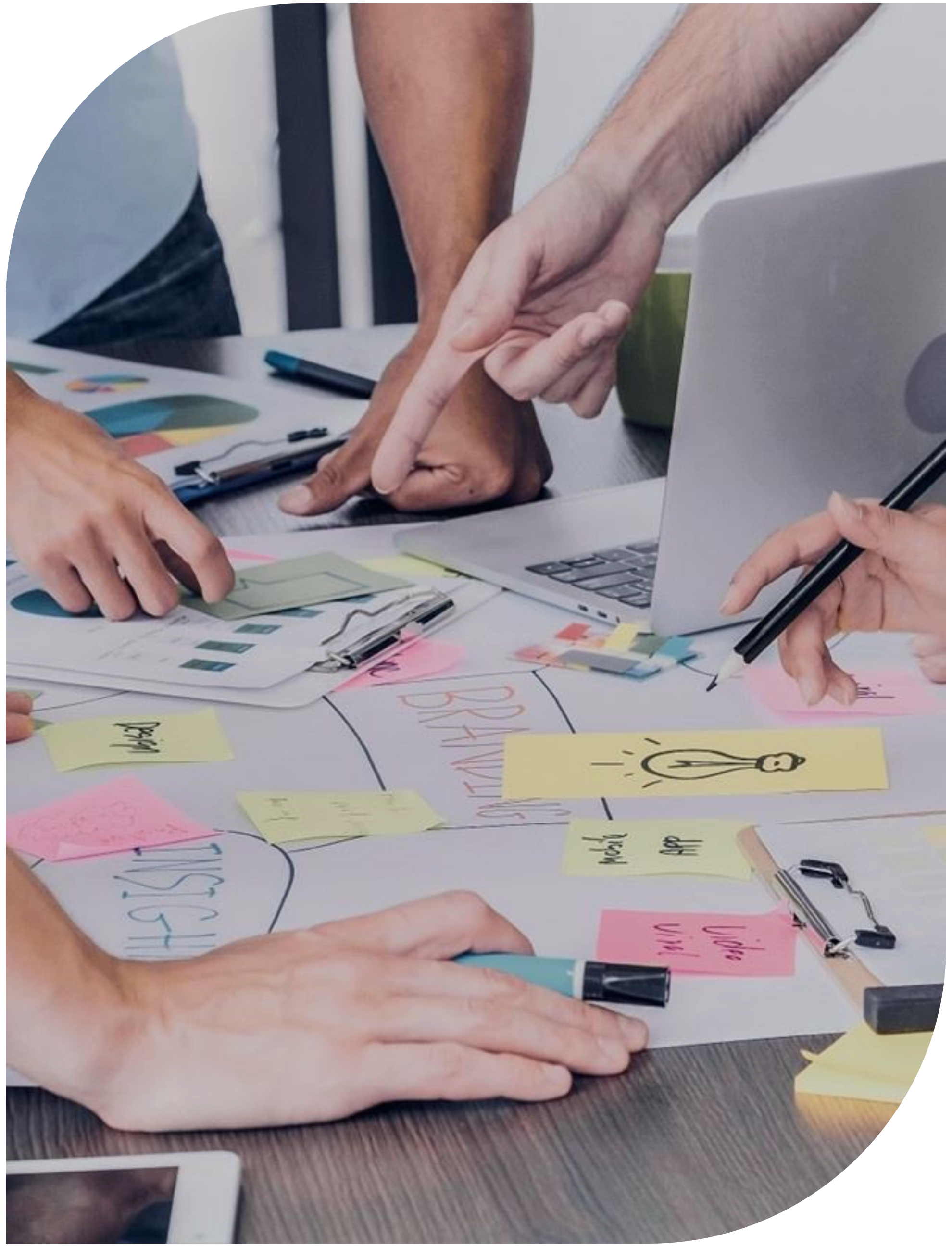
TOTAL ADDRESSABLE MARKET (TAM) FOR DEEP OBSERVABILITY WITH MARKET SHARE OVERVIEW

TO PROVIDE AN IN-DEPTH VIEW OF THE MARKET FOR THE GIGAMON DEEP OBSERVABILITY PRODUCT PORTFOLIO ALONG WITH KEY COMPETITORS AND MARKET TRENDS

PRESENTED TO GIGAMON
TAM REFRESH
JUNE 2025

FROST & SULLIVAN

TABLE OF CONTENTS



RESEARCH OBJECTIVES

Through this research activity, Gigamon aims to understand the deep observability market in depth, **the total addressable market opportunity** along with **key competitors and market share**. F&S worked with Gigamon to identify the key competitors and did an in-depth industry research comprising of primary interviews and assessments to identify market trends, growth rates and insights for end users.

RESEARCH OUTCOME

- To build the **Market Size** for the deep observability market along with a **5 Year forecast (2024-2029)**
- To research the **competitive landscape** for the deep-observability solution
- To provide insights on the **market share of 5 key competitors** (NETSCOUT, Arista Networks, Kentik, Cribl, and Keysight Technologies)
- To provide **market trends and drivers** for the deep observability market

RESEARCH INPUTS

- Primary Research with Key Competitors
- F&S Security Voice of Customer Data
- Secondary Research (Gigamon & other vendor sources)

KEY FINDINGS

MARKET OVERVIEW

- From its roots in traditional observability, the deep observability market has matured into a critical capability for organizations requiring deep packet inspection and enriched network-derived telemetry—particularly among enterprise and government stakeholders aiming to secure, manage, and optimize modern, distributed environments
- The Deep Observability ***market is expected to grow at over 32.5% CAGR*** over the next 4 years from ***`$880 million in 2025 to $2.71 billion in 2029***. This exponential growth underscores the increasing strategic importance of deep observability solutions in sectors such as telecommunications, healthcare and financial services, as organizations seek deeper network visibility and improved security posture.
- ***Gigamon remains the market leader*** in the deep observability market, followed by NETSCOUT, Arista Networks and Keysight Technologies. Cribl has seen exceptional growth through product innovation and partnerships and has increasingly gained market share since 2023. Kentik is a smaller player growing in the SMB segment.
- Enterprise adoption of deep observability is accelerating as organizations confront the limitations of traditional MELT-based monitoring in increasingly complex, hybrid, and zero-trust environments. Key adoption drivers include the need for enriched network-derived telemetry data, packet-level visibility to enhance threat detection, reduce mean time to resolution (MTTR), and compliance support in regulated industries

Note: As part of the study only 5 key competitors of Gigamon in the deep observability market were analyzed

DEEP OBSERVABILITY PRODUCT OVERVIEW

DEEP OBSERVABILITY: PRODUCT OVERVIEW AND EVOLUTION

The word “Deep” in Deep Observability refers to going beyond the traditional MELT data for analysis and insights of network packets. This product today has evolved from the broader observability market and has created a definitive need for large enterprises to adopt.

takes observability further by integrating network-derived intelligence with metric, log, event, and trace data

