AEROSPIKE

Aerospike: Bringing Real-Time Cyber Operations to Federal Agencies

USE CASE

Aerospike's Real-time Data Platform drives machine learning over billions of enterprise system events to discover and speed remediation of attacks to minutes instead of months — while also streamlining resources and cutting risk exposure.

The imperative for real-time Federal cyber operations

In today's complex cyber landscape, more data translates into more threat insights. Most of the data collected today can be categorized in one of two ways: immediately actionable or historically significant. The desire of the cyber security community is to merge these two categories to produce insights within milliseconds to enable informed responses to suspicious activity as it is occurring.

Increasingly, complex data schemas and the volume and velocity of data has made traditional deterministic approaches to intrusion detection unrealistic. Current approaches to cyber security have not kept up with the expanding threat vectors driven by remote working, mobility, social media, and virtualized cloud networks. Legacy security tools cannot handle the huge array of disparate data sources that are needed to: understand what constitutes a risk; quickly pinpoint where risks are emerging; and determine appropriate actions for investigating or remediating them.

Limited capabilities of current technologies

Federal cyber teams need new approaches to minimize the effective response time between the identification of cyber security events, the consequent remediation of active events, and the prevention and elimination of future events. Every millisecond during a cybersecurity event can significantly impact an agency, potentially causing financial losses, reputational damage, the loss of intellectual property, PII, or classified data, or even damage to national security.

This is why speed and scalability are so critical to federal cyber teams — so they can create intelligent cyber threat metrics, capture and identify active cyber threats, and minimize false positives. In short, speed and extreme scalability of their data infrastructures enable federal cyber teams to bridge the gap between analysis of the threat landscape and real-time responses to threats as they happen. The best way to understand today's evolving threat landscape in real time is through immediate access to massive quantities of data that can leverage adaptive, self-learning algorithms.

Aerospike: An effective, real-time, data-centric approach to cybersecurity

The Aerospike Real-time Data Platform enhances AI/ML-driven systems that go far beyond typical deterministic, signature-based threat detection methods. Aerospike can ingest feature-store updates and deliver those feature-stores to active AI/ML models in real-time. For example, intelligent data can be delivered at both speed and scale to computation engines running self-learning algorithms that seek patterns of suspicious behavior on a network.

Many current customers use Aerospike's multi-cloud platform to analyze tens of billions of events per day — an order of magnitude greater than legacy Security Information and Event Management (SIEM) systems. The Aerospike Real-time Data Platform can ingest and store petabytes of disaggregated data from disparate sources that can then be used for securing networks, applications, and Internet of Things (IoT) systems.

Aerospike also leverages a wide range of existing continuous diagnostics and mitigation (CDM) solutions, including threat intelligence, endpoint security, access management, cloud security, Zero Trust, account security, user activity monitoring and emerging technologies for a truly end-to-end cyber security solution. The Aerospike Real-time Data Platform mitigates risk while also serving as a powerful competitive advantage to protect classified data and proprietary intellectual property.

Not only does Aerospike master extreme scaling when it comes to real-time data management, it does so within a minimal infrastructure footprint. A recent benchmark study, for example, illustrates that Aerospike delivers 4 million to 5 million transactions per second (TPS) with sub-millisecond latencies for read-only and mixed workloads. Conducted in collaboration with AWS and Intel®, the benchmark study shows exceptional results on a remarkably small 20-node AWS cluster powered by Intel® Xeon Scalable Processors. Furthermore, it proves that even with significant data growth and extreme workloads, the Aerospike Real-time Data Platform performs with hundreds of nodes less than other databases, saving up to $10 million per application in infrastructure costs.[1]

1 https://aerospike.com/blog/petabyte-benchmark/

Aerospike's benefits for Federal cybersecurity operations

With Aerospike, federal agencies can:

- Access petabytes of real-time and historical data to fight cyber attacks
  - » Capture spurious events, perform rudimentary packet analysis, and identify unusual network activity, all in real-time, as attacks occur
  - » Enable more effective AI/ML models without the need to spill, offload, or archive data
- Reduce infrastructure TCO
  - » Reduce server/node footprint up to 80 percent
  - » Decrease SIEM system ingestion costs
  - » Reduce infrastructure and data footprint associated with Snowflake, Splunk, Elasticsearch, and others
- Identify suspicious threat profiles
  - » Deploy Aerospike's petabyte-scale Graph Database, a graphical computing framework, to deliver faster, accurate insights into complex cyber environments
- Create once and grow without limits
  - » Extend existing cybersecurity and threat management infrastructure into real-time domains and enable ancillary data operations, such as offline AL/ML modeling stores
  - » Employ almost unlimited scalability while enjoying consistent performance

Conclusion

Aerospike changes the game in Federal cybersecurity by putting lightning-fast data at almost any scale to work on behalf of your agency's cyber operations. In summary, Aerospike retains petabytes of real-time and historical data to enable more effective AI/ML models; enhances real-time event processing and analysis of existing SIEM systems; advances your AI/ML capabilities; delivers real-time relationship-based analytics at petabyte scale; and reduces server/node footprints by up to 80 percent for incredibly low TCO.

To learn more about how Aerospike can deliver real-time, extreme-scale cyber vehicle operations to your agency, please go to aerospike.com/solutions/industry/public-sector/.

AEROSPIKE

Aerospike unleashes the power of real-time data to meet the demands of The Right Now Economy. Global innovators and builders choose the Aerospike real-time, multi-model, NoSQL data platform for its predictable sub-millisecond performance at unlimited scale with dramatically reduced infrastructure costs. With support for strong consistency and globally distributed, multi-cloud environments, Aerospike is an essential part of the modern data stack for Adobe, Airtel, Criteo, DBS Bank, Experian, PayPal, Snap, Sony Interactive Entertainment, The Trade Desk, and Wayfair. A global company, Aerospike is headquartered in Mountain View, California, with offices in London, Bangalore, and Tel Aviv.

2525 E Charleston Road, Mountain View, CA, 94043 | (408) 462-2376 | aerospike.com