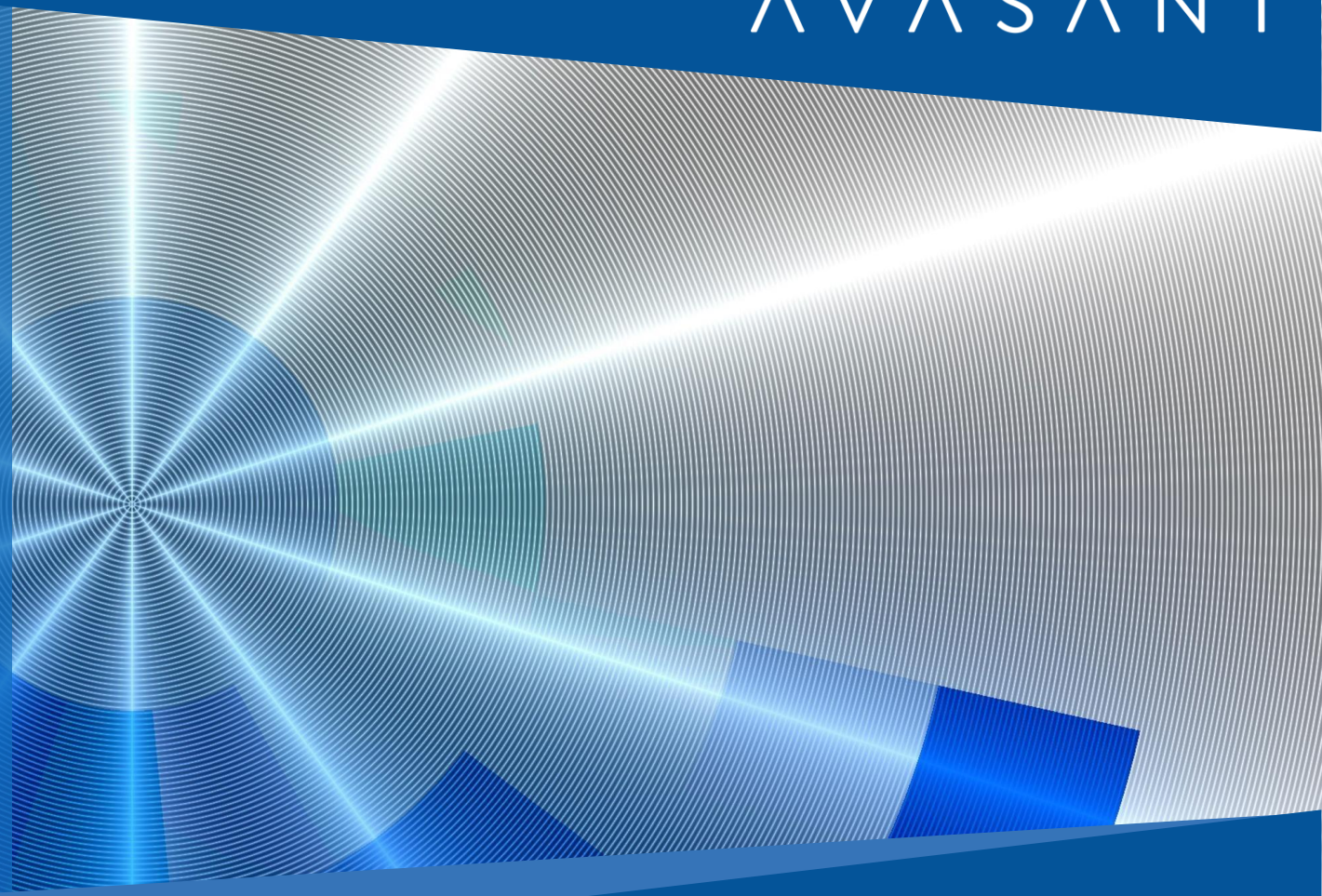
AVASANT

Cybersecurity Services 2022 RadarView: Report Excerpt

Moving from a reactive to a proactive security posture

April 2022



RADARVIEW™

Table of contents

About the Cybersecurity Services RadarView 2022 report

1. The Russia-Ukraine conflict has further escalated cyber risks in an already precarious cyber threat environment. Organizations continue to contain email cyberattacks involving phishing that are extending to their supply chain partners.

2. As businesses modernize their IT infrastructures, there is an increased interest in the zero-trust security model and deploying or refreshing necessary security controls. All these measures help companies move from a reactive to a proactive security operations center (SOC) by automating the triage process and incident response.

3. The *Cybersecurity Services RadarView 2022* report is designed to inform enterprises about best practices in this space and provide a relatively granular understanding of key service providers.

4. Avasant evaluated 35 providers using a rigorous methodology across three key dimensions: practice maturity, partner ecosystem, and investments and innovations. Of the 35, 29 are recognized as having brought the most value to the market over the last 12 months.