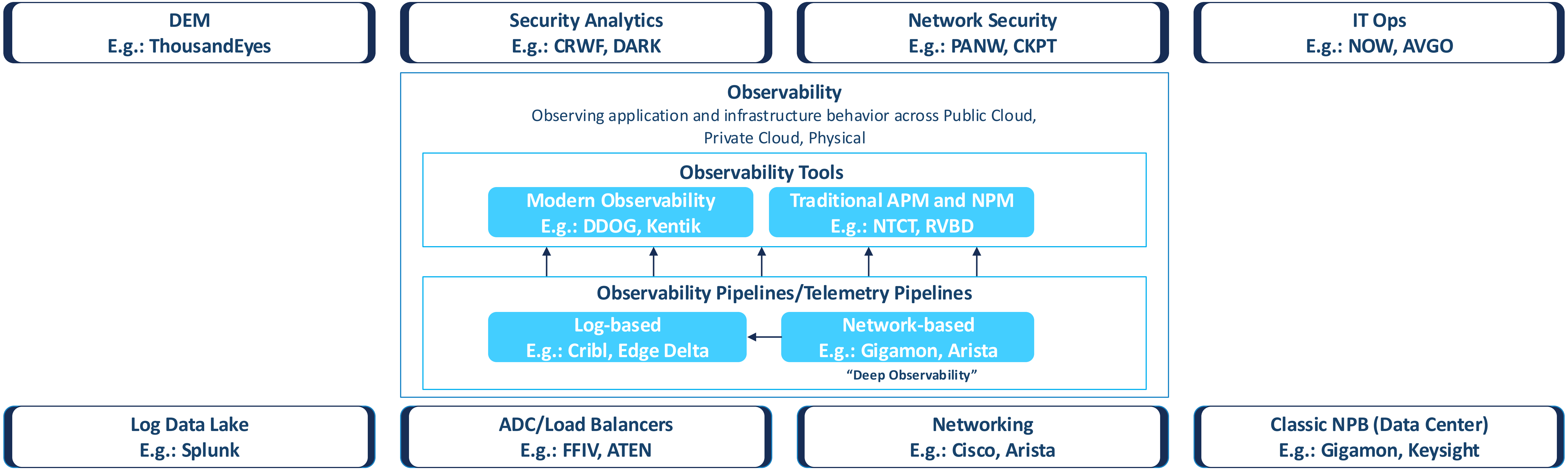
	Monitoring	Observability	Deep Observability
Definition	Basic alert system	Alert system with root cause analysis	Comprehensive intelligence system with insights across hybrid cloud infrastructure
Area of Focus	Data collection for spot-checking systems	Contextual analysis of collected data	Holistic understanding of system behavior leveraging network-derived telemetry
Traceability	Real-time data observation	Historical data analysis	Multi-source data analysis (going beyond metrics, events, logs, traces) to understand root causes and predict trends
View	Single-plane, rule-based alerts	Contextual mapping of collected data	Multi-dimensional view integrating network-derived intelligence to identify and address blind spots
Understanding	Understanding the state of the system	Actionable insights from monitoring data	Proactive risk mitigation, performance optimization, and user experience enhancement
Depth	Surface-level system status	Deep health analysis of the system and its components	Comprehensive visibility into network, security, and computing traffic across distributed environments
Sustainability	Continuous monitoring with periodic adjustments	Sustainable approach to monitoring the system over time	Ongoing effectiveness by maintaining multi-vendor support and interoperability with observability platform data lakes, enabling continuous monitoring and analysis over time
Summary	Tells you the what	Tells you the why	Tells you what, why, what to do now

Source: Gigamon, Frost and Sullivan analysis

DEEP OBSERVABILITY: PRODUCT DEFINITION AND MARKET CONTEXT

Observability which refers to inspection of telemetry and log data covering applications and infrastructure behaviour across public and private cloud, physical, on-premise and virtual and container infrastructure runs on ***observability pipeline solutions*** feeding network and log-based telemetry data to ***observability solutions.*** This provides a unified view into the health and performance of each layer of an organization's technology stack. The observability pipeline solutions which have the capability to deliver ***network-based telemetry**** from multiple networks such as public and private cloud, data centre, and colocation deployments, going beyond traditional MELT data and enhancing the organization's security posture can be classified as ***Deep Observability*** solutions. This is crucial because It eliminates blind spots by providing real-time network telemetry into lateral East-West and encrypted traffic to detect threats and performance anomalies, enabling organizations to deliver defense in depth and establish a solid foundation for Zero Trust framework implementation.

There are different products that sit alongside Observability solutions which analyse network and application data to enhance an organization's security posture. These are monitoring solutions e.g. Digital Experience Monitoring (DEM), alert and log management solutions e.g. IT Ops, Metrics and Event Management solutions e.g. Data Lakes, SIEMs, Security Analytics and traffic brokering solutions e.g. load balancers. But none of these solutions have the capability to aggregate the entire network's telemetry data independently and provide deep observability capabilities.



DEM
E.g.: ThousandEyes

Security Analytics
E.g.: CRWF, DARK

Network Security
E.g.: PANW, CKPT

IT Ops
E.g.: NOW, AVGO

Observability
Observing application and infrastructure behavior across Public Cloud, Private Cloud, Physical

Observability Tools

Modern Observability
E.g.: DDOG, Kentik

Traditional APM and NPM
E.g.: NTCT, RVBD

Observability Pipelines/Telemetry Pipelines

Log-based
E.g.: Cribl, Edge Delta

Network-based
E.g.: Gigamon, Arista
"Deep Observability"

Log Data Lake
E.g.: Splunk

ADC/Load Balancers
E.g.: FFIV, ATEN

Networking
E.g.: Cisco, Arista

Classic NPB (Data Center)
E.g.: Gigamon, Keysight

*Network-derived telemetry includes packet captures, flow records, SNMP traps, application metadata, and more

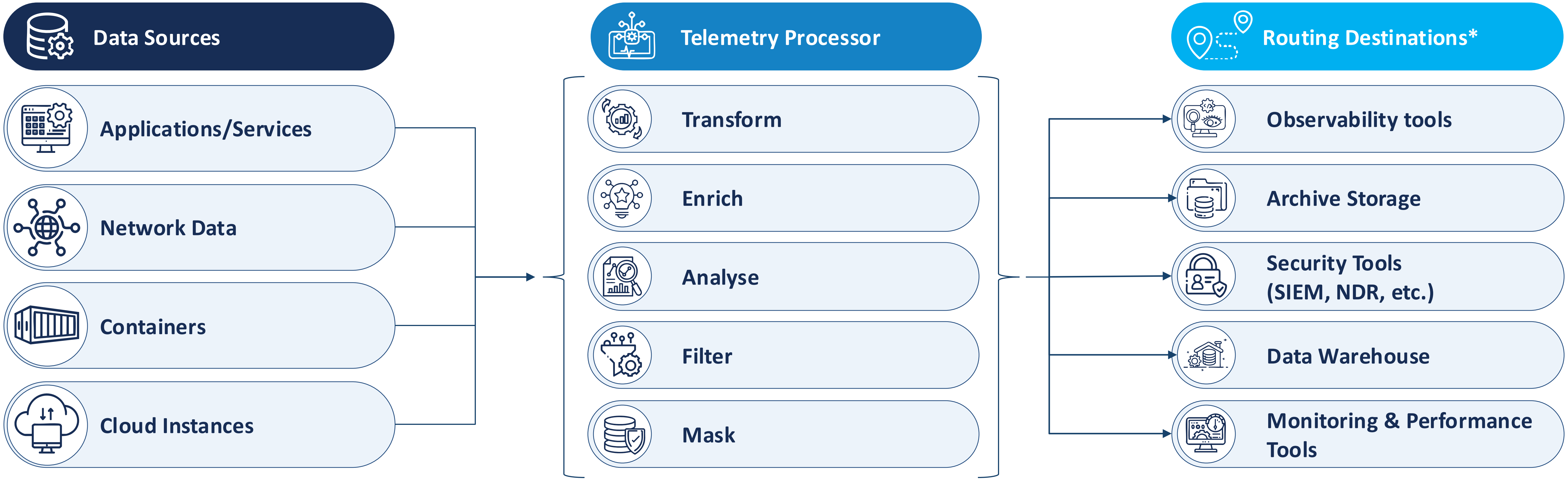
Source: Gigamon, Frost and Sullivan analysis

