Healthcare IT Security Services PEAK Matrix™ Assessment with Service Provider Landscape 2020

Healthcare IT Services (ITS)
Market Report – December 2019: Complimentary Abstract / Table of Contents

Everest Group®
PEAK MATRIX™

Our research offerings for global services

► **Market Vista™**
Global services tracking across functions, sourcing models, locations, and service providers – industry tracking reports also available

► Application Services	► Human Resources
► BPS | Banking & Financial Services	► ITS | Banking & Financial Services
► BPS | Healthcare & Life Sciences	► ITS | Healthcare
► BPS | Insurance	► ITS | Insurance
► Catalyst™	► IT Services Executive Insights™
► Cloud & Infrastructure	► ITS | Life Sciences
► Customer Experience Management Services	► Locations Insider™
► Data & Analytics	► PricePoint™
► Digital Services	► Procurement
► Engineering Services	► Recruitment & Talent Acquisition
► Enterprise Platform Services	► Service Optimization Technologies
► Finance & Accounting	

More about membership

In addition to a suite of published research, a membership may include

- Accelerators™
- Analyst access
- Data cuts
- Pinnacle Model™ reports
- PriceBook
- Virtual Roundtables
- Workshops

Custom research capabilities

- Benchmarking | Pricing, delivery model, skill portfolio
- Peer analysis | Scope, sourcing models, locations
- Locations | Cost, skills, sustainability, portfolio – plus a tracking tool
- Tracking services | Service providers, locations, risk
- Other | Market intelligence, service provider capabilities, technologies, contract assessment

Membership information

- This report is included in the following research program(s)
  – Healthcare IT Services (ITS)
- 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, unitedkingdom@everestgrp.com, or india@everestgrp.com

Everest Group® RESEARCH

Table of contents (page 1 of 2)

Table of contents

Background of the research

Healthcare challenges such as changing business and care delivery models to support patient-centricity and consumerism, growing competition from both within and outside the industry, and increasing regulatory pressures are leading to increased investments in data and technology by enterprises. Point-to-point upgrades, coupled with high technical debt levels, have increased security vulnerabilities to a large extent. The healthcare industry has been slow to respond to cyber threats and has lagged other industries when it comes to IT security investments, making healthcare a lucrative target for hackers. As a result, the past few years have seen some of the biggest attacks on healthcare enterprises, resulting in theft of millions of patient records.

As a result, senior executives in healthcare enterprises acknowledge the seriousness of the threats (such as loss of goodwill, large penalties by regulators for data breaches, and partial or complete shutdown of operations resulting in lost revenues) that cyber attacks pose to their business. Security is considered not only as an IT initiative, but also as a business imperative.

In this report, we analyze the capabilities of 13 healthcare IT security service providers. These service providers are mapped on the Everest Group PEAK Matrix, which is a composite index of a range of distinct metrics related to a vendor's vision & capability and market impact. We focus on:

- Market trends for healthcare IT security services
- The landscape of service providers for healthcare IT security services
- Assessment of the service providers on several vision & capability- and market impact-related dimensions

Scope of this report:

Geography
Global

Industry
Healthcare payers and providers

Services
Healthcare IT security services

Everest Group®
RESEARCH

This report focuses on IT security services and offers insights into the key IT security services market trends and prominent service providers operating in this space

Focus of this research

NOT EXHAUSTIVE

Security services – market definition

Consulting/assessment services
Policy and process consulting, vulnerability assessment, audits, certification services, optimization and readiness assessment services, etc.

Design and implementation services
Security architecture design and rearchitecting, security roadmap formulation, security implementation services, etc.

Management and monitoring services
Ongoing device management and continuous monitoring (including remote monitoring through security operation centers), incident management, vulnerability management, and SIEM

End-point security
End-point security (end-points including desktops, mobile devices, servers, etc.) – Host Intrusion Prevention Systems (HIPS), malware protection, managed web proxy, managed encryption, endpoint detection and response, etc.

Application security
Application security testing, application whitelisting, penetration testing, application control, web application security (including firewalls), sandboxing, SAST/DAST, code hardening, API management, SSL offloading, etc.

