Adobe

Protecting content beyond the perimeter.

The definitive guide to digital content security for government.

Contents

Letter from Adobe's Chief Technology Officer in public sector.

If you're feeling the weight of responsibility of enabling employees to work from home, or you're concerned about looming data security threats that could come from anywhere, you are not alone. And you're in the right place.

In this guide, you'll learn how government agencies can protect digital assets and safeguard sensitive information beyond network boundaries. You'll also learn various ways to mitigate the risks posed by telework, thwart increasingly sophisticated cyber attacks, and preserve security—without slowing down content production and collaboration.

Like businesses and government agencies everywhere, the pandemic forced you to find new ways of operating virtually. At a time when needs skyrocketed, access to vital services was stymied by paper-based government processes. Faced with a nearly impossible task, you scrambled to keep critical government services operational —no matter what. But you also had to fiercely protect sensitive information that could damage public trust or even pose a national security risk.

You, like everyone in the IT community, did the best you could. But is there a way to do better? Always. Cybersecurity is a never-ending journey that must keep pace with digital transformation—and one step ahead of cybercriminals.

In this guide, we show the steps agencies have taken to protect content, but we also explore the bright sides of this rapid digital transformation. Many agencies launched digital solutions they'd been planning for years—some for the first time, others expanding their digital footprint. CARES Act funding added momentum. At last, the era of digital government began, bringing with it greater efficiencies, faster processes, and better citizen experiences. New opportunities continually emerge—as do threats. Our jobs challenge us to continually address both, capitalizing on opportunities while minimizing risk.

Read on to explore content security trends, learn new methodologies, avoid pitfalls, and discover leading solutions for your peers and their partners.

Sincerely,

John Landwehr

John Landwehr

Vice President and Public-Sector Chief Technology Officer
Adobe

> “In many organizations, including government, security has largely been accomplished with perimeter-style defenses, like multiple network zones, firewalls, and encryption. But upon closer inspection, we can find a more intelligent way to help protect the infrastructure.
>
> **John Lewington**
>
> Industry Specialist
> National Security Group

Understanding the new digital security landscape.

Securing content in the wild.

Today, content security is so embedded into daily life that we take it for granted. Every time you stream TV, download files from a website, or use your bank account app, you're using content security solutions. Adobe is an industry pioneer, with a long history of creating enterprise-level content management solutions deployed by both commercial and government organizations.

The top challenge for government IT professionals is how to protect sensitive content beyond the boundaries of the secure network. Secure offices with multiple layers of perimeter-style defenses including multiple network zones, firewalls, and encryption sit nearly empty while millions of government workers now work from home.

The burden of security cannot be left to individual employees. More must be done to protect content after it has left the building. And while content security must be rigorous, it can't be complicated or time-consuming.

Everything from the federal budget and new bills to Social Security records with personally identifiable information is stored digitally, with new content being created every day. Content security refers to the security of the data itself, which has also been called data-centric security.

As attacks have evolved, so have our defenses.

Barriers to success:

Solutions have to work across a variety of devices, on different operating systems, and different computing infrastructures.

Legacy systems that don't always work well with newer ones.

Content needs to be protected all the way from the original file through its multiple final destinations and formats.

From federal agencies to local municipalities, cyber attacks and data breaches have occurred at all levels of government. While some security incidents are the work of hackers, others are caused by simple human errors, device theft, or minor mistakes. To protect the privacy of Americans, agencies need to take a comprehensive approach to data security.

