AKAMAI SOLUTION BRIEF

Enterprise Application Access for Defense

More than 3.4 million service members and civilians across more than 160 countries need to access U.S. Department of Defense (DoD) networks, systems, and data to accomplish their missions. Ensuring that each of them is authorized to access the precise tools they need, and only those tools, is immensely challenging.

This Zero Trust approach to Identity, Credential, and Access Management (ICAM), mandated in part by Executive Order 14028, is made more difficult by a broad drive to take advantage of the benefits of commercial and government off-the-shelf (COTS/GOTS) solutions.

Enterprise Application Access (EAA) for Defense helps make all of this possible.

Highly secure, continuous authorization

EAA for Defense provides Zero Trust access for service members, civilian employees, third-party contractors, and partners, regardless of location or device type, across the internet.

As a Zero Trust access proxy, it fronts every request to back-end systems to provide detailed policy enforcement per transaction and ensure continuous authorization.

Akamai's ICAM advantages

EAA for Defense eliminates 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.

Akamai's ICAM solution is unique in that it is the only one that transactionally identifies and logs all hits and requests correlatable down to the server level, and integrates with legacy systems.

EAA for Defense logs authenticator assurance level (AAL), identity assurance level (IAL), and authentication mechanisms such as Common Access Card (CAC) and MobileConnect, all of which are tied to NIST SP 800-63, the DoD's digital identity standard.

By contrast, other ICAM solutions are limited by being 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, allowing for faster resolution

Makes quick procurement and enablement possible because it is an Authorized to Operate managed solution

Eliminates the operational cost and risk of maintaining and patching VPNs or other appliance-based solutions

Can scale to support all DoD personnel and all systems requiring ICAM access

Enabling deep forensics

EAA for Defense enables system owners to use Session IDs to link enterprise transactions to their own, providing end-to-end analysis down to the server level.

Mission owners can analyze and resolve issues fast, fueling investigations related to intrusions, leaks, and insider threats, but also are able to 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

EAA for Defense is currently deployed by two branches of the U.S. armed forces with global footprints and can scale to support the entire U.S. military.

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

Sophisticated yet user-friendly

EAA for Defense 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.

Per the request of the Defense Information Systems Agency (DISA), Akamai expertly engineered EAA for Defense 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

EAA is available as an all-inclusive enterprise license, enabling procurement officers to 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 a fully cleared team that is already authorized to customize code.

> As a solution granted the Authority to Operate (ATO), EAA for Defense has been expertly engineered and tailored to address department needs.
>
> — ICAM Lead, U.S. Military

EAA for Defense

Currently services **two branches of the U.S. armed forces** and more than **3,000 DoD URLs/systems**

Currently supports more than **50 million authentication events** and **billions of transactional policy enforcement hits** monthly

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. Find out how we can help by contacting the Akamai Defense sales team.