Identity and Access Management (IAM)
Multi-factor authentication, access management, user provisioning, password management, PKI, Identity-as-a-Service, privileged identity and access management, active directory services, single sign-on, etc.

Data and content security
Security services for structured and unstructured data: Data Loss Prevention (DLP), data encryption, protection & monitoring, database security, storage security, etc.

Network security
Firewalls, email/URL gateways, Network Intrusion Prevention Systems (IPS), Distributed Denial-of-Service (DDoS) prevention & mitigation, Unified Threat Management (UTM), VPN, network control, Advanced Persistent Threat (APT) solutions, network access control, etc.

Risk management and compliance
IT Governance, Risk Management, and Compliance (GRC), threat intelligence, security analytics, cyber assurance, etc.

Cloud security
Security services specifically designed for securing and governing virtual workloads and hybrid IT environments

This report is based on several key sources of proprietary information

- Proprietary database of IT services contracts of major IT service providers with IT security services in scope of work (updated annually)
- The database tracks the following elements of each contract:
  - Buyer details including size and signing region
  - Contract details including service provider, contract type, TCV & ACV, service provider FTEs, start & end dates, duration, and delivery locations
  - Scope details including share of individual buyer locations being served in each contract, Line of Business (LOB) served, and pricing model employed

- Proprietary database of IT service providers (updated annually)
- The database tracks the following for each service provider:
  - Revenue and number of FTEs
  - Number of clients
  - FTE split by different lines of business
  - Revenue split by region
  - Location and size of delivery centers
  - Technology solutions developed

- **Service provider briefings**
  - Vision and strategy
  - Annual performance and future outlook
  - Key strengths and improvement areas
  - Emerging areas of investment

- **Buyer reference interviews, ongoing buyer surveys, and interactions**
  - Drivers and challenges for adopting IT security services
  - Assessment of service provider performance
  - Emerging priorities
  - Lessons learnt and best practices

Service providers assessed

accenture CGI Cognizant

Deloitte. DXC.technology FUJITSU

GAVS Galvanizing Success HCL IBM

NTT DaTa OPTUM UNISYS

wipro

Note: Assessments for Accenture, CGI, Deloitte, Fujitsu, IBM, and Unisys exclude service provider inputs and are based on Everest Group's proprietary Transaction Intelligence (TI) database, service provider public disclosures, and Everest Group's interaction with healthcare firms that are buyers of IT security services
The source of all content is Everest Group unless otherwise specified
Confidentiality: Everest Group takes its confidentiality pledge very seriously. Any information we collect that is contract specific will only be presented back to the industry in an aggregated fashion

Everest Group® RESEARCH

Overview and abbreviated summary of key messages (page 1 of 2)

This report examines the global healthcare IT security service provider landscape. It focuses on service provider position and growth in the healthcare IT security services market, changing market dynamics and emerging service provider trends, assessment of service provider delivery capabilities, and key healthcare IT security service provider profiles. It also identifies the key implications of the research findings for enterprises and service providers

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

Market size & growth

- The overall healthcare IT security services market is a US$4.3 billion+ opportunity and is expected to grow at a CAGR of 16-18% over 2018-2022
- This market is dominated by network security services and Identity & Access Management (IAM), amounting to ~50% of the overall market

Growth drivers

- Migration to cloud, Bring Your Own Device (BYOD), and remote patient monitoring via IoT devices are a few primary drivers of IT security services investments in healthcare
- The penalties imposed by regulatory bodies such as HIPAA as well as the costs associated with data and reputation loss are other key drivers
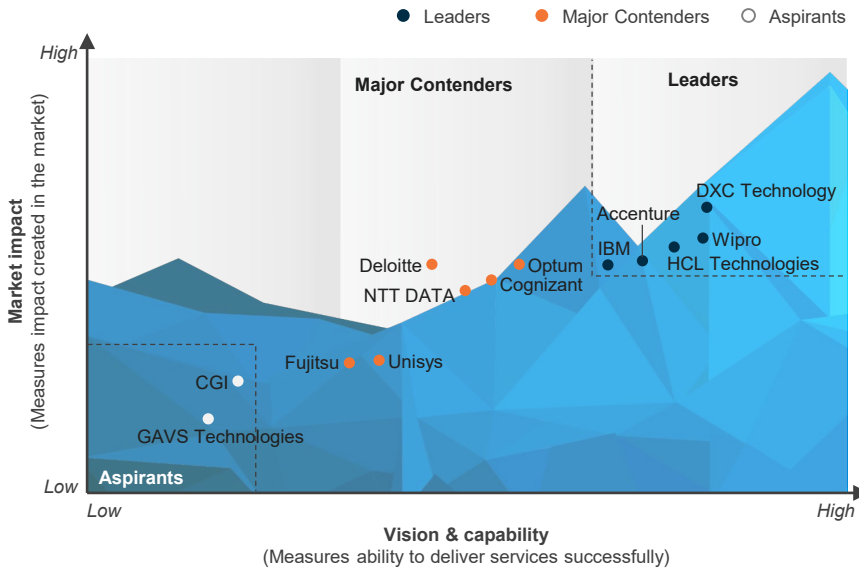
Market trends

