

Akamai Guardicore DNS Firewall

Complete visibility and control for workload DNS traffic

The Domain Name System (DNS) is essential for internet services, yet it cannot differentiate between benign and malicious requests. Consequently, enterprises have implemented DNS firewalls to inspect DNS queries, block harmful domains, and resolve safe ones. However, as DNS use extends to encompass workloads, servers, and other connected devices, the lack of visibility and control over this DNS traffic introduces further security risks.

Unified segmentation and a DNS firewall





Akamai Guardicore Segmentation combined with Akamai Guardicore DNS Firewall delivers a powerful defense for your network. By blocking malicious DNS requests and isolating critical network segments, this integration significantly reduces your attack surface and prevents the spread of threats. This dual-layered approach enhances security, ensures compliance, and maintains operational efficiency, making it an essential solution for robust network protection.

How Akamai Guardicore DNS Firewall works

Akamai Guardicore DNS Firewall can be activated in minutes to deliver security and reduce complexity without impacting performance, and can be activated in minutes. Every requested domain is checked against Akamai's real-time threat intelligence, and requests to malicious domains are automatically blocked. Using DNS as an initial security layer proactively blocks threats early in the kill chain, before any IP connection is made. In addition, DNS is designed to be effective across most ports and protocols, thus protecting against malware that does not use standard web ports and protocols.

When a DNS request is blocked, an incident is created that provides security and threat-hunting teams with in-depth information about why the threat was blocked, request source and destination that can be visualized in a map, and rich details about indicators of compromise.

Benefits for your business

-  **Comprehensive threat protection**
By filtering DNS traffic at the network perimeter and enforcing microsegmentation at the internal network level, enterprises can effectively defend against malware, phishing, command and control, and data exfiltration attempts.
-  **Enhanced threat hunting effectiveness**
Incidents help security teams better detect, analyze, and respond to emerging threats, minimizing the impact of breaches and strengthening overall cybersecurity defenses.
-  **Improved visibility and context**
Combined DNS firewall and microsegmentation provide greater visibility into DNS traffic patterns to identify potential threats and policy violations.
-  **Simplified management**
Integrating a DNS firewall with microsegmentation streamlines security management by providing unified policy creation, enforcement, and monitoring. This reduces complexity and operational overhead, enabling enterprises to efficiently manage their security infrastructure.



Akamai's cloud security intelligence

Akamai Guardicore DNS Firewall is powered by Akamai's cloud security intelligence, which delivers real-time intelligence about threats — and the risks that these threats present. Akamai's threat intelligence is designed to protect against current and relevant threats that could impact your business, and to minimize the number of false-positive alerts that your security teams must investigate. This intelligence is built on data gathered 24/7 from Akamai Connected Cloud, which manages up to 30% of global web traffic and delivers up to 14 trillion DNS queries daily. Akamai's intelligence is enhanced with hundreds of external threat feeds, and the combined dataset is continuously analyzed and curated using advanced behavioral analysis techniques, artificial intelligence, and proprietary algorithms. As new threats are identified, they are immediately added to the threat intelligence dataset to deliver real-time protection.

Akamai Connected Cloud

Akamai Guardicore DNS Firewall service is built on Akamai Connected Cloud, which is the world's most distributed platform for cloud computing, security, and content delivery. Akamai Connected Cloud delivers a 100% availability service-level agreement and ensures optimal reliability for an enterprise's DNS security.

Please visit [Akamai Zero Trust Security](#) to learn more