NIST Recommends Zero Trust Approach to Cloud Security

Continuous monitoring of assets on a cloud server amplify security and privacy.

Kate Macri

Mon, 12/28/2020 - 11:11

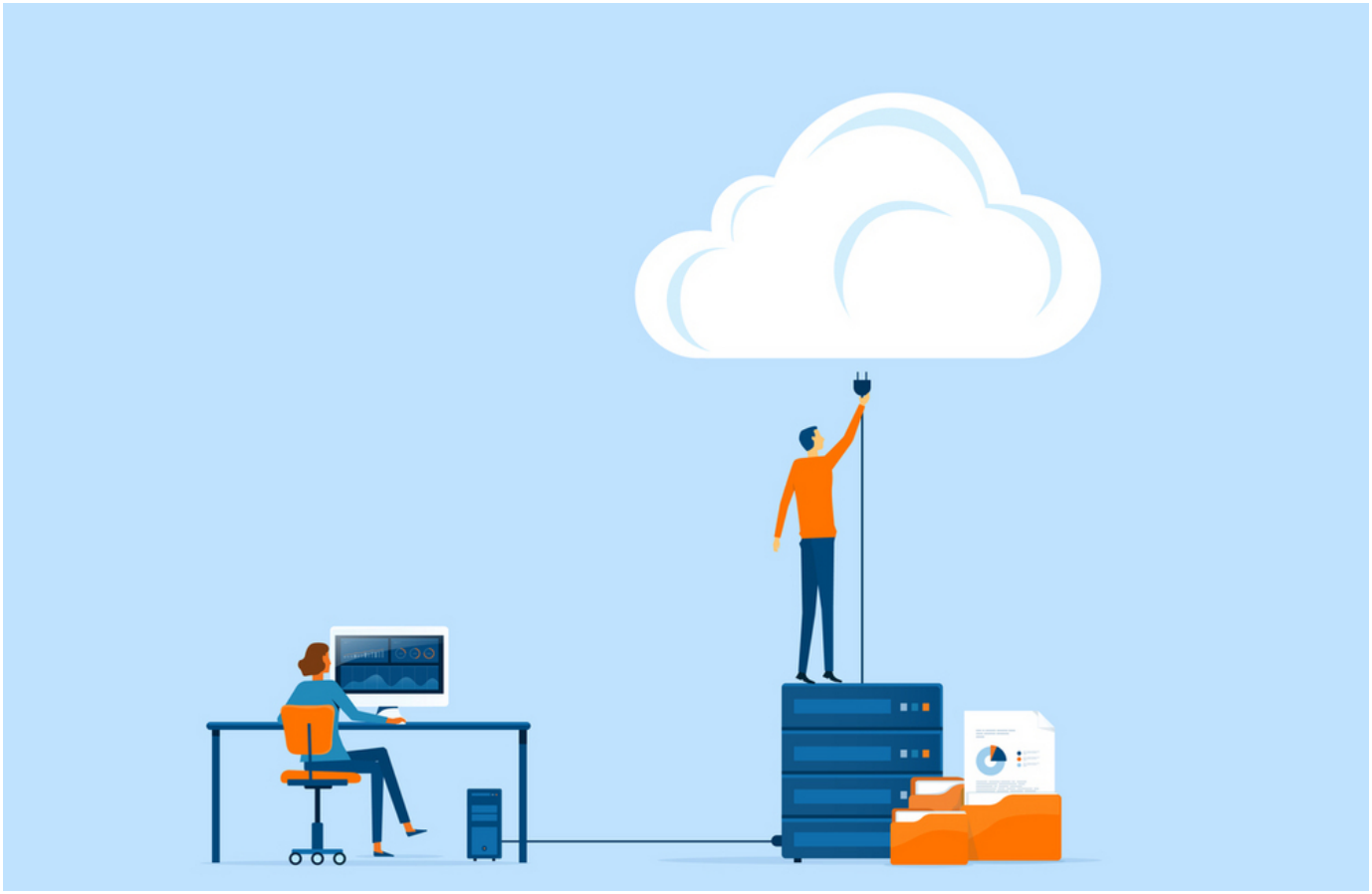

Photo Credit: TCmake_photo/iStock

The National Institute of Standards and Technology (NIST) recommends security and IT professionals deploy a zero trust strategy and continuous monitoring to optimize cloud security, according to a new report.

There are security and privacy concerns associated with shared cloud servers, according to NIST. Private companies or federal organizations need assurance that their data is protected and private from any other company or organization on the same server. Some organizations may also need to keep certain data separate with varying degrees of security and privacy controls.

Due to the increasingly globalized IT environment, some cloud servers may also host data for companies or organizations in different countries, creating additional security and privacy concerns.

“Each country has its own laws for data security, privacy and other aspects of information technology,” the report said. “Because the requirements of these laws may conflict with an organization’s policies or mandates (e.g., laws, regulations), an organization may decide that it needs to restrict which cloud servers it uses based on their location."

Using cloud services physically located in the same country as the organization is called geolocation. However, it cannot be automated or scaled and therefore cannot be fully trusted in cloud security efforts, NIST said.

NIST suggested that organizations seeking to secure their data in the cloud should configure a cloud platform as trusted, continuously audit said platform to verify trustworthiness, and “before each container worker node launch, verify (measure) the trustworthiness of the cloud server platform.”

The report also recommends “only deploy[ing] workloads to cloud servers with trusted platforms” and “asset tagging.” Chronicling information about assets on the network and continuously auditing and verifying those assets before launching workloads can enhance cloud security, NIST said.

“Achieving these goals ensures that the workloads are not launched on a server in an unsuitable boundary location,” according to the report. “This avoids issues caused by clouds spanning different physical locations (e.g., regulations, sensitivity levels, countries or states with different data security and privacy laws).”

When scrutinizing the trustworthiness of a cloud platform launch, NIST said organizations should adhere to the principle of attestation, which involves testing a signature and set of security measurements against a signature and security measurements stored within the hardware of the platform.

“Attestation requires roots of trust,” NIST said. “The platform has to have a Root-of-Trust for Measurement (RTM) that is implicitly trusted to provide an accurate measurement, and enhanced hardware-based security features provide the RTM. The platform also has to have a Root-of-Trust for Reporting (RTR) and a Root-of-Trust for Storage (RTS), and the same enhanced hardware-based security features provide these.”

In other words, zero trust can help an organization quickly authenticate its server before launching a workload.

Zero trust and continuous monitoring of assets, as with the Cybersecurity and Infrastructure Security Agency’s Continuous Diagnostics and Mitigation (CDM) program, are two cloud security strategies trending among federal agencies this year. Pandemic-induced telework boosted this trend due to federal employees using their own devices or connecting via VPN to work.

Despite their usefulness, zero trust and continuous monitoring are not the only worthwhile cloud security strategies for private or federal IT departments.

“It is important to note that the prototype implementation presented in this publication is only one possible way to solve the security challenges,” NIST said in the report. “It is not intended to preclude the use of other products, services, techniques, etc. that can also solve the problem adequately, nor is it intended to preclude the use of any cloud products or services not specifically mentioned in this publication.”

View printer friendly version
Federal Cybersecurity
CISA
NIST
CDM
Zero Trust
cloud security

Standard