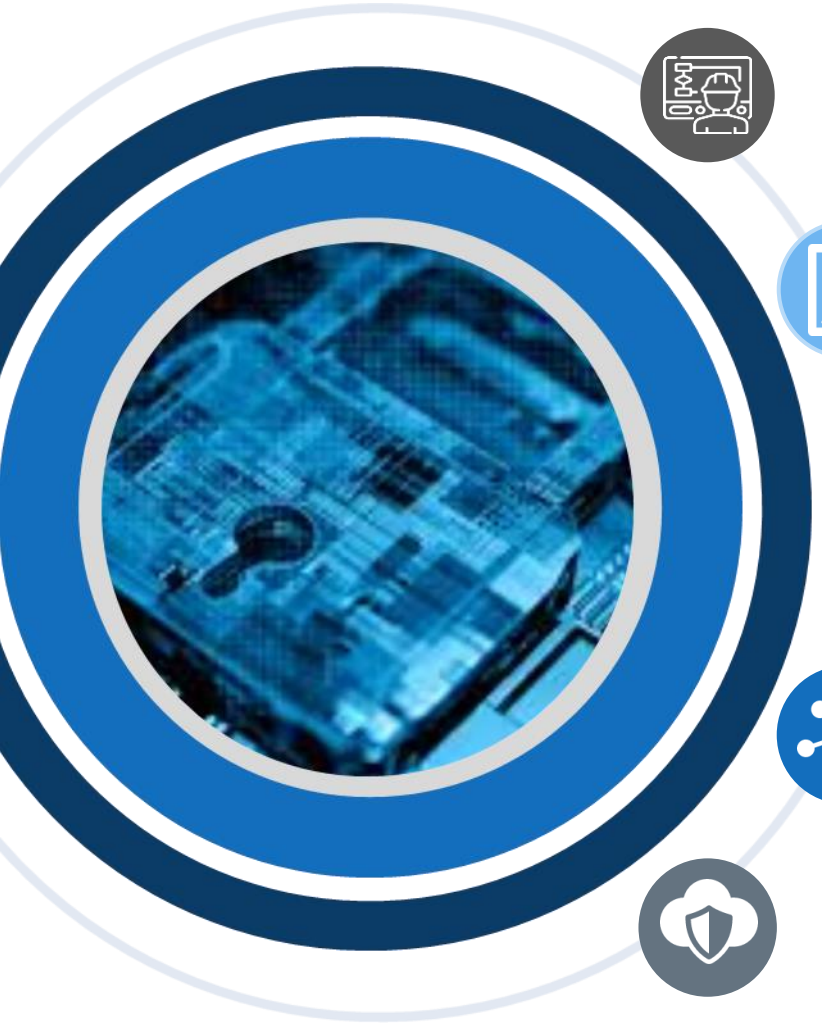
5. This report also highlights key trends in the market and Avasant's viewpoint on the future direction of the industry over the next 12 to 18 months.

AVASANT

Executive summary

Defining cybersecurity

Cybersecurity is built on the concepts of prevention, detection, response, and recovery. It is a dynamic and rapidly evolving space typically consisting of the following elements:



Application security
Measures taken during the development life cycle to protect applications from vulnerabilities due to flaws in application design, development, deployment, upgrade, or maintenance that can be exploited by internal and external threats.

Information security
Protects information from unauthorized access to avoid identity theft, information compromise, or unauthorized alteration. Communication channels include email, messaging apps, and social media, which are covered by email and messaging security and fraud and transaction security.

Disaster recovery/business resilience
Includes performing risk assessments, establishing priorities, developing recovery strategies in case of a disaster, and testing end-to-end business and infrastructure resilience processes to meet availability requirements.

Network security
Protects the integrity of the network by leveraging security tools including antivirus and antispyware, firewalls, intrusion detection/prevention systems (IDS/IPS), and cryptography/virtual private networks (VPNs). Entails the protection of the network connected to devices (mobile device security) or various endpoints (endpoint security).

Cloud security
A set of policies, procedural controls, and technologies to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is an underlying component cutting across other security aspects when employed.

Key enterprise cybersecurity trends shaping the market

RADARVIEW™

Cyber risks from the Russia-Ukraine war increase for the US	• US President, Joe Biden, recently announced strengthening US security posture amid potential cyberattacks from Russian agencies. This was followed by a caution note released by the Department of Health and Human Services about the imminent risk to the US healthcare sector. • The ongoing conflict amplifies the broader trend of increased sophistication and variations of attacks. The latest Log4j breach is one such instance, putting applications and services based on Java at risk.
Essential services continue to be prime targets	• Healthcare and banking lead the cybersecurity adoption trend followed by manufacturing when it comes to utilizing managed security services covering several domains: identity and access management (IAM), data protection and privacy (DPP), and infectious virtual machines (IVM). • These managed services can improve data masking, access governance, and end-to-end automation of the workforce, reducing manual efforts with automated security.
Large SD-WAN projects demand SASE security models	• As organizations scale up their SD-WAN projects, IT leaders are combining secured internet access and secured access to applications. • There is a lot of interest in secure access service edge (SASE) security models. These models bring cloud and network security capabilities together with WAN, firewall, data-loss protection, deep packet inspection (DPI), and cloud security tools.
Service providers scale their consulting practice	• Progressive service providers are doubling down on their consulting capabilities by acquiring skillsets via acquisitions and integrating existing business groups to take advantage of multidisciplinary teams. • Enterprise customers want to engage with a service provider that can give consulting advice, participate in board or C-suite executive discussions, help to drive strategic decisions, and improve governance, while keeping an eye on the next phase of a project.

