services
- ▶ Retirement Technologies
- ▶ Revenue Cycle Management
- ▶ Rewards and Recognition
- ▶ SAP Services
- ▶ Service Optimization Technologies
- ▶ Software Product Engineering Services
- ▶ Supply Chain Management (SCM) Services
- ▶ Sustainability Technology and Services
- ▶ Talent Genius™
- ▶ Technology Skills and Talent
- ▶ Trust and Safety
- ▶ Value and Quality Assurance (VQA)

If you want to learn whether your organization has a membership agreement or request information on pricing and membership options, please contact us at info@everestgrp.com

[Learn more about our custom research capabilities](#)

Benchmarking

Contract assessment

Peer analysis

Market intelligence

Tracking: providers, locations, risk, technologies

Locations: costs, skills, sustainability, portfolios

Contents

For more information on this and other research published by Everest Group, please contact us:

Chunky Satija, Vice President

Durga Ambati, Practice Director

Arjun Chauhan, Senior Analyst

Amala Varsheni KK, Senior Analyst

1. Introduction and overview	4
• Research methodology	5
• Focus of the research	6
2. Preview of cybersecurity market in Healthcare and Life Sciences (HLS) industry	7
• Evolving landscape of cyber threats	8
• Exposure points and key cyber attacks	9
• Cybersecurity adoption drivers	10
• Challenges faced in building cyber resilience	11
• Generative AI in cybersecurity	12
3. Key cybersecurity service opportunities in HLS industry	13
• Key security themes	14
– Identity Access Management (IAM)	15
– Data security	17
– Managed Detection and Response (MDR)	19
– Connected devices security	21
• Zero-trust model	23
4. Cybersecurity future outlook in HLS industry	24
• Recent investments by service providers	25
• Implications for service providers	26
• Implications for enterprises	27
5. Appendix	28
• Glossary	29
• Research calendar	30

Background and scope of this research

The Healthcare and Life Sciences (HLS) industry is increasingly utilizing modern technology by effectively utilizing Internet of Things(IoT)-enabled devices, automation, predictive and prescriptive analytics, and highly scalable, interconnected, digital health platforms. Despite rapid technological advances, the healthcare and life sciences industry faces significant cyber threats including targeted breaches of health records, patient databases, and pharmaceutical intellectual property. Additionally, there is a risk of disrupting IoT-based medical devices. Navigating through evolving regulations such as the Affordable Care Act (ACA), the American Healthcare Act (AHCA), Health Insurance Portability and Accountability Act (HIPAA), and Medicare reforms such as MACRA adds to the industry's challenges. Hence, the rate of outsourcing of cybersecurity services has been on an upward trajectory in the healthcare and life sciences industry.

In this report, we analyze the current state of cybersecurity adoption in the healthcare and life sciences industry, demand trends of cybersecurity services, challenges in building cyber-resilience in the HLS industry, and the emergence of new industry-specific cybersecurity themes. Further, the report discusses the cybersecurity opportunity areas for service providers to focus on in the coming years.

Scope of this report



Geography
Global



Industry
Healthcare and life sciences



Services
Cybersecurity

Overview and abbreviated summary of key messages

This report highlights the cybersecurity market in the Healthcare and Life Sciences (HLS) industry. It focuses on key drivers for the adoption of cybersecurity solutions in the HLS industry, significant challenges faced by HLS enterprises in building cyber resilience, generative AI use cases in cybersecurity, and key cybersecurity service opportunities in the HLS industry. It also identifies the key areas of investment for service providers and implications for enterprises to build cyber resilience.

Some of the findings in this report, among others, are:

Market drivers and challenges in HLS industry

- HLS industry has been increasingly vulnerable to data breaches in recent times and enterprises are implementing various measures to address the rising threat of data breaches
- Key drivers for HLS enterprises adopting cybersecurity solutions consist of patient privacy and regulations, the emerging threat landscape, and the increasing need for securing medical devices
- While enterprises are leveraging cybersecurity solutions in building cyber resilience, challenges such as outdated systems and technologies, lack of skills/talent, and complex cloud hosting environment of enterprises hinder its adoption








