How to Share Data Efficiently and Securely Across State and Local Government Lines

Governments increasingly need to share data across state and local boundaries. Whether they're monitoring purchases of prescription opioids, collaborating on criminal investigations, coordinating health and human services, or performing a wide range of other activities, state and local governments face significant challenges in cross-jurisdictional data sharing. Who owns the data? What's the most effective way to share? How can they maintain data privacy and security?

In this Q&A, Jared Pane, senior lead solutions architect at Elastic in Mountain View, Calif., talks about these issues and discusses solutions that make data sharing efficient, cost-effective and safe.

What are the most challenging aspects of sharing data across state, municipal and county lines?
When two or more government entities share data, they need to enforce policies on who can access which data, and for what purposes. These policies may vary from one jurisdiction to the next. Governments need to control who can manipulate data, and when someone does make changes, they need a single source of truth to keep the information consistent. They also need standards, protocols and technologies to protect the data. Many state and local agencies are using legacy technology that doesn't provide visibility into who's accessing data, how they're using it or whether they're changing it. That can create major problems for data integrity and security.

How do Elastic's solutions help with those ownership issues and the ease of data sharing?
Elastic provides a single trusted store of data that multiple agencies and jurisdictions access in a single environment. Because the technology resides in the cloud, users can start sharing almost immediately, with no need to implement new hardware and software. Also, Elastic lets users scale their systems horizontally rather than vertically, adding new virtual nodes as data volume swells and agencies add more users. That ease of deployment provides tremendous flexibility.

How does Elastic promote security across siloed state and local government systems?
Pane: Our security features — such as role-based access to data, encryption, and field- and document-level security — are available right out of the box. The technology includes full threat hunting capability, which allows agencies to not only monitor suspicious activity, but take proactive measures to protect their data and infrastructure. Our data sharing capabilities are all API-based, with an API keys management system that lets users monitor who is doing what, when, where and why. In addition, everything is encrypted from end to end.

To sum up, what features should governments look for in a solution for sharing data across state and/or local government lines?
Ease of implementation is important. So is flexibility. You don't know how data sharing policies will change in the coming years, or which additional local, state or federal agencies will need to access the data. If the system is easy to scale, it can evolve along with government needs. Look for a system with role-based security, limiting access to data based on who needs it and is authorized to use it. Finally, look for a system that complies with important security standards such as the Federal Information Processing Standard (FIPS). In short, to meet the need for cross-jurisdictional data sharing, seek a system that offers ease, flexibility, scalabilty and strong security.

elastic

Info