

# DEFINING THE TAM FOR THE DEEP OBSERVABILITY PRODUCT LINE ALONG WITH COMPETITOR ANALYSIS

*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  
June 2024



# CONTENTS

Executive Summary

3

Deep Observability Product Overview

5

Deep Observability Market Size, Enterprise- Global, Federal Government (US) (2023-2028)

9

Deep Observability Market Drivers and Growth Vectors

13

Key Market Players and Market Share of Identified Competitors

15

Insights and Guidance for End-Users

19





# RESEARCH OBJECTIVES

Through this research activity, Gigamon aims to understand the deep observability market in depth and the total market size along with key competitor's market share. F&S worked with Gigamon to identify the key competitors and did 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 **Total Addressable Market (TAM)** for the deep observability solution along with a **5-year forecast (2023-2028)**
- To research the **competitive landscape** for the deep observability solution
- To provide insights on the **market share of 5 key named competitors**
- 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



# KEY FINDINGS

## MARKET OVERVIEW

- The Deep Observability Market has emerged from the broader Observability market and has carved out a definitive need in large enterprises and government agencies seeking real time visibility into network traffic, going beyond traditional approaches that rely on metrics, events, logs and traces-based (MELT) data.
- The Deep Observability **market is expected to grow at close to 40% CAGR** in the next 4 years from **\$570 million in 2024 to \$2.1 billion in 2028**. This staggering growth rate is testament to the increasing awareness and adoption of the product in large enterprises, led by Communication Service Providers (CSPs) and Banking Financial Services Insurance (BFSI) verticals. The other major growth driver is the spending by Government agencies. The US Federal government is a leader globally in terms of adoption and spending on Deep Observability.
- **Gigamon is the market leader** in the deep observability market, followed by NETSCOUT, Keysight Technologies and Arista Networks (acquired Big Switch). Kentik and Cribl are new age players but have limited capabilities and presence in large enterprises.
- The key driver for the product adoption in enterprises is to improve the overall security posture of the organization by gaining better visibility into encrypted traffic of not only north-south but also lateral traffic across their hybrid cloud infrastructure, enabling them to more rapidly identify and respond to advanced threats.







# Deep Observability Product Overview



# DEEP OBSERVABILITY: PRODUCT OVERVIEW AND EVOLUTION

The word “Deep” in Deep Observability refers to going beyond traditional MELT-data approaches 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 and government agencies to adopt.

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

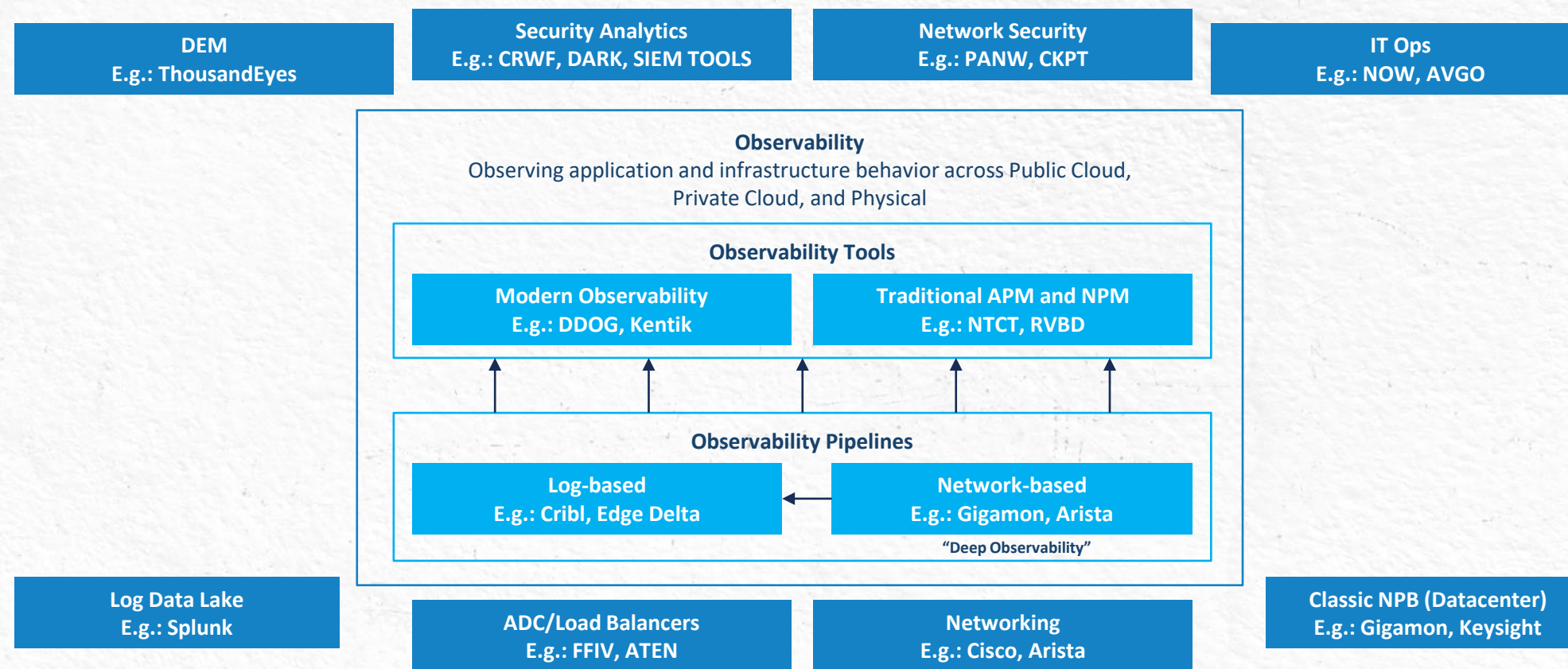
	Monitoring	Observability	Deep Observability
Definition	Basic alert system	Alert system with root cause analysis	Comprehensive intelligence system with insights across hybrid cloud infrastructure
Area of Focus	Data collection for spot-checking systems	Contextual analysis of collected data	Leveraging network-derived intelligence to gain a holistic understanding of app and user behavior and suspicious activities
Traceability	Real-time data observation	Historical data analysis	Intelligence derived from all sources: cloud, container, and encrypted traffic together with MELT to understand root causes and predict trends
View	Single-plane, rule-based alerts	Contextual mapping of collected data	Multi-dimensional view integrating network 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 diverse 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



