REFERENCE ARCHITECTURE

Observability

VERSION 1.0 — UPDATED 4/1/24

The observability architecture layers a pipeline, a platform, and a set of operational use-cases over the metrics, events, logs, and traces produced across hybrid environments.

ITOPS | SECOPS | DATAOPS | AIOPS

USE-CASES

VISUALIZATION

Visualizations in observability extend beyond dashboards to include charts, graphs, heatmaps, and timelines. These graphical representations offer diverse perspectives on system performance, facilitating effective analysis and decision-making.

ANALYTICS & INTELLIGENCE

Observability analytics extract actionable insights, including correlations, from diverse data sources, enabling proactive issue identification and long-term trending. By analyzing vast amounts of data in real-time, the observability platform enables organizations to detect and mitigate issues proactively, optimize performance, and make informed decisions to support business objectives.

STORAGE

Observability storage captures and retains metrics, events, logs, and traces for both short-term analysis and long-term trend identification, supporting performance optimization and issue resolution.

OBSERVABILITY PLATFORM

The observability platform is a comprehensive system designed to provide insights into the behavior and performance of complex IT environments. It efficiently collects and analyzes metrics, logs, events, and traces to provide insights into system performance and behavior. By aggregating and correlating this data, the observability platform enables organizations to gain a holistic understanding of system health, detect anomalies, troubleshoot issues, and optimize performance.

OBSERVABILITY PIPELINE TOOL

The observability pipeline serves as the control mechanism for the overall observability platform, acting as the initial stage for metrics, events, logs, and traces. It manages data flow, conducts pre-platform tasks like filtering and routing, and facilitates efficient troubleshooting and optimization within IT environments.

METRICS, EVENTS, LOGS, TRACES

On-Premise
APP — INFRA — DEVICE

Public Cloud
APP — INFRA — DEVICE

SaaS
APP — INFRA — DEVICE

HYBRID — INTERNET — BUSINESS SERVICE TRANSACTION

Use-Cases

ITOPS

ITOps observability involves integrating elements of end-user experience monitoring, network monitoring, infrastructure monitoring, and application monitoring. By analyzing end-to-end transactions and correlating data across various domains, organizations can identify trends, anomalies, and dependencies, facilitating efficient troubleshooting, performance optimization, and proactive issue resolution.

ACTIVITIES Monitoring, troubleshooting, performance management, capacity management

SECOPS

An observability platform for SecOps enhances detection, analysis, and response to security threats and incidents. Observability platforms integrate diverse data sources for comprehensive security visibility. They enable real-time threat detection, incident investigation, and support forensic analysis, compliance monitoring, and vulnerability management. Proactive monitoring and analysis enhance threat detection, incident response, and overall cybersecurity defenses.

ACTIVITIES Threat detection, incident response, forensic analysis, compliance monitoring, vulnerability management

DATAOPS

DataOps observability involves leveraging advanced monitoring and analytics to optimize data operations, ensure reliability, performance, and compliance. The platform provides comprehensive visibility into the data ecosystem, enabling real-time monitoring, anomaly detection, issue resolution, and capacity planning. It supports compliance monitoring and governance, ultimately enhancing operational efficiency and driving innovation.

ACTIVITIES Data monitoring, performance optimization, anomaly detection, compliance & governance, capacity planning

AIOPS

AIOps observability platforms ensure the reliability, performance, and scalability of AI models and infrastructure. By integrating data from various sources, the platform provides visibility for monitoring model performance, detecting anomalies, troubleshooting issues, and optimizing resource utilization. Automated incident response and continuous analysis of historical data drive continuous improvement across the AI lifecycle, enhancing operational efficiency and reliability.

ACTIVITIES Model performance monitoring, data quality monitoring, infrastructure monitoring, event analysis

Monitoring Domains

SECURITY MONITORING

Security monitoring continuously watches for threats in an systems, networks, and applications, detecting and responding to suspicious activities, unauthorized access, and other compromises.

NETWORK/INTERNET MONITORING

Network/internet monitoring systematically observes and analyzes data traffic, tracking metrics like bandwidth, latency, packet loss, and security incidents.

EXPERIENCE MONITORING

End-user experience monitoring continuously observes user-system interactions, tracking metrics like response times and errors to ensure a seamless experience.

INFRASTRUCTURE MONITORING

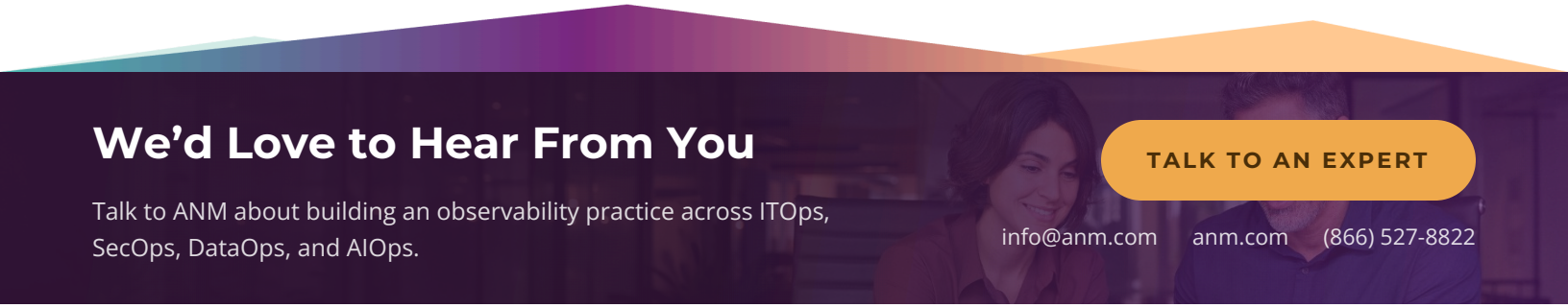
Infrastructure monitoring tracks compute, storage, virtualization, and microservices resources, using data metrics like CPU usage and storage capacity to optimize performance and ensure reliability.

APPLICATION MONITORING

Application monitoring ensures optimal performance and availability by tracking metrics like response times and resource usage, resolving issues proactively, and enhancing user experience.

DATA MONITORING

Data monitoring ensures the accuracy and integrity of data across systems and applications. By tracking data flows and quality in real-time, it enables identification of anomalies and optimization of data processes.



We'd Love to Hear From You

Talk to ANM about building an observability practice across ITOps, SecOps, DataOps, and AIOps.

TALK TO AN EXPERT

info@anm.com anm.com (866) 527-8822