AVASANT

The road ahead for enterprises

RADARVIEW™

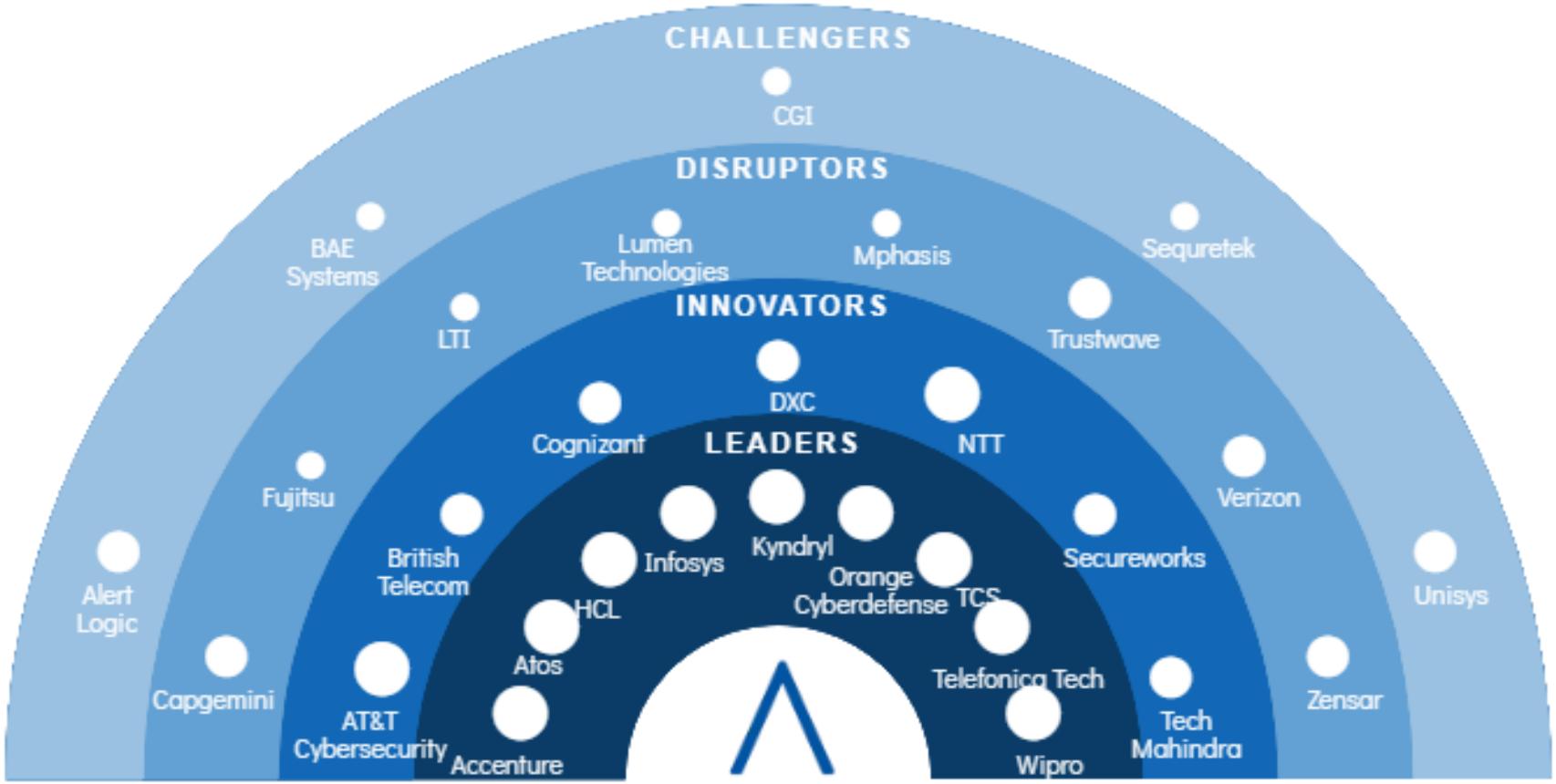
Move from a reactive to a proactive SOC	• Use machine learning (ML) and data science to model attacker behavior, for example, indicators of compromise, and proactively identify threats and automate the triage process and incident response. • To augment Extended Detection and Response (XDR) platforms, managed security service providers (MSSPs) are collaborating with specialized security providers such as Securonix and Snowflake. MSSPs are also leveraging cloud service provider (AWS and Microsoft) security capabilities.
Consider a zero-trust security model	• Enterprises have security controls across the five pillars of the enterprise IT landscape: user, device, networks, infrastructure and applications, and data. • Replace legacy VPNs and traditional internet gateways with a zero-trust solution and deploy cloud-based solutions to neutralize cyberattacks on connected operational technology (OT) devices.
Refresh necessary security controls for this evolving landscape	• Enterprise customers need to secure their hybrid environment by refreshing, enabling, and standardizing security controls deployment to address trends emerging around cloudification, Industry 4.0, and the convergence of 5G and software-defined networking (SDN). • This covers access controls for provisioning least privilege access, security controls deployments, and monitoring access across IT, OT, and SD-WAN architectures.
Layout a comprehensive audit program	• Considering the Russia-Ukraine conflict, organizations should reassess risk, analyze performance metrics, check the supply chain, and layout a comprehensive audit program. • Other measures include obtaining cyber liability insurance, performing an annual review of security measures, and monitoring continuously malicious activity and policy violations.

AVASANT

Avasant recognizes 29 top-tier providers supporting enterprise adoption of cybersecurity services

RADARVIEW™

Practice maturity



AVASANT

AVASANT

Lay of the land

Attack vectors are becoming more varied and sophisticated

After the ransomware attack on the Colonial Pipeline, the latest Log4j breach has made security professionals, yet again, scramble to fix another critical vulnerability whose final impact is still uncertain.

In December 2021, vulnerabilities were found with Log4j, allowing hackers to control target systems and execute commands remotely. This put multiple applications and services based on Java at risk.

In December 2021, Intenum Group, the French IT company, became the target of a ransomware attack. The impact was limited to certain operations in France.

In October 2021, Syniverse, an SMS routing company for all major carriers including T-Mobile, Verizon, and AT&T, disclosed that its systems and databases had been hacked for over five years.

In August 2021, a series of attacks exploiting vulnerabilities in the Microsoft Exchange Server, dubbed ProxyShell, took place. Hackers penetrated Microsoft 365 users' networks and launched phishing campaigns.

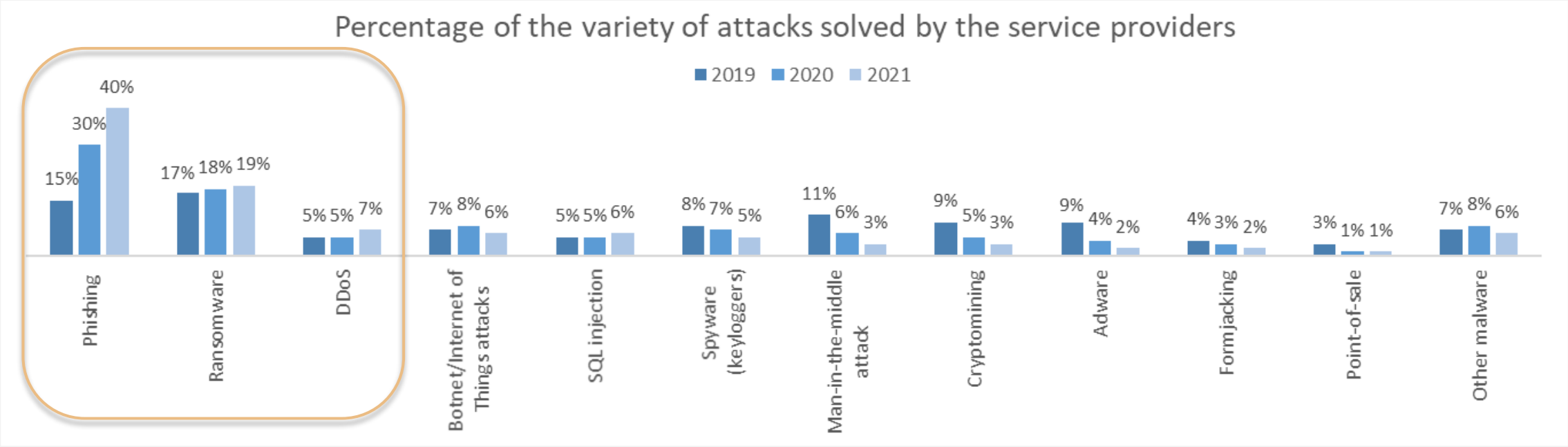
In August 2021, T-Mobile encountered its fifth breach, and one of its largest, in four years. More than 40M customers' data got hacked, including dates of birth, social security and driver's license numbers, and international mobile equipment identity (IMEI) information.

