NEAT EVALUATION FOR KYNDRYL:

Attack Surface Management

Market Segment: Overall

Introduction

This is a custom report for Kyndryl presenting the findings of the 2025 NelsonHall NEAT vendor evaluation for *Attack Surface Management* in the *Overall* market segment. It contains the NEAT graph of vendor performance, a summary vendor analysis of Kyndryl for attack surface management services, and the latest market analysis summary.

This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering attack surface management (ASM) as part of their cyber resiliency services. The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors overall, and with specific capability in automated ASM services and integrating ASM within a wider cyber resiliency strategy.

Evaluating vendors on both their 'ability to deliver immediate benefit' and their 'ability to meet future client requirements', vendors are identified in one of four categories: Leaders, High Achievers, Innovators, and Major Players.

Vendors evaluated for this NEAT are: Atos, Detectify, Kyndryl, TCS, Tech Mahindra, Unisys, and Wipro.

Further explanation of the NEAT methodology is included at the end of the report.

NEAT Evaluation: Attack Surface Management (Overall)

NelsonHall has identified Kyndryl as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects Kyndryl's overall ability to meet future client requirements as well as delivering immediate benefits to its cyber resiliency clients.

Leaders are vendors that exhibit both a high capability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet future client requirements.

Buy-side organizations can access the *Attack Surface Management* NEAT tool (*Overall*) here.

Vendor Analysis Summary for Kyndryl

Overview

Kyndryl's ASM services aim to continuously discover, classify, and prioritize internet-facing hardware, software, and cloud assets, to then perform vulnerability management, remediation planning, and monitoring of these assets.

The majority of ASM services are provided via the company's vulnerability management and advisory services using a risk-based delivery model to assess the client's risk appetite and the vulnerabilities they would face against the remediations available.

The newest service in the ASM portfolio is Continuous Security Control Validation (CSCV), that provides daily scans to detect assets and vulnerabilities using automated penetration testing to enable rapid remediation of vulnerabilities by providing users with actionable reports of the vulnerabilities.

Kyndryl uses its Kyndryl Bridge AIOps to aggregate data, validate it, and automate processes to remediate issues, and also to identify cyber maturity levels within the platform.

Kyndryl has built an inventory database as part of its AIOps platform that aims to be the single source of truth. It collects inventory information from the client's other solutions, such as ServiceNow or CMDBs, and consolidates and validates this data into a MongoDB or PostgreSQL database.

This inventory database is used as a data source within ApexaiQ's continuous asset assurance platform alongside vulnerability data from sources including Tenable, Qualys, Rapid7, and other threat information sources such as commercial threat feeds to perform further asset validation, classification, and prioritization of detected vulnerabilities and threats. The combination of these data sources allows the client to perform risk-based vulnerability management based on the criticality of the application or the infrastructure.

Kyndryl's patch management services follows on from its vulnerability management services, and integrates patch tooling management, vulnerability scans, and automated patch installation. Kyndryl uses solutions including Microsoft SCCM and WSUS, Linux SUSE Manager, Red Hat Insights and Satellite Tanium, Qualys, Tenable, and Rapid7 to perform patch management. The company currently has 1.6k clients for its patch management services.

Kyndryl offers new clients a 45-day PoC that aims to identify the current third-party risk management status and gaps. Following this point, the company performs assessments of third parties using Black Kite along with AI/ML to correlate open-source intelligence with 26 control items to provide a ransomware susceptibility rating.

The company performs penetration testing as part of its cloud infrastructure services and sells penetration tests separately as part of its cybersecurity services. It performs 1k+ penetration tests in a given year across these two services. Penetration tests are performed by the company's tier-3 SOC employees and incident response teams, alongside a dedicated team of penetration testers.

Kyndryl has ~7.5k employees delivering cyber resiliency services across 63 countries, including 1.4k practitioners providing security advisory services. It has ~400 clients across its cyber resiliency services portfolio, including 80% of the Fortune 100.

NelsonHall estimates the breakdown of ASM clients by industry to be: financial services 45%, telecoms & media 13%, manufacturing 11%, retail, 10%, government 10%, energy & utilities 5%, transportation 5%, and healthcare 1%.

Financials

Kyndryl does not release revenue figures for its ASM services. The company states in its investor material that its security & resiliency revenues account for ~14% of its total revenues.

NelsonHall estimates that the company's total cyber resiliency revenues in CY 2024 were ~$2.1bn, of which NelsonHall estimates that ASM revenue was ~$150m.

Strengths

- Kyndryl has a high level of investment in launching new cybersecurity offerings, in particular cybersecurity consulting offerings that can support organizations in building strategies and reducing/securing the attack surface
- Kyndryl Bridge can collect all information that can then be used to rate risk and action remediation into the AIOps inventory database
- The company's third-party risk management services extend to fourth parties
- The introduction of the cyber-safe passport can be used to better ensure the take-up of best practices from social engineering attack simulation and training exercises.

Challenges

Automated testing of vulnerabilities following the discovery of assets within Kyndryl's continuous controls validation service is new and currently has no case studies demonstrating its effectiveness.