- The emergence of personalized medicine along with an increased focus on specialty areas such as dental, behavioral health, and vision are increasing the demand for PHM. Points of vulnerability in PHM models need to be protected to ensure optimum performance and data security

- Multi-channel patient engagement through telehealth, social media, wearables, etc. increases the number of endpoints connected to the network, thus exposing healthcare organizations to security threats making security an important concern for enterprises

Service provider delivery capability

- Healthcare IT security service providers can be categorized into leaders, major contenders, and aspirants on a capability-market-share matrix

- Accenture, DXC Technology, HCL Technologies, IBM, and Wipro are the current leaders in the global healthcare IT security services market. However, several service providers are emerging as major contenders

Everest Group®
RESEARCH

This study offers three distinct chapters providing a deep dive into key aspects of the healthcare IT security services market; the exhibits below illustrate the depth of the report

Assessment of Healthcare IT Security Service Providers

- ● Leaders ● Major Contenders ○ Aspirants

Market impact (Measures impact created in the market) — vertical axis (Low to High)

Vision & capability (Measures ability to deliver services successfully) — horizontal axis (Low to High)

Quadrants: Major Contenders, Leaders, Aspirants

Plotted: DXC Technology, Accenture, IBM, Wipro, HCL Technologies, Optum, Cognizant, Deloitte, NTT DATA, Fujitsu, Unisys, CGI, GAVS Technologies

Note 1: PEAK Matrix specific to healthcare IT security services
Note 2: Assessments for Accenture, CGI, Deloitte, Fujitsu, IBM, and Unisys exclude service provider inputs and are based on Everest Group's proprietary Transaction Intelligence (TI) database, service provider public disclosures, and Everest Group's interaction with healthcare firms that are buyers of healthcare IT security services

Capability assessment

Illustrative example

Measure of capability: ● High ◑ Low

Service provider	Market impact				Vision & capability				
	Market adoption	Portfolio mix	Value delivered	Overall	Scope of services offered	Innovation and investments	Delivery footprint	Vision and strategy	Overall
Service provider 1	◕	◑	◕	◕	◕	◕	◕	◑	◑
Service provider 2	◔	◑	◕	◑	◑	◑	◕	◑	◑
Service provider 3	◑	◕	◕	◑	◕	◑	◑	◑	◑
Service provider 4	◕	◕	◕	◑	●	◕	◕	◕	◕
Service provider 5	◕	◕	◕	◑	◕	◕	◕	◑	◑
Service provider 6	◑	◑	◑	◑	◑	◑	◕	◑	◑
Service provider 7	◑	◑	◑	◑	●	◑	◑	◑	◑
Service provider 8	◕	◑	◑	◑	◑	◑	◑	◑	◑
Service provider 9	◔	◑	◕	◑	◕	◑	◑	◑	◑

Everest Group's remarks on service providers

Illustrative example

Measure of capability: ● High ◑ Low

Market impact				Vision & capability				
Market adoption	Portfolio mix	Value delivered	Overall	Scope of services offered	Innovation and investments	Delivery footprint	Vision and strategy	Overall
◕	◔	●	◑	●	◔	◑	◑	●

Strengths
- Balanced IT security services portfolio to deliver end-to-end transformation
- Investment in next-generation themes such as AI/ML in threat intelligence and wearables/IoT security frameworks
- Commands strong mindshare among small and mid-sized healthcare clients

Areas of improvement
- Needs to increase cloud security investments, a key demand theme among healthcare enterprises
- Needs to build and evangelize thought leadership in healthcare IT security

Everest Group® RESEARCH

The report has 13 profiles covering prominent healthcare IT security services providers

XXX | Healthcare IT security services profile (page 1 of 3)
Overview

Strengths
- Strong IP-led play through Stealth suite of applications lends credi... managed services portfolio
- Has developed significant mindshare amongst medium-sized enter...