In May 2021, Colonial Pipeline Co., the largest fuel pipeline in the US, was hit by a ransomware attack. Its IT networks were hacked, leading to a gas shortage across the East Coast.

Source: Avasant Research

Phishing continues to account for the largest percentage of cyberattacks followed by ransomware

Due to the workforce mostly working from home, phishing attacks more than doubled. Phishing requires relatively low effort, and its negative impact on a business is high.



In November 2021, IKEA was hit by a phishing attack, extending to its supply chain partners. Also, it compromised its Microsoft Exchange on-premises servers.

In May 2021, the German chemical distributor, Brenntag, paid $4.4M in Bitcoin to the Darkside ransomware group to prevent stolen data from being leaked.

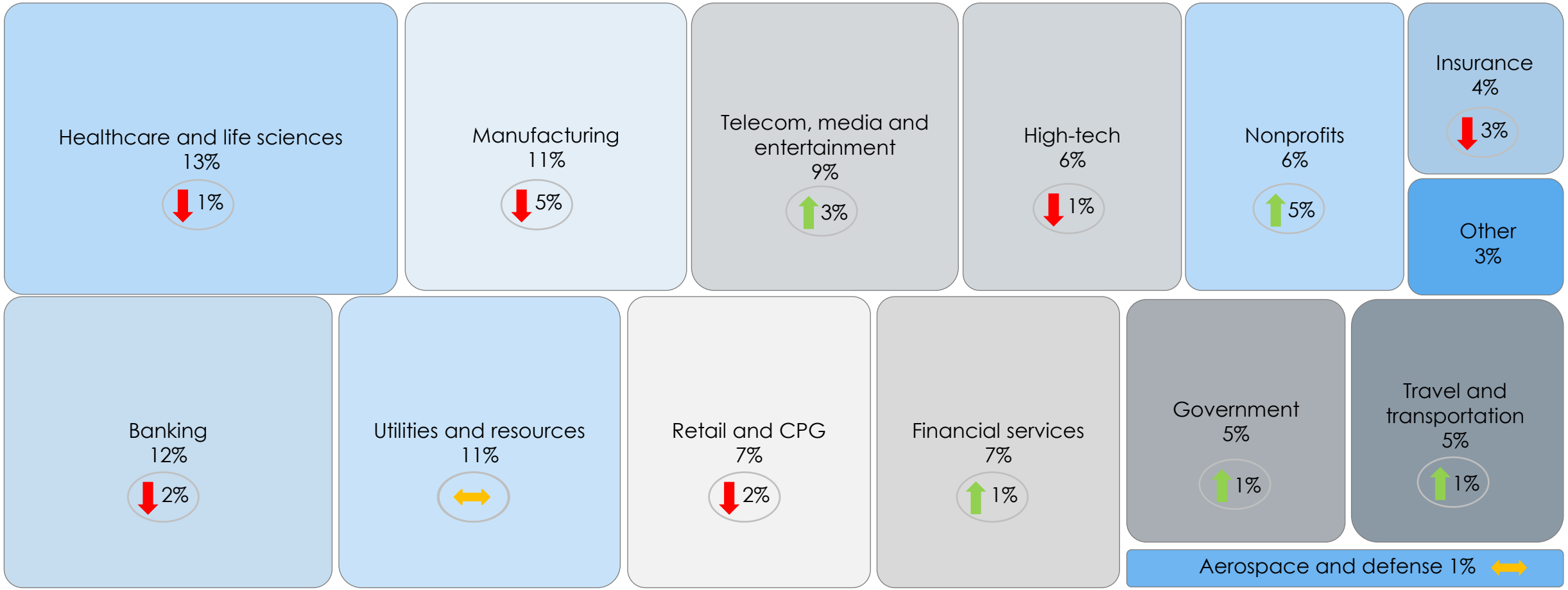
In September 2021, a series of DDoS attacks were launched toward providers in the VoIP industry, including Bandwidth.

Source: Avasant Cybersecurity Services RadarView Survey October–December 2021

Essential services, including healthcare and banking, continue to lead the cybersecurity adoption trend

Industries are investing in cyber resilience by using the zero-trust IAM approach and deploying security orchestration and automation (SOAR) runbooks and playbooks for proactive threat detection and remediation.

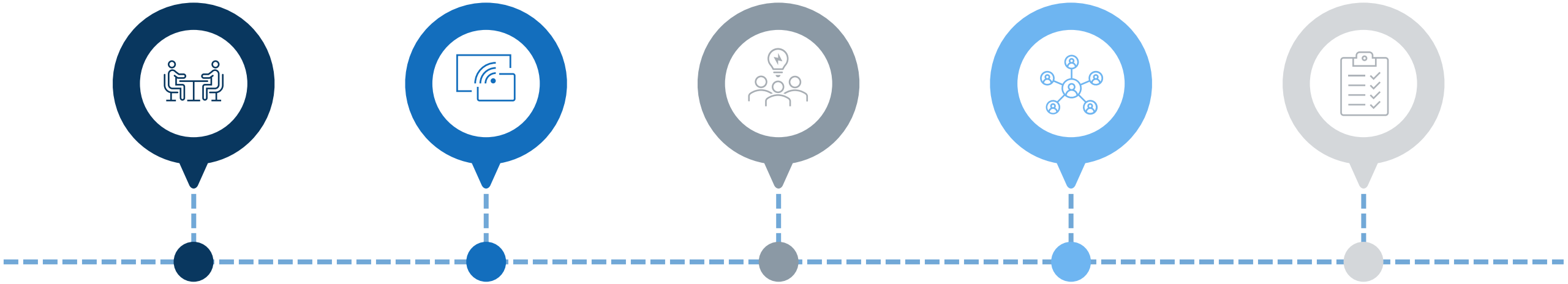
Percentage of revenue from different verticals for cybersecurity services



Source: Avasant Cybersecurity Services RadarView Survey October–December 2021

As organizations modernize their IT infrastructure, there is increased interest in the zero-trust security model

The zero-trust model involves the compartmentalization of data, including user communities, end-user devices, and applications using multifactor authentication and other security measures.