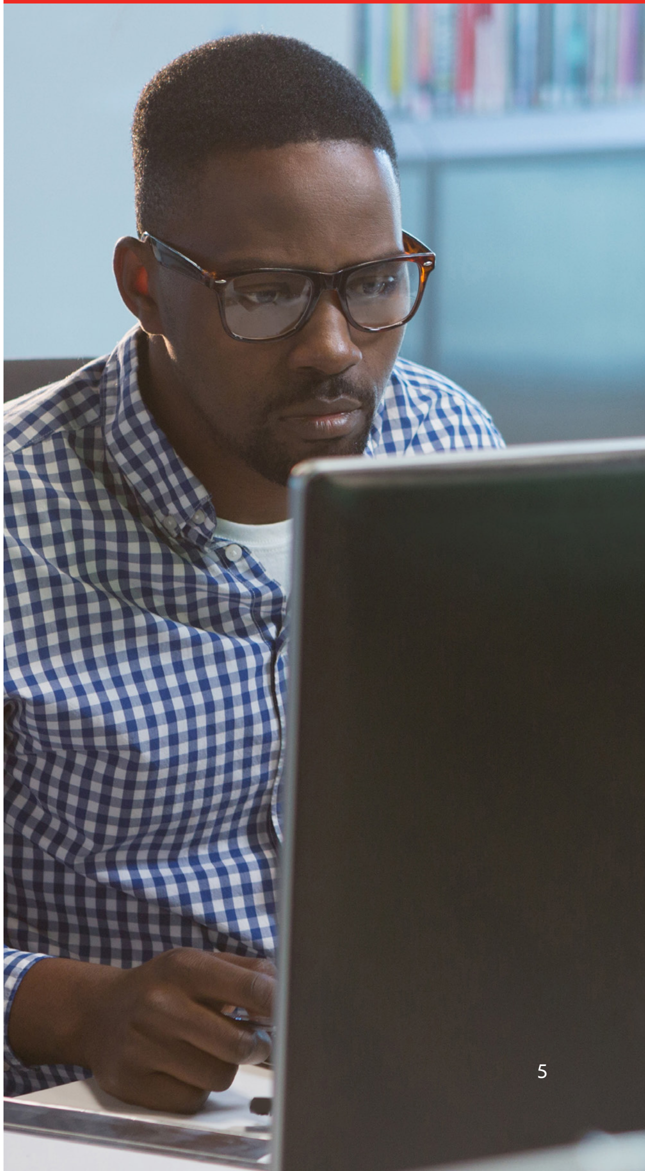
Agencies have been compromised due to lack of the proper encryption, keeping data on publicly accessible servers, database server hacks, and accidental data leaks. These cybersecurity incidents cost taxpayers millions of dollars and can even shut down vital government services.

Core risk considerations:

- Exposure of personal information like passwords, social security numbers, or payroll information can compromise citizen privacy and erode public trust.
- Some information, if accessed, could create security risks.
- Information can become compromised through employee error, cyberattacks, or malicious insiders.

While the number of breaches continues to decline, the number of records exposed has increased significantly, suggesting that hackers are going after larger targets. Content security adds a new layer of defense at the data level to help protect our most sensitive data.

> “
>
> Through strengthening our cybersecurity posture and being even more vigilant than we have been—we have been able to keep our remote workers and their data secure and prevent intrusions.
>
> **Gary Washington**
>
> Chief Information Officer
> Department of Agriculture (USDA)



The five core principles of Zero Trust.

To protect against potential security threats, IT security practitioners have started putting multiple layers of data security protections in place. According to *Zero Trust Networks: Building Secure Systems in Untrusted Networks* by Evan Gilman and Doug Barth, a Zero Trust network is built upon five fundamental assertions:

1. The network is always assumed to be hostile.
2. External and internal threats exist to the network at all times.
3. Network locality is not sufficient for deciding trust in a network.
4. Every device, user, and network flow is authenticated and authorized.
5. Policies must be dynamic and calculated from as many sources of data as possible.

What happens when one of those files is removed, whether maliciously or unintentionally, from those existing access controls?

Security measures are needed for protecting and tracking electronic documents that contain sensitive information, but it's equally important to enable flexibility and ease of use for those with authorized access.

> “Using your current back office software, you can add document security features—with no detriment to the user experience.
>
> **Jeffrey Young**
>
> Multi-Solutions Architect
> Adobe

Understanding content security.

The best content security is based on digital rights management (DRM) technology, which allows for seamless document sharing while keeping security measures in place. This makes it easier for users to access content or make adjustments regardless of where they are or what device they're using.

Document encryption: Help protect PDF, Microsoft Office, and other document types with encryption that conforms to federal standards.

