Secure Web Gateway

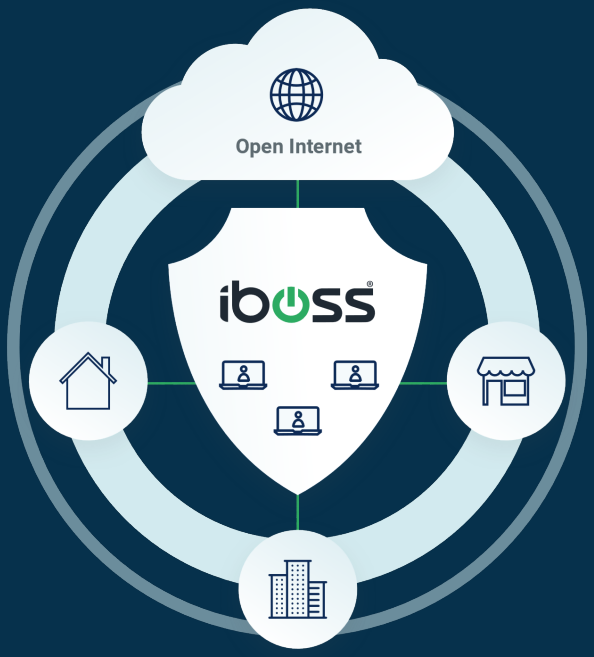
Simplify secure Internet access for users everywhere with the unified iboss SASE Platform

The iboss Secure Web Gateway (SWG) is a core component of the unified iboss SASE platform, built to provide fast and secure internet access while protecting users and data across all locations. By delivering advanced capabilities such as malware defense, data loss prevention, and deep content inspection, the iboss SWG ensures that every connection is safeguarded, whether users are working remotely or on-premises.

With consistent security policies applied across your entire organization, the iboss SWG eliminates the complexity of managing disparate systems and reduces costs by consolidating your network and security needs into a single, cloud-based solution. Seamlessly integrating with your existing infrastructure, it empowers enterprises to simplify management, enhance compliance, and enable secure connectivity for today's dynamic workforce.

By leveraging the scalability and flexibility of the iboss platform, organizations can future-proof their security strategies while delivering the fast and reliable internet access that modern businesses demand.

Key Benefits and Capabilities



Advanced Threat Protection Without Compromise

Protect against advanced threats with iboss SWG's malware defense, inspecting all content, including HTTPS traffic, without legacy throughput limitations.

Consistent Protection Across All Environments

Ensure consistent protection for on-premises and remote users with iboss SWG's unified security approach, eliminating gaps and inconsistencies.

Flexible Deployment Options

Leverage iboss SWG capabilities in the cloud with the option to extend security on-premises using gateways that deliver all cloud security features locally.

Addressing Modern Security Challenges

Challenge

As organizations embrace hybrid work environments and cloud applications, traditional security models struggle to keep up with the expanding attack surface. Cyber threats such as phishing, ransomware, and malware have become more sophisticated, targeting both users and data regardless of their location. Legacy solutions are often unable to inspect encrypted traffic or enforce security policies uniformly, leaving critical gaps in protection.

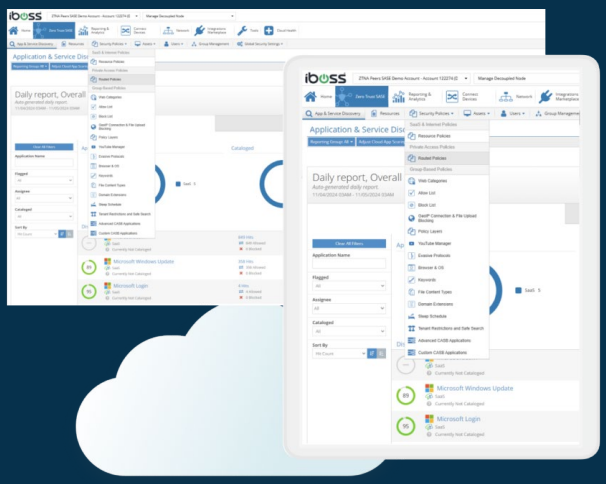
Solution

The iboss Secure Web Gateway (SWG) eliminates the limitations of legacy security models by delivering web traffic protection through a modern, cloud-first approach. Built on the iboss Zero Trust Secure Access Service Edge (SASE) architecture, the SWG secures all user internet activity regardless of location. It inspects web traffic in real time, including encrypted HTTPS traffic, without the performance bottlenecks of traditional appliances. By shifting security to the cloud, iboss ensures that protection scales seamlessly with your organization's needs, reducing complexity and enhancing flexibility.

Benefit

With consistent security policies across remote users, branch offices, and private data centers, organizations can achieve comprehensive protection regardless of location. Leveraging a cloud-first architecture, security scales effortlessly while reducing reliance on traditional appliances. For environments requiring on-premises protection, optional gateways extend the same advanced threat prevention and data protection capabilities locally, ensuring flexibility without compromising security. This unified Zero Trust approach simplifies management and reduces costs, delivering the protection modern enterprises need.

Why Choose iboss for Secure Web Gateway?



Unlike legacy web security solutions that rely on hardware appliances or fragmented approaches, iboss integrates Secure Web Gateway capabilities into a unified Zero Trust SASE platform. The iboss Secure Web Gateway (SWG) provides organizations with a cloud-native solution to secure internet access, offering advanced protection against modern threats such as malware, ransomware, and data exfiltration. By inspecting traffic in real time, including encrypted HTTPS traffic, iboss ensures that every connection is evaluated for compliance and security, regardless of user location.

iboss SWG offers the flexibility to meet diverse organizational needs, including the option to extend security to private data centers and branch offices with on-premises gateways. These gateways provide the same robust protection locally, ensuring consistency across all environments. By streamlining security policies and reducing operational overhead, iboss SWG helps organizations enhance their security posture without compromising performance and scalability.

