When U.S. retailer Target was hacked, it was not because they had not invested in the best security devices, firewalls, and security information and event management (SIEM) technologies that collect gigabytes of security data per second. It was because they could not analyze fast enough the information and events that mattered most.

**REAL-TIME ARCHITECTURE MATTERS**

At Logtrust, we have 15 years of experience in Big Data security management, and our platform has been designed for fast, real-time insights for big data. We know that the time it takes to retrieve past events is as important as the time it takes to detect anomalies as events occur.

This is the quintessential challenge with today’s security architectures. On the one hand, you have traditional, relational database-driven SIEM architectures that operate on the principle of “collect it all and figure out what to do with it later.” In other words, they are not real-time.

On the other hand, you have streaming architectures that compute in real-time data streams but don’t actually retain past events for pattern detection. At Logtrust, we refer to this as the “two architectures dilemma.” One architecture can only analyze the present but not the past. The other analyzes the past but not the present. This dichotomy leaves the onus on the organization to support two architectures and to suffer the impact of engineering and maintenance costs.

**FLAT-ULTRA-LOW-LATENCY ARCHITECTURE**

Logtrust has a single platform that performs analytics both on the present and the past in real-time. We call it the FULL™ Architecture—Flat-Ultra-Low-Latency.

Ultra-low-latency drills down and aggregates over multiple data sources then arbitrarily explores and visualizes these data flows as they arrive in real-time while simultaneously keeping the aggregated results fresh with continuous updates of past events.

[ LOGTRUST FULL™ SINGLE PLATFORM ]

---

Real-Time Security Analytics Data Sheet
By analyzing the past to understand the present, Logtrust helps identify anomalies intuitively and with statistical learning when needed. Ultimately it enables the sending of alerts with sharable queries and dashboards to accelerate the decision-making process.

Traditional relational database management system (RDBMS) driven architecture is not designed for fast data streams with unbounded data, with no persistent patterns, and arriving without end dates. As a result, scalability and performance are fundamental challenges. Logtrust can analyze multiple disconnected data streams in parallel to find hidden relationships, while traditional SIEM will spend time normalizing all the logs into the events-of-interest.

Logtrust can complement SIEM by offloading all ingestion, aggregation, and normalization of “time critical events-of-interest” by performing in real-time ultra-low-latency queries and complex event processing. Logtrust can output back into HP ArcSight common event format (CEF) or IBM QRadar log event extended format (LEEF) the results of these queries and event processing for further deep analysis with SIEM.

Logtrust provides a very intuitive drag and drop interface that does not require any coding skills. It enables users to interactively explore hidden relationships between data flows.

To perform real-time security analytics 24x7x365, you need a service that is always on. Logtrust runs natively on Cloud elastic architecture and combines both internal High Availability (HA) at the data node level, and cloud zone resources HA disaster recovery (D/R) for multi-tenant delivery models is automatically achieved across Cloud geographies.
We can ingest in real-time any data with any volume per day 1GB/1TB/1PB/... with the same response time for all searches, queries, or complex event processing.

Logtrust performance is extremely high regarding companies’ key indicators.

Queries to retrieve the most recent 10 seconds of data or the last 10 years of events will always have the same ultra fast response time.

In addition to proactive detection of issues through our security alerts, Logtrust also helps you identify source and cause. The Logtrust geolocation system allows you to identify the IP location of an attack, and when the issue is internal, you can also identify the machine and user that generated the problem. With Logtrust’s powerful correlation engine you will discover what caused the problem, when it happened, and why.

Logtrust provides an external location for your system to safely store your information. If you are subject to an attack and/or intrusion, the attacker will likely attempt to cover his tracks; the Logtrust system ensures that what occurred in your logs can never be covered up.

By combining the information from every system involved, you will be able to generate a timeline for the incident in question, achieve complete visibility, and detail exactly how the intrusion occurred and where it took place.
ALWAYS HOT DATA

Logtrust has no limitations on the volume of information. It allows you to analyze years of data and petabytes of information in real-time, all-the-time. It maintains your historical data, and there is no data temperature segregation such as hot, warm or cold. Your data is always hot.

HIGHLY RELIABLE

When faced with audits or forensics, you must be able to trust and rely on the logs in use. In the event of prosecution, you must be able to prove in a court of law that the logs are genuine and no one has tampered with them. With Logtrust’s unique cryptographic audit trail, you have proof of:

- The integrity of each raw log, proving that no log has been tampered with or been manipulated.
- The integrity of the log sequence, proving that no log has been added and no log has been deleted.

HIGHLY SECURE

All logs data are protected in-fly and at rest:

- Logtrust has unique multi-factor authentication between collectors and processors to ensure end-to-end protection.
- Logtrust enables users to encrypt their data and manage keys which can be maintained automatically by Logtrust or the customer.
- Customers maintain full control of their data privacy and data residency.

REAL-TIME ALERTING

Logtrust provides a set of generic alerts and correlation libraries, such as:

- Attack detection (on infrastructure, systems, webservers and application servers).
- User and/or system activity tracking.
- Behavioral analysis which alerts you to any change in system user behavior.

Additionally, users can define custom alerts based on the searches they are generating within the application. The alerts can be of two kinds:

- Alerts that are generated for each detected event.
- Alerts that are generated for a given period of time.

All the alerts are delivered in real-time via your chosen mechanism (email, sms, Jira, Service Desk, Pushover, PagerDuty, Logtrust mobile application and/or Logtrust web application.)