User authentication: Work within your existing user authentication measures to validate user identity.

Security integration: Interface with existing authorization systems dynamically as the policy decision point (PDP).

Confidentiality settings: Define what users or groups can do with documents, such as copy, edit, print, or view offline.

Dynamic policies: Change security policies at any time, even after the documents have been distributed.

Mobile access: Allow mobile users to access PDF documents with their mobile apps and devices.

Numbers to remember.

Content security has been top of mind for the public and government officials alike. In 2015, one large breach exposed 1.5 million records containing sensitive information, including social security numbers and fingerprint data.

15.1 billion records exposed by breaches in 2019.

(Source: Risk Based Security)

3.6 million sensitive records exposed in 83 government and military breaches in 2019.

(Source: Identity Theft Resource Center)

8.4 billion records were exposed in Q1 of 2020, a 273% increase over the same period in 2019.

(Source: Risk Based Security)

Spotlight on rules and regulations.

Although laws and policies on data and content security are intended to ease implementation and buffer protections, they can be another stumbling block if not closely scrutinized. Here are just some of the requirements to keep on your radar:

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Released in May 2017, the order calls for a review of cyber capabilities and vulnerabilities across government.

Presidential Executive Order on America's Cybersecurity Workforce

Released in May 2019, the order calls for the further development of cybersecurity expertise.

Report to the President on Federal IT Modernization

The report from the American Technology Council lays out the current and envisioned state of federal IT and focuses on cybersecurity through increased data-level protection.

Federal Risk and Authorization Management Program

FedRAMP makes using the cloud easier for government agencies by standardizing the security assessment, authorization, and continuous monitoring for cloud products and services.

DHS Continuous Diagnostics & Mitigation (CDM) Program

Provides a government-wide acquisition vehicle to deploy critical cybersecurity tools and services to federal, state, local, and tribal government entities.

Trusted Internet Connections 3.0

This helps agencies manage risk by detecting and blocking attacks and by sharing threat information. Basically it allows organizations to go straight to the cloud by being authenticated at the edge vs going through Einstein's traditional VPNs which creates choke points.

Charting a course for success.

The three pillars of content.

1 Rights management

Rights management uses encryption technology to protect content wherever it resides. A solid rights management solution can be used across platforms, not only limiting user actions like the ability to print, copy, or edit, but also revoking and expiring content, even after the content has been distributed.

Use a digital rights management (DRM) solution to efficiently manage expiration information and asset states and reduce the risk of legal penalties from using unlicensed, unapproved, or expired assets.

2 Consumption management

Consumption management is a form of analytics that watches for unusual patterns or anomalies associated with content interactions. Adobe integrates with Splunk, for example, which uses AI-driven machine learning to create dashboards and alerts. The right consumption management solution allows you to visualize what's happening and act in near real-time. If a user suddenly strays from their normal content area or starts printing volumes of documents at 1 am, IT will be able to instantly intervene.

3 Content management

Content management systems (CMS) are used to store and retrieve digital files. By categorizing and applying metadata tags to content as it is stored, access can be restricted based on any number of content criteria: object type, category, folder, project, etc. In a web environment, rather than maintaining multiple versions of the same content for different audiences, dynamic redactions can be made based on user credentials. When assets are reclassified, all references are automatically updated. The traits to look for in high-performing CMS systems include strong multi-factor authentication features, easy to use, and audit trails that show every interaction.

Real-life examples.

Moving to a Zero Trust environment by adding content-level security is now easier and more important than ever. Here are two great examples of why agencies added content-level data protection.

The Department of Defense (DoD) was growing increasingly concerned about the rise of cybercrime and theft of intellectual property. They recognized that risk could come from any of their 300,000 suppliers. The International Traffic in Arms Regulations (ITAR) restricts access to military munitions, but also related plans, diagrams, photos, and documentation.

