Everest Group®

State of the Market Report | Cybersecurity

Cybersecurity Services State of the Market 2023: Cyber Secure to Cyber Resilient

June 2023

EGR-2023-65-R-5994

Our research offerings

This report is included in the following research program(s):
Cybersecurity

- 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
- Engineering Services
- Enterprise Platform Services
- Exponential Technologies
- Finance and Accounting
- Financial Services Technology (FinTech)
- GBS Talent Excellence
- Global Business Services
- Google Cloud
- Healthcare Business Process
- Healthcare Information Technology
- 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 Services Executive Insights™
- IT Talent Excellence
- Life Sciences Business Process
- Life Sciences Commercial Technologies
- Life Sciences Information Technology
- Locations Insider™
- Marketing Services
- Market Vista™
- Microsoft Azure
- Modern Application Development (MAD)
- Mortgage Operations
- Multi-country Payroll
- Network Services and 5G
- Oracle Services
- Outsourcing Excellence
- Pricing Analytics as a Service
- Process Mining
- Process Orchestration
- Procurement and Supply Chain
- Recruitment
- Retail and CPG Information Technology
- 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:

Yugal Joshi, Partner

Kumar Avijit, Practice Director

Arjun Chauhan, Senior Analyst

Contents

01

Introduction and overview

- Research methodology
- Introduction
- Focus of the research

Our research methodology is based on four pillars of strength to produce actionable and insightful research for the industry

01

Robust definitions and frameworks

Function specific pyramid, Total Value Equation (TVE), PEAK Matrix®, and market maturity

02

Primary sources of information

Annual contractual and operational RFIs, provider briefings and buyer interviews, web-based surveys

03

Diverse set of market touchpoints

Ongoing interactions across key stakeholders, input from a mix of perspectives and interests, supports both data analysis and thought leadership

04

Fact-based research

Data-driven analysis with expert perspectives, trend-analysis across market adoption, contracting, and providers

Proprietary contractual database of over 300 cybersecurity contracts (updated annually)

Year-round tracking of 30+ cybersecurity service providers

Large repository of existing research in cybersecurity

Over 30 years of experience advising clients on strategic IT, business services, engineering services, and sourcing

Executive-level relationships with buyers, providers, technology providers, and industry associations

Background of the research

This report provides a detailed analysis, highlighting the critical shift from cyber awareness to cyber resilience. While cyber awareness entails understanding the threats and vulnerabilities inherent in digital infrastructures, cyber resilience implies a more dynamic approach. It signifies the ability of an organization to prepare, respond, and recover from cyber threats, and even goes beyond to how well organizations can learn from their industry and geography peers and stay abreast with security implications of latest technologies.

The SOTM report delves deeper into how the C-suite fails to understand that being cyber secure implies having protective measures against potential threats but does not necessarily ensure resilience. The SOTM discusses this noticeable perception gap within the C-suite executives. While many understand the technicalities of cyber threats, the broader concept of resilience is often misunderstood or underestimated. This gap can hinder the implementation of effective strategies, hence, addressing it is paramount.

To fill this gap and promote cyber resilience, we have created the 5R framework for cyber resilience. This framework will guide organizations on their journey to resilience, outlining key steps from resisting attacks to learning from them. Service providers too will have a crucial role to play in overcoming challenges in cyber resilience adoption and help the C-suite understand its importance, thereby fostering a more resilient digital ecosystem.

Scope of this report

Geography
Global

Industry
All industries

Services
Cybersecurity

This report focuses on cybersecurity services and offers insights into the key cybersecurity services market trends

NOT EXHAUSTIVE

Consulting/assessment services

Policy and process consulting, vulnerability assessment, audits, certification services, optimization and readiness assessment services

Design and implementation

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

Management and monitoring services

Device management, continuous reporting and monitoring (including remote monitoring through SOCs), incident management/response, and SIEM/SOAR

Cybersecurity services

End-point security (XDR) End-point security (end points including desktops, mobile devices, and servers) – Host Intrusion Prevention Systems (HIPS), malware protection, managed web proxy, managed encryption, end-point detection and response, etc.	**Identity and Access Management** 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.	**IoT and OT security** IoT device and data protection, asset discovery and intelligence, IoT threat intelligence, communication channel security, pre-embedded IDs and encryption, API access control, firmware update on IoT devices, OT device security, OT device monitoring etc.	**Application security** App security testing, app whitelisting, app self-protection, patching, app control, web app security (including firewalls), sandboxing, SAST/DAST, code hardening, API management, SSL offloading, etc.
Data security Security services for structured and unstructured data: Data Loss Prevention (DLP), data encryption, protection & monitoring, database security, storage security, etc.	**Cloud security** Security services specifically deigned for securing and governing virtual workloads and hybrid IT environments: cloud access security broker (CASB), threat detection and response, identity management, cloud-native application security, data security in multi/hybrid cloud environment	**Risk management and compliance** Governance, Risk Management, and Compliance (GRC), threat intelligence, security analytics, cyber assurance	**Network security** Firewalls, email/URL gateways, Network Intrusion Prevention Systems (NIPS), Distributed Denial of Service (DDoS) prevention & mitigation, Unified Threat Management (UTM), VPN, network control, Advanced Persistent Threat (APT) solutions, network access control, etc.

02

Cybersecurity services market overview – global

- Global cybersecurity services market size, growth, and drivers
- Cybersecurity services market spend by segment
- Global cybersecurity services spend by geography
- Enterprises' top cybersecurity priorities
- Top enterprise concerns
- Evolving nature of cyberattacks – a key cybersecurity challenge
- Talent conundrum – a key cybersecurity challenge

Demand for cybersecurity services continues to be robust and is poised to breach the US$100 billion mark by 2025 owing to a multitude of internal and external factors