Strategic Direction

In growing the ASM business, Kyndryl aims to meet its growth targets through a strategy of 70% upsell of ASM to existing clients versus 30% growth attributable to new client acquisition. The growth in ASM aligns with Kyndryl's current cyber resiliency growth, which has been driven by its consulting services in defining security strategies for clients.

Within ASM, Kyndryl believes that some organizations have been focusing on the discovery of assets, but have allocated less funds towards the resolution of discovered vulnerabilities. Kyndryl aims to leverage a client's existing technology deployments, ingesting security information and supporting remediations via SOaaP and Kyndryl Bridge.

Outlook

The company's Kyndryl Bridge platform is used to aggregate security data, validate it, and automate processes to remediate issues. Kyndryl has built an inventory database as part of its AIOps platform that aims to be the single source of truth. It collects inventory information from the client's other solutions, such as ServiceNow or CMDBs, and consolidates and validates this data into a MongoDB or PostgreSQL database.

Kyndryl has been focusing on building its consulting services which have included improvements to its cyber attack simulation and wargaming services that can support organizations in reducing the attack surface.

Organizations looking to better define their attack surface management strategy while leveraging existing technology investments should consider Kyndryl.

Attack Surface Management Market Summary

Overview

Attack Surface Management is the process of identifying and managing cybersecurity vulnerabilities within systems, networks, and applications. These ASM services include asset discovery, vulnerability assessments, prioritization, monitoring, remediation, penetration testing, red teaming, brand monitoring, third-party risk management, and digital risk protection reporting.

ASM providers include IT services vendors, network communication providers, ASM platform owners, and consultancies.

BFSI is the largest vertical market for ASM, as it is in the wider cyber resiliency market, due to the increased regulatory requirements facing these organizations. Similarly, within healthcare, regulations like HIPAA have driven data security requirements; these requirements will increase over time as the amount of patient data increases, and as organizations that interact with healthcare data (such as medical device companies) are mandated to create and maintain SBOMs.

Governments and critical infrastructure companies in energy & utilities have had similar requirements for some time; as national security concerns increase, increased defense spending will be mirrored in increased ASM spending.

Manufacturing growth will be supported by increased use of ASM to detect and secure OT and supply chains. Similarly, retail growth will be supported by supply chain third and fourth parties.

Buy-Side Dynamics

Organizations face the following key challenges in managing their attack surface:

- Ongoing asset sprawl, increasing the number of platforms, applications, and technologies in use
- The absence of a single source of truth for an organization’s asset inventory increases the difficulty in securing and remediating vulnerabilities
- Inadequate AppSec and vulnerability management programs that cannot detect or manage the high number of vulnerabilities within assets
- An inability to understand which vulnerabilities pose the greatest threats that can be prioritized. Solutions that do consider rating the criticality of the risk often fail to consider the importance of the asset to the business or fail to rate risks associated with users' access to systems and data. An increased focus on users as part of ASM lends itself to measuring the effectiveness of zero-trust roll outs
- Brand monitoring being slow to detect changes
- Regulatory requirements, depending on the organization’s industry and the regions in which it operates, to build and manage SBOMs, or more generally secure data and assets
- The need to integrate security best practices into application development, not only to build SBOMs, but to follow DevSecOps practices to reduce vulnerabilities, ensure compliance, and improve overall cyber resiliency

- A high number of third and fourth parties that can pose vulnerabilities to the organization, with difficulties in building a vendor inventory
- The typical way of investigating the risk associated with third parties are questionnaires which are inadequate point-in-time light-touch assessments.

Market Size & Growth

The global ASM market (including both platforms and services) was worth $9bn in 2024, and is estimated to be $11.25bn in 2025. It will grow at 15.5% CAGR to reach $20bn by 2028.

Market growth in the U.S. will be boosted by the likes of CISA directives; for example, for the creation of SBOMs and the need to follow digital adoption that leverages a relatively higher number of cloud, IoT, and similar technologies.

Toward the end of the 2025-2028 period, technology adoption such as GenAI, especially in geographies that are more likely to have regulatory requirements such as the EU, will increase the pressure on ASM requirements. Similarly, quantum computing will increase the need for ASM towards the end of the period as traditional encryption methods will become less adequate as a barrier towards data exfiltration.

Success Factors

Critical success factors for vendors within the attack surface management market are:

- The ability to work across the client's business operations, IT, and third parties
- The ability to detect assets within an organization, the configurations, and then verify these assets to build and maintain a single source of truth that can be used in vulnerability management programs
- Best-of-breed selection of tools to detect these assets and then perform vulnerability assessments and an adequate scale within penetration testing to support logical testing that cannot be automated
- An understanding of the client organization that can be used alongside vulnerability data to adequately judge the risk of the vulnerability to the organization and prioritize remediation of these vulnerabilities in a manner that addresses the largest and most immediate risks to the business
- The ability to monitor the performance of zero trust and data security protocols as part of a wider ASM program to understand what data exists, on what platforms it resides, and what access to the data there is, both from humans and machines
- Continuous brand monitoring, including on the deep and dark web to detect items such as leaked credentials before they are used
- Keeping abreast of the regulatory requirements, understanding the risks posed to the client in not meeting these requirements, and supporting the organization in meeting and monitoring adherence
- Tooling and best-practice support to embed DevSecOps within application development so the organization can increase the overall security of the applications and maintain an SBOM that can be used to monitor cyber resiliency against zero-day attacks

- Tooling and support to identify and investigate risks posed by third and fourth parties, extending beyond simple questionnaires of security posture to a minimum level of third-party brand monitoring.

