FORTANIX

The importance of a data-first approach to security

A unified security platform augments a zero trust model to protect data across its life cycle

Patrick Conte | Fortanix

For years, the government has focused on protecting data without taking the last step, which is making sure all data has a security policy applied to it. To enable employees to work with the data, agencies typically decrypt it and move it to a destination server on premises, in a private cloud or in a public cloud. But that decrypted data is vulnerable to interception.

Government and industry have tried to create moats around those servers with zero trust, identity and access management, and endpoint security. At some point, however, bad actors will find their way through those moats, and then they can use modern techniques such as memory scraping, man-in-the-middle attacks or social engineering to gain access to the data on those servers.

Taking advantage of confidential computing

To address those vulnerabilities, Fortanix has built a unified Data Security Manager based on a leading-edge technology called confidential computing, which relies on encrypted memory to protect data at every stage of its life cycle.

Our single platform replaces a whole host of legacy data security solutions. Because we use encrypted memory for holding keys, we can build a global key management solution for workloads across all IT environments. And we can add advanced kinds of encryption such as tokenization, which preserves the format of the data, and secrets management for development environments.

In addition, when we put our software-based solution inside a tamper-proof server, it achieved certification at FIPS 140-2 Level 3. All the encryption, key management and cryptographic capabilities are managed in our device, but the data can live anywhere, which gives agencies a huge amount of flexibility.

Quantum-safe keys and secure AI

When bad actors finally have access to quantum computers, they'll be able to crack existing encryption algorithms very quickly. Agencies can use our technology to begin adopting quantum-safe keys for their most valuable assets, which will save them a lot of heartache in the next five to 10 years when quantum computers come on board.

In addition, everyone is talking about artificial intelligence, but for the most part, they're talking about how to use it when the bigger challenge is how to secure it. However, many forward-thinking government agencies are using the Fortanix Data Security Manager to protect their AI environments so they can securely perform advanced analytics on even the most sensitive and valuable data.

With our technology, the government can make the most of its data and rest assured that its most valuable resource is protected at rest, in motion and in use, even if zero trust fails. ■

Patrick Conte is vice president and general manager for the Americas at Fortanix.