GUEST COLUMN CYBERSECURITY AUTOMATION

Intelligent Automation Can Dramatically Improve Cybersecurity

Tools automate routine tasks, so federal agencies can respond more quickly and effectively to cybersecurity threats.

Kirke Everson
Government Intelligent Automation Lead
KPMG LLP

Tony Hubbard
Government Cybersecurity Lead
KPMG LLP

Federal agencies have plenty to keep themselves busy these days. Mission and business requirements are expanding in size and complexity; and internal and external stakeholders are expecting more capabilities. Agencies are upgrading legacy systems to better support digital experiences, while ensuring ever-increasing data volumes remain secure, even as employees access data with an expanding variety of mobile devices.

The nature and extent of cybersecurity vulnerabilities also continues to expand, evidenced by the most recent ransomware attacks Petya and WannaCry. Despite this challenging environment, many agency budgets have grown by meager amounts, remained stagnant, or been cut. Help is on the way. Intelligent automation has the potential to dramatically impact the federal mission, business, and cybersecurity environment.

THE CHANGING THREAT LANDSCAPE

Protecting information used to mean simply warding off the bad guys at the network perimeter. That traditional "castle and moat" motif no longer applies. Criminals attack systems at every point, from the network to the application to the data itself.

The profile of the modern cybercriminal has also changed dramatically. Agencies now tussle with everything from maladjusted individuals and disgruntled insiders, to organized crime groups and even malevolent foreign powers. In response, the number of compliance laws continues to expand. For example, with the NIST SP 800 171 requirements in place, agency CIOs must ensure Department of Defense technology contractors, as well as full time employees, keep data safe. Furthermore, there are innocent employees who inadvertently create threats, for example, clicking on a phishing link in an e-mail.

Complicating the threat landscape is a shortfall in talent. A search of open cybersecurity positions on job site Indeed.com alone turned up 10,640 open positions in the U.S. The manpower shortage is only getting worse. A recent report from the U.S. Government Accountability Office notes more than 30 percent of U.S. federal employees are eligible to retire.

As large numbers of federal employee vacate their positions, who will take their place? And the federal government competes for personnel with the private sector, which also has significant needs. The top five U.S. firms in terms of stock valuations—Alphabet (Google's parent company), Amazon, Apple, Facebook, and Microsoft—are all investing heavily in cybersecurity.

THE NEED FOR SOMETHING NEW

The evolving threat landscape and limited resources drives the need for new approaches for protecting government data. Intelligent automation, the automation of mission delivery and business processes

by leveraging digital technologies, is emerging to fill the void. Also referred to as Robotic Process Automation, intelligent automation applies to a wide range of processes and technologies. Easily built digital robots can ingest massive amounts of data, look for patterns, make decisions faster than humans, and automate manual tasks. Intelligent automation's low cost, non-invasive and rich capabilities can help government agencies tackle projects previously seen as too complex or too costly.

While the term intelligent automation may be new to some, the technology is already in use across many industries, supporting processes such as user password resets. Instead of technical support personnel making those changes, the system does it itself—with user input.

Other intelligent automation applications are rapidly emerging. Managing system access and reviewing audit trail data have been a constant struggle for cybersecurity professionals. These processes are historically manually intensive, inefficient, and often prone to error. Intelligent automation can make these processes much more efficient and accurate, instead of merely sampling audit log data, a "bot" can examine all transactions and identifies potential threats.

Identity proofing is another potential area of interest. As agencies open their systems to the public, they need to be sure citizens—and not malware bots—are logging in to input data, such as mailing addresses and other personal information. Intelligent automation solutions can monitor such transactions, identify anomalies, and help prevent fraudulent transactions.

INTELLIGENT AUTOMATION IN ACTION

These use cases are more than just theory. Following the Department of the Navy's "comply to connect" policy, the U.S. Marine Corps relies on intelligent automation to automatically scan and evaluate cybersecurity threats as its users log in. After a system initially passes muster, the solution checks it hourly to ensure its connection remains secure.

KPMG is supporting government agencies in evaluating how intelligent automation can elevate the efficiency and quality of its data collection and cybersecurity processes. Intelligent automation can offer government agencies many benefits. These solutions deliver greater agility in responding to regulatory changes, more consistent cybersecurity processes, and more accurate transaction data.

Agency personnel can also benefit from workflow changes. Staff members are freed from mundane cybersecurity tasks and are thus available for more strategic duties; such as planning, research, and data analysis. For instance, employees who previously focused on data aggregation can now invest their energies in mission-focused and consumer facing system improvements.

FIND THE RIGHT PARTNER

So what should an agency look for when searching for an intelligent automation solution? First, they need a partner to help them though the evaluation process. Instead of leading with one product, the firm should have a variety of solutions at its disposal and identify the best one for the agency's use case.

"Intelligent automation solutions can monitor ... transactions, identify anomalies, and help prevent fraudulent transactions."

Nowadays, agencies face significant challenges in securing their systems. Intelligent automation can help government agencies transform business processes, reduce costs, improve citizen experience and workforce satisfaction, and truly keep their information safe.

This article represents the views of the authors only, and not necessarily the views or professional advice of KPMG LLP. The KPMG name and logo are registered trademarks or trademarks of KPMG International.