DNSi BIG DATA CONNECTOR

Harness DNS data for network and security insights

KEY HIGHLIGHTS

- Fast time to deployment
- Pre-built integration into Hadoop and Splunk
- Data architecture scales to millions of queries per second
- Complete, aggregated view of DNS data without additional hardware
- Seamless connectivity to Big Data systems or purpose-built applications in near real time
- Built-in filtering can reduce both bandwidth and data storage costs

Today's networks are data driven. Data is essential in planning so network investments can deliver the maximum ROI. Operations and security teams depend on diverse metrics to evaluate status, health, exposure to threats, and usage trends. Big Data systems enable data-driven analytics to make faster decisions and more accurate appraisals of network and security requirements. DNS infrastructure (DNSi) Big Data Connector (BDC) transforms data gathered from Akamai DNSi CacheServe resolvers so it can be used by existing Big Data systems, or purpose-built applications, to develop meaningful monitoring, trending, planning, and security metrics.

ACCESS AND ANALYZE DNS DATA FOR NETWORK AND SECURITY INSIGHTS

DNS resolution data provides a more content-aware view of network activity. It complements IP packet data, collected with NetFlow or other tools, allowing better visualization and rationalization of network traffic and performance. It can also contribute to a better understanding of security posture, and aggregated data can be used to characterize content and website preferences and trends, or identify the kinds of devices being connected to a network.

Akamai DNSi BDC is optional software to integrate DNS and other data, gathered from the Akamai solutions below, with open Big Data systems or purpose-built applications: .

- **Akamai DNSi:** CacheServe resolvers deployed throughout provider networks to improve responsiveness, availability, and security
- **Akamai Security and Personalization Services (SPS):** ThreatAvert installations to protect networks and provide visibility into subscriber infections
- **Proxies:** Used in Akamai Secure Consumer, Secure Business, Secure Public Wi-Fi, and Reach installations to protect and message subscribers.

Akamai CacheServe resolvers, ThreatAvert instances, and SPS proxies use a proprietary format to export data. BDC transforms Akamai proprietary data into a JSON format so Big Data systems like Hadoop, Splunk, or others can readily consume it.

SCALE AND INTEGRATE WITH EXISTING BIG DATA SYSTEMS

Akamai DNSi and SPS products use a robust data architecture for transporting and managing massive amounts of query, proxy, and telemetry data generated in a typical provider network. The data architecture scales to millions of queries per second. It's based on open solutions that have been proven in the world's largest networks, delivering operational excellence at web scale and speed. Data that's gathered is accessible to analytics or other applications in real time, and the solution is highly resilient through failures, offering nonstop availability. Data can be compressed at the edge of the network by converting it into an efficient binary format to reduce transmission costs. Data can also be filtered to reduce the volume of transported data to only data of interest.

Alternative solutions for gathering DNS data require dedicated hardware and/or lack an integrated data pipeline – increasing costs and incurring operational overhead to manage separate systems

DNSi BIG DATA CONNECTOR

DRIVE BETTER OUTCOMES

- **Strengthen subscriber security:** Correlate subscriber infections and unwanted activity identified with DNS with other indicators of compromise (IoC), even when subscribers connect to and transit different access technologies (fixed, mobile, Wi-Fi, etc.).
- **Improve overall security posture:** Forward malware queries to external security systems to gain deeper insights and understand broader security trends in the context of anti-abuse systems and third-party security data.
- **Refine capacity planning:** Associate traffic with applications like video streaming, gaming, or even IoT as it becomes more widespread; combining DNS data with other data, such as bandwidth usage, will yield more comprehensive capacity planning.
- **Drive service adoption:** Derive real-time insights into aggregate trends such as app usage, media consumption, and content preferences, to shape campaigns for driving adoption of new services or bundles.
- **Enhance customer satisfaction**: Correlate aggregate usage preferences and trends with service-level data to drive proactive outreach programs for upgrade offers, promotions, discounts, or other programs.

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 03/19.