# DEEP OBSERVABILITY: PRODUCT DEFINITION AND MARKET CONTEXT

Observability, which refers to inspection of telemetry and log data covering applications and infrastructure behavior across public and private cloud, physical and on-premises infrastructure runs on **observability pipeline solutions** feeding network and log-based telemetry data to **observability and SIEM tools**. 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, datacenters, and colocation deployments by 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.



\*Network telemetry includes packet capture, flow records, enhanced network-derived metadata



# OBSERVABILITY PIPELINE AND DEEP OBSERVABILITY: MAJOR USE CASES IN THE ENTERPRISE AND GOVERNMENT AGENCIES

Deep Observability solutions help an organization to gather network telemetry across hybrid cloud infrastructure, 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 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:

- 1. 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 previously undetected malware before it turns into ransomware through lateral movement and data exfiltration. It also helps route the right data to SIEM and other analytics solutions for enhanced threat detection and response.
- 2. 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, providing a solid foundation for ZT architecture implementation.
- 3. Operational Efficiency and Cost Reduction:** Reducing duplicate, invaluable data at ingress and egress, deep observability solutions can optimize the use of infrastructure and greatly reduce operational costs and increase efficiency.
- 4. 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 hybrid cloud infrastructure.
- 5. 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 before they occur, thereby maintaining network and application performance and reducing downtime.





