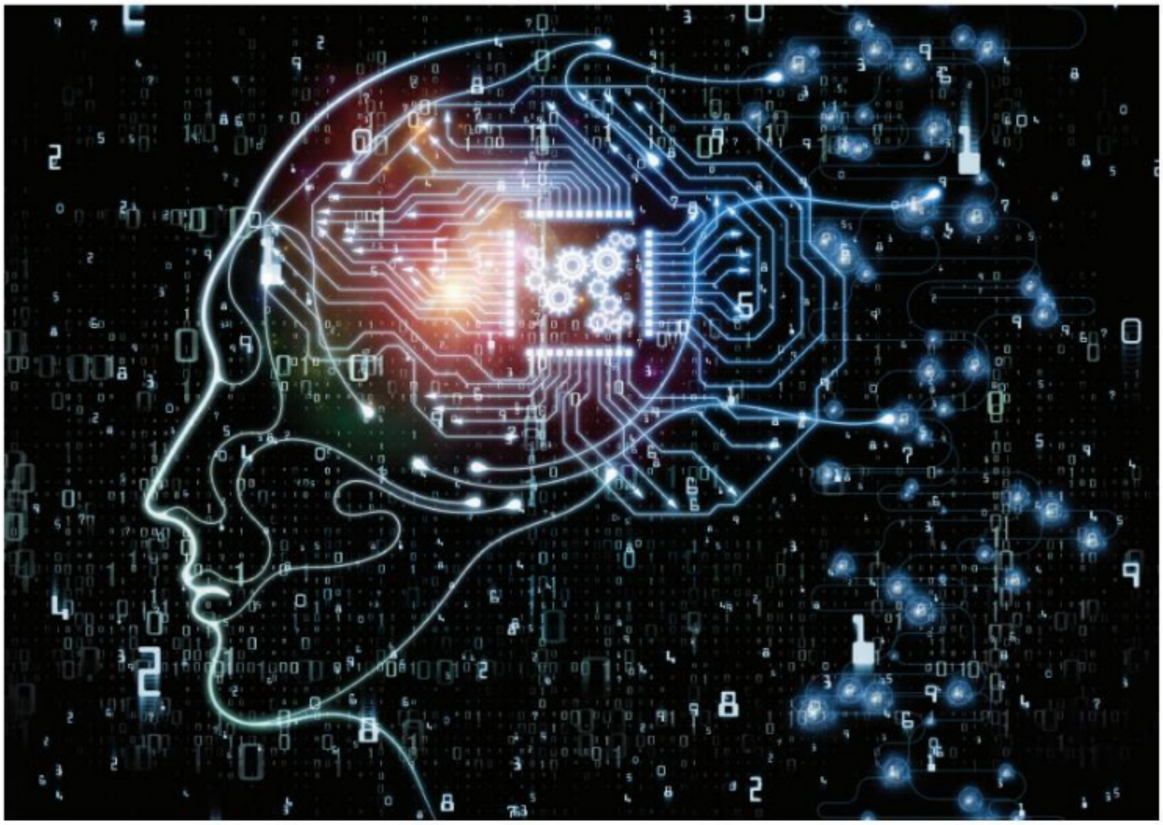

GETTY IMAGES

Built-in Protection

Artificial intelligence and machine learning combat cybercrime

BY BRITTANY SHOOT

Increasingly, major technology firms are recognizing the need to augment their systems with artificial intelligence (AI) and machine learning (ML) to help software engineers thwart massive data breaches such as those at Equifax, Sony Pictures, Target and the U.S. Office of Personnel Management.

Automated protection against cybersecurity threats can catch potential risks humans may miss, by monitoring more data, and sending reports to humans for further investigation.

Cloud computing service giants, including Oracle and Amazon Web Services, have introduced embedded, AI-driven security features engineered directly into the platform to monitor irregular activity, maintain overall system operability during regional outages and planned maintenance, as well as patch security holes as needed.

Other cloud application platforms built on compliance and security, such as Box and Salesforce, also increasingly offer more and better protection against network vulnerabilities to guard sensitive customer information.

Matt Haney, the CEO of network security firm Universal Network Solutions Inc., says that while not new, machine learning and artificial intelligence are receiving a lot of attention due to increased public awareness about cyberthreats, as well as crucial advances in technology.

“Cloud adoption coupled with AI have allowed organizations to collect and analyze data without

Larry Ellison, Oracle's co-founder and chief technology officer, announces the company's first autonomous database.

ORACLE

impacting the organization it is trying to protect," says Haney.

Augmenting human engineering skills with automated processes has never been easier, and AI and ML-led features can offer crucial protection for any business with data in a private or public cloud.

Strong network architecture is the first line of defense for protecting sensitive data, so it is especially necessary to maintain a fortified firewall against malicious attacks.

"A successful attack on a database system can cripple a company or even a whole country," warns Juan Loaiza, senior vice president of systems technology at Oracle, a company that is garnering much buzz with its new autonomous database unveiled in 2017.

> **"Cloud adoption coupled with AI have allowed organizations to collect and analyze data without impacting the organization it is trying to protect."**
>
> *— Matt Haney, CEO of Universal Network Solutions Inc.*

The AI-driven database aims to constantly identify and patch security vulnerabilities in real time, working even quicker than the most nimble security experts can operate to stay ahead of hackers.

Loaiza adds that applying machine learning to securing the network is just one more way to help customers minimize risk and protect their data and systems: "A majority of cyberattacks exploit software vulnerabilities that have existing patches." The most recent high-profile example of this was the Equifax breach, which occurred because a known vulnerability in the application system hadn't been patched.

Engineering additional automated protections can keep hackers at bay, but Haney warns that humans continue to play a crucial role in supporting even the most robustly engineered security systems.

"Machine learning still requires a person to define, build and test the program," Haney emphasizes. "But machine learning does offer a hope of simplification, scalability and even automation in an industry ripe with complicated products." ■