AI and Automation: The Next Leap in Federal Cybersecurity

This combination of power and portability gives agencies an in-house AI security capability they can use to protect sensitive data and operational technology (OT) environments.

Federal agencies have been harnessing some form of artificial intelligence (AI) and automation for years. While government has gained an increased understanding of how to do robotic process automation (RPA), many users are still operating in the nascent stages — using the technology to do rote tasks at speed.

This means agencies are only utilizing a fraction of RPA's potential. Part of the challenge now is getting agencies pointed in the direction of AI-informed RPA — intelligent automation (IA). When you start introducing IA and letting the algorithm have access to different sources of data and different kinds of connections, it can both improve productivity and raise the stakes for cybersecurity.

Fortunately, this move to from 'simple RPA' to IA is also playing out in cybersecurity in a fashion that addresses two biggest concerns we're seeing from federal partners — how do we deal with all of the security data coming in from sensors, and how do we respond when we see threats or anomalies?

Jim Richberg
Public Sector Field CISO
and VP of Information Security
Fortinet

Addressing Pain Points

Federal agencies have come to us wanting options and solutions for dealing with the torrent of security-related data being generated by network devices and sent to their operation centers. One agency told us they receive 50 TB of data per day and keeping up with that torrent of information is impossible task for analysts. However, RPA and IA can help make sense of this data flow in real time.

The same goes for the second challenge facing federal agencies — how and when to respond to potential security problems. In an age when ransomware can rapidly encrypt key portions of an agency's data, security orchestration and response must leverage IA to respond in seconds. Humans simply can't identify and quarantine threats that quickly.

AI-driven RPA applications like FortiAI are designed to address both of these pain points. They alleviate the tedious manual investigation of security alerts and threat response by automatically investigating and classifying threats and malware outbreaks in seconds and blocking them in the network.

Tools Turn Challenge Into Opportunity

These tools can also turn a challenge into an opportunity. For many organizations, the sheer size and complexity of their digital attack surface can be overwhelming. But specialized security AI can turn a complex IT environment into a collection platform capable of detecting malicious cyber activity before it succeeds and of learning from attacks directed against other targets.

Fortinet has been developing and using AI in an ever-expanding part of its cybersecurity product portfolio for more than 10 years.

This AI-driven cybersecurity is only getting more powerful. Fortinet has been developing and using AI in an ever-expanding part of its cybersecurity product portfolio for more than 10 years. Much of the core power of its enterprise-grade solutions also can be achieved in smaller versions of AI consisting of millions — as opposed to billions — of neural network nodes.

Similarly, while Fortinet's Fabric AI solution learns from an average of 100 billion pieces of data each day, research has demonstrated that a much smaller set of custom-curated training data is enough information to enable the lightweight version of this security AI to be 99%+ accurate out of the box; and to rapidly become more accurate as it learns from customer data.

This combination of power and portability gives agencies an in-house AI security capability they can use to protect sensitive data and operational technology (OT) environments.

The federal government is only just discovering the power of AI-driven automated cyber operations. But agencies shouldn't fear diving in, since there are proven and powerful commercial solutions they can leverage to take the leap into the next level of cybersecurity.

With a partner like Fortinet Federal, IT managers can harness leading-edge solutions to some of the most complex cyber challenges we face today. ■

About The Author

Mr. Richberg's role as a Fortinet CISO leverages his 30+ years' experience leading and driving innovation in cybersecurity, threat intelligence, and cyber strategy & policy for the U.S. Government and international partners.

Prior to joining Fortinet, he served as the National Intelligence Manager for Cyber, the senior Federal Executive focused on cyber intelligence within the $80B+/100,000 employee U.S. Intelligence Community (IC). He led the creation and implementation of cyber strategy for the 17 departments and agencies of the IC, set integrated priorities on cyber threat, and served as Senior Advisor to the Director of National Intelligence (DNI) on cyber issues.

FORTINET

Better threat intelligence and compliance for your agency. Everywhere you need it.

Protect the possibilities with Fortinet Federal.

With Fortinet AI-driven security operations, federal agencies are equipped to detect, mitigate, and prevent advanced persistent threats, while improving security awareness and compliance management.

Learn more at www.fortinetfederal.com.