Healthcare IT security services revenue

<US$25 million	US$25-US$50 million	US$50-US$100 million	>

Adoption by service type ■ High (>20%) ■ Medium (10-20%)

| Consulting | | Managed services |
| Design & implementation | | As-a-service |

Adoption by industry ■ High (>40%) ■ Medium (20-40%)

| Payer | | Provider |

Adoption by buyer groups ■ High (>20%) ■ Medium (10-20%)

Small (annual revenue < US$1 billion)	
Medium (annual revenue = US$1-5 billion)	
Large (annual revenue > US$5 billion)	

Source: Everest Group (2019)

Everest Group® RESEARCH

XXX | Healthcare IT security services profile (page 2 of 3)
Case studies and solutions

NOT EXHAUSTIVE

Case study 1: Provide security solutions for managing patient i...

| Business challenge | The client wanted a security solution to enhan... care and positively contribute to the clinical ou... patients |
| Solution and impact | XXX provided its security solutions including a... Information and Event Management (SIEM) sy... partnership with LogRhythm® and XXX Securi... Center to manage the SIEM system to provide... and response services. As a result, the client could safeguard confiden... information and critical medical systems by pre... attacks and minimize disruptions to hospital op... clinicians' care of patients |

Healthcare IT security regulations (representative list)

Regulation	Details
GDPR	Provides security consulting services... to stay compliant
HIPAA	XXX's SIEM offering provides easier...

Source: Everest Group (2019)

Everest Group® RESEARCH

XXX | Healthcare IT security services profile (page 3 of 3)
Investments and partnerships

NOT EXHAUSTIVE

Vision: XXX aims to focus on helping healthcare providers prevent cyber breaches and identity theft, stolen PHI, and ransomware attacks by staying updated with the changing security trends in the healthcare industry. It believes that the increasing need for security infrastructure convergence demands integration of physical and logical security functions, which can otherwise lead to risk in the overall security fabric. XXX's security portfolio aims to unify advanced products and deliver efficient, cost-saving managed services architected by its trusted consulting advisors, spanning the physical, logical, managed, and cyber domains.

Key proprietary solutions (representative list)

Solution	Details
Incident Response (IR) Ecosystem	Provides proactive maturing of organizations' IR program and deploying incident handlers
SIEM	A solution that offers an enterprise-wide protection by converging monitoring, management, compliance, security analytics, and IR mechanisms to deliver threat intelligence for a robust security posture
TrustCheck	Transforms the cyber risk conversation and enables organizations to align their security initiatives with their business strategy
XXX Stealth	A solution built on identity-based encrypted micro-segmentation that helps enterprises in transforming their on-premises as well as in the cloud network into a Zero Trust network
Zero Trust security architecture	Helps design, build, implement, and maintain a Zero Trust security architecture with a five-step method including prioritizing, protecting, predicting, isolating, and remediating services

Recent activities (representative list)

Development	Type	Details
Cylance	Partnership	To provide its clients with CylancePROTECT, an endpoint security solution that can detect and prevent malware that signature- and hash-based protection solutions lack
Healthscope	Partnership	To provide security solutions including SIEM system to protect their IT systems used to deliver quality healthcare to patients

Source: Everest Group (2019)

Everest Group® RESEARCH

Everest Group® RESEARCH

Research calendar – Healthcare IT Services (ITS)

