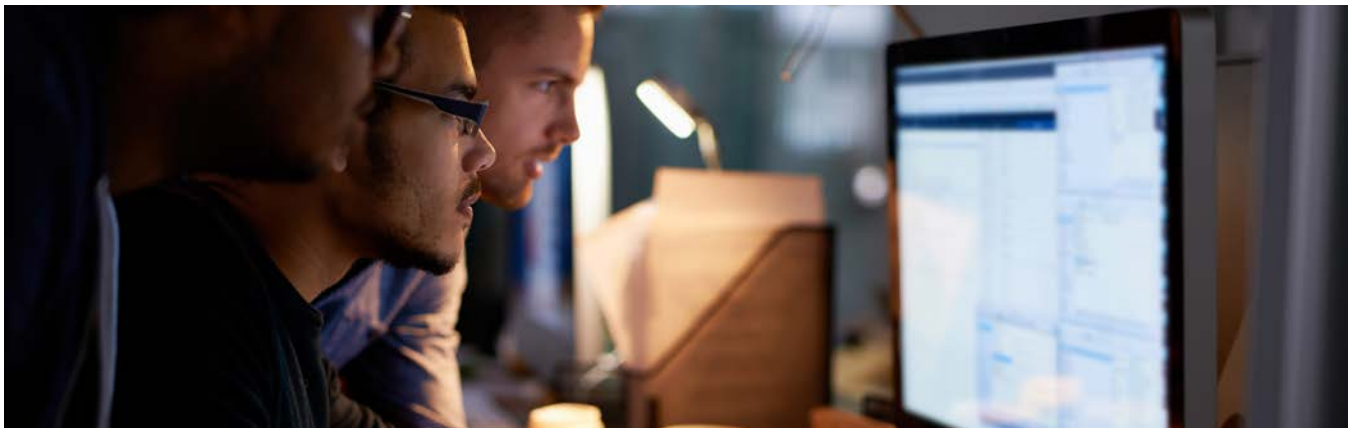


# ENHANCED CYBER-READINESS

## Cloudera's platform-based approach strengthens federal cyber posture

**82%**

of breaches happen in minutes. Quick detection and remediation contains the damage

**18**

minutes for state sponsored attacks to completely compromise the network

**8**

months on average before breach is detected

Cyberattacks are on the rise, as adversarial states and state-sponsored actors pivot quickly to take advantage of current events, including the disruptions associated with the COVID-19 pandemic. Cybersecurity is a significant problem for government agencies —a problem tailor made for big data.

Bad actors are leveraging an ever-expanding range of cyber exploits, with an emphasis on Advanced Persistent Threats. In these cases, an attack can unfold in mere minutes and once in the system, bad actors can live off the land for months or years, quietly exfiltrating vast tracts of sensitive information.

Heterogeneous infrastructures that include both legacy and cloud deployments put government at risk, with enormous volumes of data potentially exposed in both on-premise and modernized frameworks. Existing point solutions generate too many alerts, and there are simply not enough trained cybersecurity analysts available to investigate them all. Security Information Events Management (SIEM) applications typically cannot support the needed speed and scalability; nor are they able to effectively monitor the growing number of data generators at the edge—the rising tide of IoT.

Government agencies require a solution that empowers agencies to triage in real-time, with enterprise-ready security and governance built-in. They need an approach to cyber that makes data open and readily shareable across teams and across the hybrid multi-platform architecture.

### Why Cloudera Data Platform (CDP)

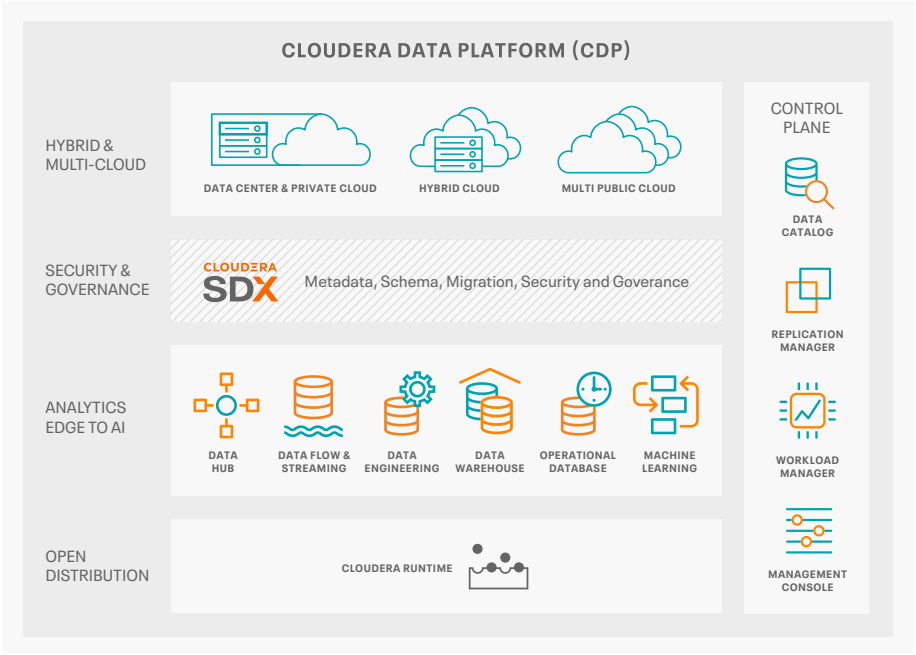
In the current environment, cyber-responders need to detect and collect all of the relevant log data and present high-fidelity alerts to analysts. They need analytics to investigate suspicious behavior, supported by alerts and automated responses. Responders also need the full context of events to understand how the attack repeats on the network, what resources were compromised, and how to remediate. Compliance teams need to retain all the required data for the required time period.

