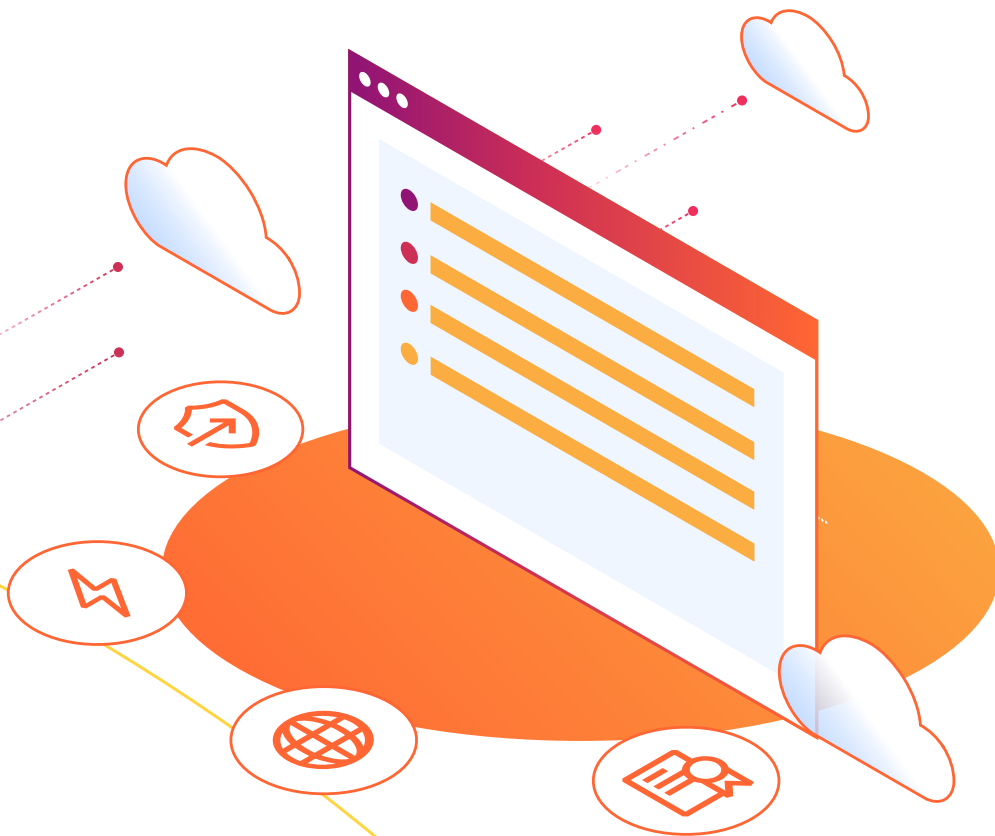


Defending the Digital Front Door:

A Strategic Approach to Website and Infrastructure Security in State and Local Government



SPONSORED BY



Introduction

In today's digital-first era, state and local governments are delivering more services online than ever before. Agency websites are no longer static pages — they are constituent-facing platforms that power transactions, manage personal data, and connect to complex backend systems.

As these systems grow in complexity, so do the risks. Cyber threats have evolved beyond simple distributed denial-of-service (DDoS) attacks and now target the entire application ecosystem with increasingly sophisticated tools and tactics, many powered by artificial intelligence.

Securing public sector websites requires more than just firewalls and patching. It calls for a comprehensive, cloud-smart approach that balances performance, accessibility, and security without compromise. A new strategic imperative is emerging: build cybersecurity into the architecture of public service websites themselves.

"Your agency's website is your digital front door," says Deborah Snyder, a senior fellow at the Center for Digital Government and the former chief information cybersecurity officer for the state of New York. "But security can't stop at the front door."

Historically, security and usability have been seen as competing priorities. That's no longer the case.



A Complex Threat Landscape

Government agencies are managing a constantly expanding digital footprint. With this expansion comes greater exposure to threats. Attackers exploit a variety of vectors — phishing, credential theft, DDoS and, more recently, AI-driven reconnaissance and content scraping.

"Phishing remains the number one attack that gets through," says Dan Kent, field chief technology officer for the Americas at Cloudflare. "Even with tools in place, training and vigilance are essential because these attacks are growing more complex."