**MARKET SIZE:  
Enterprise- Global,  
Federal Government  
(US) (2023-2028)**



# DEEP OBSERVABILITY MARKET SIZE

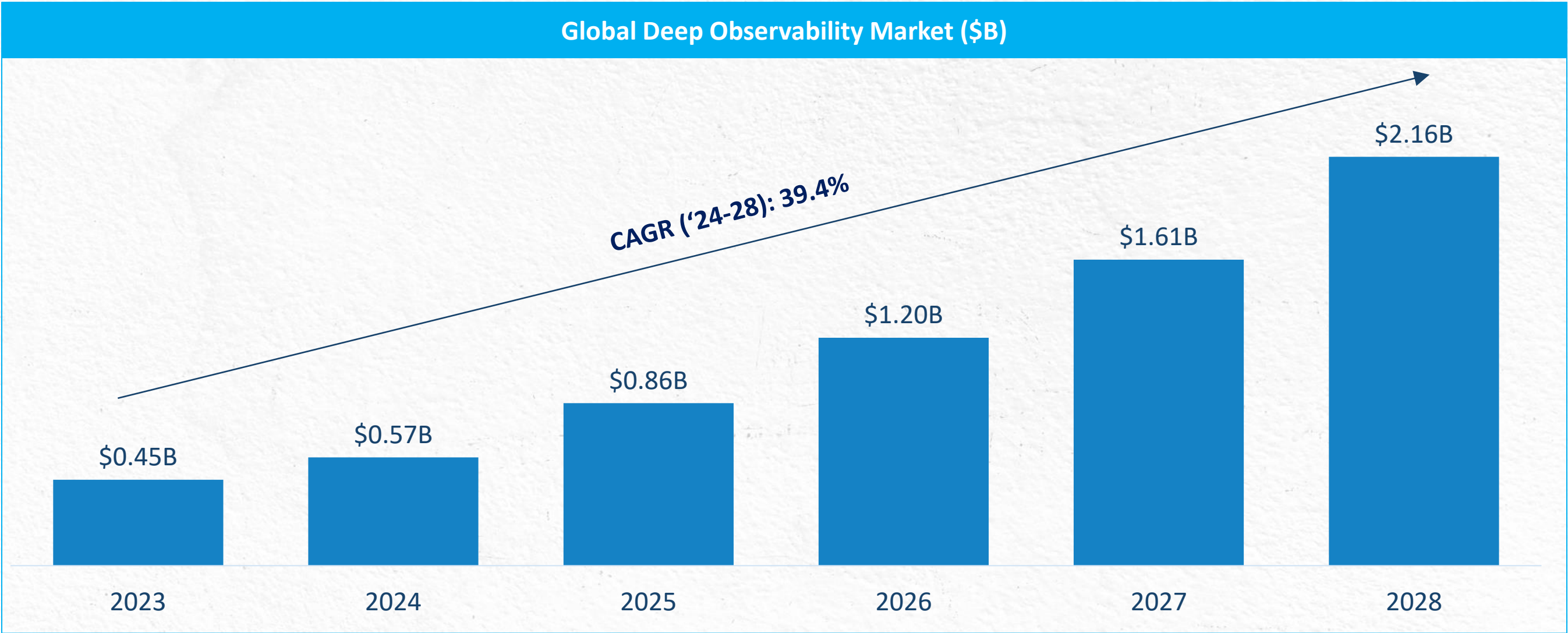
## METHODOLOGY FOR DERIVING THE MARKET SIZE, INCLUSIONS, EXCLUSIONS AND THE PRODUCT BOUNDARY

- Frost & 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 & Sullivan research as well as through primary interviews with market participants including Gigamon. The data was then used to model the current market size (2024) and project growth rates. Along with Global Enterprise, this study also estimated the size of the market for the US Federal government. US Federal agencies have the highest adoption of deep observability solutions 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 Federal 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 30%-160% YoY between 2022-2023. Frost & 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 2028.
- For the sizing of the market, Frost & Sullivan considered only those players in the deep observability space which meet with the product definition as illustrated in slide 6. Products which have the capability to gather (acquire) network, security and cloud traffic and have the ability of inspect and analyze it by going beyond MELT data. The spending for hybrid cloud deep observability consists of software and associated hardware. Hardware-based probes, agents, and taps are excluded from the market size calculations.



