AKAMAI PRODUCT BRIEF

Secure Internet Access Enterprise

With the adoption of Direct Internet Access, SaaS applications, cloud services, mobility and remote working, and the Internet of Things (IoT), organizations encounter numerous security challenges as their attack surface widens significantly. Defending against advanced targeted threats such as malware, ransomware, phishing, and data exfiltration becomes increasingly difficult. Managing security control point complexities and gaps in legacy on-premises solutions with limited resources compounds the issue.

Secure Internet Access Enterprise

Akamai's Secure Internet Access Enterprise is a cloud-based SWG built on the Akamai Intelligent Edge Platform and the carrier-grade recursive DNS service, which can be quickly configured and deployed without any need for hardware installation and maintenance. It leverages multiple layers of protection, including real-time cloud security intelligence and static and dynamic malware-detection engines, to proactively identify and block targeted threats such as malware, ransomware, phishing, and DNS-based data exfiltration.

How it works

Secure Internet Access Enterprise provides comprehensive protection through multiple layers of security such as DNS, URL, and payload analysis. This ensures a high level of security while maintaining performance and reducing complexity. Secure Internet Access Enterprise can be easily implemented by directing web traffic to the platform using various methods such as IPsec tunnels, a lightweight client, or by forwarding web traffic from an existing on-premises proxy or Akamai's managed HTTP forwarder.

Capabilities

- DNS inspection — Akamai's real-time threat intelligence is used to check every requested domain, and any requests to identified malicious domains are automatically blocked. By using DNS as an initial security layer, threats are proactively blocked early in the kill chain, before any web connection is made. DNS is designed to be effective across all ports and protocols, protecting against malware that does not use standard web ports and protocols. The type of content that a user is attempting to access can also be checked to determine if it breaches the organization's AUP and can be blocked accordingly. This multiple layer approach reduces complexity and provides effective security without impacting performance.

BENEFITS FOR YOUR BUSINESS

Migate your web security
to the cloud effortlessly using a cloud-native Secure Web Gateway (SWG) that can be configured and deployed worldwide within minutes without impacting your users, and can be rapidly scaled as per your needs.

Enhance your security defenses
Enhance your security defenses by preemptively preventing requests to malicious and ransomware drop sites, phishing sites, and malware command and control (C2) servers, and identifying DNS data exfiltration through the use of current and distinctive threat intelligence.

Improve zero-day protection
by preventing endpoint devices from being compromised by scanning requested files and web content for malicious payloads, and blocking them.

Enhance security for remote devices
without relying on a VPN, using the Secure Internet Access Enterprise client that enforces your organization's security policies and Acceptable Use Policies (AUPs) while being lightweight.

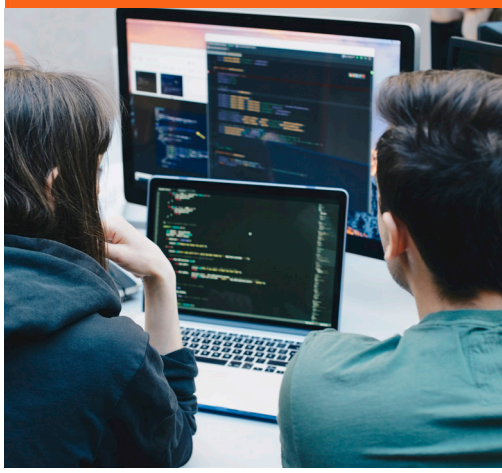
Enhance data security
Enhance data security by detecting and preventing the transmission of confidential or sensitive information like personally identifiable information (PII), payment card industry (PCI) data, or healthcare-related data governed by the Health Insurance Portability and Accountability Act (HIPAA).

- URL inspection — Requested HTTP/S URLs are checked against Akamai's real-time threat intelligence, and malicious URLs are automatically blocked.

- Payload analysis — Multiple advanced malware-detection engines scan HTTP/S payloads inline or offline, utilizing techniques such as signature, machine learning, and sandboxing to deliver comprehensive zero-day protection against potentially malicious files like executables and document files. At the point of request, Akamai's zero-day phishing and malicious JavaScript detection engine categorizes and blocks newly created malicious pages, even if the page has never been seen before. Secure Internet Access Enterprise can integrate easily with other security products and reporting tools, including firewalls, SIEMs, and external threat intelligence feeds, allowing organizations to optimize investments across all layers of their security stack. Deploying the lightweight Secure Internet Access Enterprise client on devices makes it easy for organizations to protect laptops or mobile devices used off-network.

Akamai Partnership

Akamai is a Select Partner. This title is reserved for partners who continue to invest to provide the right product knowledge and product configuration! With more than 15 years of experience with Akamai's solutions, our engineers are now as certified as can be and we got to do some great projects for amazing companies. This is how Evolane combines the benefits of a trusted local partner with the ingenious technology of an international company.



Akamai | Select Partner

Let's talk!

To learn more, click here and visit our Akamai partnerpage on the Evolane website.