User

A European consumer goods company replaced legacy VPNs and traditional Internet gateways with a zero-trust solution, Zscaler Private Access™ (ZPA™), to provide zero trust access to private applications running on its client's Azure cloud and data centers.

Device

A major financial group in South Africa followed the zero-trust IAM approach to improve remote users' security and enhance cloud applications visibility by implementing Azure multilayered controls.

Network

A European energy company implemented Zscaler SASE and its zero-trust network access (ZTNA) solution for more than 25,000 users with proxy VPN to overcome the mismanagement challenge of security controls.

Infrastructure and Application

Australia's largest producer of biscuits implemented the zero-trust approach to migrate applications from colocation data centers to the cloud using Microsoft's security stack.

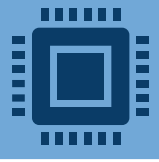
Data

A North American financial services firm implemented HP Voltage data security solution to comply with PCI mandates on secure storage of data for internal applications dealing with PCI/PII data.

 Source: Avasant Research

Companies are deploying or refreshing necessary security controls for the evolving landscape

As businesses modernize their IT infrastructure, IT leaders are combining two key components, secured Internet access, and secured application access.

Industry trends:	Security controls:	Industry use cases:
Cloudification 	• Federation of identity services • Access controls for provisioning least privilege access • Configuration management	• A financial services group in South Africa deployed security controls at different layers from perimeter to workload, improving remote user security and enhancing cloud application visibility.
Industry 4.0 	• Security controls deployment and monitoring across IT and OT • Identification and authentication • Asset map creation	• A Fortune 100 global energy corporation secured their hybrid environment by refreshing, enabling, and standardizing its security controls deployments to include monitoring across IT and OT.
Convergence of 5G and SDN 	• Network microservices segmentation • Integrated firewall and IPS capabilities • Traffic controls using a rules-based approach	• A medical technology company in North America implemented network perimeter and endpoint security solutions, including for mobile users, and enabled IPS for immediate visibility to security threats.

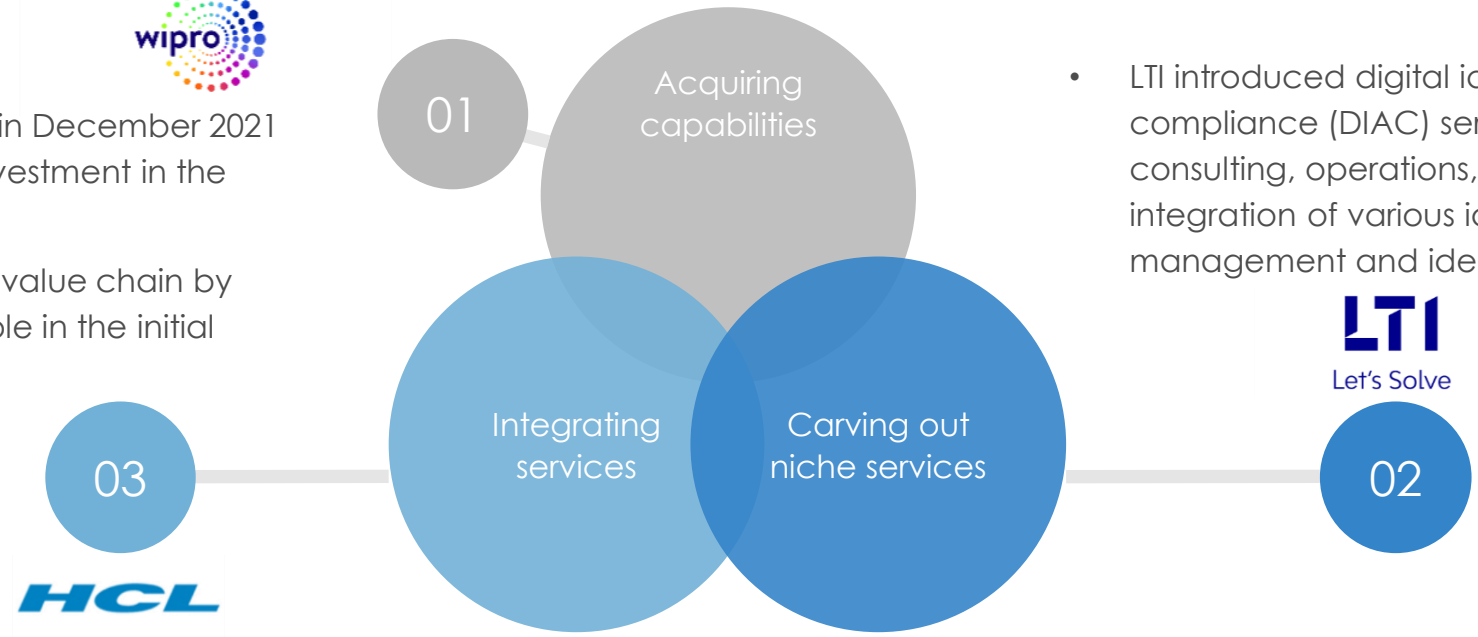
Source: Avasant Research

Engage with a provider that offers advisory services along with implementation and managed services

Organizations need a provider that can engage with the board or C-suite executives and help drive strategic decisions, keeping implementation and managed services in perspective.

Service providers are scaling their consulting practice through the following three approaches:

- Wipro acquired Edgile in December 2021 for $230M, its largest investment in the cybersecurity space.
- It aims to move up the value chain by playing an influential role in the initial stages of deals.



- LTI introduced digital identity assurance and compliance (DIAC) service, which includes consulting, operations, implementation, and integration of various identity and access management and identity governance tools.

- In 2021, HCL integrated its consulting and advisory services with Symantec's and carved out strategy consulting services called FORTIUS.
- It plans to do more posture and maturity assessments, zero-trust architecture implementations, and create more offerings in other areas within the security mesh.