# DEEP OBSERVABILITY MARKET SIZE

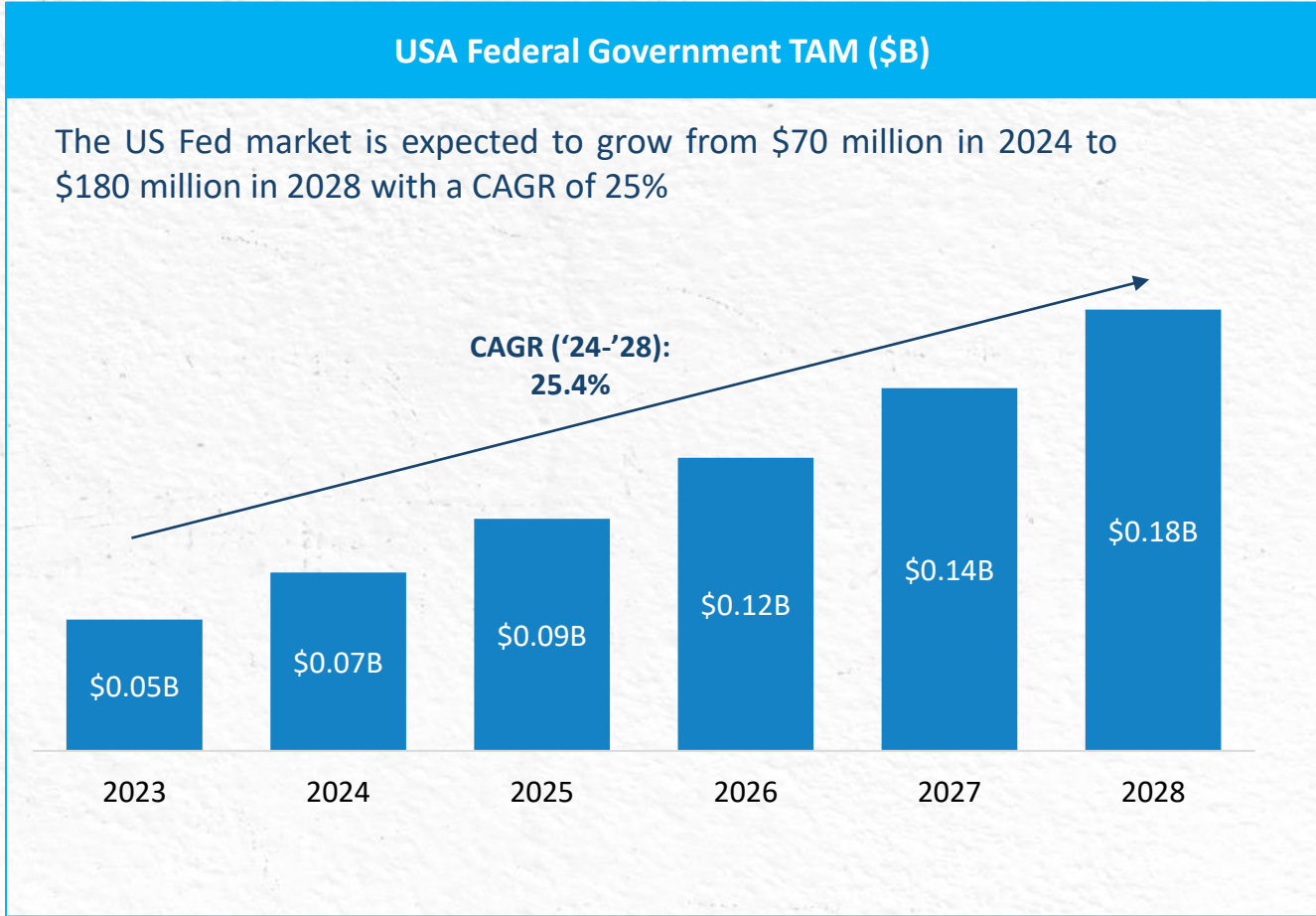
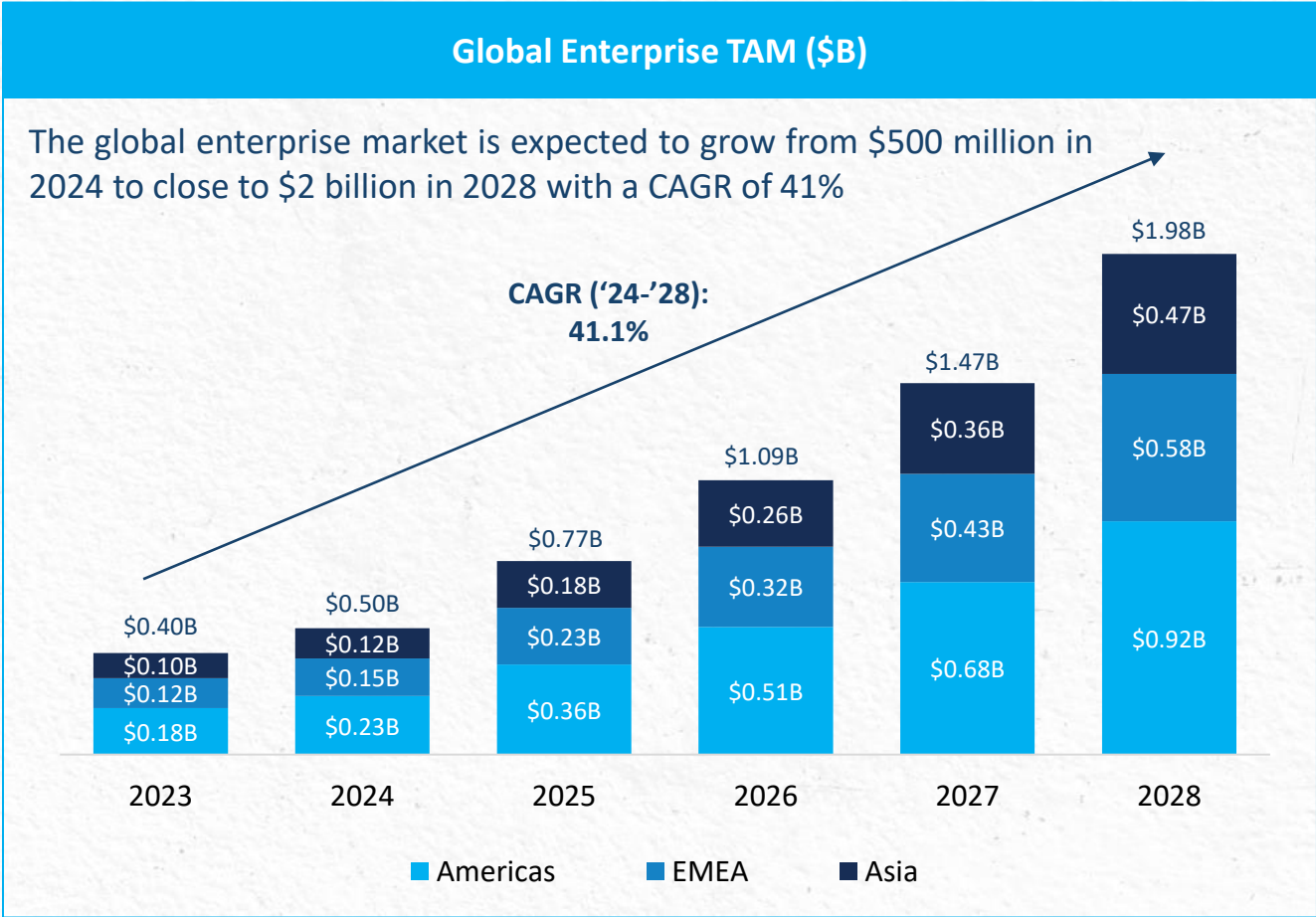
THE GLOBAL DEEP OBSERVABILITY MARKET IS PROJECTED TO EXPAND FROM \$0.57 BILLION IN 2024 TO \$2.16 BILLION BY 2028, EXPERIENCING A REMARKABLE COMPOUNDED ANNUAL GROWTH RATE (CAGR) OF 39.4%, DRIVEN BY SURGING ADOPTION IN LARGE ENTERPRISE AND US FEDERAL AGENCIES DUE TO REGULATORY PUSH AS WELL AS INCREASING PRODUCT AWARENESS.





