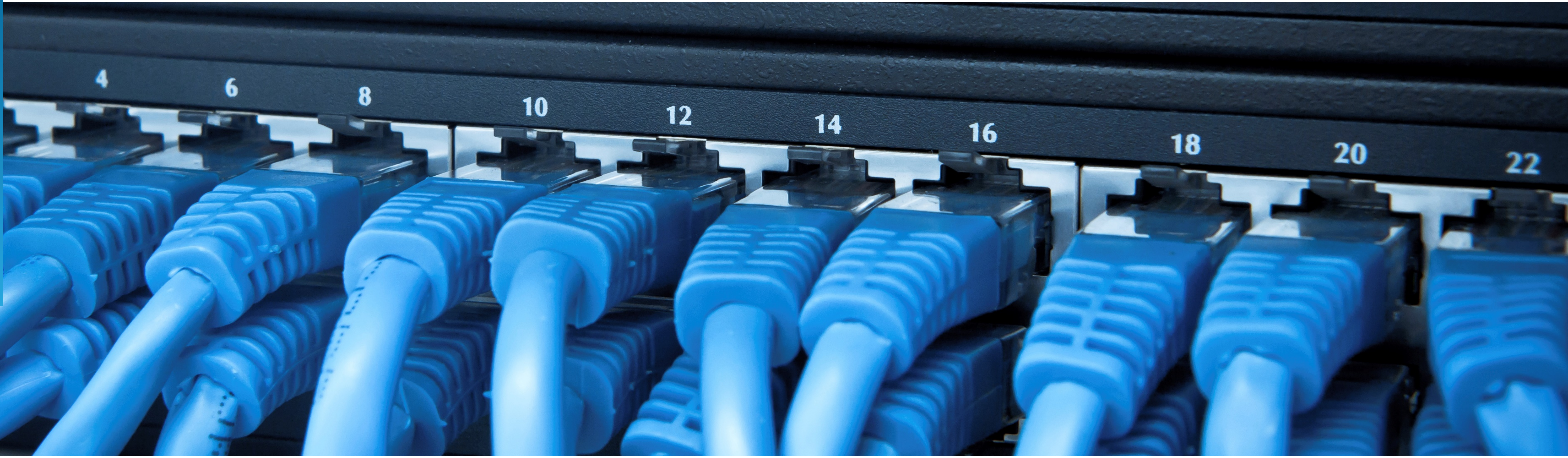
Market Report | Cloud and Infrastructure Services

Technology Vendor Overview for Next-generation Managed Security Services

October 2021: Complimentary Abstract / Table of Contents



Our research offerings

This report is included in the following research program(s):
Cloud and Infrastructure Services

- Application Services
- Banking & Financial Services BPS
- Banking & Financial Services ITS
- Catalyst™
- Clinical Development Technology
- Cloud & Infrastructure
- Contingent Workforce Management
- Conversational AI
- Cost Excellence
- Customer Experience Management Services
- Cybersecurity
- Data & Analytics
- Digital Adoption Platforms (DAP)
- Digital Services
- Engineering Services
- Enterprise Platform Services
- Finance & Accounting
- Financial Services Technology (FinTech)
- Global Business Services
- Healthcare BPS
- Healthcare ITS
- Human Resources
- Insurance BPS
- Insurance ITS
- Insurance Technology (InsurTech)
- Insurance Third-Party Administration (TPA) Services
- Intelligent Document Processing (IDP)
- Interactive Experience (IX) Services
- IT Services Executive Insights™
- Life Sciences BPS
- Life Sciences ITS
- Locations Insider™
- Marketing Services
- Market Vista™
- Mortgage Operations
- Multi-country Payroll
- Network Services & 5G
- Outsourcing Excellence
- Pricing-as-a-Service
- Process Mining
- Procurement
- Recruitment Process Outsourcing
- Retirements Technologies
- Rewards & Recognition
- Service Optimization Technologies
- Supply Chain Management (SCM) Services
- Talent Excellence GBS
- Talent Excellence ITS
- Technology Skills & Talent
- Trust and Safety
- Work at Home Agent (WAHA) Customer Experience Management (CXM)
- Workplace Services

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: service 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:

Mukesh Ranjan, Practice Director

Kumar Avijit, Practice Director

Rohit Kumar, Senior Analyst

This report focuses on leading technology vendors for managed security services

The report provides a brief overview of technology vendors aiding global system integrators (GSIs) deliver managed security services. The report, an addendum to the IT MSS PEAK Matrix assessment, covers leading technology vendors who offer products/solutions spanning SIEM, SOAR, threat intelligence platforms, threat hunting, threat detection and response services, and AI/ML-driven platforms for security operations, etc.

