AKAMAI PRODUCT BRIEF

Secure Internet Access Enterprise Cloud-Based DNS Firewall

As organizations adopt Direct Internet Access, software as a service (SaaS) applications, cloud services, work-from-anywhere policies, and the Internet of Things (IoT), their attack surface increases dramatically and they are faced with a host of new security challenges. Protecting the organization and users against advanced targeted threats such as malware, ransomware, phishing, and data exfiltration becomes exponentially more difficult. Security control-point complications and complexities, and security gaps in legacy on-premises solutions, need to be managed with limited resources.

Akamai Secure Internet Access Enterprise is a cloud-based Domain Name System (DNS) firewall that is designed to help security teams ensure that users and devices can securely connect to the internet wherever they happen to be, without the intricacy and management overheads associated with other legacy security solutions. Secure Internet Access Enterprise is powered by real-time threat intelligence based on Akamai's unrivaled global insights into internet and DNS traffic.

Secure Internet Access Enterprise

Built on the global Akamai Connected Cloud and Akamai's carrier-grade recursive DNS service, Secure Internet Access Enterprise is a quick-to-configure and easy-to-deploy cloud-based DNS firewall that requires no hardware to be installed and maintained.

Secure Internet Access Enterprise leverages real-time Akamai cloud security intelligence to proactively identify and block targeted threats such as malware, ransomware, phishing, and low-throughput DNS-based data exfiltration.

Akamai's portal enables security teams to centrally create, deploy, and enforce both unified security policies and acceptable use policies (AUPs) in minutes for all users, wherever they are connected to the internet.

BENEFITS FOR YOUR BUSINESS

Move web security to the cloud with a cloud-based DNS firewall that can be configured and deployed globally in minutes (with no disruption for users) and scaled rapidly

Improve security defenses by proactively blocking requests to malware and ransomware drop sites, phishing sites, and malware command and control (C2) servers, and identify low-throughput DNS data exfiltration based on unique and up-to-date threat intelligence

Control the use of shadow IT and unsanctioned applications by identifying and blocking applications based on category or risk score

Minimize security management time and complexity by reducing false-positive security alerts, decreasing alerts from other security products, and administering security policies and updates from anywhere in seconds to protect all locations

Akamai

How it works

Secure Internet Access Enterprise is a cloud-based security service that can be activated in minutes to deliver security and reduce complexity without impacting performance. This protection can be delivered by simply directing recursive DNS traffic to Secure Internet Access Enterprise using a range of different methods, including IPsec tunnels, a lightweight client, Akamai's managed DNS forwarder, or a modification of your existing DNS resolver.

Every requested domain is checked against Akamai's real-time threat intelligence, and requests to identified malicious domains are automatically blocked. Using DNS as an initial security layer proactively blocks threats early in the kill chain and before any web connection is made. In addition, DNS is designed to be effective across all ports and protocols, thus protecting against malware that does not use standard web ports and protocols. Domains can also be checked to determine the type of content a user is attempting to access, and blocked if the content breaches the organization's AUP.

For additional protection, risky domains can be forwarded to a cloud proxy for URL inspection — requested HTTP/S URLs are checked against Akamai's real-time threat intelligence and malicious URLs are automatically blocked.

Secure Internet Access Enterprise easily integrates with other security products and reporting tools, including firewalls and security information and event management (SIEM) solutions, as well as external threat intelligence feeds, allowing you to maximize investments across all layers of your security stack.

Additionally, deploying the lightweight Secure Internet Access Enterprise client on devices lets organizations quickly and easily protect laptops or mobile devices used off network.

Akamai cloud security intelligence

The Secure Internet Access Enterprise 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 provide protection 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 11 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, machine learning, and proprietary algorithms. As new threats are identified, they are immediately added to the Secure Internet Access Enterprise service, delivering real-time protection.

Akamai Connected Cloud

The Secure Internet Access Enterprise 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 (SLA) and ensures optimal reliability for an enterprise's web security.

BENEFITS FOR YOUR BUSINESS

Reduce risk and improve security for off-network devices without using a VPN with the lightweight Secure Internet Access Enterprise client, which enforces both your security policies and AUPs

Enforce compliance and your AUPs quickly and uniformly by blocking access to objectionable or inappropriate domains and content categories

Increase resilience and reliability with Akamai Connected Cloud and Akamai's carrier-grade DNS platform

Cloud-based management portal

Configuration and ongoing management of Secure Internet Access Enterprise are done through the cloud-based Akamai Control Center portal, enabling management from any location at any time.

Policy management is quick and easy, and changes can be pushed out globally in minutes to ensure that all your locations and users are protected. Real-time email notifications and scheduled reports can be configured to alert security teams about critical policy events so that immediate remediation steps can be taken to identify and resolve potential threats. A real-time dashboard provides an overview of traffic, threat, and AUP events. Detailed information on any activity can be viewed through drill-down on individual dashboard elements. This detailed information provides a valuable resource for analysis and remediation of security incidents.

All portal functionality can be accessed via APIs, and data logs can be exported to a SIEM, allowing Secure Internet Access Enterprise to easily and effectively integrate with your other security solutions and reporting tools.

Features

Security
Block malware, ransomware, and phishing delivery domains and URLs
Block malware C2 requests
Identify DNS-based data exfiltration
Proxy risky domains for requested HTTP and HTTPS URL inspection
Create a customized list of domains for HTTP and HTTPS URL inspection
Perform look-back analyses of customer traffic logs to identify and alert on newly discovered threats
Create custom allow/deny lists
Incorporate additional threat intelligence feeds
Customize error pages
Query Akamai's threat database to gain intelligence on malicious domains and URLs
Enforce security for off-network devices (Windows, macOS, iOS, Android, Chrome)
Acceptable use policy (AUP)
Create group-based AUP policies
Monitor or block AUP violations for on-network and off-network users
Enforce SafeSearch for Google, Bing, and YouTube

Cloud access security broker (inline)
Identify and block shadow IT applications
Block applications on risk score or application group
SaaS tenant enforcement
Reporting, monitoring, and administration
IDP and Active Directory integration
Enterprise-wide view of all activity with customizable dashboards
Detailed analysis of all threat and AUP events
Full logging and visibility of all onboarded traffic requests and threat and AUP events
Log delivery of all logs; logs are retained for 30 days and can be exported via an API
Configuration, custom security lists, and events available via an API
Integrate with other security systems, such as SIEMs, via an API
Email-based real-time security alerts
Scheduled daily or weekly email reports
Delegated administration
Akamai Connected Cloud platform
Dedicated IPv4 and IPv6 VIPs per customer for recursive DNS
SLA for 100% availability
Anycast DNS routing for optimal performance
DNSSEC, DoH, and DoT enforced for increased security
Enterprise device attribution
Inline attribution using DNS forwarder
Offline attribution using Security Connector
Client-based attribution for laptops and mobile devices (Windows, macOS, iOS, Android, Chrome)

To learn more about Secure Internet Access Enterprise and sign up for a free trial, visit akamai.com.