DELL TECHNOLOGIES

Why AI is a game changer for cybersecurity

AI's lightning-fast analytical capabilities make it a natural fit for modernizing threat detection and response

Dirk Wiker
Dell Technologies

Artificial intelligence can be used to analyze very large quantities of data at speeds and scales humans aren't capable of, which has profound implications for securing government systems. Before I joined Dell Technologies, I led cybersecurity operations teams at a couple of federal agencies. I realized that technologies like AI and machine learning are absolutely necessary for government security analysts to make sense of the massive number (sometimes millions) of cyberthreat alerts they receive on a daily basis.

Finding the threat is like finding a needle in a haystack. AI is crucial because it can identify patterns, anomalies and potential threats by sifting through huge amounts of data from a variety of sources very quickly. For example, information on network traffic, user behavior patterns and past security incidents are all stored in a security information and event management solution.

> "AI can help automate routine cybersecurity tasks to free analysts to focus on more complex challenges such as in-depth threat hunting."

AI can also find things that don't necessarily look like threats on their own, but when taken together with other indicators, they could signal an incoming attack. For example, zero-day threats can be much easier to pinpoint ahead of time with AI. In addition, AI can help automate routine cybersecurity tasks to free analysts to focus on more complex challenges such as in-depth threat hunting.

How AI maximizes the benefits of zero trust

The zero trust approach to cybersecurity operates on the principle "Never trust, always verify." The approach requires verification from anyone trying to access resources in a government network, regardless of whether they are inside or outside the network's perimeter.

AI can maximize the benefits of a zero trust approach by making real-time decisions about access requests based on a continuous assessment of trust and risk factors. That involves analyzing user behaviors, the security of a user's device and other contextual information to enforce policies in a dynamic way.

In addition, AI can be used to classify and tag data in an automated fashion to facilitate an enforcement technology such as data loss prevention or digital rights management. AI enhances the detection of malicious activities and anomalies by analyzing data from multiple sources for signs of compromise. The technology can then be used to help automate responses, such as isolating an affected system or revoking a user's access.

iStock

Pairing hardware with best-in-class security solutions

Dell can help agencies incorporate AI into their cybersecurity efforts through a combination of hardware, software and services tailored to meet the government's unique challenges. We also offer several Dell-validated designs with AI-ready solutions that support the complex algorithms and machine learning models that enable agencies to detect, analyze and respond to cybersecurity threats more effectively.

No single product or suite of products from a single vendor can offer everything an agency needs to implement zero trust. That's why Dell pairs our hardware with best-in-class security solutions from our large network of partners. For example, we are developing an end-to-end zero trust architecture called Project Fort Zero that implements all applicable 152 activities in the Defense Department's Zero Trust Strategy by incorporating security solutions from close to 40 partners. It takes the integration effort away from government agencies so they can simply migrate workloads to the platform.

Finally, Dell's consulting and professional services can guide agencies as they plan, implement and manage the integration of AI into their cybersecurity initiatives. We help them identify opportunities for AI enhancement and provide ongoing support and training so they can optimize their use of AI in securing government systems. ■

Dirk Wiker is chief cyber/zero trust architect at Dell Technologies, Federal.