**Cybersecurity from Edge to AI with CDP**

- Prioritize cybersecurity events in real-time
- Detect advanced persistent threats
- Reduce false positives
- Leverage machine learning to assist analysts and threat hunters

The Cloudera Data Platform (CDP) addresses these needs. A platform-based approach to cybersecurity, CDP is horizontally scalable across the data center and the cloud. It allows users to share data securely with full governance, and it scales to multiple petabytes and thousands of users. This enables IT to store all of the needed context in support of investigation and remediation.

A suite of high-end capabilities, CDP makes available a common workbench where analysts can gain insight into both real-time and historic information, supported by machine learning and artificial intelligence.




Hundreds of government agencies spanning

**40+**

countries rely on Cloudera

Analytics functionality enriches the logs with organization-specific reference data about assets and users and applies threat intelligence supported by user behavior profiling, machine learning models, and other techniques to triage and prioritize threats.

The CDP hub stores prepared data in a scalable data warehouse that provides open and secure access for various use cases including behavior analytics, threat hunting, and security orchestration, and automated response. Investigators and compliance teams have years of data at their fingertips for thorough and accurate investigations and reports.

When data scientists are ready to explore and build models, Cloudera Machine Learning brings open source tools such as Apache Spark to support collaborative data science. Models can then be deployed to classify and identify threats and make the threat triaging even more effective. Visual apps, dashboards, and visualizations all help analysts make informed decisions.

## An Open and Shareable Solution

As an open-source solution, CDP frees government from the fiscal trap of vendor lock-in, while ensuring there are many capable eyes from a range of disciplines reviewing the code. Open source likewise offers a future-proofed solution, one that will continue to evolve as new threats and new defensive stratagems emerge.

**Why Cloudera**

Cloudera Data Platform enables organizations to effectively execute their data and analytics strategy to address current and evolving customer expectations.

EDGE TO AI ANALYTICS

Analytics for the complete data lifecycle combined in a single platform, eliminating the need for costly and cumbersome point products.

DATA SECURITY & COMPLIANCE

Maintains consistent data security and governance across all environments.

HYBRID AND MULTI-CLOUD

Delivers the same data management capabilities across all clouds and data centers.

100% OPEN SOURCE

Open compute and open storage ensures zero vendor lock-in and maximum interoperability.

**About Cloudera**

At Cloudera, we believe that data can make what is impossible today, possible tomorrow. We empower people to transform complex data into clear and actionable insights. Cloudera delivers an enterprise data cloud for any data, anywhere, from the Edge to AI. Powered by the relentless innovation of the open source community, Cloudera advances digital transformation for the world's largest enterprises.

Learn more at cloudera.com

CDP's shared workbench is customizable to ingest many different commonly used cyber machine system source and application protocols. It can ingest telemetry data from a range of sources including both legacy and cloud applications, as well as the growing galaxy of edge data sources. By storing logs over the long term—literally billions of rows of transaction and petabytes of storage—Cloudera is able to leverage machine learning to seek out long-term trends.

The platform shifts cybersecurity from reactive to proactive mode, enabling analysts to better identify potential chinks in the armor before the enemy can exploit those vulnerabilities. This empowers resource-constrained government agencies to make the most effective use of their human capital.

As a common framework underlying the SIEM environment, CDP is able to put big data to work as a critical tool in the cybersecurity arsenal. Long-term analytics in turn enable the system to more readily identify potential anomalies—suspicious instances that might otherwise go undetected.

## A Seamless and Transparent Transition

Government agencies have invested heavily in a wide array of security solutions, and it makes little financial sense to scrap those in favor of something new. Understandably risk-averse, IT leaders are loath to contemplate a rip-and-replace solution to their cyber woes.

Nor do they need to consider such drastic measures. Cloudera's solution works in association with existing SIEM approaches, giving analysts a common framework supported by big data and key analytic tools. Adoption of CDP is invisible to the end-users: what is noticed is better, timelier information. The transition to CDP is both seamless and transparent, bringing to bear new tools and new efficiencies without disrupting the existing cyber workflow or introducing new risk.

As an open-source, platform-based solution, CDP solves a number of key problems for federal IT leaders. Unlike conventional SIEM solutions, it delivers the scalability needed to safeguard an ever-widening threat surface, along with the flexibility needed to adapt to the constantly changing landscape of data sources and network connections. Rather than add complexity to an already complex endeavor, the shared workbench approach simplifies the routine work of cyber hygiene, freeing key personnel to devote their attention to higher-level tasks going forward.

Learn how Cloudera allows government agencies to put data to work at cloudera.com/solutions/public-sector.

CLOUDERA

Cloudera, Inc. 5470 Great America Parkway, Santa Clara CA 95054 USA cloudera.com