To strengthen the security of their supply chain, they developed a cybersecurity model, with certification, verifications, and processes. Vendor ratings determined whether they were eligible to continue being a supplier and the steps they needed to take in order to increase their cybersecurity rating. This Cybersecurity Maturity Model Certification (CMMC) builds upon Defense Federal Acquisition Regulations Supplement (DFARS) Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Additionally, the Department of Homeland Security wanted to ensure the protection of sensitive information and high-value assets. Safeguarding these assets is critical to the safety of the American people and our allies. Not only do they have multiple layers of content security in place, they participated in the Continuous Diagnostics and Mitigation (CDM) program that uses automated tools to monitor and manage vulnerabilities. Agency-installed sensors perform ongoing, automated searches and create prioritized alert responses, based on the severity of the risk.

Similar access control and monitoring is done in many agencies for assets containing Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI).

Building your action plan.

Your strategic road map.

1 Get started.

Content security experts recommend starting simply with the goal of improving your security stance over time. Prioritize small consistent improvements over daunting large-scale plans. For example, you can encrypt PDF documents to limit capabilities to a select individual or group of people. In a few clicks, you can manage editing rights or print capabilities. Then you might add a dynamic watermark that adds a timestamp, which gets updated automatically each time the document is updated or opened.

2 Create

Once you get comfortable with basic document protections, consider how you can put content and people into security groups. Start adding metadata to content. Add tags and content categories to make information easier to find. Start with one area that contains sensitive information and consider the best ways to restrict access. On the people side, you can create simple security groups and grow from there. Over time, you can layer on content protections with role-, identity-, and attribute-based restrictions, whatever works best for your agency.

Verifying a trusted signature.

Data-centric security also provides integrity and authenticity via digital signatures. Documents with digital signatures require additional levels of verification to prove the identity of the signattors and that the document has not been altered in transit.

Both Adobe Acrobat and Reader ask these key questions to validate the signature:

- Is the digital certificate that signed the document still valid? Has it expired or been revoked?
- Has the document been changed since it was signed? Has the integrity of the document been affected? If there are changes, are they allowed changes or not?
- Finally, does this certificate chain up to a certificate listed in the Trusted Identity list? If so, the signature will be trusted automatically.

3 Audit and analyze.

Knowing “what’s normal” is the first step to being able to spot trends and content consumption anomalies. Your content management solution should allow you to visualize content consumption in real-time and determine how the content is being consumed. Over time, you should be able to detect anomalies by affinity (associating users with content) and by correlation (combining content and user activity with other data). Real-time analytics and alerts provide an advantage. In 93% of cases, it takes attackers just minutes to compromise systems, but without ongoing monitoring, it can take organizations months to discover the breach.

4 Continually improve.

Create good cybersecurity habits for your agency. Start by setting reminders to frequently check analytics reports. Once you’ve figured out all the edge cases of what constitutes a normal variation, build workflows that intervene automatically. In a simple example, agencies lock out login attempts after three tries. Try a cybersecurity sprint that targets a specific area. Set goals to expand your efforts on a regular interval. Remember to include employees in your ongoing cybersecurity efforts. Even vigilant, well-intended employees can make mistakes that lead to a data breach. Take time to share real case studies. Train employees how to identify suspicious emails and what to do if they suspect a security problem.

Improve data security with Adobe.

As the security landscape grows increasingly complex and challenging, traditional perimeter-style security architecture needs to be rethought.

Adobe continues to be recognized as an industry leader in content security especially in the public sector. By assuming that nothing is trusted inside or outside the perimeter, Zero Trust aims to dynamically verify all access to system resources. With DRM, we can extend Zero Trust principles down to the content level and provide much stronger protections and mitigations against potential issues.

Adobe Experience Manager can also help your agency increase content velocity, achieve personalization, and create adequate content governance.

Using Adobe's easy, built-in features for government, you're able to extend cybersecurity practices to the content level and provide much stronger protections and mitigations against potential issues.