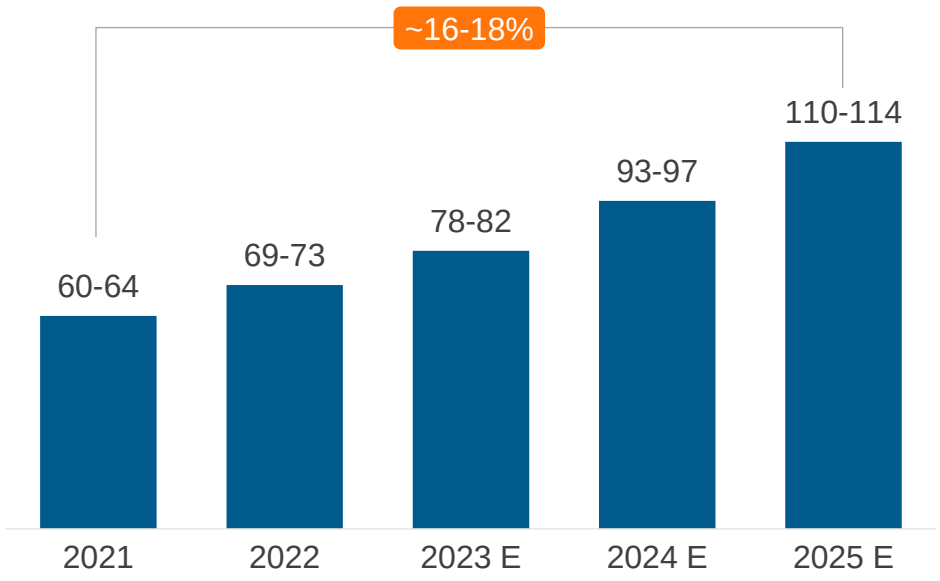
Global cybersecurity services market size (2022)

US$70-73 billion

Cybersecurity services CAGR (2021-25)

16-18%

Global cybersecurity services market
US$ billion



Source: Everest Group (2023)

Cybersecurity demand drivers

Increased incidents of cyberattacks and threats

Multi-fold rise in number and severity of cyberattacks, such as phishing, malware, social engineering, DDoS, and ransomware, making organization realize the importance of having robust security

Enterprises' digitalization mandates

Enterprise digitalization initiatives further fueled by the COVID-19 pandemic leading to an increased adoption of cloud, AI/ML, 5G, edge, IoT, and other next-generation technologies resulting in broadening of attack surfaces

Government initiatives

Government regulations, support, and enforcement initiatives to reduce the risk associated with cyberattacks, cyber espionage, cyber warfare, and data privacy have led to an increased focus on cybersecurity

Changing end-user behavior

Remote working, increased internet penetration, and growth of e-commerce, tele-health, digital payments, and OTT have increased the technology footprint of both individual and enterprise, necessitating taking adequate steps to secure it

Enterprises are increasingly adopting cloud-based and cloud-focused solutions and services; demand for risk management, compliance, and data security services is also on the rise

Cybersecurity services market breakdown – by service type

100% = US$70-73 billion

Cybersecurity services market breakdown – by segment

21%

Identity and Access Management (IAM)

Enterprises are going for cloud-focused IAM modernization with adaptive authentication, identity proofing, and privilege management.

16%

Application security

DevSecOps adoption, web applications security assessments, source code reviews, API security, and application vulnerability remediation services are in demand.

19%

Cloud security

Enterprises are demanding cloud-native security management, cloud security governance, securing landing zone, cloud security posture management, and multi-cloud security.

13%

Risk management and compliance

Move toward an integrated platform architecture, automating risk and compliance processes, rationalization of controls, and emphasis on supplier risk management are driving the demand.

8%

Data security

Enterprises are focusing on data loss prevention, data security and access governance, data encryptions, data recovery, policies design and enforcement, and data privacy.

12%

End-point security

Enterprises are looking for cloud-based and AI/ML-powered proactive solutions with continuous management and automation in demand.

6%

Network security

Cloud-based network security, move from VPN to ZTNA and SASE, next-generation firewall adoption, and network threat detection and response are driving the demand for network security.