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.

Managed services

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

Managed security services

Managed application security

Managed SAST/DAST, vulnerability detection and management, public and internal web app scanning, advanced dynamic web client testing, and compliance reporting. DevSecOps-as-a-Service, enterprise platform security (ERP, CRM, etc.)

Managed cloud security

Cloud security configuration, controls, and policies across enterprise cloud foundation; cloud risk management; cloud networking monitoring and automated events-based playbooks for threat detection and incident response in cloud; VPC security; cloud governance

Managed endpoint security

Managed Endpoint Security Host intrusion detection and prevention management; Managed antivirus/anti-malware, proactive patch management, managed encryption services, managed data loss prevention; Data integrity monitoring; Change management

Managed network security

Managed firewall, WAF management, DDoS mitigation and management, Network intrusion detection / prevention system management; web content filtering; gateway anti-virus management

Managed IAM

Identity governance and lifecycle management; PIM/PAM managed services; identity platform management; active directory services

Managed risk and compliance

Risk assessment as-a-service; security threat, risk analytics, and event correlation; enterprise compliance monitoring; security awareness training

Managed threat operations

Managed SIEM; threat hunting services; threat intelligence services; managed detection and response services; security infrastructure management; malware analysis; forensics investigations

Introduction

IT security – Technology vendors for next-generation managed security services

- With the ever-increasing complexity of the cyberattack surface and the evolving global threat landscape, organizations of all types and sizes now need to make conscious efforts to protect their critical data against cyber-attacks.
- In the past decades, technology has been built with a primary mission to monitor client environments on a 24/7 basis, alert them in case of incidents, and strengthen their cybersecurity posture. However, traditional technology for managed security services delivery has faced immense difficulties catching up. The increasing connectivity of today's environments, devices, and applications has created the need for next-generation technology enablement for managed security services delivery.
- The next generation of managed security needs to leverage innovative technologies and strategies to help organizations protect their complex, interconnected environments. The realization, that managed security services delivery needs to be underpinned by innovative technologies, is propelling technology vendors to deliver fit-for-purpose technology based on enterprise needs and requirements
- At Everest Group, we have been tracking the managed security services market for the past few years. In early 2021, we published IT Managed Security Services PEAK Matrix® Assessment 2021, where we presented an analysis of 28 global service providers providing managed security services. Our recently published work, Next-generation Managed Security Service (MSS): Tussling to Keep the Battle Alive provides an overview of the managed security services market, typical deal characteristics, enterprise challenges and best practices, and implications for service providers.
- As a part of our ongoing research agenda, this document presents insights into the leading technology vendor in managed security services ecosystem. These technology vendors have gained significant importance over the past few years, as they cater to rising enterprise demand of security services. Enterprises approach these technology vendors to consume next generation managed security services requirement stemming from the increased adoption of digital transformation

