PRESIDIO FEDERAL

Silver Business Partner IBM

Solving the Federal Government's Biggest Threat Using Hybrid Cloud

With cyberattacks increasing and the supply chain becoming a lucrative target for malicious actors, hybrid cloud promises to help the government address these security concerns.

LAST YEAR, sophisticated supply chain attacks dominated headlines. This year is shaping up to be no different. Malicious threat actors seek to exploit vulnerabilities in the supply chain at an alarming rate.

According to IBM's X-Force Threat Intelligence Index 2022, "the number of incidents due to supply chain vulnerabilities jumped by 33% from 2020 to 2021." The spike is concerning for many security operations teams as supply chain vulnerabilities are often the first element in a network that threat actors seek to leverage when trying to gain access.

Two of the most prominent cyberattacks to date — SolarWinds and Colonial Pipeline — exploited those supply chain vulnerabilities. In response, the Executive Order on Improving the Nation's Cybersecurity sought to provide federal agencies with comprehensive guidance for securing their networks, data and people. But what are some of the platforms that can help them best protect their information?

The answer isn't as cloudy as it may seem.

How Hybrid Cloud Is Reshaping Public Sector Security Requirements

Researchers found in a recent report that "nearly 70% of government IT decision-makers are concerned about security risks when migrating to modern cloud platforms." Decision-makers also cited legacy security concerns as one of the main drivers for cloud adoption.

Therefore, as government agencies look to balance legacy technology and cloud adoption, a hybrid environment emerges.

The growth of this hybrid cloud has led to new cybersecurity requirements. As organizations process and share data between legacy and cloud environments, SecOps teams must ensure data remains secure.

Hybrid cloud architectures address this distinct concern via confidential, encrypted computing methods. CPU enclaves work to quarantine data from users, rendering the information invisible, allowing only authorized programs to access the data. At the user level, this means data-in-transit and in use are protected from unauthorized access, thereby mitigating the risk of malicious insider attacks.

However, despite the best-laid plans, threats are evolving. To effectively combat emerging and advanced persistent threats, organizations must have visibility into and across their network. Unlike the simplicity of private or public cloud, the hybrid cloud adds a new layer of complexity. To effectively secure the network, security operations teams must leverage security information and events management tools to create a holistic security picture. Failure to adopt a holistic approach means SecOps teams are operating with one eye closed.

Hardening Existing Networks Against Emerging Threats

SIEM-based solutions can help agencies distill their entire operating picture — on-premises architecture, private or public cloud — into one location, thereby reducing complexity and improving logging capabilities within hybrid environments.

Complexity, however, isn't the only challenge SecOps teams face.

Due to a variety of factors, government organizations struggle to attract, recruit, and retain cybersecurity talent, thus compacting the challenge to keep up with today's cyberthreats. By creating or expanding training programs, however, agencies can build the cybersecurity skills they need to harden existing networks with the teams they have.

Moreover, private sector organizations are available to partner with agencies as they seek to augment their cybersecurity teams and make use of modern architectures and tools.

How IBM Is Helping Public Sector Agencies Build a More Resilient Future

IBM is prepared to help the public sector build resilient networks designed to meet tomorrow's cyber realities. IBM has a suite of solutions designed to help agencies no matter where they are in the process — from IBM's Security QRadar SIEM to courses on cybersecurity.

And as government institutions look to inject greater cyber resilience into their architectures, decision-makers should remember that no one journey is alike. Don't compare. Instead, seek out partners like Presidio Federal who can address your bespoke security needs and match agency requirements with effective tools.

"The federal government and the private sector need to work together to create cybersecurity policies that are adaptable to rapidly emerging threats, are based on effective risk management and tap public-private partnerships," said Howard Boville, head of IBM's Hybrid Cloud Platform, in a recent press release. "It is critical to ensure we are fighting against the constantly evolving cyber and compliance threat landscape to protect the world's data."

Check out how IBM is helping federal agencies build resilient, secure solutions and how we work together to support our customer's mission.