



# Why data is a critical cybersecurity tool

AI-powered analysis of system data can help agencies strengthen their response to cyberthreats



**Carolyn Duby**  
Field CTO and Cybersecurity Lead,  
Cloudera

**D**ATA PLAYS AN INTEGRAL ROLE in the government's efforts to secure its systems from cyberattacks. It is the key to deriving deeper insights into agencies' networks and boosting their ability to hunt for threats rather than just respond to them.

Each cybersecurity tool collects data based on a specific point of view. By bringing all the point solutions together, agencies can gain a fuller understanding of what's happening in their networks and can then detect, respond to and investigate threats.

When agencies combine all that data over a long period of time, they have the ability to go back and see how an intrusion occurred, how to stop it and how to prevent it from happening again. Furthermore, when agencies have all the information they need, they can proactively look at their networks and see if something is developing that they haven't seen before.

## AI and behavior-based threat detection

Success in this area requires agencies to move to a real-time ingestion protocol. They should adopt a platform that can ingest many types of data in diverse formats and put everything into a schema that is consistent across all the different sources. In addition, the platform must be able to adapt to varying amounts of data so that

it can scale up or down to ensure optimal performance and cost-efficiency.

Once agencies have gathered their data in a scalable, flexible platform, they can apply artificial intelligence to derive insights from the data. AI speeds analysis and is particularly effective when agencies move from signature-based to behavior-based threat detection. A signature-based approach is good for detecting threats we already know about, but a behavior-based AI approach can adapt to new threats by looking for anomalies such as changes in the behavior of a server or endpoint device.

AI also helps with investigations by

reconstructing the sequence of events that happened during an intrusion, which fuels agencies' ability to prevent future attacks. With AI, agencies can start to apply more sophisticated algorithms in their hunt for vulnerabilities and cyberthreats.

## Strategic alliances with industry leaders

Many breaches occur because of cybersecurity hygiene issues and misconfigurations. At Cloudera, we're looking for ways to avoid those common problems by, for example, evaluating system logs to identify misconfigurations before they become vulnerabilities or





**When agencies have all the information they need,** they can proactively look at their networks and see if something is developing that they haven't seen before.



uncover anomalies such as employees who have access to a particular system that few or none of their peers are authorized to access.

That approach could also help agencies automate security compliance. When AI is used to analyze comprehensive sets of data, agencies can more readily ensure that they're adhering to government mandates and following good cyber hygiene principles.

At Cloudera, we are constantly

expanding our ability to support agencies' cybersecurity needs by building strategic alliances with other industry leaders. For example, our partnership with NVIDIA is helping us accelerate our use of AI and increase our efficiency. NVIDIA's expertise also contributes to our products' scalability and effectiveness.

In addition, we have combined Cloudera's Data Cloud with Raytheon Intelligence and Space's REDPro platform

so that agencies can fully harness the power of their data, regardless of where that data lives.

Agencies have valuable data at their fingertips. By putting the latest technology to work, they can become more forward-thinking and develop stronger, more effective cybersecurity strategies. ■

**Carolyn Duby** is field CTO and cybersecurity lead at Cloudera.

# There's never been a better time to move forward.

Delivering vaccines to millions of people **in months, not years.**

Reducing winter weather management operations from **2 days to 35 seconds.**

The right data is a springboard for leaders who want to bring their vision to life faster, sooner. Cloudera's enterprise data cloud platform helps our customers move their teams and their organizations forward to thrive.

[cloudera.com/publicsector](https://cloudera.com/publicsector)

**CLUDERA**  
Data That Moves You