THE IMPORTANCE OF OBSERVABILITY/TELEMETRY PIPELINES

Modern telemetry pipelines are evolving from a "collect everything and analyze later" model to a smarter, ingestion-time processing approach. This evolution is critical to overcome today's core data challenges: 1. **Volume:** massive data from apps, cloud, and infrastructure 2. **Velocity:** the need to analyze traffic and telemetry in real-time and 3. **Complexity:** disparate data formats, sources, and silos. The right telemetry pipeline strengthens deep observability by enabling:

- **Context Preservation** : Enriches data in real-time (e.g., with user, app, or threat context), preserving relationships lost in batch methods
- **Intelligent Filtering**: Drops noise while prioritizing what matters – ensuring critical signals are retained, not missed
- **Cross-Domain Correlation**: Correlates insights across network, app, and cloud layers, enabling faster investigation and deeper context

Network-derived telemetry delivers **agentless, full-fidelity traffic visibility** at ingestion, enabling smarter security and performance decisions without system disruption.



*not exhaustive

FROST & SULLIVAN

Source: Frost and Sullivan analysis

TELEMETRY PIPELINE AND DEEP OBSERVABILITY: MAJOR USE CASES IN THE ENTERPRISE

Deep Observability solutions help an organization to gather network telemetry across on-premise and cloud, decrypt inline and out of band network packets and efficiently deliver traffic to solutions based on layer 4-7 application intelligence and metadata derived from packets, flows, and metadata, going beyond NetFlow. This creates a significant edge for an organization to gain visibility and confidence in its security posture.

The top 5 use cases for deep observability adoption are:

Improving Security Posture

Visibility into encrypted traffic is crucial for detecting threats hidden in encrypted data. This capability helps organizations to identify and respond to malware potentially turning into ransomware through lateral movement and data exfiltration that would otherwise remain hidden. It also helps route the right data to SIEM and other analytics solutions for enhanced threat detection and response..

Zero-Trust Architecture Implementation

Deep observability solutions can help organizations to enforce strict access controls and continuous monitoring, thereby reducing the attack surface and improving the overall security posture to provide a solid foundation for ZT architecture implementation.

Operational Efficiency and Cost Reduction

Reducing duplicate, invaluable data at ingress and egress, deep observability solutions can optimise the use of infrastructure and greatly reduce operational costs and increase efficiency

Improving Compliance and Cloud Governance

Deep observability solutions can provide complete visibility for maintaining governance over the data and network activities across an organization's diverse multi-cloud environments

Network and Application Performance Management

Deep observability solutions enable IT teams to monitor and analyse network traffic in real-time and help predict network and performance issues even before they occur thereby maintaining network performance and reducing downtime.

MARKET SIZE: ENTERPRISE- GLOBAL, FEDERAL GOVERNMENT (US) (2023-2028)

DEEP OBSERVABILITY MARKET SIZE

Methodology for deriving the market size, inclusions, exclusions and the product boundary.

Frost and Sullivan conducted a top-down analysis of the Deep Observability Market by estimating the total number of large enterprises globally, adoption of the deep observability solution and the average spending of an enterprise on the solution. This data was gathered by Frost and Sullivan research as well as through primary interviews with market participants including Gigamon. The data was then used to model the current market size (2025) and project growth rates. Along with Global Enterprise, this study also estimated the size of the market for US Federal government. US Fed agencies have the highest adoption of the deep observability solution, globally among governments largely owing to regulations around stricter Zero Trust implementation and improving the overall visibility and security of its on-premise and cloud networks. (US Fed agencies follow NIST guidelines for Zero Trust Architecture which emphasizes the importance of deep observability for identifying threats and providing necessary data for network security.)

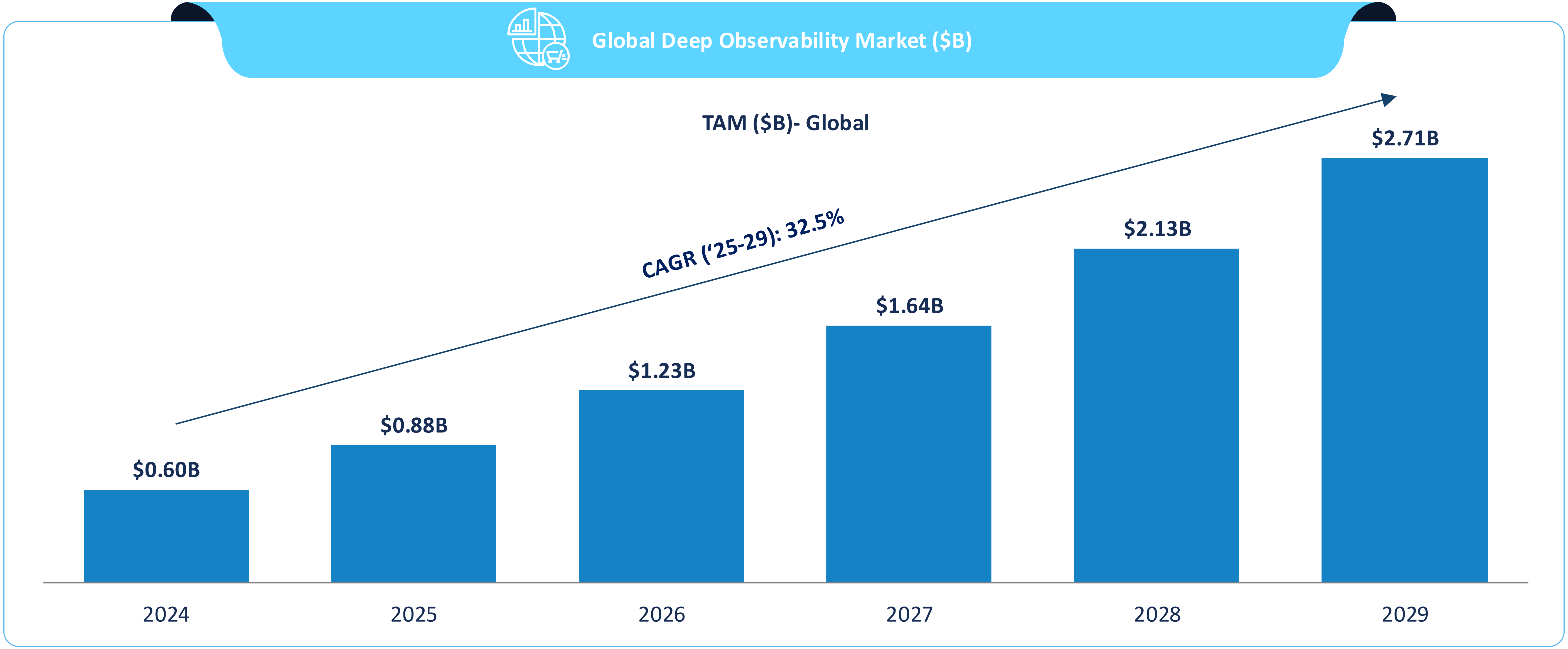
Large Enterprises defined as enterprises with more than 5000 FTEs across industry verticals are considered addressable for this study. All major US Federal government agencies are considered addressable for this study.

