AKAMAI PRODUCT BRIEF

Secure Internet Access Cloud Secure Web Gateway

As organizations adopt Direct Internet Access, SaaS applications, cloud services, mobility and remote working, 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.

Secure Internet Access is a cloud-based secure web gateway (SWG) 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 is powered by real-time threat intelligence based on Akamai's unrivaled global insights into internet and domain name system (DNS) traffic and multiple malware-detection engines.

Secure Internet Access

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

Secure Internet Access has multiple layers of protection that leverage real-time Akamai cloud security intelligence and multiple static and dynamic malware-detection engines to proactively identify and block targeted threats such as malware, ransomware, phishing, and 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.

How it works

Secure Internet Access has multiple layers of protection — DNS, URL, and payload analysis — delivering security and reducing complexity, without impacting performance. All of this protection can be delivered by simply directing web traffic to Secure Internet Access using a range of different methods including IPsec tunnels, a lightweight client, or by forwarding web traffic from an existing on-premises proxy or Akamai's managed HTTP forwarder.

BENEFITS TO YOUR BUSINESS

- Move web security to the cloud with a cloud-based SWG 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 DNS data exfiltration based on unique and up-to-date threat intelligence
- Block malicious payloads for improved zero-day protection by scanning requested files and web content to stop threats before they compromise endpoint devices
- Control the use of shadow IT and unsanctioned applications by identifying and blocking applications based on risk score and limiting application features

Akamai

DNS inspection: 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.

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

Payload analysis: The HTTP/S payloads are scanned inline or offline using multiple advanced malware-detection engines. These engines use a variety of techniques — including signature, machine learning, and sandboxing — that deliver comprehensive zero-day protection against potentially malicious files, such as executables and document files. In addition, Akamai's zero-day phishing and malicious JavaScript detection engine categorizes and blocks newly created malicious pages at the point of request even if the page has never been seen before.

Secure Internet Access easily integrates with other security products and reporting tools, including firewalls and SIEMs, 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 client on devices lets organizations quickly and easily protect laptops or mobile devices used off network.

Akamai cloud security intelligence

Secure Internet Access 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 the Akamai Intelligent Edge Platform, which manages up to 30% of global web traffic and delivers up to 7 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 service, delivering real-time protection.

BENEFITS TO YOUR BUSINESS

- Prevent data loss by identifying and blocking the uploading of sensitive or confidential data such as PII, PCI, or HIPAA
- 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
- Reduce risk and improve security for off-network devices without using a VPN with the lightweight Secure Internet Access 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 the Akamai Intelligent Edge Platform

Akamai Intelligent Edge Platform

The Secure Internet Access service is built on the Akamai Intelligent Edge Platform, which is fast, intelligent, and secure. Distributed globally, the platform delivers a 100% availability SLA and ensures optimal reliability for an enterprise's web security.

Cloud-based management portal

Configuration and ongoing management of Secure Internet Access 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 to easily and effectively integrate with your other security solutions and reporting tools.

Key Capabilities

Akamai-categorized threats: Up-to-the-minute threat intelligence based on Akamai's visibility into 7 trillion DNS requests, CDN traffic, and logs from other Akamai security services

Customer-categorized threats: Security teams can quickly integrate existing threat intelligence feeds, extending value from your current security investments

Inline and offline payload analysis: Five advanced malware-detection engines identify and block complex advanced threats and improve zero-day protection

Data loss prevention: Block or monitor file uploads that contain PII, PCI, DSS, or HIPAA data

Application visibility and control: Identify and block usage of unsanctioned applications based on risk score, or limit application features

TLS inspection: Inspect TLS-encrypted requests and payloads

Off-network protection: Protect laptops and mobile devices used off network

Acceptable use policies: Enforce AUPs and compliance by limiting which content categories can and cannot be accessed

Analysis, reports, and logs: Real-time dashboards provide insights into traffic, security, and AUP alerts while logs can be exported or integrated into a SIEM

DoT, or DoH and DNSSEC: Deploy DNS over TLS or DNS over HTTPS and DNSSEC to provide end-to-end security for DNS traffic

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

Security	Essentials	Standard	Advanced
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	✓	✓	✓
Proxy all web traffic for DNS and URL inspection		✓	✓
Inline and offline* analysis of HTTP and HTTPS payloads using multiple malware analysis and detection engines			✓
Cloud sandbox for offline dynamic payload analysis*			✓
Real-time inline analysis of web pages to detect zero-day phishing and malicious JavaScript pages			✓
Real-time inline or offline* analysis of files downloaded from file-sharing sites			✓
Create a customized list of domains for HTTP and HTTPS URL inspection	✓	✓	✓
Create a customized list of domains for inline/offline* payload analysis			✓
Lookback analysis of customer traffic logs to identify and alert on newly discovered threats	✓	✓	✓
Create custom allow/deny lists	✓	✓	✓
Incorporate additional threat intelligence feeds	✓	✓	✓
Customizable 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)	**Essentials**	**Standard**	**Advanced**
Create group-based AUP policies		✓	✓
Monitor or block AUP violations for on-network and off-network users	✓	✓	✓
Enforce SafeSearch for Google, Bing, and YouTube	✓	✓	✓
Integrated Data Leakage Prevention	**Essentials**	**Standard**	**Advanced**
Standard dictionaries for PCI, PII, and HIPAA, and custom dictionaries			✓
Block or monitor policy actions			✓
Reporting			✓

Cloud Access Security Broker (inline)	Essentials	Standard	Advanced
Identify and block shadow IT applications	✓	✓	✓
Block applications on risk score or application group	✓	✓	✓
Block/allow application operations		✓	✓
SaaS tenant enforcement	✓	✓	✓
Reporting, Monitoring, and Administration	**Essentials**	**Standard**	**Advanced**
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 Intelligent Edge Platform	**Essentials**	**Standard**	**Advanced**
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	**Essentials**	**Standard**	**Advanced**
Inline attribution using DNS Forwarder	✓	✓	✓
Offline attribution using Security Connector	✓	✓	✓
Client-based attribution for laptops and mobile devices (Windows, macOS, iOS, Android, Chrome)	✓	✓	✓

* Cloud sandbox is an optional add-on and is required for offline analysis of large files.