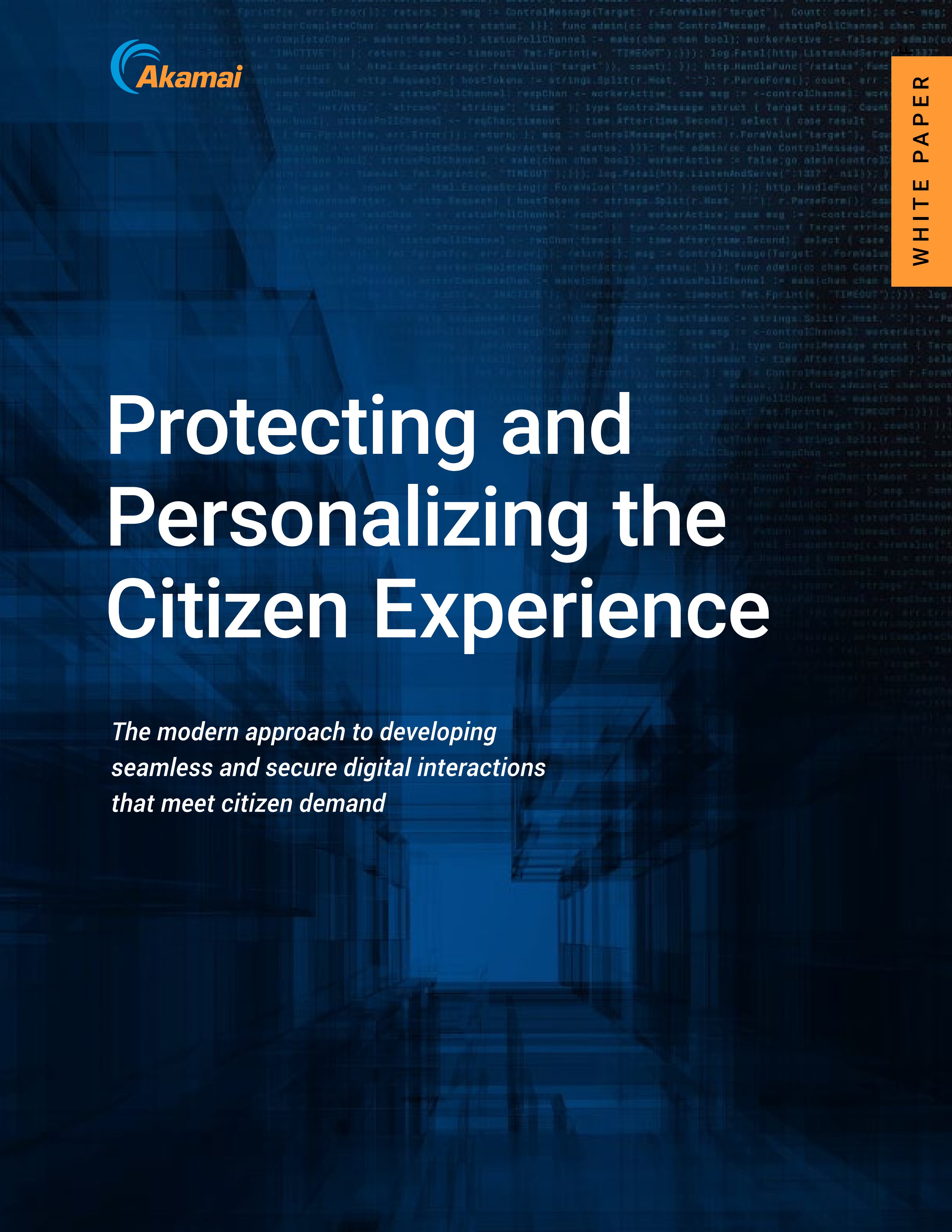


WHITE PAPER

Protecting and Personalizing the Citizen Experience

The modern approach to developing seamless and secure digital interactions that meet citizen demand

The Crucial Role of User Experience

When considering user experience (UX), problem-solving efforts often revolve around the interface between the user and the application. However, the breadth of that landscape, especially in government services, extends far beyond design. To foster trust and enhance the citizen experience, interactions must be fast, reliable, and secure while also protecting sensitive personally identifiable information (PII) and enhancing the UX with features like digital waiting rooms.

