Akamai Solution Brief

Enterprise Application Access for U.S. Federal

Providing secure access to internal applications for civilian employees, third-party contractors, and partners is critical for U.S. federal agencies. Past reliance on legacy VPNs and appliance-based solutions invites risk, while some Identity, Credential, and Access Management (ICAM) solutions lack the continuous authorization and deep forensic visibility required to investigate intrusions, leaks, and insider threats.

Akamai Enterprise Application Access, authorized at the FedRAMP Moderate level, solves these problems by delivering a Zero Trust access proxy that provides highly secure, continuous authorization and authentication enforced at the edge.

Highly secure, continuous authorization

Enterprise Application Access provides Zero Trust access for civilian employees, third-party contractors, and partners across the internet, regardless of location or device type.

As a Zero Trust access proxy, Enterprise Application Access provides **continuous authorization and authentication**, meaning it constantly verifies a user's identity and their permissions to access data. Specifically, it fronts every request to back-end systems, providing detailed policy enforcement for each transaction.

Akamai's ICAM advantages

Enterprise Application Access removes the operational cost and risk of VPNs and appliance-based solutions by providing microperimeter-style access to an individual application enforced at the edge, versus broad network-level access.

Enterprise Application Access uniquely supports U.S. federal agencies:

- Transactionally identifies and logs all hits and requests correlatable down to the server level
- Logs authenticator assurance level (AAL), identity assurance level (IAL), and authentication mechanisms (e.g., PIV), all of which are tied to NIST SP 800-63
- Integrates with legacy systems that don't use SAML or OIDC

By contrast, other ICAM solutions are in-line only for the initial authentication and authorization event. This means each back-end system must handle continuous authorization, which increases the potential for misconfiguration and compromise. Moreover, other solutions work in fail-open mode, providing the requestor initially unauthenticated access to the origin/source system.

Benefits

- Ensures continuous authorization and authentication
- Fuels deep forensics, resulting in more accurate root cause analysis and faster resolution
- Accelerates procurement and enablement as managed solution with FedRAMP Moderate authorization
- Removes the operational cost and risk of maintaining and patching VPNs or other appliance-based solutions
- Can scale to support millions of personnel and all systems requiring ICAM access

Akamai

Enabling deep forensics

System owners can use session IDs to link enterprise transactions to their own, providing end-to-end analysis down to the server level.

With Enterprise Application Access, U.S. federal agencies can:

- Analyze and resolve issues fast, fueling investigations related to intrusions, leaks, and insider threats
- Troubleshoot issues related to non-malicious events such as system failures caused by user error

Other ICAM solutions that are in-line only for the initial event have limited forensic visibility.

Globally scalable

Built on the world's most distributed platform for cloud computing, security, and content delivery, Enterprise Application Access is currently deployed by healthcare organizations, universities, financial institutions, and the U.S. military to support critical missions and citizen services.

By contrast, other ICAM solutions are regionally constrained, meaning all authentication traffic is required to traverse to a small number of contiguous U.S. (CONUS) locations.

Sophisticated yet user-friendly

Enterprise Application Access authorized at FedRAMP Moderate is based on the same commercial-grade solution used by some of the world's biggest banks, retailers, and manufacturing companies. This results in more intuitive processes for users and administrators.

Akamai expertly engineered the FedRAMP Moderate version of Enterprise Application Access to enable even easier central governance and knowledge sharing via easy-to-understand managed policies, authorization roles, and policy engine configuration.

Available via enterprise license

Enterprise Application Access is available as an all-inclusive enterprise license, so procurement officers can more easily budget for usage growth. Additional features to address new and evolving needs can be purchased and executed through continuous integration/continuous delivery (CI/CD) and via our experienced teams.

> **With Enterprise Application Access, I've now been able to publish or make things available on the outside that I couldn't make available otherwise.**
>
> **CIO, Arc of Ulster-Greene, U.S. not-for-profit organization**

Akamai for the U.S. government: By the numbers

Deployed commercially in more than 125 countries across more than 4,120 points of presence and a global footprint on NIPRNet and SIPRNet

Secures more than 50 million authentication events each month

Protects and accelerates more than 5,000 government agency digital properties

Processes more than 60 million DNS queries daily

Blocks more than 1,000 malicious requests daily

Supports more than 20 U.S. government entities

Ready to take advantage of the commercial internet in your environment?

In an ever-changing security threat landscape, Akamai stands for both stability and innovation. **Contact the Akamai Federal Civilian sales team** to find out how we can help.

© 2026 Akamai Technologies | Support | | Published 05/26