The importance of **future-proofing cybersecurity**

The latest security advances are keeping pace with ever-changing threats to government networks and data

Gina Scinta

Thales TCT

Over the years, it has become clear that security must be top of mind in all activities. It's much easier to incorporate security at the beginning of a project than try to retrofit it into that project later. Perimeter-based security is no longer sufficient. Data is now the perimeter, and therefore, the most effective way to secure data is by applying protections to the data itself, not just to the perimeter.

Bad actors are always trying to access government data whether it's housed on premises, in the cloud or at the edge. Therefore, it is necessary to apply the proper access controls to limit who or what has access to data and prevent bad actors from reaching it.

In the wake of major data breaches, such as SolarWinds and Colonial Pipeline, the White House Executive Order on Improving the Nation's Cybersecurity (EO 14028) and the National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (NSM-8) mandate the use of several security best practices to protect data.

Securing data from core to edge

Access control through multifactor authentication is an important aspect of both directives. The combination of username and password is not sufficient to secure access to IT systems. Agencies also need to deploy strong multifactor authentication that relies on some type of hardware- or software-based token for granting access to the environment and then to the data. Furthermore, the White House executive order mandates the protection of data through encryption not only when it is at rest but also when it is moving to and from the network edge and beyond.

Security becomes even more important at the edge. Data generated and collected at the edge is often very sensitive. Agencies must be able to apply the same level of security deployed in the core and the cloud to edge environments in order to adequately protect data.

In addition, containers are becoming an increasingly important component of edge computing as part of the evolution from servers to virtualization, and industry leaders like Thales TCT are focused on providing ways to secure data used by containers.

Cryptography for a post-quantum world

Cybersecurity concerns continue to evolve, and a hot topic is the impact that quantum computing will have on today's encrypted data. It's only a matter of time until quantum computers will be able to break the classic PKI-based cryptography currently used to encrypt data. When that happens, data previously harvested by bad actors will be vulnerable to decryption and exposure. Agencies need to protect their data today with crypto-agile solutions that support classic cryptography and emerging quantum-resistant standards.

Pawel Czerwinski

> Bad actors are always trying to access government data **whether it's housed on premises, in the cloud or at the edge."**

The National Institute of Standards and Technology (NIST) recently announced its selection of four quantum-resistant cryptographic algorithms that will form the basis of a post-quantum standard, and NIST expects to finalize that standard in the next two years. In the meantime, however, agencies should evaluate their PKIs and identify any weaknesses. Then they can future-proof their systems by adopting solutions that are crypto agile, meaning they will be able to utilize classic cryptography today and post-quantum cryptography without costly retrofitting.

At Thales TCT, we have already embedded some of NIST's approved quantum-resistant algorithms into our encryption solutions so that we can offer a test bed for our customers to experiment with these new and exciting security options. We are also participating in the Migration to Post-Quantum Cryptography Project with the NIST-hosted National Cybersecurity Center of Excellence.

All those activities are part of our ongoing commitment to offering innovative solutions to the government's most pressing security challenges. ■

Gina Scinta is deputy CTO at Thales Trusted Cyber Technologies.