5%

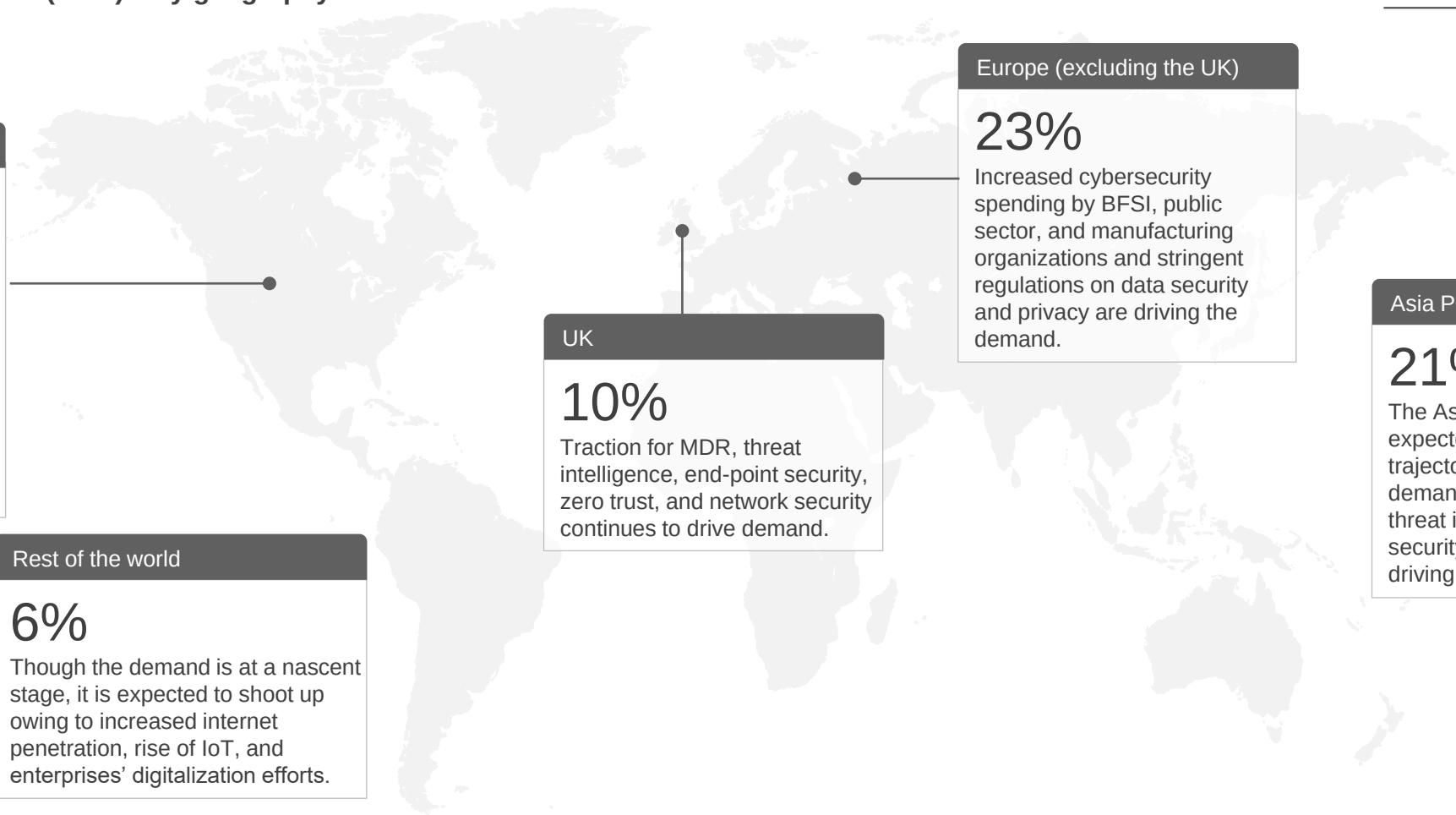
IoT and OT security

Enterprises are demanding OT strategy design and deployment, vendor security assessments, and continuous threat detection and response for the OT and IoT. ecosystem.

North America continues to lead the global cybersecurity services market owing to increased cybersecurity spending and growing incidents of cyberattacks; Europe follows

Global cybersecurity services (2022) – by geography

EVEREST GROUP ESTIMATES



North America

40%

North America remains the largest market with demand continuing to grow due to increased cyberattacks, increased adoption of cloud and other next-generation technologies and the need to secure it, and increased cybersecurity spending by large organizations.

Europe (excluding the UK)

23%

Increased cybersecurity spending by BFSI, public sector, and manufacturing organizations and stringent regulations on data security and privacy are driving the demand.

UK

10%

Traction for MDR, threat intelligence, end-point security, zero trust, and network security continues to drive demand.

Asia Pacific

21%

The Asia Pacific market is expected to continue its growth trajectory owing to the strong demand for cloud security, threat intelligence, and network security with BFSI sector driving the demand.

Rest of the world

6%

Though the demand is at a nascent stage, it is expected to shoot up owing to increased internet penetration, rise of IoT, and enterprises' digitalization efforts.

Source: Everest Group (2022)

Enterprises are looking for intelligent solutions and services that ensure robust 360-degree security without compromising on simplicity, experience, and compliance

Enterprises' top six cybersecurity priorities

Security and vulnerability management

Increasing security vulnerabilities is leading to a rise in demand for intelligent vulnerability management solutions involving vulnerability scanning, contextual risk-based prioritization, remediation, and governance in an as-a-service model.

Threat detection and prevention

XDR solutions encompassing SIEM, EDR, UEBA, SOAR, NTA, threat intelligence, hunting, and security orchestration that covers the entire IT landscape are gaining traction as a result of increasing sophistication, incidents, and impact of cyberattacks.

Security Information and Event Management (SIEM)

SIEM solutions are increasingly being integrated as a part of MDR and SoC offerings with a focus on threat intelligence, ensuring visibility, and integrating new log sources in a bid to better leverage security data and improve threat detection.

Secure remote access and teleworking infrastructure

Shift toward a perimeter-less model is leading to an increased demand for securing remote work through offerings that are based on zero-trust architecture, SASE, and CASB.

Next-generation firewall

Increased network complexity and sophistication of attacks is driving demand for SASE-supported next-generation firewall and next-generation firewall-as-a-service.

Data privacy

Region-specific compliance norms is leading to an increased demand for consulting, advisory, and strategy design services with the goal of having a robust data management and protection solution encompassing data residency, DLP, rights management, and privacy by design.

However, enterprises are struggling to keep pace with the continuously evolving nature of cyberattacks while managing the talent conundrum

Top enterprise concerns[1]

Evolving nature of attacks such as spyware, ransomware, and phishing

Rise of AI-powered cyberattacks, such as smart malware and ransomware, increased instances of 5G-enabled swarm attacks, threat of state-sponsored cyber warfare, cryptojacking, and man-in-the-middle attacks along with newer versions of viruses, trojans, and worms, highlights the continuous evolutions of cyberattacks making it difficult for enterprises to secure themselves.

Lack of skills/talent

Enterprises are struggling to attract new cybersecurity talent and retain experienced professionals as many of them are leaving the industry. This, along with rising talent costs, extensive certification and training requirements, and skill gap among professionals, is adding to the already increasing talent concerns of enterprises.

Securing cloud environments

The continuously sprawling cloud landscape and increasing cloud complexity of enterprises are making it difficult to secure cloud environments. Challenges, such as securing the increased attack surfaces and end points, preventing data breaches, implementing IAM and compliance solutions across the IT landscape, and misconfigurations, continue to plague enterprises.

Identity and access management

Complex and expensive IAM deployments, balancing user experience with security, and difficulty in modernizing IAM to support cloud transformation and enterprise digitalization initiatives are some of the challenges enterprises are facing with respect to IAM.

Governance and compliance

Enterprises are struggling to aggregate, visualize, and report GRC information to relevant stakeholders in an effective manner. Inefficiencies of manual risk reporting and challenges in managing compliance in a multi-geography setup are also adding to their worries.

