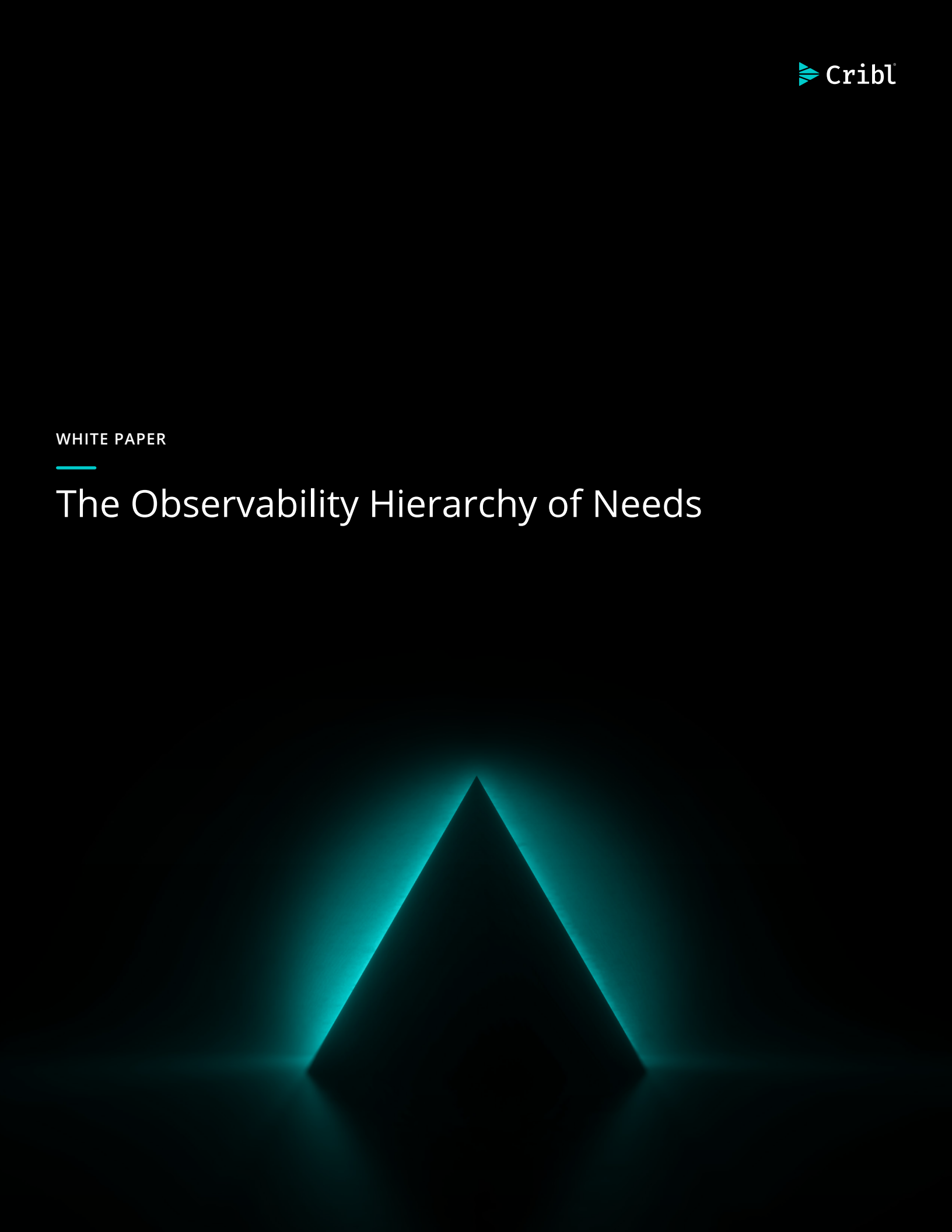
Cribl

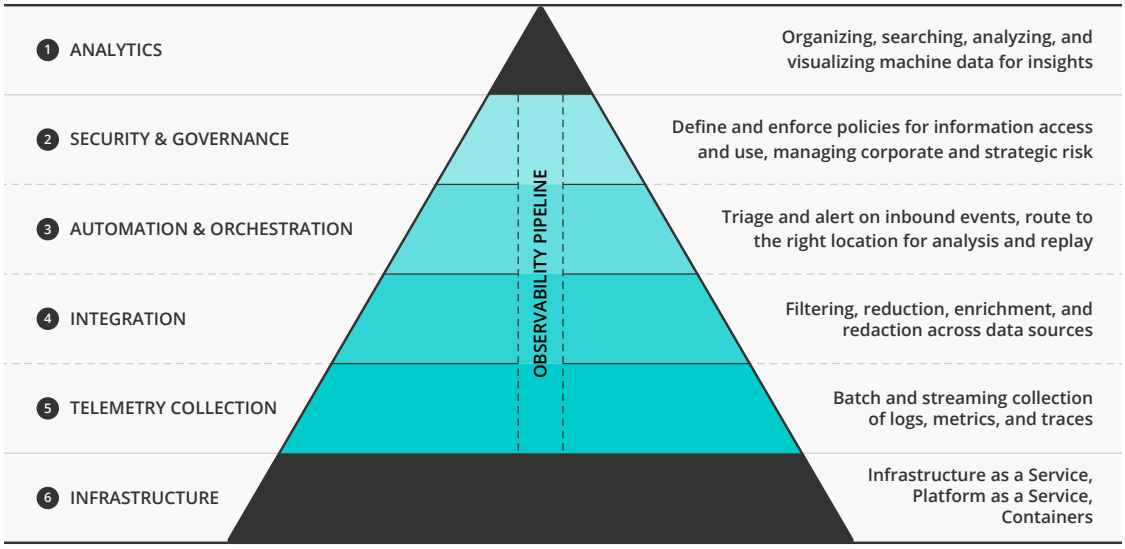
WHITE PAPER

The Observability Hierarchy of Needs



WHITE PAPER

The Observability Hierarchy of Needs



Building modern observable systems goes far beyond logging analytics and application performance management (APM); Observability requires an intelligent pipeline from infrastructure all the way through to analysis.

ITOps and SecOps teams struggle understanding complex operational environments spanning multiple clouds, container-based deployments, and ever-expanding security surfaces.

Traditional monitoring is failing these teams in three ways:

- ***Exorbitant costs forces teams to compromise on what they're monitoring.*** *Forced into decisions about which logs, metrics, and traces to keep to stay within budget, teams simply can't store everything they need to stay informed about their environment.*
- ***Pre-built dashboards and alerts don't reflect today's infrastructure reality.*** *Systems scale dynamically, and DevOps teams may deploy code across thousands of containers dozens of times each day. The static views offered by traditional monitoring systems don't reflect this reality.*
- ***Monitoring is a point solution, targeting a single application or service.*** *Today's applications comprise hundreds or thousands of independent services. A failure in one service cascades to others, and unraveling those errors is well beyond the scope of monitoring applications.*

OBSERVABILITY IS AN ATTRIBUTE OF SOFTWARE AND SYSTEMS ALLOWING THEM TO BE "SEEN," AND TO ANSWER QUESTIONS ABOUT THEIR BEHAVIOR.

Addressing these challenges means infrastructure and operations teams must shift from isolated monitoring applications to holistic observability.

THE STANDARD APPROACH OF DEPLOYING AGENTS EVERYWHERE HASN'T SCALED. EACH MONITORING SOLUTION HAS ITS OWN AGENT, AND ITS OWN COSTS.

Observability is an attribute of software and systems allowing them to be "seen," and to answer questions about their behavior. Building observable systems goes beyond logging analytics and application performance management (APM). Observability requires an intelligent pipeline to:

- ***Collect*** *disparate data from a range of infrastructure components without deploying expensive agents.*
- ***Integrate, filter, redact, and enrich*** *data sources, as well as reduce data volumes delivered to upstream systems to control costs.*
- ***Automated alerting and orchestration*** *of data delivery across systems, delivering the right data to the right place.*
- ***Security and governance*** *features allowing data sharing while also ensuring regulatory and compliance for sensitive data.*

COLLECT

