GOVERNMENT

Improving the Nation's Cybersecurity

Executive Order 14028, "Improving the Nation's Cybersecurity" is an important step towards protecting against the increasing volume and danger of cyber attacks. This mandate reinforces the need for log and event management and explicitly notes the importance of collecting, sharing, and storing event data.

While the executive order and subsequent memos are unquestionably setting the right direction, there are challenges around cost and speed of delivery for this ambitious scope of requirements. Confluent stands ready to help agencies realize this new vision for federal cybersecurity by meeting the data demands and requirements while leveraging existing investments.

Bolstering Log and Event Management is Key to Cybersecurity

A central piece of the executive order is the collection, logging, and sharing of events in near real-time across tools and organizations. Collecting, correlating, and getting a view across events is the only way to be aware of all active and potential attack vectors adversaries can take. As with anything else, it's important to use the right tooling for the problem.

Security Incident and Event Management (SIEM) solutions are optimized for data at rest and search rather than data in motion, the way data about today's fast moving threat landscape should be accessed and analyzed.

"Rather than storing the data away in silos, where it's static, and bringing retroactive questions to the data, what you want to do is publish your data as a constant stream and deliver it to the questions for real-time analysis."

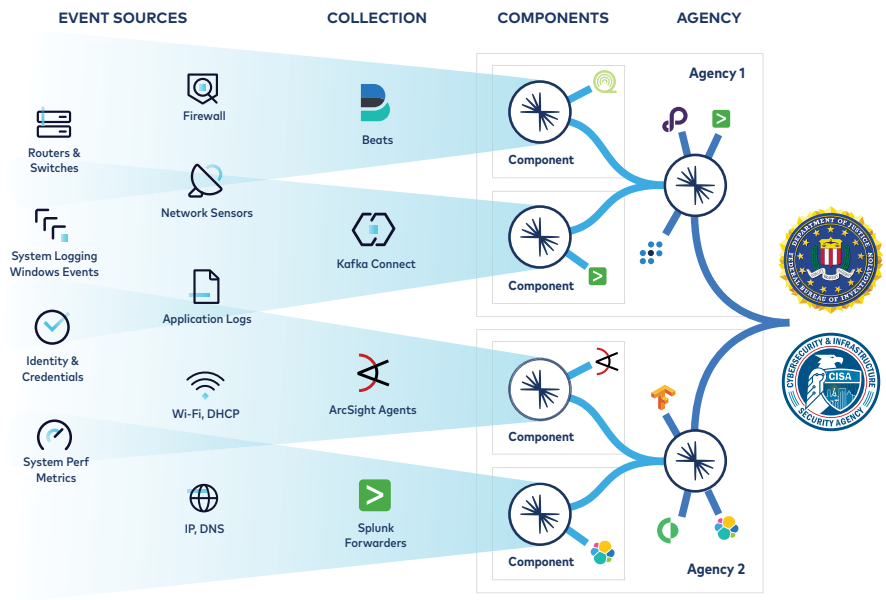
— WILL LAFOREST, CONFLUENT PUBLIC SECTOR CTO

Confluent, powered by Apache Kafka®, is the data-in-motion platform purpose-built for scalable, durable, and highly efficient event logging and sharing. Confluent enables customers to create a central nervous system so that tools can rapidly get the right data and feed it to organizations when and how they want it.

The Role of Data Mesh

Data mesh is an architecture that embraces the ubiquity of data in connecting processes. It decouples all the different actors within an organization, so they can all produce and consume independently. It views data as a product, a shift from the traditional monolithic data infrastructures focused on the consumption, transformation, and storage into numerous data stores of different types. Instead, data mesh allows each domain to handle their own pipelines and independently produce data for downstream consumers. Data mesh is the connective tissue between these domains and their associated data assets to create a universal interoperability layer.

Modern cyber defense architecture must move to event streaming to provide a data mesh for receiving, logging, processing, and sharing data with cyber defense tools like SIEM, SOAR, and Machine Learning. The commonly seen 1-to-1 direct data path is ineffective for enterprises that typically have multiple tools both commercial and open source, and operational environments that need to be able to selectively access data.



Confluent helps meet the Executive Order requirement for event forwarding and event log management in collecting, aggregating, routing, and sharing data.

Data in Motion in Practice

A large Defense agency program was responsible for supporting cyber defense across over 20 locations and multiple tiers as a shared service. In addition to monitoring and detecting threats they also needed to provide the data to numerous mission partners for their own operations. They found that using a SIEM vendor stack alone was cost prohibitive for the volumes of data they had. Additionally the SIEMs had to be treated independently and could not be tied together for a holistic, global view of the data and made it hard to share data with all the stakeholders. Finally, the SIEM was not designed for the volume of data ingestion and analysis required by the program and it often failed to meet performance requirements.

The agency began using Confluent as a data fabric for all the cyber data, running in all their locations where it receives and processes the data (normalizing, enriching, and routing with Kafka streams and KSQL). Confluent's multi-region replication aggregates up into regional hubs, and then into a central location.

This architecture allows them to perform real time data processing and analysis, allows their customers to subscribe to Kafka for the real time feeds of data that they care about while enforcing authorizations and permissions. It also decreases cost and improves scale, and makes global operations practical while optimizing network bandwidth.

Get Your Data Moving

A Data in Motion approach will enable a more proactive approach to cybersecurity while also:

- Reducing storage, network, and licensing costs
- Enabling tiered and cold storage out of the box to support OMB requirements in a cost effective manner
- Providing aggregation at the Component and Agency level through Confluent replication
- Leveraging existing cyber investments via connectors
- Making data available to FBI and CISA in real time with out-of-the-box capabilities
- Providing real time threat detection abilities at edge
- Enabling open ecosystem and preventing vendor lock-in
- Providing built in auditing to support requirements on tracking usage of data
- Providing RBAC to lock down data to only those who have a job related need
- Providing Schema catalog with APIs for sharing of data schemas with consumers

Getting your data in motion requires careful planning and the right partner. Confluent powers an event streaming platform with the needed flexibility, durability, resilience, and security required for complex, large scale cybersecurity operations. Confluent Platform supports Government goals of zero trust, logging, endpoint detection response, and software security.

Ready to get started? Contact a Confluent expert today

Email us on publicsector@confluent.io | Or visit confluent.io/get-started for more details