1 Everest Group interactions with enterprise buyers during Security Services PEAK Matrix® Assessment 2022 interactions

Rising incidents of next-generation cyberattacks with innovative entry points and wide-ranging motivations are making it difficult for enterprises to protect themselves

	Emerging cyberattacks	Prominent entry points	Key industries at risk
Malware	Watering hole attack, ransomware-as-a-service, fileless malware, and smart malware	E-mails, malicious URL, removable devices, and end points	BFSI; Public sector; Energy & utilities
Phishing	Spear phishing, smishing, and vishing, deep fake-powered impersonations, and sniffing	Email, messaging platforms, social media, and web pages	BFSI; Healthcare; Retail
Man-in-the-middle attack	Rouge access points, email hijacking, DNS spoofing, session hijacking, and IP spoofing	Unsecured network, email, user device, and web applications	BFSI; Telecom & media; Retail
Denial of service	Multi-vendor and/or crowd-sourced DDoS attack, botnet infection, and application layer attacks	Web servers, applications, devices, and networks	Telecom & media; Public sector; Retail
Zero-day exploit	Targeting open-source software and SaaS offerings	Software applications, web browsers, operating systems, and IoT devices	BFSI; Technology; Retail
IoT and OT attacks	Cyber-physical attacks, privilege escalation attacks, and brute force attacks	IoT devices, removable hardware, industrial OT devices, and applications	Manufacturing; Healthcare; Energy & utilities

Enterprises have taken cognizance of the talent crisis plaguing the cybersecurity industry and are adopting comprehensive strategies and investing in emerging roles to mitigate it

63% of enterprises have mentioned lack of skills/talent as among their top three biggest challenges when it comes to cybersecurity

Key talent challenges

- Shortage of new and experienced talents
- Skill gap among professionals
- Extensive training and certification requirements
- Rising talent costs

Top four talent strategies being leveraged to address talent-related challenges

- Nurturing a talent community (skill mining)
- Building career pathways
- Investment in curriculum, community college, etc.
- Initiatives to widen the talent pool

Top five security roles gaining traction

- Cloud security architect
- Threat hunters
- Digital identity related roles
- Industry domain security consultants
- Governance, risk, and compliance roles

03

Cybersecurity services market overview – North America

- North America cybersecurity services market by region, CAGR, and key highlights
- North America cybersecurity services market by industry
- North America cybersecurity deal trends

The US continues to dominate the cybersecurity services market in North America as a result of enterprises' digitalization initiatives and proximity to the provider ecosystem

North America cybersecurity market size (2022)

US$27-29 billion

2021-25 cybersecurity CAGR

17-19%

Cybersecurity services market breakdown by geography (North America)

US	Canada	Mexico
		
92%	6%	2%
17-19% CAGR The US continues to dominate the cybersecurity market in North America due to increased risk from cyberattacks, enterprise digitalization initiatives, and close presence of mature cybersecurity technology and service providers.	**18-19% CAGR** Increased cyberattacks in regions of Quebec and Ontario, rise in numbers of ransomware attacks and business email compromise, and demand for cloud and network security are driving the demand in Canada.	**16-17% CAGR** Most of the current demand exists around securing the on-premise enterprise landscape with network security representing a significant chunk. However, enterprises' digitalization initiatives is leading to a growth in demand for advance security services.

Source: Everest Group (2023)

BFSI has emerged as the biggest industry for cybersecurity services in North America followed by retail, distribution, and CPG and healthcare and life sciences

Enterprise cybersecurity services market size – by industry
2022; annual revenue in US$ billion
100% = US$27-29 billion

								
25%	13%	13%	11%	9%	9%	9%	8%	3%
BFSI	Retail, distribution, & CPG	Healthcare & life sciences	Energy & utilities	Manufacturing	Technology	Public sector	Telecom, media, & entertainment	Others

Key industry trends:

- **BFSI**: need for securing customer and other confidential data, managing stricter regulations, ensuring end-point security for insurance organizations, and securely handling targeted threats are driving the demand for hybrid/multi-cloud security, penetration testing and vulnerability management, MDR, application and API security, security automation, and data security
- **Retail, distribution, & CPG**: threat from ransomware, phishing scams, security breaches such as attack on payment systems and third-party vendor, and supply chain attack are making retail, distribution, and CPG enterprises recalibrate their cybersecurity strategy. This has led to an increased focus on cloud security, data security, and application security
- **Healthcare and life sciences:** increased investments in cybersecurity solutions by providers, need for safeguarding healthcare data, threats from hackers and hacktivists, and the demand for encryption, IAM, and risk and compliance solutions are driving the demand of healthcare industry in North America
- **Energy and utilities:** increasing digitization, growing threat landscape, compliance requirements, data protection, and rising awareness of the potential impact and costs of cybersecurity breaches

Source: Everest Group (2023)

North American enterprises are on the lookout for service providers that can bundle cybersecurity with other components and can provide a competitive value proposition

North America cybersecurity services deal by scope breakdown (2021)

Enterprises in North America are increasingly signing cybersecurity contracts bundled with other applications and/or infrastructure components due to cost, integration, and simplicity benefits.

North America cybersecurity services deal breakdown by buyer size (2021)

71%

Large

Revenue
>US$5 billion

20%

Medium

Revenue
US$1-5 billion

9%

Small

Revenue
<US$1 billion

Large organizations continue to be the biggest enterprise segment contributor to the overall cybersecurity demand.

North America cybersecurity services deal by bidding types breakdown (2021)

34%
Incumbent + sole-sourced

25%
Incumbent + competitive

7%
Non-incumbent + sole-sourced

33%
Non-incumbent + competitive

- Incumbents that have demonstrated their capabilities in other parts of the accounts continued to be the preferred providers for new deals
- However, enterprises in North America are reassessing their service provider landscape and are increasingly preferring to partner with non-incumbents after they have proven their capabilities in competitive rounds

04

Cybersecurity services market overview – Europe

- Europe cybersecurity services market by region, CAGR, and key highlights
- Europe cybersecurity services market by industry
- Europe cybersecurity deal trends

The Western and Northern European regions continue to be the most mature European regions for cybersecurity services and dominate the demand in the area

Europe cybersecurity market size (2021)

US$23-25 billion

2021-25 cybersecurity CAGR

15-16%

Cybersecurity services market breakdown by geography (Europe)

UKI	France & Southern Europe	DACH	Nordics	Benelux	Others
					
30%	25%	22%	12%	10%	1%
16-17% CAGR	**13-14% CAGR**	**15-16% CAGR**	**15-16% CAGR**	**14-15% CAGR**	**19-20% CAGR**
Increasing incidents of cyberattacks, acceptance of cybersecurity as a strategic issue among the board, and rapid adoption of new innovative technologies and the need to secure them	Government's push for security, increased demand from retail sector, and the need to secure a widened attack surface due to adoption of IoT, BYOD, and remote working	Strong government support, increasing cost of data breaches, demand for intrusion detection and prevention solutions, and growth of cybersecurity start-ups	Demand for IAM, infrastructure protection solutions, integrated risk management, and OT security with an increased interest from manufacturing, healthcare, and maritime sector	Increased threat of data leakage, phishing, malware, and vulnerability exploits, increasing cybersecurity budget, and demand from utilities, manufacturing, and life sciences industries	Increasing awareness among enterprises and government and being complaint to GDPR and other regulations