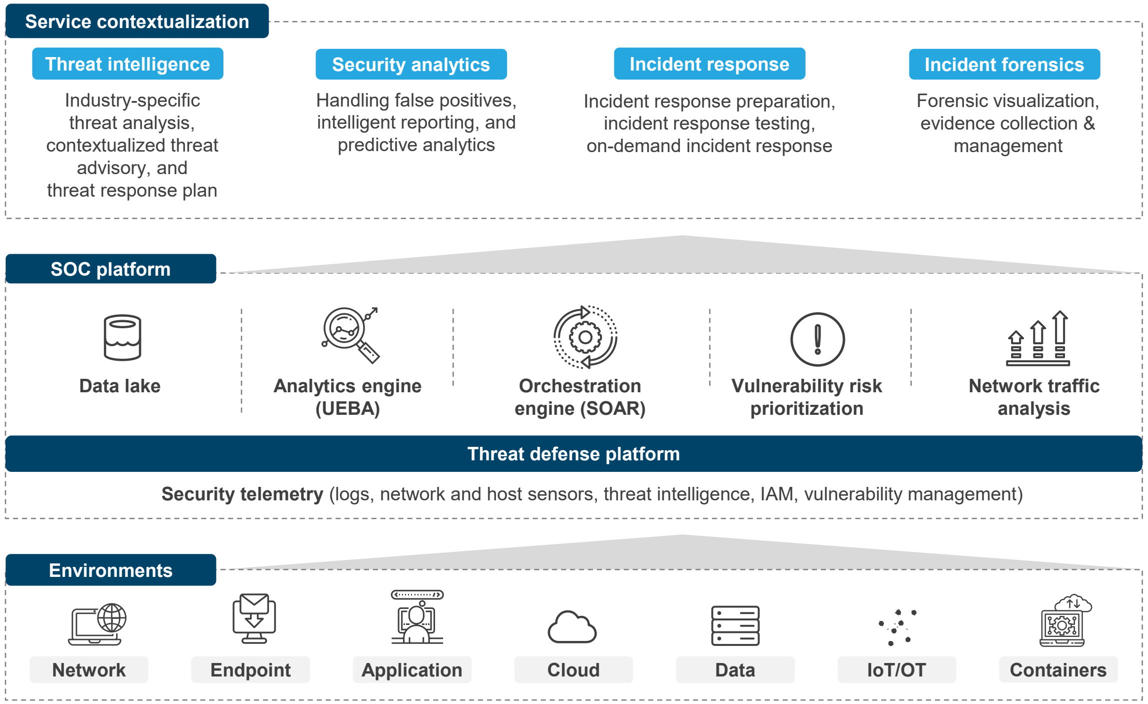
Scope of this report:

Geography
Global

Services
IT security services

This study offers provides a deep dive into key aspects of technology vendor; below are two charts to illustrate the depth of the report

Next-generation managed security services delivery



Service contextualization

Threat intelligence
Industry-specific threat analysis, contextualized threat advisory, and threat response plan

Security analytics
Handling false positives, intelligent reporting, and predictive analytics

Incident response
Incident response preparation, incident response testing, on-demand incident response

Incident forensics
Forensic visualization, evidence collection & management

SOC platform

Data lake

Analytics engine (UEBA)

Orchestration engine (SOAR)

Vulnerability risk prioritization

Network traffic analysis

Threat defense platform

Security telemetry (logs, network and host sensors, threat intelligence, IAM, vulnerability management)

Environments

Network

Endpoint

Application

Cloud

Data

IoT/OT

Containers

Overview of technology vendors for next-generation managed security services

Leading technology vendors and their flagship solutions or managed security services

Vendor name	Solution	Category	Brief description	Value proposition
Check Point	R81 Cybersecurity Platform	Threat prevention	An autonomous threat prevention system that has curated policies aimed at enhancing operational efficiency and lowering complexity of managing enterprise security. Delivers centralized management control across enterprise networks and cloud environments	• AI-enabled threat prevention • Zero day protection
CROWDSTRIKE	Falcon OverWatch	Threat detection and management	Managed threat hunting and detection service, built on CrowdStrike Falcon platform, OverWatch provides in-depth and continuous human analysis round the clock to hunt for novel or anomalous threat actors that may evade standard technology tools.	• Team of cross-disciplinary specialists • Extension to CrowdStrike's Threat Graph • Cloud-scale telemetry
DARKTRACE	Enterprise Immune System	Threat detection and management	The solution, modeled on self-learning AI, protects enterprises against threats from cloud, email, IoT, networks, and industrial systems. Coverage spans threat vectors such as insider threat, industrial espionage, IoT compromises, zero-day malware, data loss, supply chain risk, and long-term infrastructure vulnerabilities.	• Autonomous threat response technology • Open and extensible architecture
deepinstinct	Deep Instinct – Automated threat analysis	Threat detection and management	Threat intelligence platform, underpinned by deep learning technology, provides automated threat analysis and classification of malicious attacks. This helps SOC teams understand different security events and remediate threats.	• Real-time threat classification • End-to-end threat analysis and visibility • Threat management console
FIREEYE	Helix Security Platform	Security operations	Cloud-hosted security platform that enables enterprises to take control of incidents from detection to response and remediation. Integrates existing security tools and augments them with next-generation SIEM, orchestration, and threat intelligence capabilities	• Event management and behavioral analysis • Workflow management • Integrated SOAR
FORTINET	Security Fabric	Security operations	AI-enabled SOC platform that allows integration and automation across various security segments (endpoint, network, etc.) to help enterprises reduce risk and increase efficiency. Also provides advanced threat detection and response capabilities along with centralized security monitoring and optimization	• AI-driven security operations • Advanced threat protection