All major players in the deep-observability market reported a healthy segmental revenue growth of 35%-140% YoY between 2023-2024. Frost and Sullivan based on its research factored in the increase in adoption of the product along with the rise of average spending (linked to inflation data) and estimated the overall market growth rate through 2029.

For market sizing, Frost and Sullivan considered only those vendors in the deep observability space which meet with the product definition as illustrated in slide 6. Only those products are included which have the capability to gather (tap) network, security and cloud traffic and have the ability of inspect and analyze the traffic by going beyond Metrics, Events, Logs and Traces (MELT) data. The spending for deep observability consists of software and associated hardware. Hardware-based probes, agents, and taps are excluded from the market size.

DEEP OBSERVABILITY MARKET SIZE

The global deep observability market is projected to expand from $0.88 billion in 2025 to $2.71 billion by 2029, experiencing a remarkable compounded annual growth rate (CAGR) of 32.5%. It is one of the fastest growing product segments in enterprise security owing to its crucial importance for enterprises to have full control and visibility into all data in motion and to ensure successful Zero Trust architecture implementations.



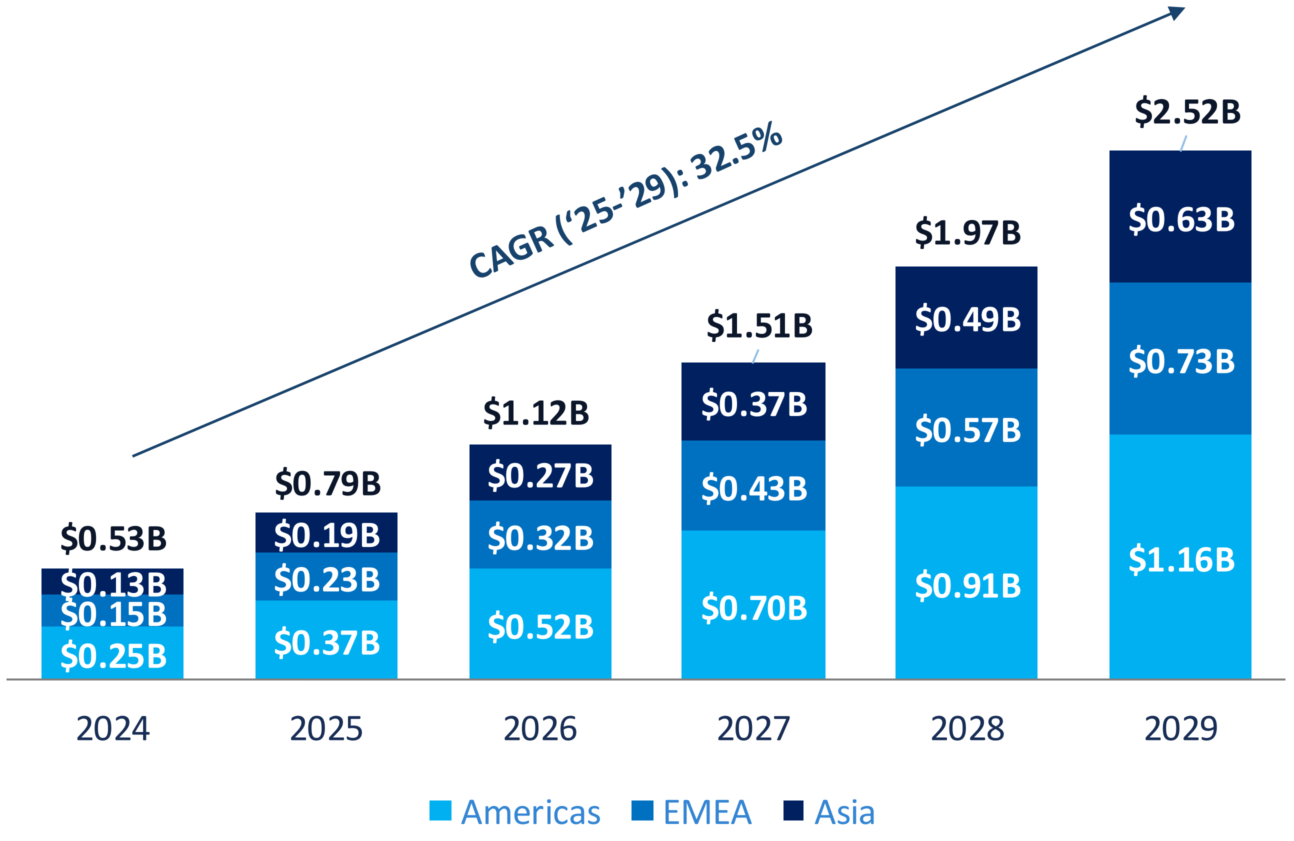
Source: Frost and Sullivan analysis

TAM FORECAST

The global deep observability market is being shaped by strong adoption among large enterprises (5,000+ employees), with the Americas region leading this growth. Key industry sectors fueling demand include telecommunications service providers (CSPs), banking and financial institutions, and government entities—each dealing with highly complex network environments. While the US Federal sector remains a major early adopter, enterprise demand is expected to outpace it over the forecast period, driven by expanding use cases and broader global deployment.