Source: Everest Group (2023)

BFSI has emerged as the biggest industry for cybersecurity services in Europe followed by retail, distribution, and CPG and public sector

Enterprise cybersecurity services market size – by industry
2021; annual revenue in US$ billion
100% = US$21-23 billion

26%	13%	13%	12%	9%	9%	9%	8%	4%
BFSI	Retail, distribution, & CPG	Public sector	Manufacturing	Healthcare & life sciences	Energy & utilities	Telecom, media, & entertainment	Electronics, hi-tech, & technology	Others

- **BFSI**: need for securing customer and other confidential data, ensuring compliance to regulations and guidelines such as GDPR, NIS Directive, PSD2, and EBA, and securely handling targeted threats are driving the demand for hybrid/multi-cloud security, risk and compliance solutions, MDR, application and API security, security automation, and data security
- **Retail, distribution, & CPG**: threat from ransomware, phishing scams, security breaches such as attack on payment systems and third-party vendors, and supply chain attack is making retail, distribution, and CPG enterprises recalibrate their cybersecurity strategy. This has led to an increased focus on cloud security, data security, and application security
- **Public sector**: increased attacks on government and other public sector enterprises, threat of cyber espionage especially due to the Russia-Ukraine conflict, increasing investments by government to strengthen its security posture, and emergence of public sector contextualized security solutions are driving the demand
- **Manufacturing:** sharp increase in the number of cyber incidents such as phishing, ransomware attacks, DDoS attacks, and increasing threat of OT attacks and data theft along with increasing awareness and spending among enterprises to safeguard the IT-OT landscape is driving demand for cybersecurity services in the manufacturing sector

Source: Everest Group (2023)

European enterprises are being cautious while selecting their service providers and are preferring standalone deals due to stricter regulations and compliance norms

Europe cybersecurity services deal by scope (2021)

Although enterprises in Europe are increasingly preferring bundled deals, standalone cybersecurity contracts continue to be the preferred choice.

Europe cybersecurity services deal breakdown by buyer size (2021)

71%

Large

Revenue
>US$5 billion

20%

Medium

Revenue
US$1-5 billion

9%

Small

Revenue
<US$1 billion

Large organizations continue to be the biggest enterprise segment contributor to the overall cybersecurity demand.

Europe cybersecurity services deal by bidding types breakdown (2021)

34%
Incumbent + sole-sourced

36%
Incumbent + competitive

8%
Non-incumbent + sole-sourced

22%
Non-incumbent + competitive

- European enterprises are more cautious than their North American counterparts and prefer to partner with service providers with whom they have had prior engagement experience
- They have shown an increased preference for glocal providers due to region-specific compliance norms

05

From cyber aware to cyber resilient: prioritizing resilience focus

- What is cyber resilience
- Journey map for cyber resilience
- Challenges in cyber resilience adoption
- 5R framework
- Boardroom perception gap
- Implications for system integrators

Enterprises comprehend the significance of cybersecurity in business resilience, but they fall short in formulating comprehensive strategies for overall cyber resilience, giving minimal attention to post-breach stages

Cybersecurity alone does not equal cyber resilience

One critical thing to understand is that cybersecurity and cyber resilience are different – cybersecurity is just one component of cyber resilience. The latter is a much broader concept that not just includes preventive measures, but also covers areas in post-breach stages such as responding, recovering, learning, and revamping. Enterprises fail to understand this subtle difference and end up spending a majority of their budget in preventive controls.

> Enterprises often use cyber resilience and cybersecurity synonymously and there is still much to be done to establish the distinction between the two; 59% of respondents indicated that cyber resilience and cybersecurity are synonymous, with their differences not well understood. With cyber resilience still being a relatively new concept to executive thinking, there is currently a lack of clarity as companies begin to discuss cyber resilience more frequently.[1]

Inadequate cyber resilience results in compromised business resilience

If an enterprise lacks a robust cyber resilience strategy, it exposes itself to potential data breaches and system disruptions. Moreover, failure to recover promptly from a cyberattack can result in operational downtime for the company and hence, having a comprehensive cyber resilience strategy is critical in safeguarding long-term viability and success for any business.

1 World Economic Forum's 2022 Global Cybersecurity Outlook

Optimize existing cybersecurity tools by prioritizing strong integration over unnecessary new purchases to accelerate the journey from cyber aware to cyber resilient

Parameters	Cyber aware	Cyber secure	Cyber resilient
People	Lack of accountability, poor security understanding, and low engagement in security practices • Limited cybersecurity awareness • No dedicated leadership • Minimal alignment of business and cybersecurity	Dedicated cybersecurity roles, better security understanding, and engagement in secure behavior • Regular cybersecurity training • Designated cybersecurity leader • Functional alignment of business and cybersecurity	Cybersecurity embedded in all roles, robust security understanding, and proactive engagement in secure behavior • Comprehensive cybersecurity training at all levels • Unified cybersecurity leadership • Deep alignment of business and cybersecurity
Process	Ad hoc processes, delayed response, and failure to learn from breaches • Minimal security processes • Reactive incident response • Little learning from incidents	Defined and documented processes, timely response, and lessons from breaches • Established security processes • Proactive incident response • Learning and adjustment post-incidents	Agile and adaptable processes, rapid and effective response, and learning-driven process improvement • Adaptive security processes • Fully-refined proactive incident response • Continuous improvement from past incidents
Technology	Outdated technologies, infrequent system checks, and high vulnerability to threats • Minimal security controls • Infrequent system monitoring	Up-to-date technologies, regular system checks, and controlled vulnerability • Robust security controls • Regular system monitoring and auditing	Cutting-edge technologies, continuous system checks, and resilience against evolving threats • Advanced and AI-driven security controls • Real-time continuous monitoring with automated threat detection

In the post-pandemic landscape, cybersecurity challenges have exacerbated – further impeding enterprises' progress from cyber aware to cyber resilient

Top enterprise challenges when it comes to adoption of cyber resilience

Inadequate workforce education: unaware employees often become the weakest link in the cyber resilience strategy and lack of proper trainings and awareness programs can leave employees ill-equipped to identify and respond to cyber threats, undermining the effectiveness of a cyber resilience strategy.

