BUSINESS INTEGRA

Flying higher, together.

SINCE 2001

CYBER DATA LAKEHOUSE

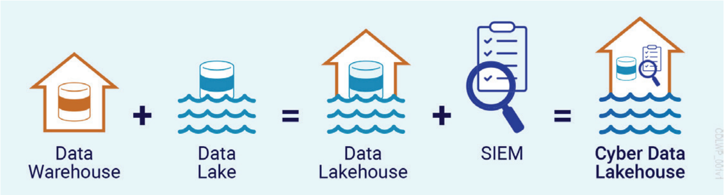
Sophisticated nation-state attacks are on the rise...and so is the number and impact of their data breaches.

With cybersecurity talent under pressure and in short supply, now is the right time to augment or replace your Security Information and Event Management (SIEM) with a Cyber Data Lakehouse (CDL) architecture.

The CDL is an innovative advance in Data Lakehouse Architecture that aligns with logging and retention requirements in the White House's Executive Order on Improving the Nation's Cybersecurity (EO 14028), specifically in Section 8, which focuses on improving the federal government's investigative and remediation capabilities. Our CDL reference architecture provides a technology-agnostic framework to address logging requirements, retention periods, and maturity levels necessary to meet the aggressive timelines outlined in the Office of Management and Budget (OMB) memo M-21-31, which resulted from EO 14028.

We have advised 21+ Federal agencies, since May 2021, on the convergence of cybersecurity and data science for enriched threat intelligence.

CDL solutions bring together data warehouse and data lake capabilities built upon a Data Science platform to cost-effectively and efficiently solve modern cybersecurity challenges at the petabyte scale required for ingesting all Zero Trust log sources. Enhanced by leading-edge Artificial Intelligence (AI) and Machine Learning (ML), the CDL enables progress in the Automation and Orchestration pillar of Zero Trust.



For enterprises struggling with rising SIEM costs and facing challenges in implementing new Zero Trust mandates, the Cyber Data Lakehouse can reduce log storage costs, enable longer log retention, automate threat hunting, and provide centralized threat intelligence. Unlike traditional SIEM solutions that struggle to cost-effectively ingest and retain log data for 365 days as mandated in OMB M-21-31, Cyber Data Lakehouse solutions offer cheaper storage and longer data retention through modern data platforms that separate storage from compute costs.

They also enable faster data ingestion using distributed and in-memory processing required for big data cloud computing. Whether you are considering SIEM augmentation or replacement, we can tailor our CDL reference architecture to help you navigate the convergence of cybersecurity and data science. Our solution solves the Zero Trust big data problem and empowers your cybersecurity teams with centralized threat intelligence, refined results, and advanced detections.

SOLUTION BENEFITS

Reduced Log Storage Costs

Centralized & Enriched Telemetry

Zero Trust Automation & Orchestration

Improved Threat Intelligence

Improved Incident Response Times

Faster Data Ingestion at Petabyte Scale

VENDOR PARTNERS

databricks

securonix

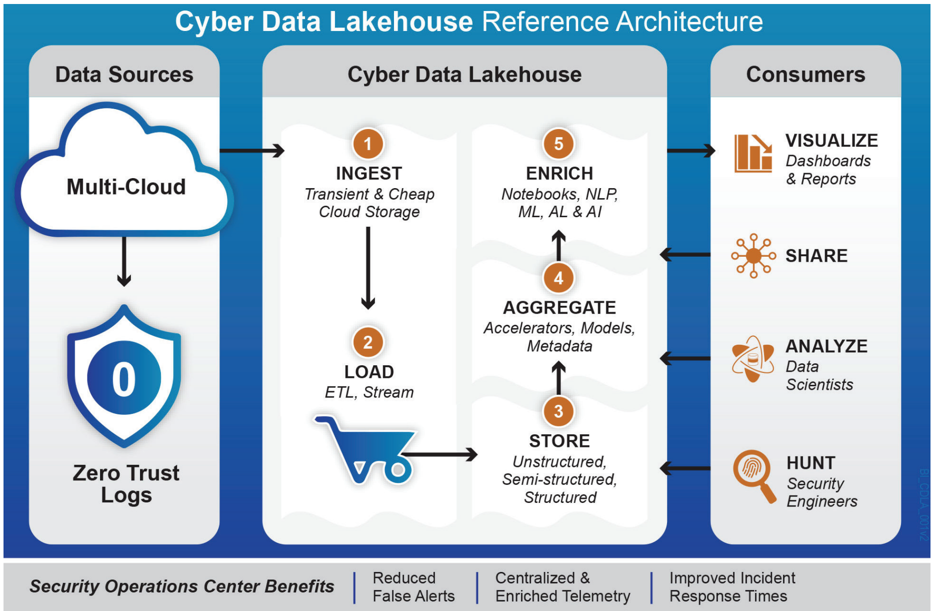
Trellix

Microsoft Silver Partner

snowflake

SOLUTION HIGHLIGHTS

- **Mission Driven –** Evolved customer needs and market/solution fit for EO 14028, M-21-31, and M-22-09
- **Reference Architecture –** Ingest, load, store, aggregate, and enrich Zero Trust logs to visualize Threat Intelligence
- **SIEM augmentation/replacement –** Cybersecurity-specific solution, built upon a Lakehouse architecture
- **Industry-leading Data Science Platforms –** For advanced threat detections across all Zero Trust logs
- **Fit for Purpose –** Solution vetted and informed by thought leaders across 21+ federal agencies
- **Leverages Existing Investments –** Solution tailored to customer investments and preferences



Cyber Data Lakehouse Reference Architecture

Security Operations Center Benefits | Reduced False Alerts | Centralized & Enriched Telemetry | Improved Incident Response Times

ABOUT BI

Large business, Domestically-owned
CAGE Code: 3BGU6

Headquarters: 6550 Rock Spring Dr., Suite 600
Bethesda, MD 20817

Questions? growth@businessintegra.com

CURIOUS?
Dive deeper into Cyber Data Lakehouse...

Download the
WHITE PAPER