Outlook

Over the next five years, NelsonHall expects to see:

- A higher percentage of automation in penetration testing
- ASM platforms with more connections to data discovery, IAM, and SAST/DAST/SOAR platforms to detect more risks and manage detected risks
- Threat hunting and deep/dark web monitoring will become standard services in each ASM engagement, similar to threat intelligence gathering. Threat hunting will also start to consider supply chain/third-party attacks and attacks on ML datasets
- Third-party risk management will be extended into fourth-party risk management (i.e. the third parties of third parties)
- Organizations will also move beyond simple questionnaire assessments for third parties of mid to high importance, instead requiring external assessment, penetration testing, and code reviews performed by independent third-party security firms to better measure the security posture of these firms
- Social engineering will combine with ID-ASM efforts to educate users to avoid cyber attacks
- Identity ASM (ID-ASM) to become a recognized service for integrating ID governance, PAM, and asset management systems.

NEAT Methodology for Attack Surface Management

NelsonHall's (vendor) Evaluation & Assessment Tool (NEAT) is a method by which strategic sourcing managers can evaluate outsourcing vendors and is part of NelsonHall's *Speed-to-Source* initiative. The NEAT tool sits at the front-end of the vendor screening process and consists of a two-axis model: assessing vendors against their 'ability to deliver immediate benefit' to buy-side organizations and their 'ability to meet future client requirements'. The latter axis is a pragmatic assessment of the vendor's ability to take clients on an innovation journey over the lifetime of their next contract.

The 'ability to deliver immediate benefit' assessment is based on the criteria shown in Exhibit 1, typically reflecting the current maturity of the vendor's offerings, delivery capability, benefits achievement on behalf of clients, and customer presence.

The 'ability to meet future client requirements' assessment is based on the criteria shown in Exhibit 2, and provides a measure of the extent to which the supplier is well-positioned to support the customer journey over the life of a contract. This includes criteria such as the level of partnership established with clients, the mechanisms in place to drive innovation, the level of investment in the service, and the financial stability of the vendor.

The vendors covered in NelsonHall NEAT projects are typically the leaders in their fields. However, within this context, the categorization of vendors within NelsonHall NEAT projects is as follows:

- Leaders: vendors that exhibit both a high capability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet future client requirements
- High Achievers: vendors that exhibit a high capability relative to their peers to deliver immediate benefit but have scope to enhance their ability to meet future client requirements
- Innovators: vendors that exhibit a high capability relative to their peers to meet future client requirements but have scope to enhance their ability to deliver immediate benefit
- Major Players: other significant vendors for this service type.

The scoring of the vendors is based on a combination of analyst assessment, principally around measurements of the ability to deliver immediate benefit; and feedback from interviewing of vendor clients, principally in support of measurements of levels of partnership and ability to meet future client requirements.

Note that, to ensure maximum value to buy-side users (typically strategic sourcing managers), vendor participation in NelsonHall NEAT evaluations is free of charge and all key vendors are invited to participate at the outset of the project.

Exhibit 1

'Ability to deliver immediate benefit': Assessment criteria

Assessment Category	Assessment Criteria
Offerings	Compliance and regulatory monitoring Risk scoring and prioritization Risk remediation Penetration testing/red teaming Brand monitoring Third-party risk management Threat intelligence Threat hunting Internal Attack Surface Management External Attack Surface Management Application scanning
Delivery Capability	Manual attack surface management capability Automated external attack surface management capability Tooling in support of DevSecOps Use of security accelerators, templates, custom queries
Benefits Achieved	Asset visibility Identification of risks Identification and management of third-party risks Proactive threat mitigation Reporting and dashboards available to clients Reduction in the number of incidents Ability to support the meeting of related regulations Continuous understanding of cyber risk

Exhibit 2

'Ability to meet client future requirements': Assessment criteria

Assessment Category	Assessment Criteria
Service Innovation Culture	Investment in threat intelligence and hunting
	Investment in internal attack surface management
	Investment in external attack surface management
	Investment in automation within ASM
	Investment in scoring and managing risks
	Investment in third-party risk management
	Investment in tooling in support of DevSecOps

For more information on other NelsonHall NEAT evaluations, please contact the NelsonHall relationship manager listed below.

research.nelson-hall.com

Sales Inquiries

NelsonHall will be pleased to discuss how we can bring benefit to your organization. You can contact us via the following relationship manager:

Darrin Grove at darrin.grove@nelson-hall.com