Underutilized technology stack: enterprises often underutilize their existing security tools and overlook their capabilities and invest in flashy new technologies, leading to unnecessary spending. Enterprises should conduct comprehensive tool assessments, provide training, and foster a culture of maximizing the capabilities of their incumbent solutions.

Unit-specific focus over holistic business approach: in large-sized organizations, inadequate cross-team communication and collaboration becomes a challenge for cyber resilience because it impedes the development of a cohesive cyber resilience strategy. Enterprises need to draw an analogy from how DevOps, buttressed by strong communication, transformed engineering and operations whereas cybersecurity is still siloed.

Limited resources and budget constraints: implementing a comprehensive cyber resilience strategy not only requires dedicated financial investments, but also requires skilled talent across all stages. Hence, enterprises with budget constraints struggle to allocate adequate funding and manpower to develop and maintain a comprehensive cyber resilience program.

34% cyber leaders questioned during the survey agreed that they have training and skills gaps in certain areas while 13% agreed that they lack critical people and skills for cybersecurity.[1]

Disconnect between business objectives and cyber initiatives: although business leaders are now more aware about cybersecurity than ever before, there is still a disconnect in cyber initiatives and business objectives. Additionally, usage of cybersecurity and cyber resilience interchangeably has created market confusion and resultantly, the C-suite is more focused on preventive measures rather than thinking about the overall cyber resilience.

Global geopolitical instability has helped to close the perception gap between business and cyber leaders' views on the importance of cyber-risk management, with 91% of all respondents believing that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years.[1]

1 World Economic Forum Global Security Outlook Report 2023

Leveraging a framework-led approach enables enterprises to decompose cyber resilience into smaller, more manageable components, thereby facilitating accelerated transition from cyber aware to cyber resilient

Everest Group believes that the challenges can be addressed by following the 5R framework

5R framework





Ready | **R**espond | **R**ecover | **R**einforce | **R**evamp

Meaning of 5Rs

Ready: build defenses to avert cyberattacks

Respond: detect and remediate if any incident happens

Recover: recover to business-as-usual state after remediation

Reinforce: learn from industry best practices and recalibrate

Revamp: adopt new technologies while keeping security in mind

Ready state embodies a proactive and comprehensive approach to security, and encompasses preparation for any potential cyberattack

Ready | Respond | Recover | Reinforce | Revamp

> More than 74% of the enterprises believe that the cybersecurity budgets will increase by at least 6% in 2023 amidst the economic slowdown.[1]

Risk assessment and mitigation

Assessing risks and planning to mitigate them by leveraging risk assessment frameworks.

Examples of cybersecurity risk assessment frameworks:

- NIST Cybersecurity Framework
- ISO/IEC 27001

Enterprises need to make sure that they are compliant to all critical regulations from a security perspective and their defenses are aligned with globally accepted security risk assessment frameworks.

Security policies and procedures

Implementing security policies and procedures to thwart cyberattacks. Enterprises can leverage service providers to implement these policies and procedures, or even choose to go fully in-house.

Examples of cybersecurity services:

- IAM services
- Cloud security services
- Application security services
- MDR services

Security policies and procedures are ongoing efforts to defend against potential attacks, and consequently consume the majority of the security budget and resources.

1 Everest Group Key Issues Survey 2023

Respond state includes all the measures in the event of a security breach, ranging from initial detection to the ultimate resolution of the issue

Ready | **Respond** | Recover | Reinforce | Revamp

> "Enterprise responses for why cyber resiliency has not improved were an inability to reduce silo and turf issues (69%), fragmented IT and security infrastructure (65%), lack of visibility into applications and data assets (60%), and delay in patching vulnerabilities (59%).[1]"

Incident detection

Timely detection of unauthorized access to an enterprise's internal data or recognizing unusual activities in the system.

Parameters that can be leveraged for incident detection include:

- System logs
- Network traffic
- User behavior
- File integrity

Limiting the impact

Containing the breach with the sole aim of preventing any additional damage or data loss. The primary way of breach containment is by isolating the device/user from the system network.

There are multiple ways that can be used for user/device isolation:

- Disconnecting the device from the network
- Disabling compromised users accounts
- Blocking outgoing traffic from the device

1 IBM's Cyber Resilient Organization Study 2021

Recover state pertains to the phase where enterprises direct their efforts toward restoring their systems and operations to normalcy

Ready | Respond | **Recover** | Reinforce | Revamp

> In 2022 it took an average of 207 days to identify the breach and 70 days to contain the breach. A data breach life cycle of less than 200 days was associated with an average cost of US$3.74 million in 2022, compared to US$4.86 million for breaches with a life cycle of greater than 200 days. This difference represents an average cost saving of US$1.12 million, or 26.5%, for breaches with the shorter than 200-day life cycle.[1]

1 IBM's Cost of a Data Breach Report 2022

Damage assessment

Assessing the impact of the breach to better understand what all damage has been done. Damage can be in the form of encrypted devices, data loss, or lost systems, etc.

Some levers that enterprises can consider during the damage assessment phase:

- Timeframe of the attack
- Type of attack
- Sensitivity of lost data

Restoring steady state

Restoring steady states comes in when the damage assessment has been done and the enterprise has a deeper understanding of what all has happened and is sure that the vulnerability has been patched.

Restoring ready state has three phases:

- Phase 1: creating a restoration plan
- Phase 2: restoring system based on the plan
- Phase 3: testing the restored systems

Communication with stakeholder group

Communicating with multiple stakeholders during a cyberattack becomes critical, especially if it is a publicly listed organization. For any crisis situation, such as a cyberattack, enterprises should have a clear understanding of three things – who to say (internal versus external), where to say (press releases, conferences, social media channels, etc.), and what to say (degree of information that needs to be shared).

Reinforce is a continuous state of enterprise learning, encompassing not only the cyberattacks targeted toward them but also toward the broader peer group

Ready | Respond | Recover | **Reinforce** | Revamp

> "Organizations that had invested in internal cybersecurity trainings and awareness programs, experienced lower overall cost of breach by an average of US$247,758.[1]"

Recalibrating Ready state

Once the enterprise is back to the steady state and business has been restored to normal, the enterprise then needs to shift its focus on learning from the attack and dig deeper into how it happened in the first place, how did the attacker pass the security measures, and what can be done to stop it in the future.