Public-facing websites are increasingly targeted as points of entry. The threat landscape extends to backend systems through overlooked attack surfaces such as application programming interfaces, or APIs. "Most agencies are unaware of how many API endpoints they actually have," Kent notes. "We often discover 30% more than they thought existed. That's a massive expansion of their attack surface."

These blind spots, coupled with legacy systems and limited visibility, create structural vulnerabilities. As Steve Caimi, cyber specialist for the U.S. public sector at Cloudflare, puts it: "You can't protect what you can't see. Visibility is the starting point for any effective website security strategy."

Securing Websites at Scale in the Cloud Era

Cloud adoption and multi-cloud environments have become the norm across government. Yet many agencies still rely on siloed, legacy tools that can't scale to meet current demands.

"The traditional perimeter is gone. Today, 80% of traffic flows outside agency walls," says Kent. "That demands a security model that operates at the edge and across clouds."

A modern security posture must extend protections closer to the users and threats targeting agency websites. Cloud-native security platforms enable agencies to detect and block attacks in real time—before they ever reach critical infrastructure.

"It's not just about placing protections near your applications," Kent says. "It's about placing them where the threats originate. If an attack comes from overseas, stop it there — don't let it ride the internet to your servers."

This approach not only improves website security, but also boosts resilience, scalability and user experience.

Here are some additional best practices to keep in mind:

Consider security in tandem with user experience.

Historically, agencies have viewed security and usability as competing priorities. That's no longer the case.

"Modern tools have evolved to reduce friction while improving security," Caimi explains. "Technologies like passkeys, intelligent multifactor authentication and bot detection make it easier for users to access services without compromising defenses."

Kent points to the importance of integrating security early in website development: "The shift-left approach means embedding security in the application lifecycle — not bolting it on later," he says. "It's about building with security in mind from day one."

This proactive stance is essential as more governments adopt centralized digital service portals. Standardizing website security across services not only protects constituent data, but also improves public trust and service delivery.

Lean in to AI.

Artificial intelligence presents a dual cyber challenge. Adversaries use AI to scale attacks, craft realistic phishing messages and exploit vulnerabilities faster. But defenders can also harness AI to detect threats earlier and respond more efficiently.

"We've been using machine learning for years to detect anomalies and identify threats," Kent says. "Now, generative AI lets us automate even more — from summarizing incidents to configuring policies and accelerating response."

AI also enhances public-facing websites. "We're starting to see AI-powered assistants that help constituents find services or complete applications," Caimi notes. "That has enormous potential to improve access and equity."

Strategic AI adoption means securing website data inputs, monitoring usage and training staff on appropriate applications. "Every agency needs a data governance strategy that keeps pace with its use of AI," Kent says.

The threats are evolving, but so are the tools to fight them.



Don't neglect the fundamentals.

In the rush to modernize websites, agencies must not neglect foundational cyber hygiene. Asset inventories, patch management, protective DNS and vulnerability scanning remain critical.

"Before you automate or implement AI, make sure your basic defenses are solid," Kent emphasizes. "It's like DDoS — we see thousands of attacks every day, but few succeed because we've built strong foundational protections."

Caimi agrees: "Frameworks like the Zero Trust Maturity Model provide a roadmap. Start with identity, data and device visibility, then layer in automation and analytics."

A Call to Strategic Leadership

Website and infrastructure security is no longer a back-office IT concern. It is a mission-critical function that underpins trust, resilience and service delivery.

"This is the moment to step back and assess your architecture," Kent says. "If you had to build it from scratch today, would it support the agility, scalability and protection you need for the next 15 years?"

For government leaders, the answer lies in proactive investment, collaborative strategy, and a commitment to secure, constituent-centered digital experiences.

The threats are evolving, but so are the tools to fight them. With the right architecture, partnerships and mindset, agencies can secure their websites, protect their infrastructure and deliver services with confidence in a rapidly shifting digital landscape.

*This piece was written and produced by the Government Technology Content Studio,
with information and input from Cloudflare.*



Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com



Sponsored by Cloudflare

Cloudflare is the security, performance, and reliability company on a mission to build a better Internet for state and local governments. Today it runs one of the world's largest networks that powers anything connected to the Internet.

www.cloudflare.com