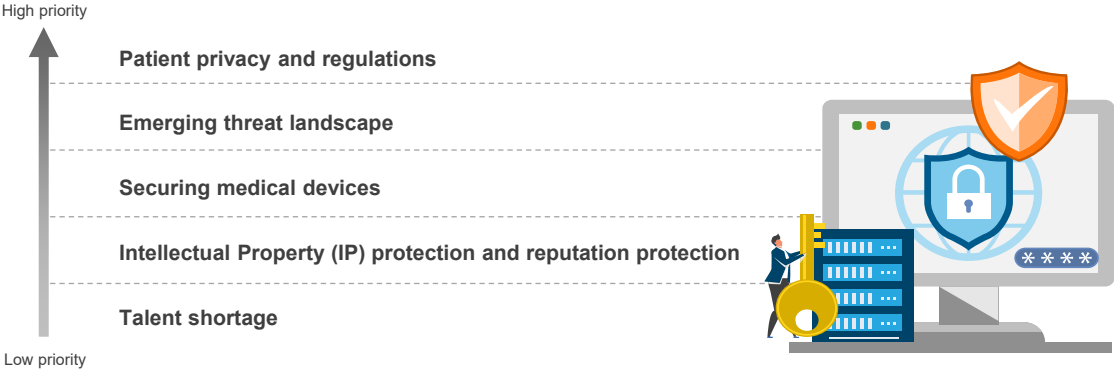
















Key cybersecurity service opportunities

- Four themes including Identity Access Management (IAM), data security, Managed Detective Services (MDR), and connected devices security are identified to be significant in the HLS industry. In HLS enterprises,
 - Implementation of robust access controls and user identity management to safeguard patient health records and sensitive research data is imperative
 - Identifying data breach origins and implementing robust security measures addressing both internal and external risks is important
 - MDR services assist in promptly detecting and responding to security incidents, especially when lacking internal resources or expertise for effective security operations
 - Connected devices can be secured through continuous monitoring, automated third-party penetration testing, and real-time vulnerability management
- Zero-trust security is increasingly adopted in HLS sectors to safeguard sensitive data and systems from security threats

Future outlook

- Moving forward, threat intelligence programs, unified IAM solutions, and AI/ML-powered behavior analytics tools are found as potential investment areas for service providers
- Evaluating cyber risks and purchasing cyber insurance policies remain a key priority strategy for HLS enterprises to build a cyber-resilient organization

This study offers the cybersecurity services market in the HLS industry providing a deep dive into key aspects of emerging opportunities in the market; below are four charts to illustrate the depth of the report

Exposure points and cyber threats	Cybersecurity adoption drivers						
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p><u>Exposure points that compromise cybersecurity</u></p> <ul style="list-style-type: none">  Mismanaged cloud hosting  Employee negligence  Unsecure data sharing with third parties </div> <div style="width: 48%;"> <p><u>Cyber threats/attacks</u></p> <ul style="list-style-type: none">  Ransomware attacks  Insider threat  Phishing scams  Medical device security breach </div> </div>	<p>Drivers for adoption of cybersecurity measures in HLS</p>  <ul style="list-style-type: none"> High priority Patient privacy and regulations Emerging threat landscape Securing medical devices Intellectual Property (IP) protection and reputation protection Talent shortage Low priority 						
Key security opportunities	Implications for service providers						
<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 33%;"> IAM</td> <td style="width: 33%;"> Data security</td> <td style="width: 33%;"> MDR</td> </tr> <tr> <td colspan="2"> Connected devices security</td> <td></td> </tr> </table>	 IAM	 Data security	 MDR	 Connected devices security			<ul style="list-style-type: none">  Threat intelligence programs / service offerings  Unified identity and access management  AI/ML-powered user behavior analytics tools  APIs and the template to ensure secure configuration of systems running in the public cloud
 IAM	 Data security	 MDR					
 Connected devices security							

Research calendar

Payer and Provider Information Technology

Published Planned Current release

Reports title	Release date
Care Management Trailblazers	July 2023
Healthcare Data & Analytics Services – Provider Compendium 2023	August 2023
Rising adoption of Home-based Healthcare Solutions	September 2023
Rising adoption of Behavioral and Mental Health Services by Healthcare Enterprises	September 2023
Patient Engagement Platforms PEAK Matrix® Assessment 2023	October 2023
Revenue Cycle Management (RCM) Platforms PEAK Matrix® Assessment 2023	November 2023
Transforming Healthcare through Generative AI: A Game-changing Impact	December 2023
Healthcare Payer Digital Services PEAK Matrix® Assessment 2023	December 2023
Importance of IT Security Amid Evolving Care Models in Healthcare and Life Sciences	February 2024
Member Engagement Trailblazers	Q1 2024
Rising Adoption of Behavioral and Mental Health Services by Healthcare Enterprises	Q1 2024
Healthcare Outlook for 2024	Q1 2024
Patient and Member Engagement Technology	Q1 2024
Healthcare Industry Cloud Services PEAK Matrix® Assessment 2024	Q2 2024
Key Trends in the Europe and Asia-Pacific Healthcare Markets	Q2 2024

Note: [Click](#) to see a list of all of our published Payer and Provider Information Technology reports

Research calendar

Life Sciences Information Technology

Published Planned Current release

Reports title	Release date
Life Sciences Digital Services PEAK Matrix® Assessment 2022	September 2022
Life Sciences Customer Experience Platforms (CXP) PEAK Matrix® Assessment 2023	December 2022
Medical Devices Digital Services PEAK Matrix® Assessment 2023	May 2023
Life Sciences Smart Manufacturing Services PEAK Matrix® Assessment 2023	August 2023
Life Sciences Smart Manufacturing Services – Provider Compendium 2023	October 2023
Life Sciences Next-generation Customer Engagement Platforms (CEP) PEAK Matrix® Assessment 2023	November 2023
Life Sciences Next-generation Customer Engagement Platforms (CEP) – Provider Compendium 2023	December 2023
Life Sciences Digital Services Specialists PEAK Matrix® Assessment 2024	January 2024
Importance of IT Security Amid Evolving Care Models in Healthcare and Life Sciences	February 2024
Life Sciences Digital Services Specialists – Provider Compendium 2024	Q1 2024
Life Sciences Customer Experience Platform (CXP) Adoption Playbook	Q1 2024
Life Sciences Platform Services PEAK Matrix® Assessment 2024	Q2 2024
Life Sciences Digital Services for Mid-market Enterprises – Service Provider Compendium 2024	Q2 2024
Future of the Hybrid Commercial Model – Orchestrating Hyper-Personalized Customer Journeys	Q2 2024
Life Sciences Platform Services – Provider Compendium 2024	Q2 2024