Accordingly, enterprises need to recalibrate their Ready state and make sure that they can defend against similar attacks. One thing that enterprises often tend to overlook is the fact that if the peer gets attacked, then staying cautious alone will not help – they will have to proactively take measures based on what all disclosures the peers are making in the market.

Training and awareness

Training and awareness is one of the critical pieces in any organization's cybersecurity program. However, employees often get overwhelmed by these trainings and tend to overlook the problem and start believing that it cannot happen with them, which mostly turns out false.

Here are some considerations that enterprises should keep in mind while imparting cybersecurity trainings:

- Make sure that the trainings do not become too technical
- Trainings should not be too long and cover only the important topics
- Choose to give practical advice to employees instead of using fear tactics
- Do not blame employees for security breaches
- Factor in the human-error in your cybersecurity strategy

1 IBM's Cost of a Data Breach Report 2022

Revamp represents a forward-looking state in which enterprises take proactive measures to fortify security for nascent technologies such as the metaverse, 5G, and edge computing

Ready | Respond | Recover | Reinforce | **Revamp**

> "Experts predict the number of active Internet of Things (IoT) devices will grow to 14.4 billion by the end of 2022, reflecting an 18% year-over-year growth rate. The number of vulnerabilities related to IoT devices grew 16% in 2022 alone, compared to a growth rate of only 0.4% for all vulnerabilities.[1]"

Emerging attack vectors

While developing cybersecurity strategies, enterprises should make sure that their cybersecurity strategy has factored in the adoption of these next-generation technologies and the attack vectors that they can bring. For example, adoption of edge computing can open a Pandora's box of vulnerabilities from edge devices; similarly, 5G infrastructure can pose a security challenge.

Apart from the direct impact, attackers can also use these next-generation technologies for social engineering and other tactics to trick users into revealing sensitive information or compromising their security. For example, attackers may use the metaverse to create realistic-looking scams.

1 IBM's report on cybersecurity trends in 2023

To advance to the cyber resilient stage, enterprises must holistically address key aspects of cyber resilience and close the perception gap

5Rs of cyber resilience	 Ready	 Respond	 Recover	 Reinforce	 Revamp
Current C-suite focus[1]	**High**	**High**	**Medium**	**Low**	**Low**
Everest Group comments	C-suite is extensively focusing on preemptive measures to secure themselves from cyberattacks and are investing in cutting-edge technologies.	There is rapid adoption of XDR tools in the market and service providers too are now focusing on automated incident response to cut down on standard metric of MTTR.	There is very little focus on the recovery aspect from the C-suite, underpinned by the challenges of data fragmentation, infected backups, and meeting Recovery Time Objective (RTO) that are visible across the C-suite.	C-suite is not focused on learning from cyberattacks on peer organizations and building defenses accordingly. In most cases, the C-suite lacks a comprehensive vision of security and instead remains reactive.	C-suite is not acting agile enough to focus on the next-generation technology and thinking a step beyond on how to secure itself from the new attack vectors that the new shiny tech brings.

WEF survey indicates that whereas about 85% of cyber leaders agree that cyber resilience is a business priority for their organization, one of their most prominent challenges is to gain decision-makers' support when prioritizing cyber risks against a plurality of other risks[2].

1 Everest Group
2 World Economic Forum's 2022 Global Cybersecurity Outlook

System Integrators (SIs) need to play a critical role in accelerating the adoption of cyber resilience through their expertise and solutions

Services

Deliver comprehensive set of services across key emerging themes, such as zero trust, SASE, SOAR, and XDR, encompassing all aspects of cyber resilience, not just cybersecurity.

Solutions

Invest in building IPs, such as integrated platforms and protected backups, coupled with driving a security-aware culture that can accelerate the cyber resilience journey.

Partnerships

Forge deeper partnerships with technology providers to co-develop solutions while keeping integrability as the cornerstone; interoperability takes precedence over best-of-breed in cyber resilient organizations.

Talent

Create a workforce planning roadmap to cater to the demand for cyber resiliency; giving due importance to post-breach stages of response and recovery.

Engagement models

Lead with an outcome-based pricing model that is tied to an enterprise's transition from cyber aware or cyber secure to cyber resilient; enables service providers to showcase greater stakes in the output.

SIs must take on a crucial role in connecting businesses and cyber leaders by delivering context-driven Return on Investment (RoI) and positioning cyber resilience as an enabler rather than an impedance to business success

Services

Resilience advisory services: focus on providing resilience advisory and creating a cyber resilience roadmap that is aligned to business and cyber leaders, while giving contextualized RoI to both stakeholder groups.

Cyber integration services: leverage your expertise in unifying siloed cyber programs to design and implement organization-wide integrated cyber resilience posture.

Cyber resilience optimization services: ensure that the client's organizational structure and processes are optimized to effectively address cyber resilience challenges.

Solutions

Risk-responsive solutions: develop solutions that can dynamically assess risk, highlight exposures, and empower clients for quicker response.

Adaptive backup and recovery solutions: build flexible backup and recovery solutions that can be changed according to a client's individual RTO, RPO, and backup strategy requirements**.**

Comprehensive cyber resilient MDR: take a platform-led approach to MDR services delivery for better integration capabilities, coupled with a robust set of adjunct offerings.

Partnerships

Technology providers: partner with technology providers to grow expertise in next-generation technologies to stay ahead of attackers, especially on the generative AI front.

Clients: collaborate with clients to create contextualized resiliency solutions based on client requirements.

SIs need to prioritize outcome-driven pricing models for comprehensive cyber resilience efforts, demonstrating their commitment to the overall success of the business in tandem with providing high quality resources

Talent

Hire: hire the right talent to provide end-to-end cyber resiliency services and give due importance to technical skills, adaptability, and experience.

Retain: understand the professional development requirements of resources and fulfill them by providing growth opportunities, coupled with competitive compensation and cross-functional deployments.

Train: provide upskilling and cross-skilling opportunities and leverage the partner ecosystem to train and certify resources on next-generation technologies and certifications.

Engagement models

Zero-cost approach: stay price conscious as clients are grappling with an economic slowdown. So, highlighting cost takeout opportunities to offset the overall engagement cost would go well with clients.