Key Use Cases

Enhance Threat Protection

iboss SWG delivers advanced malware and threat detection through real-time traffic analysis, blocking malicious activity before it compromises users or systems. By leveraging threat intelligence and behavioral analysis, the solution identifies and mitigates risks, including zero-day threats, ensuring a proactive security posture for organizations.

Prevent Data Loss

Integrated Data Loss Prevention (DLP) features within iboss SWG monitor and control sensitive data transfers, ensuring compliance with regulatory standards such as GDPR and HIPAA. The solution prevents unauthorized data exfiltration through detailed inspection of web traffic, securing confidential information while maintaining transparency and trust across the organization.

Inspect Encrypted Web Traffic

iboss SWG performs real-time inspection of encrypted HTTPS traffic, addressing the critical challenge of hidden threats within encrypted data. By leveraging advanced SSL decryption and inspection capabilities, it ensures threats are blocked before they reach users, without impacting performance. This capability is essential for organizations that prioritize visibility and security in encrypted environments.

Protect Remote Workforces

iboss SWG ensures seamless security for remote users by enforcing consistent policies and inspecting all web traffic, including encrypted connections. This eliminates the need for VPN backhauling, providing direct-to-cloud security that enhances performance while reducing complexity. Remote users remain protected from malware, phishing, and data exfiltration, ensuring secure access to the internet and cloud applications, regardless of location or device.

Secure Hybrid Environments

With support for cloud and on-premises deployment, iboss SWG secures hybrid environments by unifying security policies across remote users, branch offices, and data centers. Optional on-premises gateways provide localized protection while maintaining the same robust cloud-based capabilities, ensuring consistent security for critical resources.

Consolidate Security Tools

By combining multiple security functions—including firewall, URL filtering, malware protection, and DLP—into a single solution, iboss SWG simplifies security architectures. This reduces the need for disparate tools, streamlining management and lowering operational costs while providing comprehensive protection for web traffic across the organization.

How it Works

1. User Authentication via iboss Cloud Connector

Users connect through the iboss Cloud Connector, which establishes a secure tunnel to the iboss platform. iboss integrates with Identity Providers (IdPs) to authenticate users, ensuring only authorized individuals gain access.

2. Device Posture Assessment

iboss evaluates device compliance, checking for factors like anti-malware status, firewall activation, and disk encryption to confirm that devices meet security standards before granting access.

3. Contextual Access Evaluation

iboss assesses contextual factors, such as geolocation and IP address, to determine the legitimacy of each access request.

4. Granular Policy Enforcement

Based on user identity, device posture, and contextual information, iboss enforces resource-specific access policies, ensuring users can only access authorized resources, thereby minimizing the attack surface.

5. Continuous Monitoring & Threat Containment

iboss continuously monitors user traffic for anomalies and threats, allowing for real-time responses to potential security incidents. If a device is detected as compromised, iboss automatically revokes its access to prevent the spread of malware or ransomware.

6. Comprehensive Logging and Reporting

iboss logs every access request, session, and resource interaction, providing detailed visibility into user activity.

Features

Advanced Malware Defense
Protect against advanced threats with real-time traffic inspection, including HTTPS, without performance limitations.

AI-Powered Data Loss Prevention
Prevent unauthorized data transfers with advanced DLP, leveraging AI/ML and OCR to detect sensitive information in documents.

Inline SaaS Application Control
Secure and control SaaS app usage with inline CASB capabilities, enforcing granular policies and preventing data exfiltration.

Comprehensive Logging and Visibility
Gain detailed user activity insights with full transaction logs, essential for compliance, auditing, and proactive security.

Unified Security Across Environments
Enforce consistent security policies for remote and on-premises users, eliminating protection gaps and inconsistencies.

Flexible On-Premises Gateway Option
Extend cloud capabilities on-premises with gateways delivering all features locally for branch offices and data centers.

Consolidated Networking and Security
Replace multiple devices with a single solution offering SWG, ZTNA, SD-WAN, and firewall capabilities.

High-Performance Architecture
HTTPS decryption and deep content inspection that does not slow down your network—no matter the volume of data.

Seamless Infrastructure Integration
Integrate with existing systems effortlessly, using standard protocols for smooth deployment without disruptions.

Enhanced User Experience
Direct traffic to SaaS and cloud destinations without detours, ensuring improved performance and seamless connectivity.

Extensive Authentication Support
Leverage SSO, Kerberos, and other authentication methods to replace legacy proxies while maintaining seamless user access.

Competitive Security Advantage
Outperform legacy and competing solutions with iboss' integrated approach, offering better security and lower costs.

Supported Platforms & Systems

Endpoint Cloud Connector

- Windows
- macOS
- Linux
- ChromeOS
- iOS
- Android

Network Connector

- AWS
- Docker
- VMware OVF

Policy Enforcement Points

- iboss Global Cloud (100+ POPs)
- Azure
- Private Locations

Fast and Secure Access

Advanced threat protection, data loss prevention, and comprehensive visibility—all within the unified iboss SASE platform.

iboss Secure Web Gateway (SWG) is an integral part of the iboss SASE platform, providing advanced malware defense, data loss prevention, and deep content inspection. Protect users across all locations with consistent security policies, whether they are remote or on-premises. Simplify management, reduce costs, and enhance security with a solution that seamlessly integrates with your existing infrastructure.

Request a Demo Today

To speak with an iboss representative, please call: Americas: +1-877-742-6832 ext. 1 UK&I : +44 020 3884 0360 International: +1-858-568-7051 ext.