Global Enterprise TAM ($B)

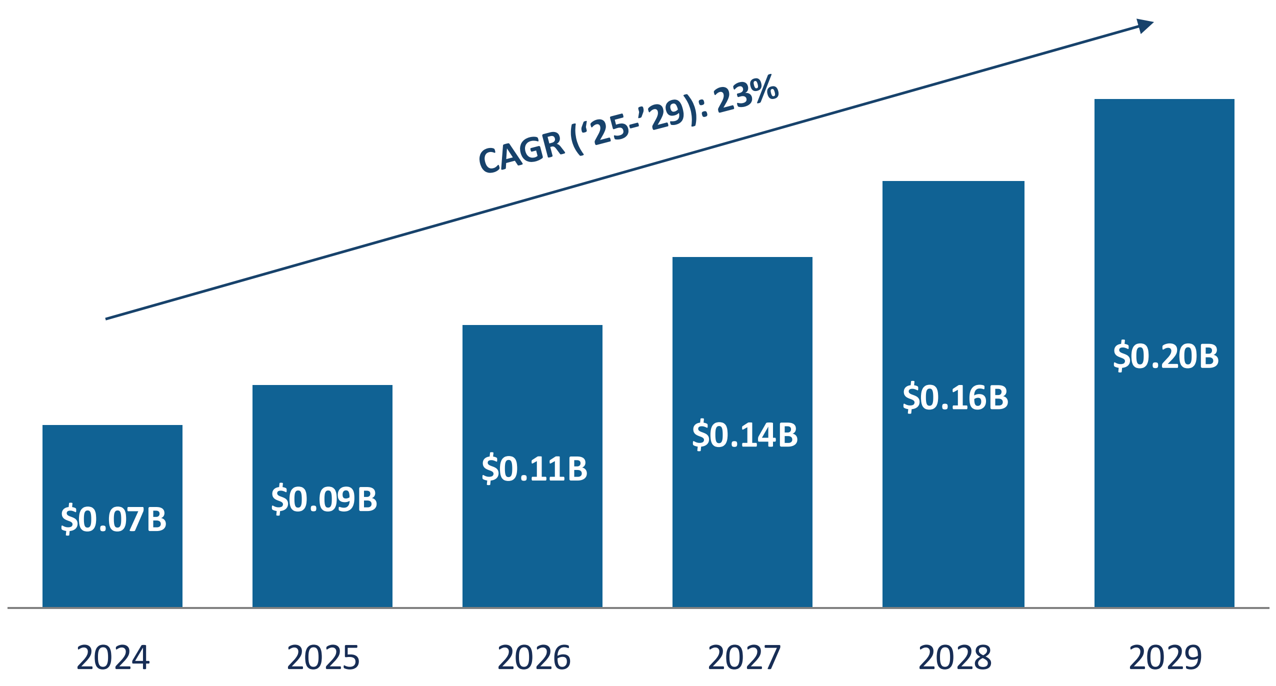
The global enterprise market is expected to grow from `$800 million in 2025 to `$2.5 billion in 2029 with a CAGR of 32.5%.



USA Federal Government TAM ($B)

The US Fed market is expected to grow from $90 million in 2025 to $200 million in 2029 with a CAGR of 23%.

Federal Agencies (USA)



FROST & SULLIVAN

Source: Frost and Sullivan analysis

MARKET DRIVERS AND GROWTH VECTORS

MARKET DRIVERS

Key Findings on Factors that Drive Deep Observability Adoption

Increasing need of Comprehensive Network Traffic Insights

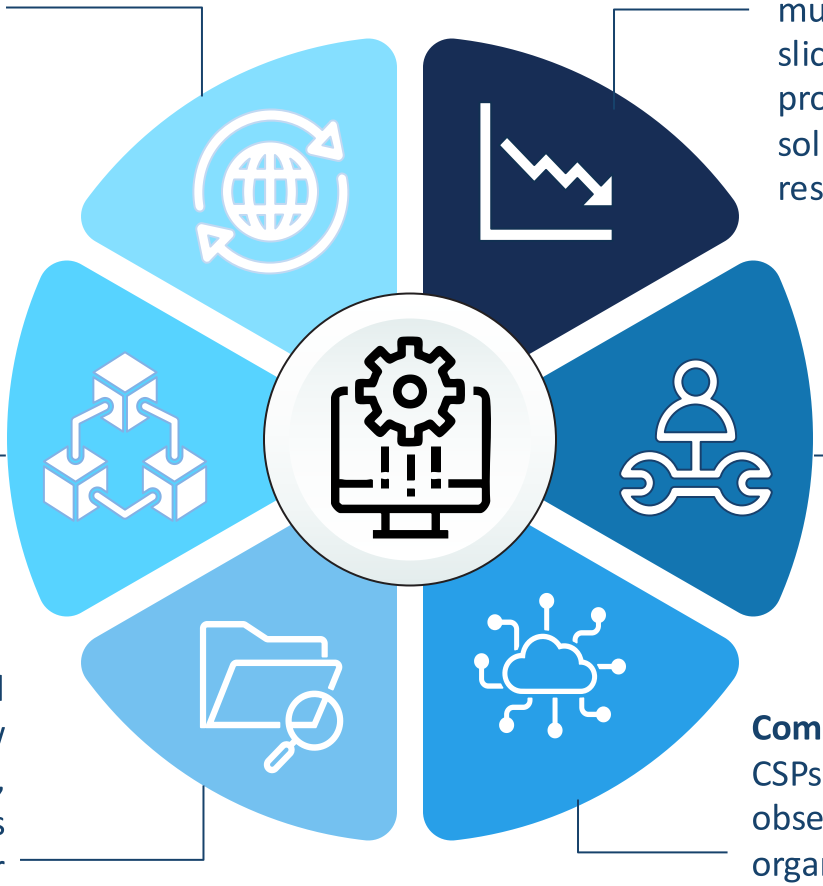
Deep observability solutions offer the capability to capture traffic from any VM, container, or physical network infrastructure. This can give organizations complete visibility not just into the North-South traffic but also East-West encrypted and container traffic across hybrid cloud environments, ensuring that visibility is maintained as cloud deployments scale.

Empowering Security Analysts through DPI

Managing a multi-vendor architecture can be complex and often results in limited visibility among organizations. Deep Packet Inspection (DPI) provides the ability to inspect and analyze diverse network traffic in real time, provide better contextualization with data feeding into analytics solutions such as SIEM tools thereby empowering analysts to make stronger correlations and risk assessments.

Increasing need to detect Advanced Threats

AI-driven threats are evolving faster than traditional detection systems can keep up. Attackers are now leveraging machine learning to craft more evasive malware, automate reconnaissance, and manipulate traffic patterns in ways that are difficult to detect with signature-based or MELT-reliant tools creating new visibility gaps. Enterprises need deep observability solutions to detect and respond to advanced, dynamic threats.



The need to reduce Operational IT Costs

Cost reduction and consolidation will continue to be a key focus of organizational decision makers. Deep observability solutions offer multiple capabilities such as filtering, packet de-duplication, flow slicing, load balancing, and NetFlow generation can streamline data processing, enhance the efficiency of security and monitoring solutions, and enable managing larger volumes of traffic with fewer resources, ultimately reducing costs.

Increasing Implementation of Zero-Trust Architecture

Achieving a true Zero-Trust security model is difficult without complete visibility into all packets and data streams across cloud or hybrid networks. Deep observability technologies provide the necessary insight into lateral East-West traffic, encrypted data, and container traffic within an organization's IT systems driving secure zero trust implementations.