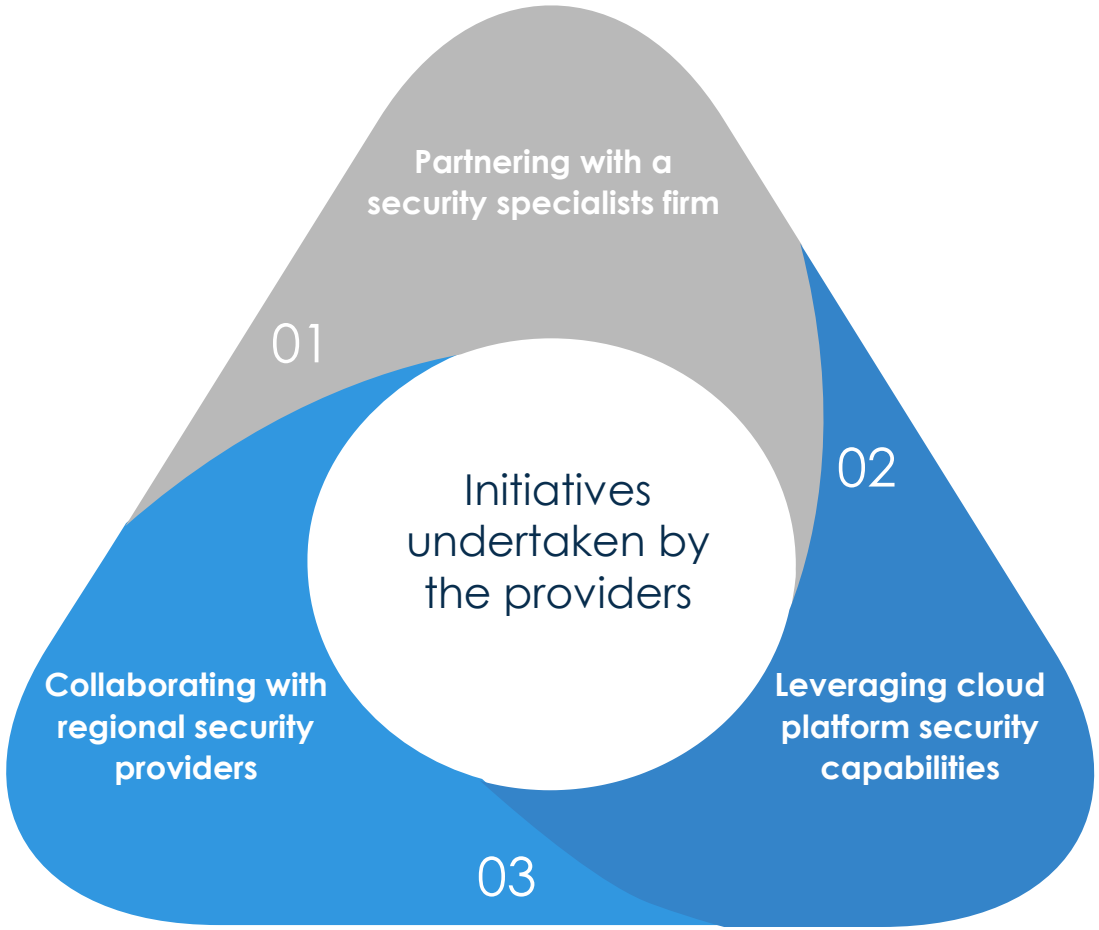
Source: Avasant Research

Companies are moving from a reactive to a proactive SOC and automating the triage process and incident response

RADARVIEW™

This includes the use of ML and data science to model attacker behavior and identify threats before they occur.

Service providers are taking various initiatives to augment their threat detection and response capabilities:



LTI Let's Solve

1 In January 2022, LTI partnered with Securonix and Snowflake to augment its Active eXtended Detection and Response platform (Active XDR). It aims to contextualize and accelerate threat detection and automate incident response time.

Tech Mahindra

2 In September 2021, it achieved AWS Level 1 Managed Security Service Provider (MSSP) Competency status. This allows Tech Mahindra to address cloud security challenges, including 24x7 event monitoring and incident response, triaging, and delivering best practices around AWS service configuration.

Capgemini

3 In June 2021, it partnered with TEHTRIS, a French cybersecurity provider, to codevelop sovereign solutions to address cybersecurity needs for French public organizations. Through this partnership, it plans to codevelop an attack detection and automated response offering specifically to handle ransomware attacks.

Source: Avasant Research

Organizations should prepare for cyber risks posed by the Russia-Ukraine war

Recent warnings from US President, Joe Biden, and the Department of Health and Human Services for the US to strengthen its security posture amid cyber risk from Russian agencies reflect the severity of the situation.

Considering current events, organizations should contemplate the following measures:

Understand the local exposure

Design a risk-mitigation strategy for data stored, systems installed, and suppliers based out of high-risk regions.

Revise vendor SLAs, OLAs, and KPIs

Focus on metrics that better reflect cybersecurity requirements.

Obtain cyber liability insurance

Provide for data loss or security breaches, technology errors and omissions, and privacy and network security liability insurance.

Review security measures annually

Perform annual penetration testing, inspections, vulnerability assessments, and evaluations of MFA and encryption.

Monitor continuously malicious activity and policy violations

Establish network, application, database, and platform security measures that include firewalls and intrusion detection/prevention systems.

Do thorough audits

Inspect the level of compliance and service maturity.

Source: Avasant Research

AVASANT

RadarView overview

Avasant's Cybersecurity Services RadarView assesses service providers across three dimensions

RADARVIEW™

Practice maturity	• This dimension considers the current state of a provider's cybersecurity practice in terms of its strategic importance for the provider, the maturity of its offerings and capabilities, and client engagement. • The crucial aspects in this dimension are the width and depth of the client base, use of proprietary/outsourced tools and platforms, and quality of talent and execution capabilities.
Partner ecosystem	• This dimension assesses the nature of the ecosystem partnerships of the provider, objectives of the partnerships (codevelopment and co-innovation), and its engagement with solutions providers, startup communities, and industry associations. • Vital aspects in this dimension are evaluation of joint development programs around offerings, go-to-market approaches, and the overall depth in partnerships.
Investments and innovation	• This dimension measures the strategic direction of investments and resultant innovations in the offerings and commercial model and how it aligns with the future direction of the industry. • The critical aspects of this dimension include both organic and inorganic investments toward capability and offering growth, technology development, and human capital development, along with innovative solutions developed with strategic partners.