	Published	Planned	Current release

Flagship Healthcare ITS reports	Release date
Healthcare Payer Annual Report 2018: Payers Look at Digital to Reinvent in a Turbulent Healthcare Market	March 2018
Healthcare Payer Digital Services PEAK Matrix™ Assessment and Service Provider Landscape – 2019	December 2018
Healthcare Provider Digital IT Services – Service Provider Landscape with Services PEAK Matrix™ Assessment 2018	December 2018
Healthcare Payer Payment Integrity Solutions PEAK Matrix™ Assessment 2020	October 2019
Healthcare IT Security Services PEAK Matrix™ Assessment with Service Provider Landscape 2020	**December 2019**
Healthcare Payer Digital Services PEAK Matrix™ Assessment and Service Provider Landscape – 2020	Q4 2019

Thematic Healthcare ITS reports	
Dr. Robot Will See You Now: Unpacking the State of Artificial Intelligence in Healthcare – 2019	November 2018
Guidebook for Blockchain Adoption in Healthcare and Life Sciences: A Compilation of Insights from 40+ Blockchain Projects	March 2019
Healthcare Report Card 2018 – A Guidebook of Key Trends and Service Provider Performance	March 2019
Big Tech in Healthcare: What it Means for CIOs?	November 2019

Note: For a list of all our published HLS ITS reports, please refer to our website page

Additional HLS IT services research references

The following documents are recommended for additional insights on the topic covered in this report. The recommended documents either provide additional details or complementary content that may be of interest

1. **BigTechs in Healthcare: Reimagining the Ecosystem** (EGR-2019-45-R-3418); November 2019. BigTechs such as Amazon, Apple, Facebook, and Google have a track record of disrupting industries such as retail and telecommunications. The tech giants are now eyeing healthcare – with many having already made significant investments in the industry. This interest is driven by factors such as increasing healthcare spend, demand for data analytics, and rising member/patient expectations. The maximum disruption has been created in areas largely outside the traditional scope (payer, provider, PBM, etc.) of the healthcare industry

2. **Healthcare Payer Payment Integrity Solutions PEAK Matrix™ Assessment 2020** (EGR-2019-32-R-3371); October 2019. Claims processing is becoming ever more complex for payers, given issues such as the need to transform healthcare plans' business models to accommodate new markets and new lines of business, increasing inflow of members, and increasing regulatory mandates. Payment integrity is a potential help – it can reduce rising healthcare waste and fraud to ensure that the medical claims are paid correctly and free of wasteful and abusive practices

3. **Healthcare Report Card 2018 – A Guidebook of Key Trends and Service Provider Performance** (EGR-2019-20-R-3117); March 2019. In this report, we talk about key themes that dominated the U.S. healthcare market in 2018. On one side, payers continued their quest for consolidation across the value chain by merging with PBMs and investing in technology consortia; on the other side, healthcare providers too tried to expand their influence through large mergers as well as by acquiring small physician practices. The ongoing issues pertaining to value-based care transition and cybersecurity also continued to push the payers and providers to invest in new technologies (analytics, automation, IoT, cloud, etc.)

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

Abhishek Singh, Vice President: abhishek.singh@everestgrp.com

Nitish Mittal, Practice Director: nitish.mittal@everestgrp.com

Kanika Gupta, Senior Analyst: Kanika.Gupta@everestgrp.com

Nisarg Shah, Senior Analyst   Nisarg.Shah@everestgrp.com

Sarweshwer Gupta, Senior Analyst   Sarweshwer.Gupta@everestgrp.com

Website: https://www.everestgrp.com/ | Phone: +1-214-451-3000 | Email: info@everestgrp.com

About Everest Group

Everest Group is a consulting and research firm focused on strategic IT, business services, and sourcing. We are trusted advisors to senior executives of leading enterprises, providers, and investors. Our firm helps clients improve operational and financial performance through a hands-on process that supports them in making well-informed decisions that deliver high-impact results and achieve sustained value. Our insight and guidance empower clients to improve organizational efficiency, effectiveness, agility, and responsiveness. What sets Everest Group apart is the integration of deep sourcing knowledge, problem-solving skills and original research. Details and in-depth content are available at www.everestgrp.com.

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

New York
info@everestgrp.com
+1-646-805-4000

Toronto
canada@everestgrp.com
+1-416-388-6765

Stay connected

Website

www.everestgrp.com

Social Media
@EverestGroup
@Everest Group

Blog

www.everestgrp.com/blog/