Three Ways Digital Transformation Thwarts Government Fraud

Digital transformation opens new channels for providing and consuming services; this journey is fundamentally changing the end-user experience. Evolving technology, expectations, and the threat landscape also have profound effects on the operations of customer-facing organizations, including government agencies providing citizen services.

In both finance and the public sector, sensitive data such as personally identifiable information or financial records are necessary for institutions to provide services—but they're also prime targets for fraud and theft carried out online. However, with the right security architectures, protective measures, and expertise, banks, regulators, and government agencies alike can better deter fraud and financial crime.

1 Pro: Masses of end-users' data is online, so it's easier to offer better, tailored services.

Con: Masses of end-users' data is online, so it's easier to use for nefarious purposes.

The federal government's emerging requirements for improved citizen experience have agency leaders looking to industry for ways to be customer-friendly. Want to access your accounts, renew your tags, apply for a loan, or reach a live person? Your bank's app on your phone can do much of that in an instant, and agencies are catching up.

But that ease of access can also be afforded to someone pretending to be you—or someone who doesn't even exist. After months or years, a fake persona created through data found online can access untold money through credit lines or loans. In the public sector, fake personas can be used for smaller-scale financial crimes like payroll fraud—or worse, particularly at larger organizations.

Money laundering is a chief concern: For example, it's how criminals profit from the $150 billion-per-year forced-labor industry. It's also heavily used to finance terrorist activities. The push to orient around consumers has created countless new end points, and as a result, systems are straining under the weight of billions of dollars' worth of malicious behavior.

©2019 Cloudera, Inc. All rights reserved. Cloudera and the Cloudera logo are trademarks or registered trademarks of Cloudera Inc. in the USA and other countries. All other trademarks are the property of their respective companies. Information is subject to change without notice.

2 All that data produces substantial gains.

What customers buy (and when, where, and how), citizens' interactions with government institutions, and a host of other online behaviors generate volumes of data that can paint a comprehensive picture—especially when it's layered with other information, such as bills, bank accounts, car insurance, or most-visited websites.

All of that data is a boon for government agencies embracing the technological curve, tracking citizen activity to better meet their needs and monitoring network activity to detect anomalous behaviors. The latter goals may vary by agency—they may be seeking terror suspects, human traffickers, or federal employees engaging in corruption—but they're using the same tools: hackathons, data analytics, and advanced algorithms, to name a few.

A significant hurdle, though, is that public- and private-sector organizations often rely on databases that only store months' worth of data. But these crimes can span years, and those high-tech tools only work if applied to massive pools of diverse data capturing long-term transaction histories. In the case of at least one Cloudera customer, after instituting a more-comprehensive solution through which years' worth of network activity could be accessed, processed, and analyzed, the organization discovered a billion-dollar fraud scheme that had been under way for years.

3 Making sense of it all can improve government—and help prevent financial crime.

Whether you're a bank, a regulatory body or a government agency, no matter how much you're investing in security, there's always more to do. Not only are threat actors becoming more sophisticated, digital transformation and the customer journey continue to evolve. While the data deluge can be overwhelming, organizations can use those mass quantities of information to understand their networks and consumers, to balance the end-user experience and the expanding threat landscape, and to safeguard against fraud and other financial crimes.

Here are a few ways Cloudera solutions can help do that:

- ✓ Create data lakes under forward-leaning architectures that offer large-scale storage. These can then be used to search, analyze, report on, and improve the citizen experience as well as the institution's security—and reputation.
- ✓ Augment existing networks and systems with open source technology that is constantly evolving and improving, offering cutting-edge algorithms that can detect anomalous behavior.
- ✓ Understand how data moves through an organization. Think of it like the food supply chain: Where does the data originate, and where does it go from there? What happens to it along the way? Who can touch it? Like the food supply chain, data provenance and lineage are sensitive.
- ✓ Institute a variety of defenses. We know by now that perimeter defense alone cannot provide adequate security; layered network defenses that extend to end points are critical. Equally important is the ability to perform internal analyses, including on employees and relevant individuals. Many breaches start internally, so including everyone and everything that can factor into security helps maintain a holistic picture and stronger, proactive defenses going forward.

©2019 Cloudera, Inc. All rights reserved. Cloudera and the Cloudera logo are trademarks or registered trademarks of Cloudera Inc. in the USA and other countries. All other trademarks are the property of their respective companies. Information is subject to change without notice.