Secure Collaboration for the Work-from-Anywhere Future

The massive shift to remote work highlighted the need to modernize the way state and local governments protect content used in collaboration and workflows. ***Murtaza Masood****, managing director for state and local government at Box, discusses how government leaders can secure content while making it seamlessly available to workers and constituents.*

How have the past few years impacted collaboration, content sharing and the security of content workflows?

In response to the pandemic, CIOs had to immediately enable secure employee workflows that were available anywhere, anytime, and on any device or network. They also had to enable constituent services on demand, so people could reliably and securely engage with their state or local government to do things like pay fees or apply for permits, benefits and jobs — regardless of their location or device. This shift in demand patterns required a rethink of traditional collaboration and content management strategies. Collaboration had to be on demand with frictionless security and provide a great user experience.

With multiple people collaborating and sharing content, what's the best way to protect data?

There's no silver bullet. As government organizations move to cloud-enabled platforms to empower their workforce and deliver constituent services, they need to invest in foundational cloud technologies and capabilities that form a comprehensive ecosystem to secure data and content while powering seamless workflows. They need a roadmap to address the entire spectrum of capabilities — identity management, device security, application modernization, re-imagining case management and other related issues.

What should organizations look for when considering a Zero-Trust solution?

Zero Trust is a comprehensive strategy, not a specific solution. To enable cross-platform or cross-application identity management, Zero Trust must include device security and multifactor authentication to establish who is logging in with single sign-on. Then you have to consider content access, privileges and control lists, which often exist across multiple platforms. Once you adopt the right tools, you get to a more comprehensive state where you can securely log in anytime, anywhere, with any device and have the right workflows and content surfaced for you.

How can artificial intelligence (AI) and automation help organizations protect against threats and alleviate IT staffing burdens?

The last two years have taught us that the business of public service must operate beyond brick-and-mortar boundaries. AI and machine learning let organizations secure content and augment the user experience by automating malware detection on the delivery end, automating encryption throughout the content life cycle, automating threat removal within business workflows and more. Work can continue seamlessly while these advanced technologies automatically enable a real-time security posture.

How can organizations meet compliance requirements as they share content with diverse users?

The first step is to look at your content governance model. What does that content life cycle look like from ingestion or creation to consumption and archive? Compliance must be part of that entire process. Then, it comes down to your platform and tools. Are you selecting a platform like Box, where your entire content repository is unified and ensures compliance from the point of entry to the point of disposition — all while offering a seamless user experience? Or are you signing up for a disparate and disconnected strategy where you are now responsible for tracking and making sure that different data sources are compliant? Content fragmentation, even in the cloud, can introduce unnecessary exposure and a compliance risk.

Where can state and local governments start their journey toward more secure content sharing and collaboration?

User experience should take a primary seat in planning and strategy. Start with your governance model. Then seek platforms and tools that match user expectations, can achieve key criteria — for example, a seamless user experience, frictionless security, and built-in compliance and security protection — and provide the content management features and benefits that you would expect of a modern platform. Finally, stay ahead by educating yourself through your ecosystem and participating in thought leadership groups such as those within the National Association of Counties and the National Association of State Chief Information Officers.

box

Box for government

Modernize your mission-critical processes

State and local governments are feeling the pressure to meet citizen requests and improve stakeholder experiences. From the field to IT, Box enables your teams to work from anywhere with seamless, cross-agency collaboration, faster citizen and case intake, and secure mission-critical processes.

Visit box.com/government