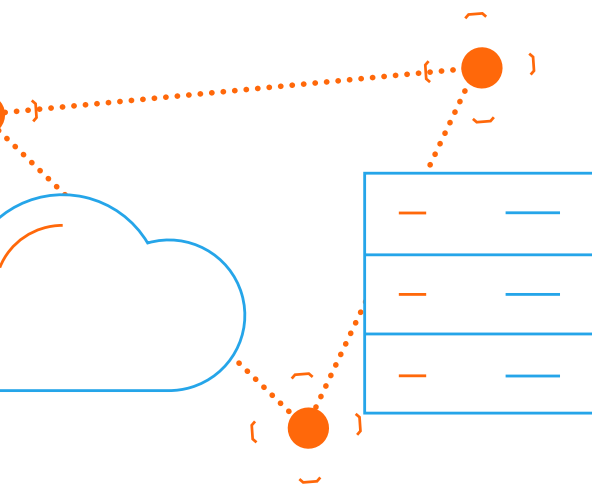


Cloud Retention

Bricata Removes the Barrier of Cloud Visibility & Retention

The types of data Bricata captures and stores, and how long data is retained, can be easily customized and tailored to meet your organization's specific requirements.

Security teams can significantly reduce risks when they have easy access to the critical network data and context that enriches the analysts' workflow while performing threat assessments and responding to incidents. Until recently, organizations that wanted to retain more than a few hours of their network metadata had to build a data lake or some other repository, which was expensive and took a long time to deploy.



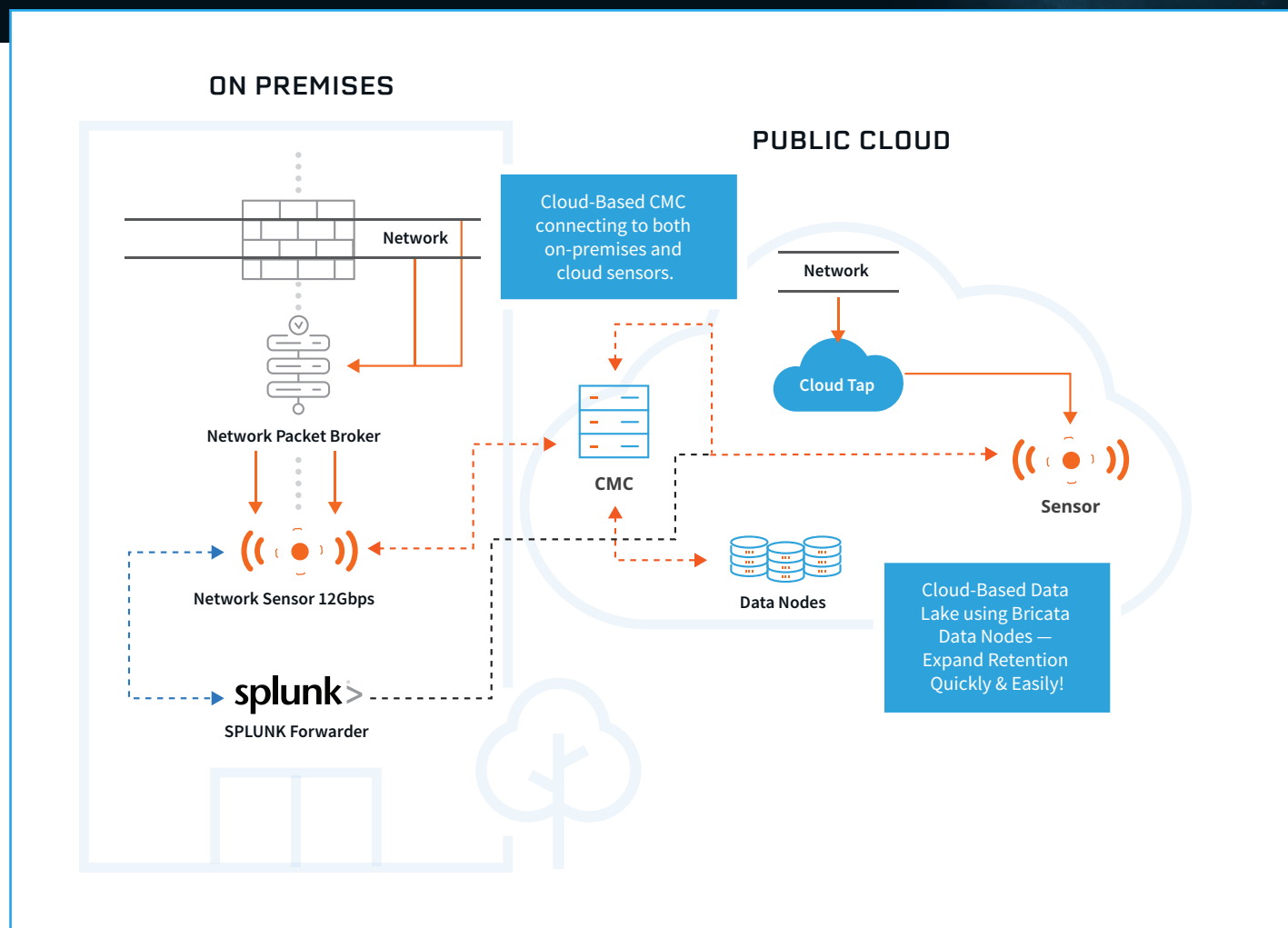
The Bricata network security platform includes integrated data nodes that store network metadata in the cloud or on premises. SmartPCAP data is also captured and stored in Bricata's software-based sensors for long periods of time (e.g. months). With Bricata, security analysts and threat hunters can immediately access the high-fidelity metadata and PCAP data from either a central management console (CMC) or via their existing SIEM platform to perform rapid threat assessments and successful remediations, improve threat investigations, and gain deeper insights about the security of the network.

The types of data Bricata captures and stores, and how long data is retained, can be easily customized and tailored to meet your organization's specific requirements. Bricata data nodes and CMCs can be quickly deployed on premises or in AWS, Azure or Google cloud environments, and additional nodes and management consoles can be added as needed at the click of a button.

Bricata provides you with complete control over the types of data you retain, with over 30 different log types and more than 400 fields extracted from every network transaction (e.g., connection summaries, HTTP records and DNS traffic).

Bricata's pay-for-what-you-need subscription pricing model is focused solely on the average throughput the sensor grid analyzes. This allows the user to deploy as many sensor and data node components needed to strike the right balance between visibility and retention.

With Bricata, your security team can easily query all of your network metadata and PCAP data from a single dashboard. Data can also be exported to a SIEM or other systems as required.



ABOUT

Bricata is leading the next generation of advanced network detection and response for the enterprise. By fusing real-time visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform, Bricata provides organizations with end-to-end visibility and context for direct answers and powerful insight to take immediate action.

BRICATA.COM | INFO@BRICATA.COM | 888.468.0610 |   

Copyright 2020 Bricata, Inc.

BRICATA