The impetus to advance the citizen experience arises from numerous sources, including the push from the recent Executive Order 14058, "Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government." This has tasked federal agencies with the mission to improve and personalize the digital citizen experience to strengthen the democratic process.

Also, there's an ongoing drive for digital renovation by state and local governments (SLGs). A wave of digital transformation is sweeping across SLGs, overhauling digital experiences to meet citizen demand, streamline processes, and foster improved collaboration. This means striking a vital balance between providing better user experiences while maintaining regulatory compliance within agencies, which comes with its own set of challenges, including:

- **Mounting cybersecurity challenges:** With an upsurge in threats, ransomware, and malware attacks, the escalating fraud concerning digital government services and lack of visibility into users, devices, apps, and APIs are significant cybersecurity hurdles.
- **Agency legacy systems and tools:** These systems often become roadblocks, standing in the way of providing simple, seamless service experiences.
- **Citizen and agency pains:** Slow performance, unreliable access due to scalability issues, and lack of flexibility preventing continuous improvement strategies are just some of the issues plaguing both citizens and agencies.

The above factors drive the need to modernize and the ability of agencies to securely and effectively leverage modern digital capabilities that rely on apps and APIs. To address these challenges, agencies at both federal and state levels need to quickly create and deliver personalized, responsive, consistent, and secure digital experiences. The call to innovate necessitates a serverless and scalable light-lift approach that offloads complexity, bottlenecks, costs, and risk exposure.

Securing Government Apps and APIs: The Role of Akamai Web Application and API Protection (WAAP)

Government agencies at all levels increasingly integrate apps and APIs across their systems due to the rising trends toward digital transformation. They aim to improve service delivery and operational efficiency and elevate citizen engagement. This interoperability and integration drive, with open data initiatives aiming to make government data more accessible and usable through APIs, also requires a higher volume of apps and APIs.

While an infrastructure rich in apps and APIs forms the foundation for an excellent digital experience, the high level of interoperability can expand the attack surface, leading to development and security challenges. Limited resources and legacy tools compound these issues, leaving agencies seeking to accelerate the delivery of modern digital services in a difficult position. Key issues include:

- **Overwhelmed security teams:** With limited resources, security teams often struggle to control access for a large number of APIs.
- **Lack of collaboration:** The cooperation between developers and security teams is not automated, and developers often lack access to security libraries of functions and classes that would enable them to produce more secure code.
- **Legacy tools and integration complexity:** These tools often lack automation, requiring manual processes that are slow and prone to errors. Moreover, the integration complexity can halt the flow of data and connectivity between systems.

To overcome these obstacles, agencies need to acquire visibility of apps and APIs. This is where Akamai's WAAP comes into play, offering a suite of capabilities to secure infrastructures against app and API vulnerabilities.

WAAP: The Guardian of Digital Experiences in Government Services

Akamai's WAAP is a powerful tool designed specifically to secure modern digital government services. It comes packed with automation features, making it efficient and easy to integrate. It addresses a plethora of challenges posed by the expanding endpoints and evolving threats.

Agencies can keep an eye on all apps and API systems in one place with unified visibility and automated controls. This increases the safety of online services. Advanced decision-making logic helps stop common and specific attacks. The tool is able to change based on each agency's different users and needs.

The system also improves service delivery. Agencies can make their online services better without increasing system complexity or cost. By reducing delays and making sure services can handle lots of users simultaneously, any agency can heighten the online experience for everyone.