Complement Cloud Service Providers (CSPs)' Monitoring Capabilities

CSPs offer monitoring solutions, but they often lack comprehensive observability for hybrid and multi-cloud setups. This limitation forces organizations to use separate, non-integrated interfaces, leading to inefficiencies, especially in monitoring East-West traffic between public cloud instances. Deep observability solutions address this gap.

Source: Frost and Sullivan analysis

OVERVIEW OF THE DEEP OBSERVABILITY COMPETITOR LANDSCAPE

OBSERVABILITY MARKET LANDSCAPE

Monitoring and Observability

- The broader Observability market has seen the emergence of many players creating their own niche in the market. Despite the many players in the market the core need of **accurately pinpointing issues and optimizing performance in modern, complex distributed IT environments and hybrid cloud infrastructure** remains for enterprises
- Major observability vendors in the market today include Datadog, Dynatrace, Elastic, New Relic, and Honeycomb, Edge Delta among others that offer unified platforms that integrate metrics, logs, events, traces, and other telemetry data to provide comprehensive visibility and automated insights.
- Grafana Labs, the creator of the open-source data visualization platform Grafana, has also made significant strides in the observability market with its Grafana Cloud and open-source offerings
- Other vendors like **Darktrace and Palo Alto Networks specialize network analytics and advanced threat detection** using AI and machine learning to enhance cybersecurity. ExtraHop and Arista Networks focus on providing scalable, flexible solutions that integrate seamlessly with existing IT infrastructures.
- Large IT vendors also offer observability such as IBM Instana Observability, Microsoft Azure Monitoring, Amazon CloudWatch, and Splunk Observability Cloud. However, these are quite limited in features often focusing on one aspect of an organization's IT environment (e.g., application monitoring)
- With this complex and broad ecosystem, ***observability pipeline*** products emerged to further enhance observability solutions with accurate network-derived telemetry data. **Gigamon, Ixia (acquired by Keysight Technologies), NETSCOUT, Arista Networks, APCON, Cisco, and Broadcom** offer products in this segment. More recently, vendors like **Kentik and Cribl** have emerged with superior data lake interoperability and analytics offerings. Deep observability vendors offer deep packet inspection, real-time data processing, and extensive metadata analysis across the hybrid cloud infrastructure for comprehensive monitoring and security. These vendors focus on managing complex IT infrastructures and ensuring seamless data flow across hybrid and multi-cloud environments.

