box

The Content Cloud and Zero-Trust Architecture

Supporting your government agency's journey across all five ZTA pillars

The need to implement Zero-Trust Architecture (ZTA) has influenced major investments and priorities among federal CIOs. While most agencies began this journey several years ago, zero-trust efforts have accelerated after the guidance and direction provided in Presidential Executive Order 14028 and OMB Directive M22-09. However, as agencies navigate executive guidance for implementation at the end of fiscal year 2024, planning and investing in the right technology the journey to ZTA can prove complex and time-consuming.

Moving to **the Content Cloud** can help accelerate an agency's journey towards ZTA. The Content Cloud is a secure, easy-to-use platform built for the entire content lifecycle, that supports the principle of "Least Privilege." With built-in, frictionless security, Box supports your agency's journey to true zero trust across all five pillars of ZTA.

Box fulfills the five pillars of Zero Trust Architecture

Identity

Identity and access management are the core building blocks to any agency's zero trust strategy. With **single sign-on (SSO)** capabilities in the Content Cloud, you can better manage identity and access management — while integrating your tools directly into the identity stores you have in place today.

Enhance content security with **native controls for multi-factor authentication (MFA)** or time-based one-time password (TOTP) authenticators (for both internal and external users) to ensure the highest level of identity management and access control on content stored in the Content Cloud.

Devices

Device Trust performs a device posture check as users access content. If a device doesn't meet requirements, both user and device are blocked from accessing data. Alternatively, if a device meets posture check requirements, but the data should not be accessed from a mobile device, Box's **Smart Access** policy prevents that data from being accessed from desktop or mobile applications.

Box gives every customer the ability to integrate with mobile device management (MDM) tools, allowing agencies to continuously manage authorized devices and sanctioned applications on those devices.

Networks

Protecting networks and the flow of data is critical to any security architecture. Box runs a secure enterprise service and network as part of our everyday operations. We leverage granular data flow control and data association within the application to provide complete data separation based on admin-defined and internal Box data classifications.

All data is protected not only at rest using 256-bit AES encryption, but also in transit using TLS 1.2 encryption. With **Box KeySafe**, agencies can add a third layer of encryption while keeping all the usability and functionality within the Box applications.

Threat Detection spots anomalous user behaviors, identify compromised accounts or data exfiltration, and immediately notify your agency admin.

Applications and Workflows

Designed as a digital-first, cloud-only application since inception, Box provides high levels of security and compliance with a single platform application for both commercial and government customers.

In addition, all layers of the Content Cloud are secure, audited, and rigorously adhere to most compliance standards. The Content Cloud also undergoes regular evaluations by third-party auditors.

Access to data stored in the Content Cloud is controlled by role-based access, granting users only the level of content access that meets their needs. As data flows through the Content Cloud, our native **Malware Deep Scan** detects and protects users while still allowing them access to the data with native preview functionality.

Data

Data security is at the heart of the Content Cloud. Agencies can define data classification labels and automate classification based on content contained within documents uploaded to Box. By applying these data labels, access policies can be applied to the content to control who the content can be shared with as well as external data sharing. You can also apply watermarking, prevent data leaks, and keep certain apps from accessing data. Along with our data encryption, Box allows for an additional layer of encryption using **Box KeySafe** technology with Amazon Web Services KMS and Customer keys. Lastly, audit and reporting on all content stored in the Content Cloud is always available to the agency's administrative teams.

Visibility and analytics

Automation and orchestration

Governance

With **Box Governance**, agencies can programmatically set data retention and content disposition policies across all content in their apps and workflows

With **event-based retention**, automatically apply retention policies based on business event trigger dates to connect policies to business processes

Intelligent monitoring and reporting tools in the **Admin Console** help you mitigate security risks