Compliant Modernization with FedRAMP

Moving to the cloud securely has never been more important. As agencies become fully entrenched in the new normal, ensuring that you can continue to realize your mission for your constituents while staying secure, available, and compliant doesn't need to be a compromise.

That's why Akamai has maintained a Joint Authorization Board (JAB) Provisional Authority to Operate (P-JAB-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) since 2013. Akamai's cloud services can be used directly or with other front-end FedRAMP-compliant solutions. Combined, these offer you an end-to-end and compliant solution designed to streamline the use of shared cloud services.

This fact sheet outlines the accreditation boundary of Akamai's FedRAMP P-JAB-ATO.

FedRAMP at the edge

Akamai's FedRAMP accreditation boundary includes the majority of the Akamai Intelligent Edge Platform. Our massively distributed architecture includes more than 350,000 servers deployed in over 135 countries across 4,200 networks. More than 136,000 of those servers are within the United States, putting the Akamai edge within a single network hop of 85% of all end users in the country.

The edge is where Akamai's business logic and security capabilities are applied. This puts business logic such as offload and routing within a single network hop of all client users. This also puts security capabilities and policy enforcement at the same place – within one network hop.

With authorized solutions operating at the edge, Akamai provides many of the security capabilities outlined in the TIC 3.0 use cases. More important, the Akamai Intelligent Edge Platform provides the foundation for developing a secure access service edge (SASE) architecture.

Akamai's FedRAMP accreditation boundary

Cloud Security: Akamai extends security capabilities to Akamai's edge with cloud-based solutions that are designed to ensure the availability and security of your online properties. This includes our industry-leading DDoS mitigation, web application firewall, bot management, authoritative DNS, and threat intelligence.

Optimized Performance: Extending security capabilities and business logic to the edge has been shown to improve overall performance and public engagement. Akamai's edge can apply logic to adapt content to client users based on device capabilities, without needing to make additional callbacks. The offload not only reduces the operational impact on government resources, but also reduces operational costs.

FedRAMP

Service Name
Akamai – Content Delivery Services

Service Model
IaaS

Deployment Model
Public Cloud

Impact Level
Moderate

Authorization Date
August 23, 2013

Package ID
F1206061353

3PAO
Coalfire Systems, Inc.

Contact Information
Akamai FedRAMP Team
fedramp_info@akamai.com

Akamai

Modernized Ecosystem: Collectively, the Akamai Intelligent Edge Platform and underlying solutions will empower you to have an agile multi-cloud environment with the foundational features for developing a SASE architecture. This includes providing TIC 3.0 security capabilities, a powerful suite of APIs for developers to integrate into a DevOps environment.

Accredited solution sets include:

- Application layer security, including web application firewall and bot management
- Akamai cloud storage
- Authoritative DNS with DNSSEC- and DNS-based traffic management
- Akamai management interfaces and APIs
- Edge delivery network

… and more

Package request – U.S. federal agencies may request access to Akamai's FedRAMP package on OMB MAX by submitting the package request form.

To learn more, visit akamai.com or contact your Akamai sales team.

FedRAMP

FedRAMP is a U.S. government program that standardizes the approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP's guiding principle is reuse: do once, use many times. The 325 controls in the FedRAMP Moderate baseline leverage National Institute of Standards and Technology (NIST) guidelines to provide standardized security requirements for cloud services. Once authorized, cloud service providers are responsible for continuous monitoring, which includes vulnerability scanning, penetration testing, and annual control testing by third-party assessment organizations (3PAO).

 | Support | Published 09/21