Source: Frost and Sullivan analysis

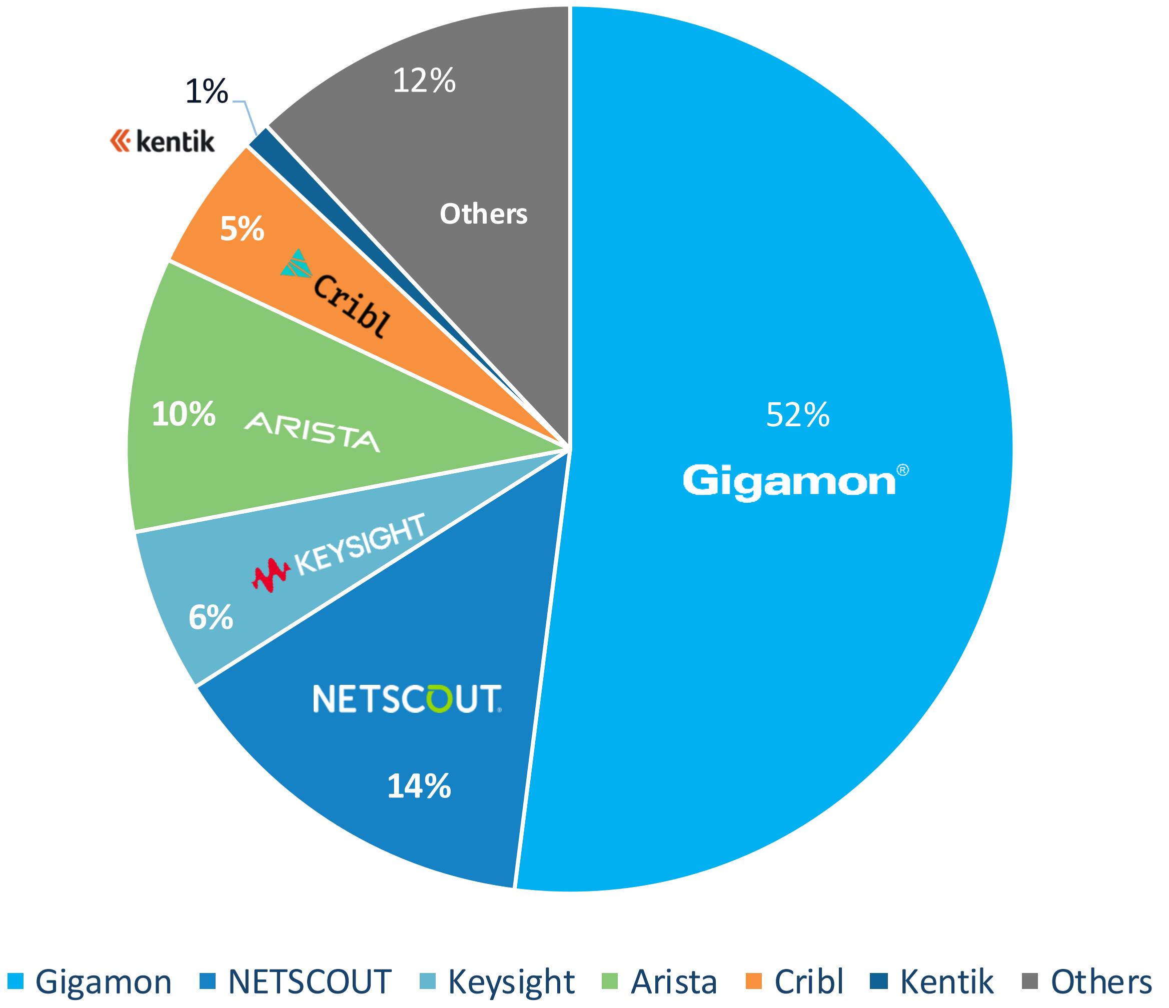
KEY DEEP OBSERVABILITY VENDOR OVERVIEW

	Vendor Overview	Observability Offering
Gigamon®	Gigamon is the leader in the deep observability market. It is the leading provider of deep observability solutions, empowering organizations to enhance performance, security, and user experience.	It offers a deep observability pipeline that efficiently delivers actionable network-derived intelligence and insights to cloud, security, and observability tools. It goes beyond traditional security and observability approaches that rely exclusively on metrics, events, logs, and traces (MELT) data.
NETSCOUT	NetScout has a strong Communication Service Providers (CSPs) business with its observability offering. It is the 2nd biggest player in the deep observability domain with a strong market offering across 3000+ customers.	Launched in 2023, NetScout's "Visibility Without Borders" platform approach to network visibility incorporates many of their existing products. NetScout intends to focus further on providing a flexible platform for visibility across any cloud, network, enterprise, application and service.
KEYSIGHT	Keysight is a leading test and measurement provider with a complete portfolio of test, visibility, and security solutions. The company's acquisition of Ixia in 2017 established it among the leading players in network visibility and observability space.	It defines network visibility as monitoring all the traffic and data flowing across a network at any given time. It has a suite of network visibility products and solutions that aims to deliver rich data about network traffic, applications, and users across any networking environment.
ARISTA	Arista is a leader in high-speed data center Ethernet switching markets, particularly for 10 GbE and above. Due to its strength in networking, Arista has expanded into the network observability market and has found a strong product adjacency.	Arista addresses the market through three tiers offering Network Packet Brokers (NPB), Network Detection and Response (NDR) solutions, and its recently launched CloudVision Universal Network Observability (CV UNO), offering a multi-domain network observability platform
Cribl	Cribl positions itself as the "Data Engine for IT and Security teams". Its suite of products are all built on a unified data processing engine: Cribl Stream for observability pipeline, Cribl Edge an intelligent, vendor-neutral agent, Cribl search-in-place solution, and Cribl data lake. It is an emerging vendor in the space with limited market share in large enterprises.	Cribl Stream is a robust, vendor-agnostic streams processing engine focused on centralized parsing and processing of data. It has a strong observability pipeline capabilities build on collecting log data. It can route, reduce, reformat, enrich, or otherwise structure data in flight then send it to any destination.
kentik.	Kentik positions itself as a leading network observability company. Amongst the competitors studied as part of this report, Kentik has the lowest revenues and market share predominantly because of its small team and focus enterprise segments. It is emerging from Network monitoring towards observability	Its Network Observability Platform transforms network telemetry, including VPC logs, into actionable insights. Through this platform, Kentik securely gathers and organizes telemetry data, empowering customers to explore and analyze it through pre-defined and custom queries.

Source: Frost and Sullivan analysis

KEY PLAYERS IN DEEP OBSERVABILITY

Deep Observability, Revenue Market Share of Top Participants, 2024



Others include Cisco, APCON, Edge Delta, Broadcom etc.

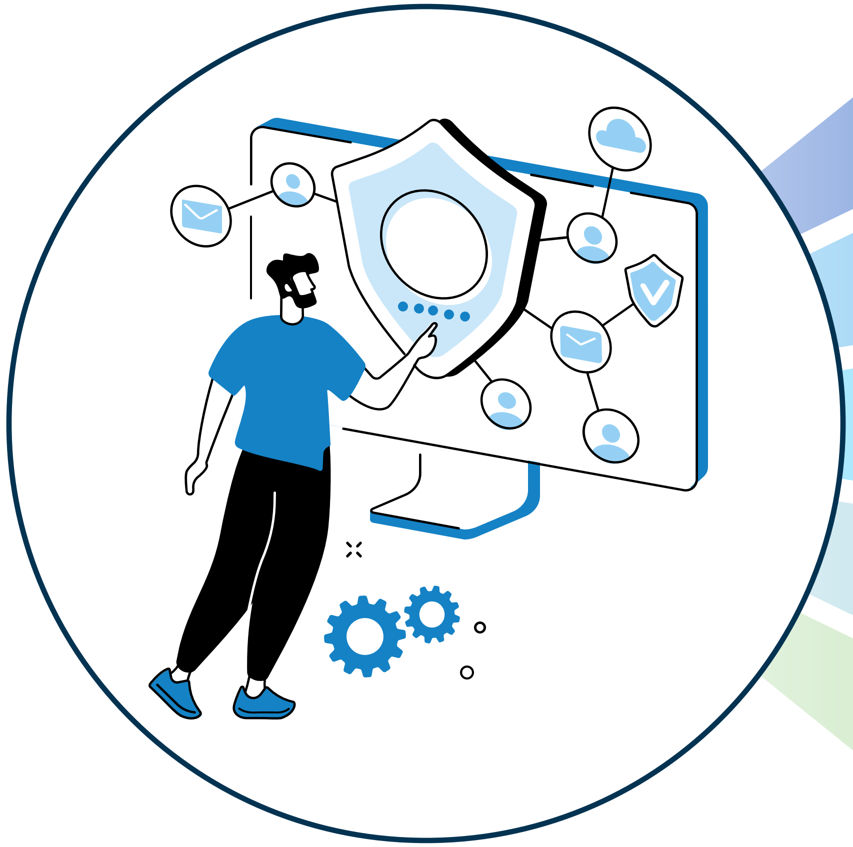
Commentary

- **Gigamon** has the most comprehensive deep observability pipeline and the highest revenues in the industry attributable to its Deep Observability Pipeline. It has more than 4000+ customers globally with strong revenue base enabling it to capture a substantial 52% market share.
- **NetScout** is the 2nd biggest player with estimated 14% market share with its “Visibility Without Borders” platform, enhancing visibility across cloud, network, enterprise applications, and services. This builds on their well-established reputation in wireless network monitoring and service assurance, particularly for Communication Service Providers (CSPs).
- Historically, **Keysight** has been a market leader in measurement instrumentation and software. Keysight established itself as a player in the deep observability market by acquiring Ixia in 2017. Keysight has a vast global clientele, presenting numerous up-sell opportunities for its observability solutions, especially as customers upgrade their existing infrastructure. It is estimated to have about 6% of the overall market share in 2024.
- **Arista Networks** market share is predominantly due to its Big Switch acquisition in 2020. Arista Networks has shown strong revenue growth in 2023-2024 and has been able to increase its overall market share in the domain with its CV-UNO product line.
- Additionally, start-ups like **Cribl and Kentik** are making inroads into the deep observability market with their targeted solutions, aiming to capture a share of this growing sector. Cribl has shown tremendous growth and product potential in the last year thereby increasing its market share across customer segments. Kentik is a smaller player focused on the SMB segment.

Source: Frost and Sullivan analysis

INSIGHTS AND GUIDANCE FOR END USERS

WHY ADOPT DEEP OBSERVABILITY?



01 REAL-TIME DATA PROCESSING AND ANALYSIS

02 UNCOVERING BLIND SPOTS

03 ADVANCED DATA INSPECTION AND GATHERING

04 CONCRETE ROI

05 ACHIEVE REGULATORY COMPLIANCE

DEEP OBSERVABILITY IN THE AI ERA

Key insights from the Gigamon 2025 Hybrid Cloud Survey:

- Global AI investment is projected to surpass $300B in 2025 and reach $750B by 2028*
- 1 in 3 organizations say AI has doubled network data volumes in two years
- 47% report more LLM-targeted attacks; 58% face rising AI-powered threats
- 70% of IT leaders see public cloud as the highest security risk - yet it’s the top choice for AI workloads

Frost & Sullivan research indicates that AI and AI-enabled applications are expected to drive a surge in network traffic. This adds to the complexity of network management and security where deep observability becomes essential. The right deep observability solution prevents teams from flying blind and delivers real-time, surgical insight into AI-generated risk. By transforming raw network traffic into context-rich intelligence, organizations gain 360° visibility to secure and optimize hybrid and AI workloads.