# TAM FORECAST

THE GLOBAL DEEP OBSERVABILITY MARKET IS SIGNIFICANTLY INFLUENCED BY THE HIGH ADOPTION RATES AMONG LARGE ENTERPRISES (5000+ EMPLOYEES), WITH THE AMERICAS REGION BEING THE KEY DRIVER. THE KEY INDUSTRY VERTICALS DRIVING THIS DEMAND ARE TELCOS/COMMUNICATION SERVICES PROVIDERS (CSPS), BANKING AND FINANCIAL INSTITUTIONS AND GOVERNMENTS AS THEY MANAGE COMPLEX NETWORK TRAFFIC. THE GLOBAL ENTERPRISE TAM GROWTH RATES IN THE FORECAST PERIOD ARE EXPECTED TO BE SIGNIFICANTLY HIGHER THAN US FEDERAL GOVERNMENT DUE TO HIGHER DEMAND AND EXPANSION OF FIRMS IN THAT SEGMENT.







# 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) is the ability to inspect and analyze diverse network traffic in real time, reduce unwanted data going feeding into analytics solutions such as SIEM tools, thereby empowering analysts to work only on relevant and precise threat data.

### Increasing need to detect Advanced Threats

Deep observability solutions have advanced capabilities to detect network anomalies and ransomware, which is often challenging with less sophisticated solutions. Unlike traditional monitoring solutions that primarily focus on network-end analysis, deep observability offers comprehensive visibility across both network and application layers.