As-a-service: offer cloud-delivered solutions with as-a-service option, leading with differentiations such as cost savings, scalability, reduced maintenance, and faster deployment.

Modular services: be flexible in your engagement model and if it is platform-led, then it is better to keep offerings modular as the same bundling methodology might not resonate well with all.

06

Appendix

- Glossary
- Research calendar

Glossary of key terms used in this report

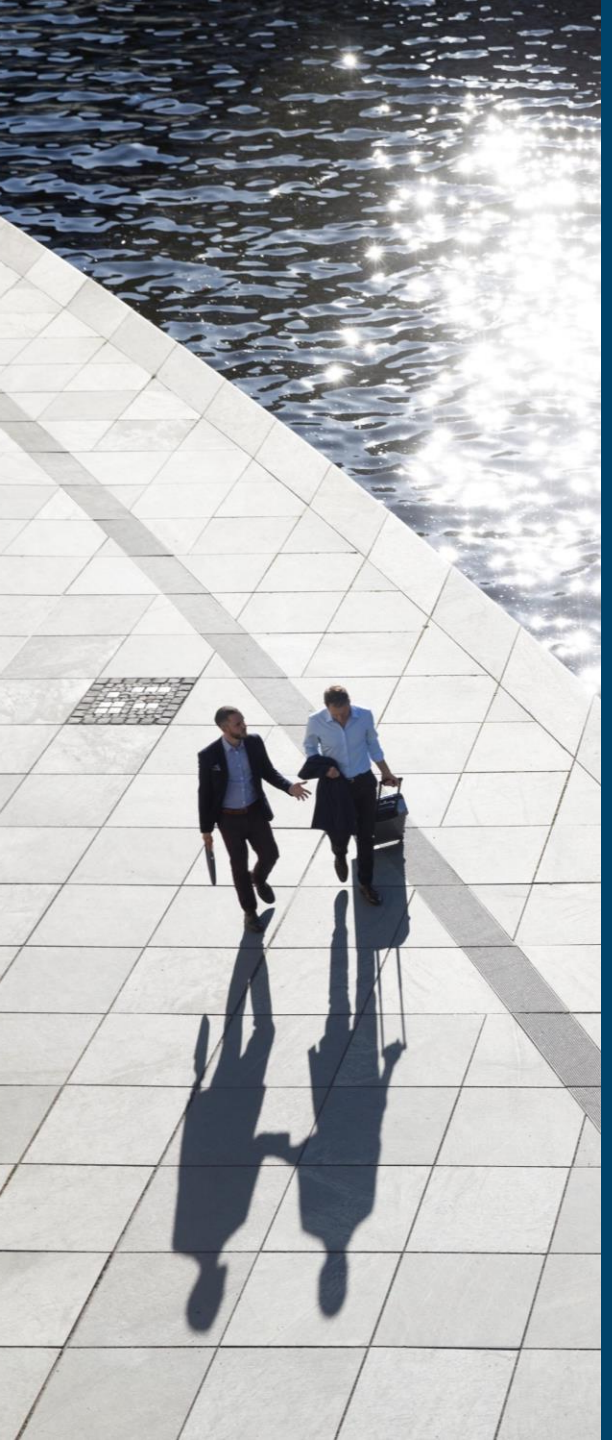
DDoS	Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt traffic to a targeted server, service, or network by overwhelming the target or the surrounding IT infrastructure with a flood of internet traffic
DevSecOps	Involves the introduction of security at scale earlier in the software development life cycle to minimize vulnerabilities and bring security closer to IT and business objectives
EDR	End-point Detection and Response (EDR) detects and investigates suspicious activities on end points and employs a high degree of automation to quickly identify and respond to threats
End-point security	Includes protection of end-user devices (e.g., desktops, laptops, mobiles, and tablets), data protection, and Host Intrusion Prevention Systems (HIPSs)
GRC	Governance, Risk Management, and Compliance
Identity and Access Management (IAM/IDAM)	Covers authentication, access services, single sign-on, password and storage management, authorization services, fraud management (transaction monitoring, anti-phishing, adaptive authentication, and anti-malware), etc.
MDR	MDR stands for Managed Detection and Response. It is an offering that combines four basic services – threat hunting, threat intelligence, incident detection and triaging, and incident response delivered from a cloud-based platform from Security Operations Centers (SOCs)
Operational Technology (OT) / ICS	Combination of computing and communication systems to manage, monitor, and control industrial operations. Focuses on physical devices and processes that they use
Security Operations Center (SOC)	A centralized service provider unit for managing enterprise security issues by providing services such as security logs and event management, security incident response, malware analysis, and forensics
SIEM	Security Information and Event Management

Research calendar
Cybersecurity

Published | Planned | Current release

Reports title	Release date
Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2023	December 2022
Managed Detection and Response (MDR) Services Provider Compendium 2023	February 2023
Cautious Optimism Amid Disruption – 2023 Key Issues, Enterprise IT Perspective	March 2023
Enterprise Pulse for Technology Services 2023: Sharp Decline in Customer Satisfaction	April 2023
Talent Demand Trends | India IT Services – H2 2022	May 2023
Cyber without Perimeters: Starting Your Zero-trust Journey with Identity	May 2023
Cybersecurity Services State of the Market 2023: Cyber Secure to Cyber Resilient	**June 2023**
From Risk Mitigation to ESG Leadership: The Untapped Potential of Managed Detection and Response (MDR)	Q3 2023
Identity and Access Management (IAM) Services PEAK Matrix® Assessment 2023	Q3 2023
Cloud Security Services PEAK Matrix® Assessment 2023	Q3 2023
Identity and Access Management Services Provider Compendium 2023	Q3 2023
Cloud Security Services Compendium 2023	Q3 2023
Operational Technology (OT) Security Providers PEAK Matrix Assessment	Q3 2023
Network Security and Security at the Edge	Q4 2023
Managed Security Services Specialists PEAK Matrix® Assessment 2023	Q4 2023
Identity and Access Management (IAM) Tech Provider Report	Q4 2023

Note: Click to see a list of all of our published cybersecurity reports



Everest Group®
With you on the journey

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
+1-647-557-3475

Website
everestgrp.com

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

Blog
everestgrp.com/blog

NOTICE AND DISCLAIMERS