1

From Network Data to Business Intelligence through AI-enhanced Metadata

Gigamon transforms network-derived telemetry into enriched, context-aware intelligence that bridges the gap between infrastructure and application layers. By correlating telemetry with application metadata and injecting real-time context, Gigamon enables complete visibility across public cloud, private data centers, and edge. This enriched metadata foundation powers AI-driven analytics, helping teams detect anomalies faster, optimize performance, and align security with business outcomes.

2

Automated Compliance and Zero-Trust Through Enriched Intelligence

Gigamon enables AI-powered threat detection, continuous compliance monitoring, and identity-aware analytics to accelerate Zero Trust outcomes. By analyzing DNS, ports, and traffic patterns at scale, Gigamon reveals malicious behavior like spoofing, lateral movement, and unauthorized access. Metadata enriched with user identity and behavioral context ensures organizations can verify trust continuously and respond in real-time - even across distributed hybrid cloud environments.

3

AI + Metadata + Observability = Autonomous Security

Frost & Sullivan research indicates a solid evolution pattern in Observability:

- Wave 1 (2024-2026) : Enriched metadata for context aware monitoring
- Wave 2 (2026-2028) : AI- native tools shift the landscape from "detect and respond" to "predict and prevent“
- Wave 3 (2028 -) : Autonomous, self-healing security infrastructure

WHAT TO LOOK FOR IN AN OBSERVABILITY/TELEMETRY PIPELINE VENDOR

Advanced Data Inspection Capabilities 01

Organizations must check if the deep observability vendor offers solutions capable of inspecting and gathering network, security, and computing traffic and even encrypted data by extracting event metadata from packets or computing infrastructure. This feature goes beyond event-based logging, providing a richer, more detailed data set.

Multi-Vendor Support 02

It is imperative that organizations choose a vendor that can support their multi-vendor systems. This interoperability allows seamless integration with a variety of existing solutions and platforms, preventing vendor lock-in and ensuring that organizations can still leverage their previous IT investments while enhancing their observability capabilities.

Support for Multi-Cloud Strategy 03

Organizations must choose a deep observability vendor that can support various IT systems whether on cloud, on-prem, or hybrid environments. This should also cover public cloud, private data centers, and colocation deployments as well. This feature is crucial for organizations with diverse and complex infrastructures, enabling comprehensive visibility across all operational domains.

Interoperability with Data Lakes 04

Organizations look for a deep observability solution which can integrate with various security data lakes. This interoperability feature is crucial for consolidating and analyzing large volumes of telemetry data from multiple sources across the organization's environment.

Comprehensive Security Features to tackle AI threats 05

The vendor should offer robust security features that go beyond basic monitoring. This includes the ability to detect anomalies, perform deep packet inspection, and provide insights into encrypted traffic. AI-powered causal mapping that can accelerate Mean time to detect (MTTD) and respond (MTTR).

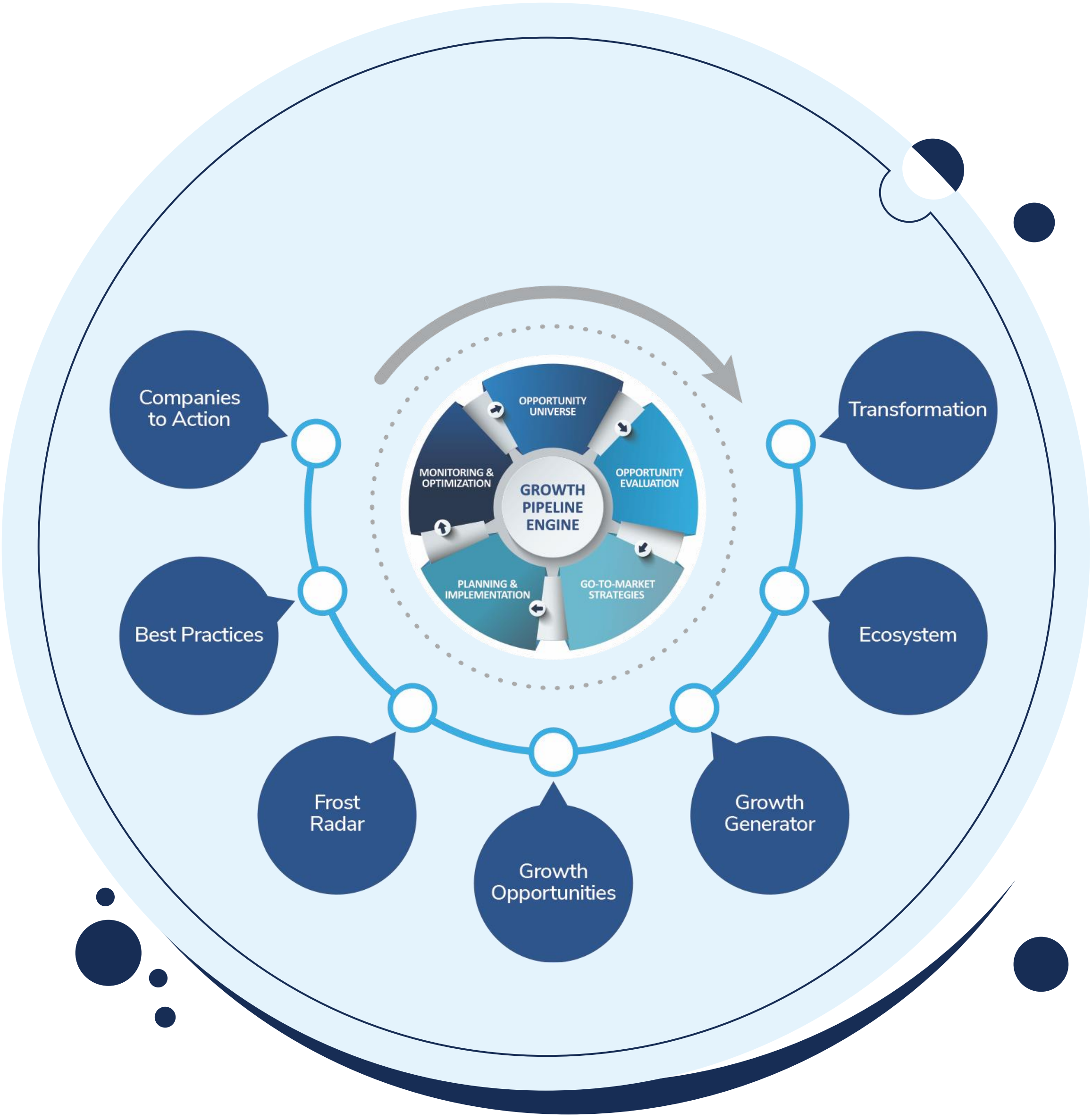
Data Rich User Interface 05

Choose a deep observability solution that has a data rich interface and comprehensive reporting capabilities. An intuitive dashboard that allows for easy visualization of data on a single pane of glass that enables the IT teams get the most out of the observability solution without increasing the skills gap in the organization

Source: Frost and Sullivan analysis

TRANSFORMATIONAL GROWTH JOURNEY

"Powered by the Growth Pipeline Engine"



Vinay Biradar

Associate Director, Cybersecurity Advisory

vinay.biradar@frost.com

FROST & SULLIVAN