A decade ago, the concept of a Cloud Access Security Broker (CASB) emerged to address the complex security needs of emerging cloud infrastructures. As cloud has become a mainstay in state and local government, there is new urgency for cloud-specific security measures.

In this Q&A, Ned Miller, public sector chief technical strategist for McAfee, talks about new CASB capabilities that can support cloud deployments in general, and zero trust specifically.

Why was CASB first introduced?
CASB was originally intended to help organizations gain additional visibility and control over data as it was moving into the cloud.

Operators and defenders needed a more sophisticated means of managing security, especially with data residing in multiple cloud infrastructures. The original management and security tools did not take that kind of infrastructure into consideration.

How has that need changed over time?
With widespread cloud adoption, the complexity of the problem has evolved. Organizations face new issues: Where is my data being stored? How is it being accessed? Who is accessing it? And do we have the appropriate governance models in place?

With government’s cloud-first mentality, software-as-a-service applications have become pervasive. We have also seen the rise of shadow IT: People leveraging cloud applications without the direct involvement of the IT department. Government needs new tools to manage and govern all those applications.

How does McAfee make that happen?
We designed McAfee MVISION Cloud to address shadow IT, with configuration management and policy enforcement. There’s also the cloud-native application protection and container security.

Lately, we are focused on protecting data that is traveling across clouds or even in between cloud-based applications. For example, with Zoom and Microsoft Teams meetings, what is governing the content that we are sending each other? Today’s CASB has the ability to do that.

How has CASB evolved to meet that need?
CASB has grown beyond the initial core functionality to become more of a security platform and address things like shadow IT and the need for multi-cloud governance.

At McAfee, we now support all four of the major cloud service providers with tools like configuration management, malware detection and policy enforcement. All those things have evolved over time, as the environments have become more complex. For example, CASB now addresses security needs around dev-ops — the effort to provide a modernized development environment using cloud-based infrastructure or containers. We have enhanced the CASB platform to accommodate cloud-native application protection and container security.

So, it has gone beyond just protecting the cloud infrastructure?
Exactly. Now we also must protect the applications that are built inside of those infrastructures.

How does McAfee make that happen?
We designed McAfee MVISION Cloud to address shadow IT, with configuration management and policy enforcement. There’s also the cloud-native application protection and container security.

Lately, we are focused on protecting data that is traveling across clouds or even in between cloud-based applications. For example, with Zoom and Microsoft Teams meetings, what is governing the content that we are sending each other? Today’s CASB has the ability to do that.

How does all this support zero trust?
At its heart, zero trust is a data-centric security model. CASB delivers continuous data protection, conditional and contextual access to data, threat landscape data and user behavior monitoring. The most important asset you have is data, and CASB is a comprehensive, single policy-enforcement engine for data protection.