### The need to reduce Operational IT Costs

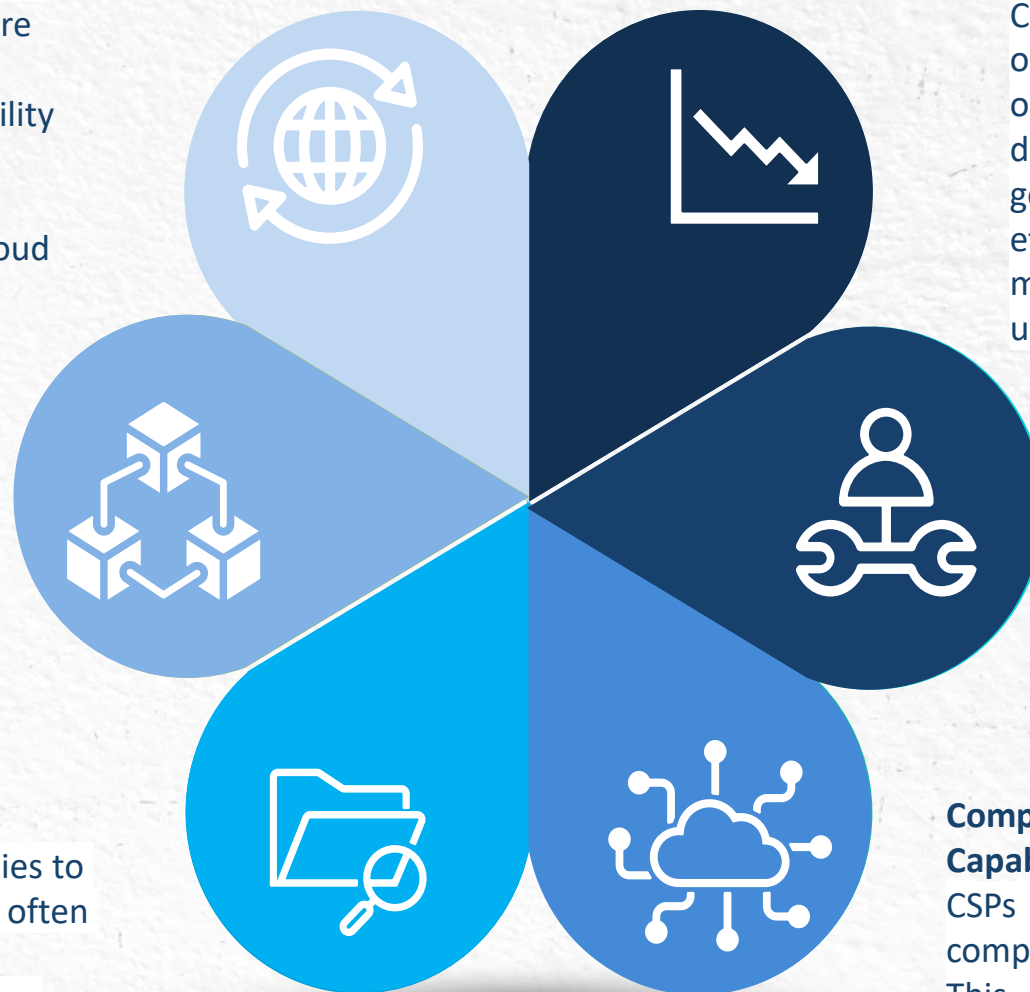
Cost reduction and consolidation will continue to be a key focus of organizational decision makers. Deep observability solutions offer multiple capabilities such as filtering, packet de-duplication, flow slicing, load balancing, and NetFlow generation that can streamline data processing, enhance the efficiency of security and monitoring solutions, and enable management of 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 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 lateral traffic between public cloud instances. Deep observability solutions address this gap.







**Overview of the  
Deep Observability  
Competitor  
Landscape**









# OBSERVABILITY MARKET LANDSCAPE

## Monitoring and Observability

- The broader Observability market has seen the emergence of many vendors creating their own niche in the market. Despite the many vendors in the market, the core need for **accurately pinpointing issues and optimizing performance in modern, complex, distributed IT environments and hybrid cloud infrastructure** still remains for organizations.
- Major observability vendors in the market today include Datadog, Dynatrace, Elastic, New Relic, and Honeycomb among others that offer unified platforms that integrate MELT 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 Vectra, **Darktrace and Palo Alto Networks specialize in 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 the observability solutions with accurate Network and Log based telemetry data. **Gigamon, Ixia (acquired by Keysight), NetScout, Arista (acquired Big Switch), APCON, Cisco, and Broadcom** offer products in this segment. Newer players 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.



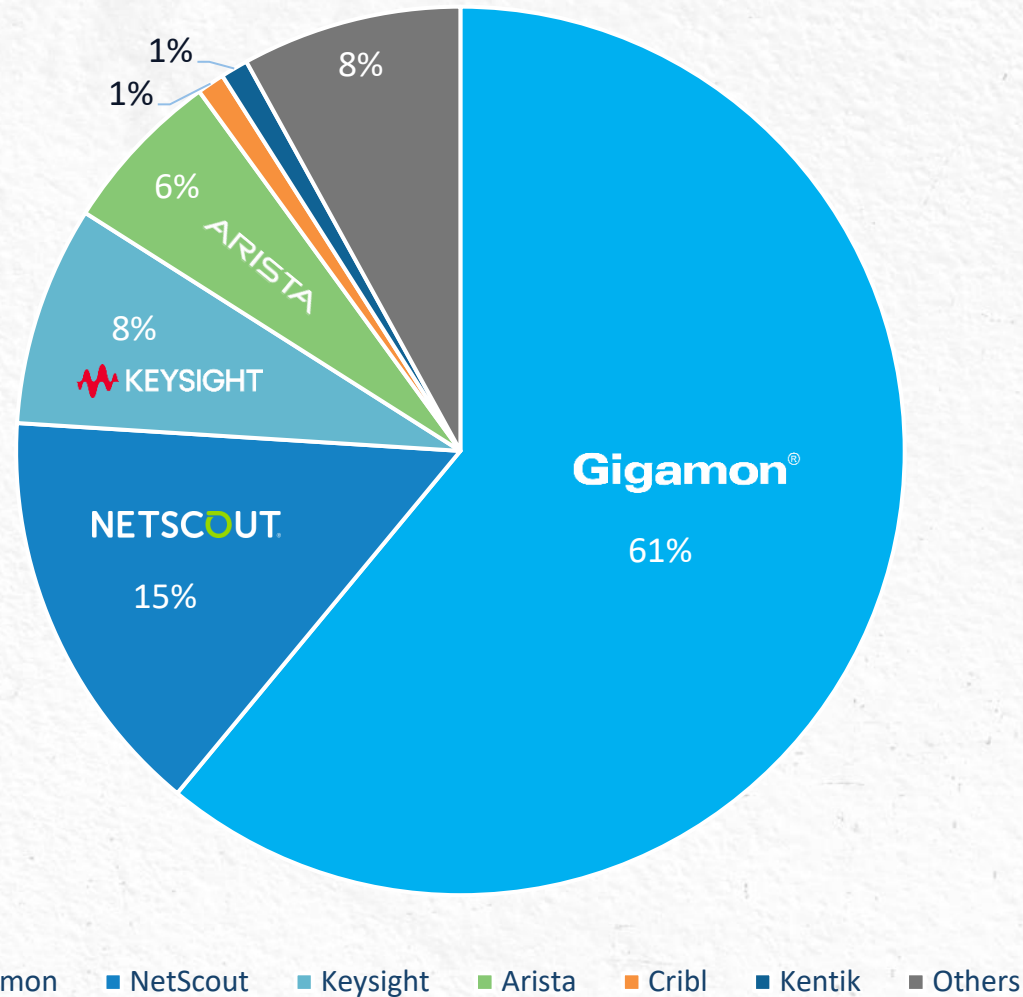
# KEY DEEP OBSERVABILITY VENDOR OVERVIEW