In today's deployment environments, data comes from everywhere. Data floods in from firewalls, containers, SNMP traps, and HTTP sources. Data must be fetched from object stores, data hubs, and messaging sources like Kafka. Coping with increasing data volumes is a challenge for every infrastructure and operations team. The standard approach of deploying agents everywhere hasn't scaled. Each monitoring solution has its own agent, and its own costs.

INTEGRATE, FILTER, REDACT, AND ENRICH

With data collected, it must be intelligently processed. The next, and most important, level in the observability hierarchy is integration. The logs, metrics, and traces comprising observability data can inundate downstream systems with irrelevant data. Worse, the data may not have the level of enrichment needed to support observable systems, or it may contain data that downstream consumers shouldn't see.

An observability pipeline lets you take control of how your data is processed. This drives down infrastructure costs for logging and logging analytics while also providing a better data product for developers, infrastructure & operations teams, and SecOps staff.

AUTOMATION AND ORCHESTRATION

Integrated data flows must be stored, but it must be stored in the right place. An observability pipeline places data in one or more locations based on:

- *The data context determined by analyzing the content of the logs, metrics and traces*
- *The available storage tiers and search characteristics*
- *The rules defined and inferred by infrastructure and operations teams around retention and security policies*

An observability pipeline's data orchestration capabilities support automated responses from application performance management, SIEM, SOAR and UEBA platforms already deployed in the enterprise.

THE FINAL ELEMENT OF AN OBSERVABILITY PIPELINE ARE THE SECURITY AND GOVERNANCE CAPABILITIES SUPPORTING GOVERNED DATA SHARING AND ANALYSIS.

SECURITY AND GOVERNANCE

Logging data represents massive value, but it is still underutilized in many organizations. As more teams realize the value of ad hoc exploration of logging data, managing access becomes essential. The final element of an observability pipeline are the security and governance capabilities supporting governed data sharing and analysis. Doing this requires rich role and attribute based access controls, and persona-based data redaction and masking.

In Summary

Implementing an observability pipeline gives enterprises faster and more flexible access to their logs, metrics and traces, accelerating root cause analysis of performance challenges. Resolving problems faster improves customer satisfaction, increasing revenues over time. Observing infrastructure, rather than just monitoring it, makes continuous optimization a reality and lowers infrastructure costs.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and machine data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.