Security credentials at a glance:

- Protects sensitive information and transactions with solutions that are certified compliant with FedRAMP, SOC 2 Type 2, ISO 27001, and PCI DSS.
- Assures that the e-signatures you collect are legally binding and in compliance with the ESIGN-Act, UETA, and regulatory requirements such as HIPAA, FERPAC, GLBA, and FDA 21 CFR Part 11.
- Verifies signer identities using single or multi-factor authentication, Government IDs, or certificate-based digital signatures such as PIV/CAC cards or CSC cloud signatures.
- Provides unsurpassed tools for creating and enhancing documents so they're accessible to people with disabilities such as blindness, low vision, or mobility challenges.
- DRM encrypts sensitive content and documents at 256-bit FIPS-140 Suite B encryption to persistently and dynamically protect them, independent of storage (Azure, AWS, on-premise) or transport.

> “ You can have a document with security measures in place using your current enterprise technologies while being able to collaborate with no detriment to the user experience.
>
> **Jeffrey Young**
>
> Multi-Solutions Architect
> Adobe

About Adobe

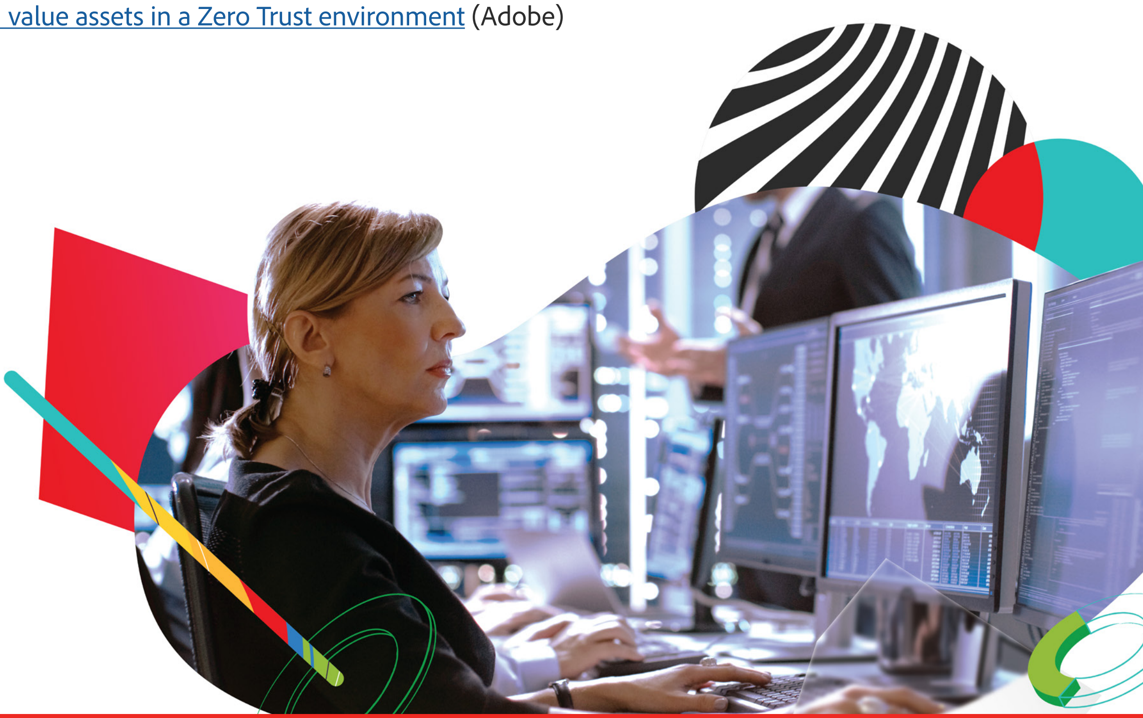
Adobe enables next-generation enterprise digital government services with trusted, proven, and integrated enterprise solutions that help drive agency efficiency, deliver remarkable experiences, and protect mission-critical data.

Learn more about how Adobe helps government agencies stay protected well beyond the perimeter.

Visit Adobe.com or contact us at 1-800-87ADOBE or DRM@adobe.com.

Looking for more information? Get up to speed with these additional resources:

Interview with Michael Chertoff and John Landwehr (Federal News Radio)
Protect your most sensitive digital assets while working from home (Adobe)
Securing the supply chain and high value assets in a Zero Trust environment (Adobe)



Adobe

01/2021