	Vendor Overview	Observability Offering
	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 has a strong Communication Service Providers (CSPs) business with its observability offering. It is the 2 <sup>nd</sup> 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 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 is a leader in high-speed datacenter 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 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 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.



# KEY PLAYERS IN DEEP OBSERVABILITY

Deep Observability, Revenue Market Share of Top Participants, 2023



Others include Cisco, APCON, Broadcom etc.

## Commentary

- **Gigamon** has the most comprehensive deep observability pipeline and the highest revenues in the industry attributable to the deep observability pipeline offering. It has more than 4000+ customers globally with strong revenue base enabling it to capture a substantial 61% market share.
- **NetScout** is the 2<sup>nd</sup> biggest player with estimated 15% 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 8% of the overall market share in 2023.
- **Arista’s** market share is predominantly due to its Big Switch acquisition in 2020. Its flanking and upselling strategy focuses on existing customer base rather than heavily engaging in direct competition for observability market share.
- 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. They remain focused on the mid-market and lower end of the spectrum and hence have limited market share in the large enterprises. Their average deal size remains lower than the other bigger players in the market.





---

# Insights and Guidance for End Users



# WHY ADOPT DEEP OBSERVABILITY?





# WHY ADOPT DEEP OBSERVABILITY?

## Advanced Data Inspection and Gathering

- **Deep Insights:** Inspect and gather network, security, and computing traffic by extracting event metadata from packets and computing infrastructure.
- **Clear Results:** More precise detection of anomalies and threats, enabling proactive mitigation.

## Uncovering Blind Spots

- **Unified View:** Gain end-to-end visibility across hybrid, multi-cloud, and on-prem environments, eliminating blind spots.
- **Detailed Insights:** Capture and analyze granular data on network traffic, including encrypted data, to uncover hidden threats.

## Real-Time Data Processing and Analysis

- **Real-Time Detection:** Leverage continuous monitoring and real-time alerts to detect and respond to threats immediately.
- **Enhanced Security:** Enables quicker detection of issues and faster response times.

## Concrete ROI

- **Optimize Resources:** Reduce solution redundancy, license fees, and operational costs.
- **ROI:** Features such as filtering, packet de-duplication, flow slicing, load balancing, and NetFlow generation, deep observability solutions significantly reduce operational costs and enhance the efficiency of your security analysts.

## Achieve Regulatory Compliance

- **Audit Trails:** Maintain detailed logs and reports to meet regulatory requirements, avoiding penalties and ensuring compliance.
- **Data Governance:** Ensure visibility and control over data flows to comply with privacy laws and protect sensitive information.

Given the growing importance of accurate, complete, and optimized telemetry for security and monitoring tools, as well as AI engines, it is essential to allocate a dedicated budget for this purpose. Historically, data collection has been embedded within individual tools, but telemetry is now emerging as a distinct function, fueling market growth. Therefore, it is crucial to consider a separate line item for telemetry in your security budget, rather than integrating it solely within the budget for tools.