Glossary of key terms used in this report

DAST Dynamic Application Security Testing is performed to detect conditions indicative of a security vulnerability in an application in its running state

DDoS Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt traffic to targeted server, service or network by overwhelming the target or the surrounding IT infrastructure with a flood of internet traffic

DevSecOps Introducing security earlier in the software development life cycle to minimize vulnerabilities and bring security closer to IT and business objectives

EDR Endpoint Detection and Response (EDR) detects and investigates suspicious activities on endpoints and employs a high degree of automation to quickly identify and respond to threats

Endpoint security Includes protection of end-user devices (e.g., desktops, laptops, mobiles, and tablets), data protection, and Host Intrusion Prevention Systems (HIPS)

IAM Covers authentication, access services, single sign-on, password and storage management, authorization services, fraud management (transaction monitoring, anti-phishing, adaptive authentication, anti-malware), etc.

NTA Network Traffic Analysis (NTA) is the process of intercepting, recording, and analyzing network traffic in order to respond to security threats

Operational Technology (OT) 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 A software solution that gives enterprises both insight into and track record of activities within their systems. Analyzes logs and event data in real-time

SOAR A solution stack that allows an organization to collect security data from multiple sources and respond to security events without human assistance

Threat intelligence platform A platform that helps organizations aggregate, correlate, and analyze threat data from multiple sources in real time to support enterprise defensive actions

UEBA User and Entity Behavior Analytics that tracks the conduct of users and entities in the system to detect any anomalous behavior, using machine learning, algorithms, and statistical analysis

WAF Web Application Firewall protects web applications by filtering and monitoring the traffic between the web application and the internet

Research calendar
Cloud and Infrastructure Services (CIS)

🟦 Published ⬜ Planned ⬛ Current release

Flagship reports	Release date
IT Managed Security Services (MSS) PEAK Matrix® Assessment 2021	June 2021
IT Managed Security Services (MSS) Compendium 2021	July 2021
Network Transformation and Managed Services PEAK Matrix® Assessment 2021	July 2021
Aware Automation immunity is the Key to Combat the COVID-19 crisis	July 2021
SD-WAN Services PEAK Matrix® Assessment 2021	September 2021
Next-generation Managed Security Service (MSS): Tussling to Keep the Battle Alive	September 2021
Technology Vendor Overview for Next-generation Managed Security Services	**October 2021**
Digital Workplace Services PEAK Matrix® Assessment 2021	Q4 2021
Mainframe services PEAK Matrix® Assessment 2021	Q4 2021
State of the Market: IT Infrastructure Services	Q4 2021

Thematic reports	Release date
Future-proofing Enterprise Transformation with Cloud-agnostic Managed Services	February 2021
Upcoming Contract Renewals – Infrastructure Services 2021	March 2021
Enterprise Pulse Report: From Dissatisfaction to Delight: Sustaining Client Satisfaction in a Post-pandemic World	March 2021
Tech Bytes for Business Leaders: Containers	August 2021
Tech Bytes for Business Leaders: Workplace-as-a-Service (WaaS)of a Future-Ready Enterprise	August 2021

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

Everest Group®
With you on the journey

Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our clients include leading global companies, service providers, and investors. Clients use our services to guide their journeys to achieve heightened operational and financial performance, accelerated value delivery, and high-impact business outcomes. Details and in-depth content are available at **www.everestgrp.com**.

Stay connected

Website
everestgrp.com

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

Blog
everestgrp.com/blog

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

This document is for informational purposes only, and it is being provided "as is" and "as available" without any warranty of any kind, including any warranties of completeness, adequacy, or fitness for a particular purpose. Everest Group is not a legal or investment adviser; the contents of this document should not be construed as legal, tax, or investment advice. This document should not be used as a substitute for consultation with professional advisors, and Everest Group disclaims liability for any actions or decisions not to act that are taken as a result of any material in this publication.