Key WAAP Capabilities

- **Adaptive protections:** The auto-update feature consistently pushes the latest protections for apps and APIs
- **GitOps workflows:** Enables collaboration between DevOps and security teams in a GitOps workflow, speeding up development times
- **DevOps integration:** DevOps integration expedited through a simple GUI or with Terraform provider, APIs, or the Akamai CLI
- **Self-tuning:** Advanced machine learning automatically analyzes all security triggers, including actual attacks and false positives, to develop policy-specific tuning recommendations
- **Bot protection:** Real-time detection of malicious bots and botnet traffic, without hindering third-party and partner bots
- **API discovery and protection:** Automatic discovery of a full range of known, unknown, and evolving web APIs across all web traffic
- **Programmable APIs:** Manage functionality as code and streamline tasks like onboarding new apps and testing and debugging code

An Adaptive Solution: Utilizing Insights from 300+ Terabytes of Daily Traffic Data

By utilizing the data derived from insights from over 300 terabytes of daily traffic, Akamai's adaptive security engine improves outcomes while reducing overhead. This vast wealth of data is continuously analyzed to refine security protections, making WAAP a continually evolving security solution that adapts to emerging threats.

Unleashing the Power of the Edge: Akamai EdgeWorkers and EdgeKV

Edge computing, the technology enabling the creation, execution of microservices, and the deployment of serverless computing closest to locations of source data and end users, opens the door for efficiency, agility, and innovation. By reducing latency, scaling to meet any demand, and securing the edge by keeping service engagements off the core infrastructure, edge computing brings substantial benefits.

When sources, users, and developers are in close proximity, latency reduces and response times speed up. This ensures decisions are informed by accurate and up-to-the-minute data. The result is a streamlined decision-making process that reacts swiftly to changing conditions, relying on the most current and relevant data available. In terms of improved efficiency and lower costs, having computational power close to where data is produced and consumed alleviates the burden on centralized networks. It cuts down bandwidth requirements, eases network congestion, and reduces costs associated with data transfers between the edge and centralized infrastructure.

Furthermore, processing and analyzing data locally enhances data privacy and security. Data in transit can be a security risk, but local analysis minimizes this exposure. The system also demonstrates greater resilience by reducing dependency on centralized infrastructure. Decentralization allows for uninterrupted operation, regardless of circumstances.

Akamai's EdgeWorkers and EdgeKV play a crucial role in enabling a light-lift approach to transform digital services by providing serverless computing capabilities at the edge.

Akamai EdgeWorkers: The Power to Personalize at the Edge for Government Services

Akamai EdgeWorkers empowers developers by allowing them to use JavaScript to create highly personalized experiences at the edge, closest to the users. These user-specific customizations, which range from content modifications to custom headers, provide a highly tailored and responsive digital experience.

Key EdgeWorkers Capabilities

- **Tailored citizen experience:** Personalized digital experiences based on user attributes, allowing dynamic interaction between the user and the digital interface
- **Enhanced collaboration:** Enable seamless workflows between development, operations, and security teams, leading to higher productivity and improved delivery times
- **Ease of deployment:** Implement updates and changes quickly across a globally distributed network
- **Efficient coding practices:** Leverage modern and familiar JavaScript for serverless computing at the edge, reducing development times and the learning curve

Akamai EdgeKV: Reliable Data Access at the Edge of the Agency

Akamai EdgeKV complements EdgeWorkers by providing a key-value data store at the edge. EdgeKV enhances the capabilities of EdgeWorkers by offering fast, consistent, and reliable access to data, allowing for dynamic content customization based on user preferences, location, device type, and more.

Key benefits of EdgeKV include:

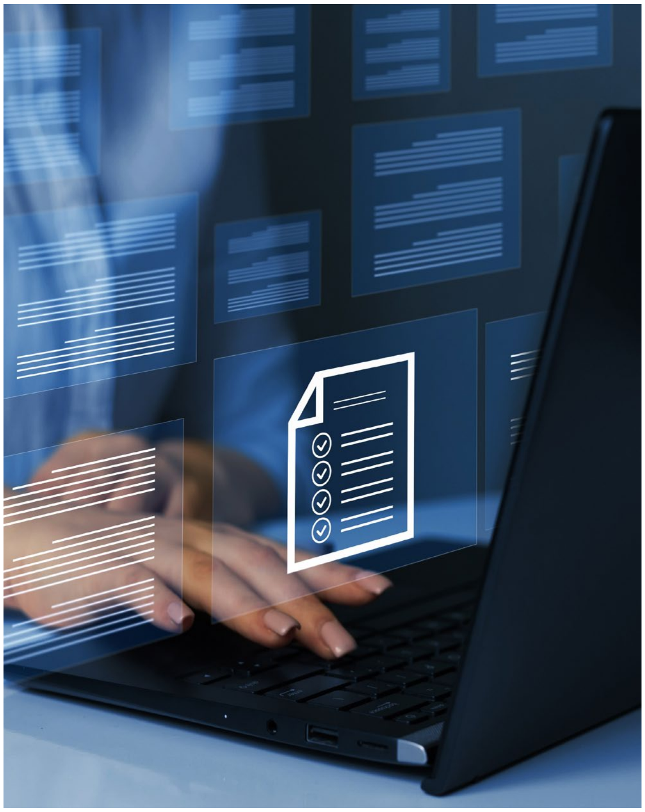
- **Speed and reliability:** Provide access to data quickly and consistently, regardless of where users are located, for a seamless experience.
- **Personalization:** Enable more dynamic, personalized experiences by accessing data based on key characteristics.
- **Scalability:** As the data store is at the edge, the infrastructure can scale smoothly to meet demand, ensuring consistent performance even during high-traffic periods.

How EdgeWorkers and EdgeKV address edge computing risks

EDGE COMPUTING RISKS	THE AKAMAI CONNECTED CLOUD PLATFORM APPROACH
Expanded attack surface: Unpatched systems, inadequate security measures, weak authentication, and vulnerable code present opportunities for attackers	Akamai protects microservices running at the edge against DDoS and web application attacks
Endpoint vulnerabilities: Level of risk is increased if data is stored locally on devices that are not secured properly against unauthorized access or other exploits	The Akamai Connected Cloud platform includes security solutions that protect against malicious attacks against any device
Disruptions and downtime: Although edge computing reduces reliance on centralized infrastructure, services may become unavailable if local systems cannot access the network	Akamai's edge infrastructure is covered by a 100% SLA, ensuring agencies using EdgeWorkers and EdgeKV can continue local operations, even in the face of hardware or software failures, power outages, or connectivity issues
Data chaos: Determining ownership of and responsibility for data and ensuring proper use and compliance are challenging to address at the edge unless clear policies and frameworks exist	EdgeWorkers and EdgeKV provide centralized management capabilities that enable agencies to apply consistent data governance practices
Network rigidity: Scaling an edge environment can be resource-intensive, especially when needing to meet peak demands, coordinate maintenance, and monitor operations across distributed locations	Akamai offers the largest and most distributed edge platform, which dynamically scales on demand

Strengthening Government Services in a Digital World

In the face of rapid digitization, providing secure, reliable, and personalized digital experiences is becoming critical. Akamai's suite of services offers comprehensive solutions to meet these needs, with tools like WAAP and EdgeWorkers leading the way. WAAP focuses on robust cybersecurity, safeguarding digital services by protecting applications and APIs against vulnerabilities. In tandem, EdgeWorkers enhances the customization of digital services, offering tailored experiences based on individual user attributes. Both technologies operate at the edge, significantly improving speed and efficiency while ensuring a high degree of personalization and security.



Leveraging these innovations, government agencies can meet the growing demands of modern citizen services. Akamai's services not only drive digital transformation efforts but also empower these agencies to deliver secure, fast, and highly personalized digital experiences. This significantly enhances citizen engagement and trust, marking a transformative shift in the way government agencies interact with citizens in the digital age.

As a whole, Akamai's Connected Cloud Platform is an invaluable tool for government agencies in this increasingly digital world. By capitalizing on its strengths in cybersecurity, personalization, and data reliability, agencies can ensure they are equipped to offer premier digital experiences to their constituents.

Leverage the edge to transform citizen digital experiences.
Visit akamai.com/publicsector to get started or for more information.

Scan the code above or visit
akamai.com/publicsector
to learn more.

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's Connected Cloud platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 09/23.