# WHAT TO LOOK FOR IN A DEEP OBSERVABILITY VENDOR

## Advanced Data Inspection Capabilities



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.

## Interoperability with Data Lakes



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.

## Multi-Vendor Support



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.

## Comprehensive Security Features



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. Advanced security capabilities are essential for protecting the organization against the increasing sophistication of cyber threats.

## Support for Multi-Cloud Strategy



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

## Data Rich User Interface



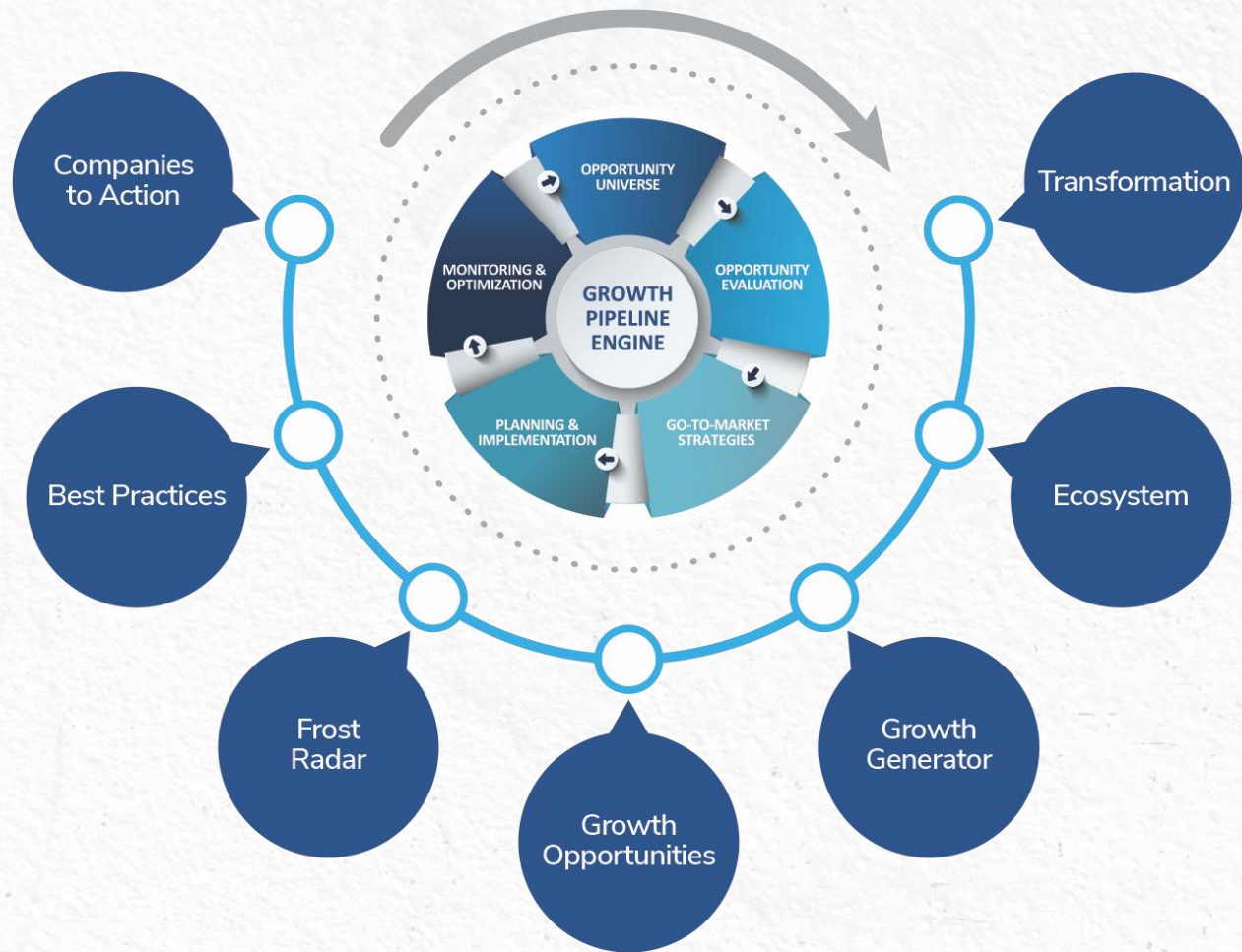
Choose a deep observability solution that has a data rich interface and comprehensive reporting capabilities. An intuitive dashboard that allows for easy visualization of data on a single pane of glass that enables the IT teams get the most out of the observability solution without increasing the skills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





# TRANSFORMATIONAL GROWTH JOURNEY

*“Powered by the Growth Pipeline Engine”*



**Vinay Biradar**

Associate Director, Cybersecurity Advisory

[vinay.biradar@frost.com](mailto:vinay.biradar@frost.com)