Research methodology and coverage

RADARVIEW™

Avasant based its analysis on several sources:

Public disclosures	Publicly available information such as Securities and Exchange Commission (SEC) filings, annual reports, quarterly earnings calls, and executive interviews and statements
Market interactions	Discussions with enterprise executives leading digital initiatives and influencing service provider selection and engagement
Provider inputs	Inputs collected through an online questionnaire and structured briefings in October–December 2021

Of the 35 service providers assessed, the final 29 featured in the Cybersecurity Services RadarView for 2022 are:

accenture, Alert Logic by HelpSystems, AT&T Cybersecurity, Atos, BAE Systems, BT, Capgemini, CGI, Cognizant, DXC.technology, Fujitsu, HCL, Infosys, kyndryl, LTI Let's Solve, Lumen, Mphasis The Next Applied, NTT, Orange Cyberdefense, Secureworks, Sequretek Simplify Security, TCS Tata Consultancy Services, Tech Mahindra, Telefónica Tech, Trustwave, Unisys, verizon, wipro, ZenSar

Note: Assessments for Accenture, Alert Logic, AT&T Cybersecurity, BAE Systems, British Telecom, Capgemini, CGI, DXC, Fujitsu, Lumen Technologies, NTT, Secureworks, TCS, Trustwave, Unisys, and Verizon were conducted based on public disclosures and market interactions only.

AVASANT

AVASANT

Cybersecurity Services 2022 RadarView

Reading the RadarView

Avasant has recognized service providers in four classifications:

Leaders show consistent excellence across all key dimensions of the RadarView assessment (practice maturity, partner ecosystem, and investments and innovation) and have had a superior impact on the marketplace. These providers have shown true creativity and innovation and have established trends and best practices for the industry. They have proven their commitment to the industry and are recognized as thought leaders in their space, setting the standard for the rest in the industry to follow. Leaders display a superior quality of execution and a reliable depth and breadth across verticals.

Innovators show a penchant for reinventing concepts and avenues, changing the very nature of how things are done from the ground up. Unlike leaders, innovators have chosen to dominate a few select areas or industries and distinguish themselves based on superior innovation. These radicals are always hungry to create pioneering advancements in the industry and are actively sought after as trailblazers, redefining the rules of the game.

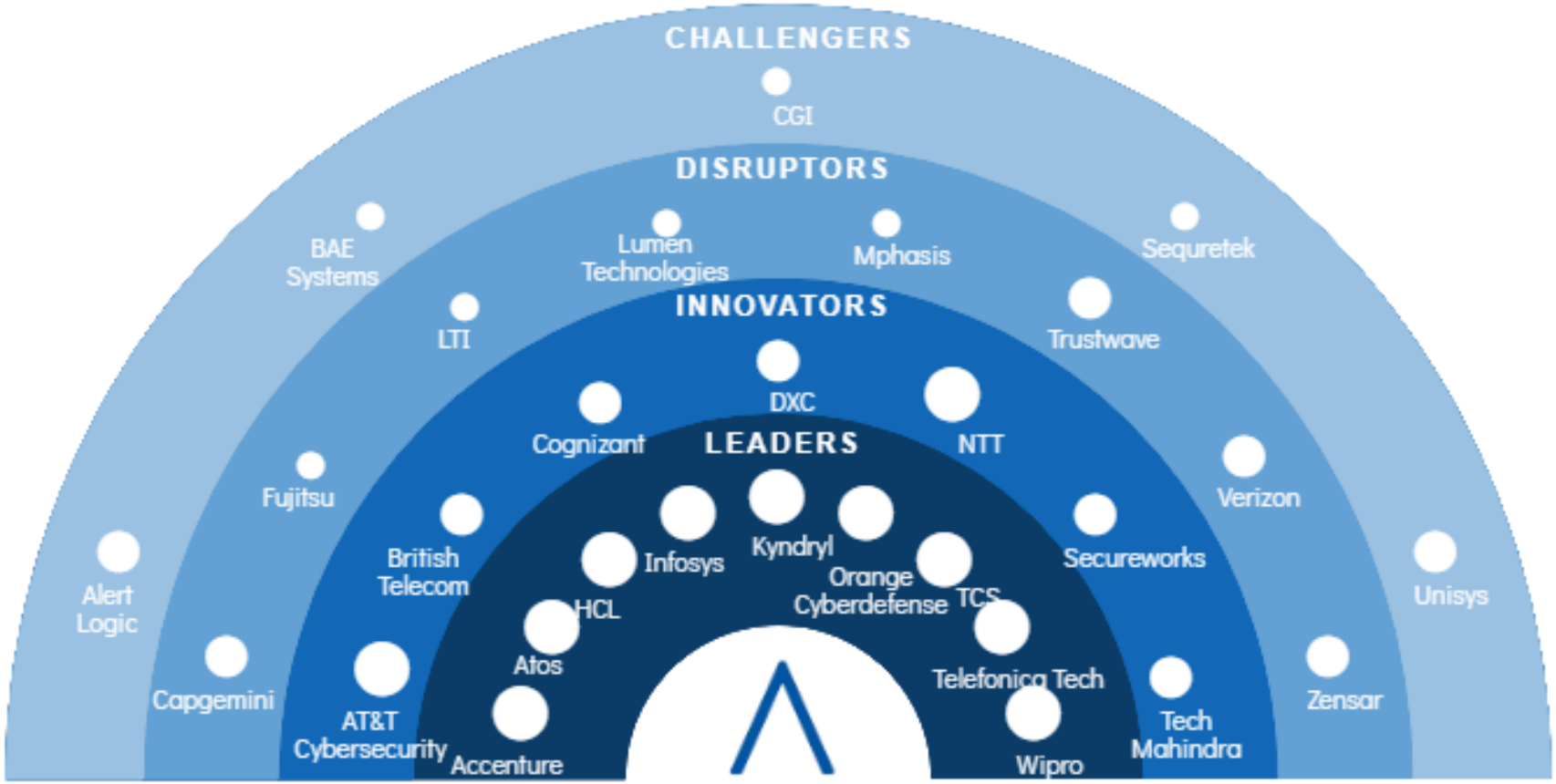
Disruptors enjoy inverting established norms and developing novel approaches that invigorate the industry. These providers choose to have a razor-sharp focus on a few specific areas and address those at a high level of granularity and commitment, which results in tectonic shifts. While disruptors might not have the consistent depth and breadth across many verticals like leaders or the innovation capabilities of innovators, they exhibit superior capabilities in their areas of focus.