Note: [Click](#) to see a list of all of our published Life Sciences Information Technology reports

Research calendar

Cybersecurity

Published
 Planned
 Current release

Reports title	Release date
Identity and Access Management (IAM) Services PEAK Matrix® Assessment 2023	July 2023
Cloud Security Services PEAK Matrix® Assessment 2023	November 2023
Operational Technology (OT) Security Products PEAK Matrix® Assessment 2023	November 2023
Identity and Access Management (IAM) Services – Provider Compendium 2023	December 2023
From Risk Mitigation to ESG Leadership: The Untapped Potential of MDR	January 2024
Cloud Security Services – Provider Compendium 2024	January 2024
Importance of IT Security Amid Evolving Care Models in Healthcare and Life Sciences	February 2024
Cybersecurity Specialist Services PEAK Matrix® Assessment 2024	Q1 2024
Cybersecurity Specialist Services Provider Compendium 2024	Q2 2024
Cybersecurity Services PEAK Matrix® Assessment 2024 – North America	Q2 2024
Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe	Q2 2024
Identity and Access Management (IAM) State of the Market 2024	Q3 2024
Cybersecurity Services Provider Compendium 2024 – North America & Europe	Q3 2024

Note: [Click](#) to see a list of all of our published Cybersecurity reports



Everest Group is a leading research firm helping business leaders make confident decisions. We guide clients through today's market challenges and strengthen their strategies by applying contextualized problem-solving to their unique situations. This drives maximized operational and financial performance and transformative experiences. Our deep expertise and tenacious research focused on technology, business processes, and engineering through the lenses of talent, sustainability, and sourcing delivers precise and action-oriented guidance. Find further details and in-depth content at www.everestgrp.com.

Stay connected

Dallas (Headquarters)
info@everestgrp.com
+1-214-451-3000

Bangalore
india@everestgrp.com
+91-80-61463500

Delhi
india@everestgrp.com
+91-124-496-1000

London
unitedkingdom@everestgrp.com
+44-207-129-1318

Toronto
canada@everestgrp.com
+1-214-451-3000

Website
everestgrp.com

Social Media
 @EverestGroup
 @Everest Group
 @Everest Group
 @Everest Group

Blog
everestgrp.com/blog

NOTICE AND DISCLAIMERS

IMPORTANT INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY AND IN ITS ENTIRETY. THROUGH YOUR ACCESS, YOU AGREE TO EVEREST GROUP'S TERMS OF USE.

Everest Group's Terms of Use, available at www.everestgrp.com/terms-of-use/, is hereby incorporated by reference as if fully reproduced herein. Parts of these terms are pasted below for convenience; please refer to the link above for the full version of the Terms of Use.

Everest Group is not registered as an investment adviser or research analyst with the U.S. Securities and Exchange Commission, the Financial Industry Regulatory Authority (FINRA), or any state or foreign securities regulatory authority. For the avoidance of doubt, Everest Group is not providing any advice concerning securities as defined by the law or any regulatory entity or an analysis of equity securities as defined by the law or any regulatory entity.

All Everest Group Products and/or Services are for informational purposes only and are provided "as is" without any warranty of any kind. You understand and expressly agree that you assume the entire risk as to your use and any reliance upon any Product or Service. Everest Group is not a legal, tax, financial, or investment advisor, and nothing provided by Everest Group is legal, tax, financial, or investment advice. Nothing Everest Group provides is an offer to sell or a solicitation of an offer to purchase any securities or instruments from any entity. Nothing from Everest Group may be used or relied upon in evaluating the merits of any investment. Do not base any investment decisions, in whole or part, on anything provided by Everest Group.

Products and/or Services represent research opinions or viewpoints, not representations or statements of fact. Accessing, using, or receiving a grant of access to an Everest Group Product and/or Service does not constitute any recommendation by Everest Group that recipient (1) take any action or refrain from taking any action or (2) enter into a particular transaction. Nothing from Everest Group will be relied upon or interpreted as a promise or representation as to past, present, or future performance of a business or a market. The information contained in any Everest Group Product and/or Service is as of the date prepared, and Everest Group has no duty or obligation to update or revise the information or documentation. Everest Group may have obtained information that appears in its Products and/or Services from the parties mentioned therein, public sources, or third-party sources, including information related to financials, estimates, and/or forecasts. Everest Group has not audited such information and assumes no responsibility for independently verifying such information as Everest Group has relied on such information being complete and accurate in all respects. Note, companies mentioned in Products and/or Services may be customers of Everest Group or have interacted with Everest Group in some other way, including, without limitation, participating in Everest Group research activities.