Challengers strive to break the mold and develop groundbreaking techniques, technologies, and methodologies on their way to establishing a unique position. While they may not have the scale of the providers in other categories, challengers are eager and nimble and use their high speed of execution to great effect as they scale heights in the industry. Challengers have a track record of delivering quality projects for their most demanding Global 2000 clients. In select areas and industries, challengers might have capabilities that match or exceed those of the providers in other categories.

Cybersecurity Services 2022 RadarView

RADARVIEW™

Practice maturity



AVASANT

AVASANT

Kyndryl profile

Kyndryl: RadarView profile

kyndryl

Practice maturity ★★★★★

Partner ecosystem ★★★★★

Investments & innovation ★★★★

16 strategic partners, including IBM, to provide services similar to QRadar. Focusing on building IPs/assets for workflow automation and runbook automation.

Practice overview

- Practice size: 7,500+
- Certified and trained resources: N/A
- Active clients: 4,000+
- Delivery highlights: Seven global and five regional security operation centers

475+	800+
Security patents granted	DR orchestration library

Client case studies

- Helped a multinational CPG company build cyber resilience capability to address any vulnerabilities to its two data centers situated in high-risk regions. It helped to deploy 70% of the solution in first phase itself and helped to achieve compliance and faster recovery.
- It co-created a recovery solution with AWS for an UK based multi-national bank to enable an automated cyber recovery capability that allowed the bank to rapidly recover from breaches or attacks. This helped to ensure recovery from cyberattacks in hours instead of days and 24/7 forensics checking, alerting and quarantine.
- Implemented resiliency orchestration software to orchestrate and automate DR runbook for a US based international airline. Reduced recovery time objective(RTO) significantly.
- Leveraged its resiliency orchestration capabilities for an US based utility company to solve the problem of business outages and provided a robust business continuity and resilience strategy. It helped the client to achieve six hour RTO with no data loss.

Key IP and assets

- Resiliency Orchestration software: AI based tool to detect anomalies and malware with highest accuracy.

Key partnerships

Platform providers

aws, Google Cloud, IBM, Microsoft

Software providers

vmware, Red Hat, NetApp, cisco, Lenovo

Sample clients

- Multinational CPG company
- UK based multinational bank
- US based utility company
- US based international airline
- India based bank
- Pitney Bowes
- Bangalore International Airport
- Investment bank in Bulgaria
- Rimac Seguros
- Catalonia Health System
- Field Safe Solutions

Industry coverage

- Aerospace & defense
- Banking
- Financial services
- Government
- Healthcare & life sciences
- High-tech
- Insurance
- Manufacturing
- Nonprofits
- Retail & CPG
- Telecom, media & entertainment
- Travel & transportation
- Utilities & resources

Darker color indicates higher industry coverage through digital services

Kyndryl: RadarView profile

Analyst insights

Practice maturity ★★★★★

- In November 2021, IBM separated the services part of cybersecurity portfolio and retained QRadar. Kyndryl then inherited services such as risk and compliance services, identity and assessment services, infrastructure protection and business continuity, and disaster recovery services.
- Its cyber resiliency portfolio consists of security assurance services, zero-trust services, SOC and response services, and incident recovery services.
- It provides protection across the threat life cycle through different services, such as risk identification, AI-driven threat intelligence, vulnerability management, managed detection and response, data protection and disaster recovery (DR).
- One of its key focus lies in DR orchestration. It has built a library of more than 800 predefined automation patterns for accelerated time to market as well reliable recovery of data from different levels.
- Apart from inheriting managed services from IBM, It is currently focusing on building IPs/assets for workflow automation and runbook automation through different types of connectors. Apart from that, it is focused on helping its clients with region-specific compliances.

Partner ecosystem ★★★★★

- Kyndryl currently has 16 strategic partners, including IBM, to provide services similar to QRadar. They are Trustwave, Secureworks, BT, and Nokia. They offer SOC as a service to its clients, thus helping them to avoid any vendor locking or extra investments.
- In November 2021, Kyndryl added Microsoft as its first global alliance partner after its spinoff from IBM. The partnership aims expand its portfolio around cybersecurity and codevelop cybersecurity solutions, leveraging expertise of both the partners.
- Kyndryl has partnered with multiple industry organizations to accelerate its cybersecurity journey, including material science company Dow and Spanish financial institution BBVA. The companies are working together to integrate advanced security in their environments.

Investments and innovation ★★★★

- Its clientele is mostly looking for security services as part of big cloud transformation projects. It collaborates with its clients as a strategic partner to integrate all its capabilities with its clients' solutions.
- In February 2022, it partnered with AWS to build AWS Cloud Center of Excellence to develop industry-specific services or solutions that can be leveraged by a wide number of its clients.
- It employs more than 7,500 skilled professionals around the globe to manage distributed environment for clients and help them with region-specific compliance requirements.

Key contacts

Gaurav Dewan
Associate Research Director
gaurav.dewan@avasant.com

Mark Gaffney
Director
mark.gaffney@avasant.com

John Caruthers
Senior Fellow
John.caruthers@avasant.com

Swapnil Bhatnagar
Senior Research Director
swapnil.bhatnagar@avasant.com

Taniya Chandra
Senior Analyst
taniya.chandra@avasant.com

Disclaimer

Avasant does not endorse any provider, product, or service depicted in its research publications, including RadarView, and does not advise users to select only those providers recognized in these publications. Avasant's research publications are based on information from the best available sources and Avasant's opinion at the time of publication, and their contents should not be construed as statements of fact. Avasant disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

AVASANT

Empowering Beyond

GET CONNECTED

www.Avasant.com