

The iboss Distributed Gateway Platform

Cybersecurity for the Distributed Organization

Meeting the Challenges of Distributed Organizations

The iboss Distributed Gateway Platform™ is specifically designed to solve the challenges of securing distributed organizations. It is the first and only solution that leverages an elastic, node-based architecture that is built for the cloud. The iboss Distributed Gateway Platform provides the advanced security organizations need and the scalability they require to meet their ever-increasing bandwidth demands.

Unlike traditional secure web gateways (SWG), the iboss Distributed Gateway Platform delivers high-performance cybersecurity in a 100% SaaS subscription model, meaning global enterprises never have to purchase or manage on-prem appliances again.

The iboss Difference

Innovation for today with flexibility for tomorrow:

- Ideal for distributed organizations with many branch locations and mobile workers
- Flexible deployment options—cloud gateways, optional physical gateways, or both—and feature packages
- Eliminates costly data backhaul, expensive legacy SWG appliances, and unnecessary load balancers

Advantages of the iboss Distributed Gateway Platform

The iboss Distributed Gateway Platform delivers a range of operational, financial, and technological benefits including:

Cuts backhaul, bandwidth and infrastructure costs –

Eliminates the need for backhaul appliances and expensive VPN and MPLS links, delivering immediate ROI. This also reduces future costs due to increasing backhauled bandwidth.

Requires no network reconfiguration – Unique architecture enables drop-in replacement of legacy SWG appliances with no disruption to the existing network topology, configuration, or processes, shortening implementation times and reducing costs.

Eliminates CAPEX costs – Customers never need to buy SWG hardware appliances again. Instead, they can easily add capacity or additional functionality seamlessly through their iboss SaaS subscription.

Creates data center efficiencies – Eliminates ancillary power, space, and operating costs associated with server farms and load balancers.


Offers on-demand scalability – Elastic scaling enables customers to easily add target capacity and capabilities to support organizational growth, increased bandwidth, and evolving requirements for device support.

Provides complete control – Unique, non-shared cloud and physical gateways let customers take back control of change management schedules, and improves overall system security.

Establishes a consistent user experience – All features, functions, policies, and security services are consistent across the distributed enterprise, regardless of device or location.

Packaging Overview

Customers can choose from one of three feature packages, based on their gateway security needs. All Distributed Gateway Platform packages include customized, real-time reporting; centralized management and administration in the cloud; flexible data redirection for any device, anywhere; and unmatched LIVE 12-hour support.



Core —
Essential web gateway features for both on- and off-network devices

Advanced —
Core Package features plus advanced malware defense and more

Premium —
Advanced Package features plus advanced data loss prevention capabilities

Key Features The iboss Distributed Gateway Platform

Complete web content filtering – For effective blocking of access to harmful, objectionable, or otherwise unwanted online content. Capabilities include: Stream-based protection covering all ports and protocols, granular category- and user-based filtering, alerts on user-defined keywords and events, port access management, and a dynamic URL database.

Unmatched malware prevention – A robust and dynamic set of malware detection and prevention capabilities that protect organizations against viruses, worms, Trojans, ransomware, and attacks that use evasive applications, such as TOR. Features include: signature-based malware prevention and breach detection, CnC callback monitoring across all ports and protocols, automated locking of infected devices, crowd-sourced threat intelligence, and rapid response capabilities.

Industry-leading SSL traffic management – Monitors and manages the growing amounts of SSL traffic on organizations' networks, enabling them to detect, block, and respond to SSL-based threats faster and more effectively. Capabilities include: the fastest and most scalable SSL decryption available, and micro-segmentation for selective decryption based on content, device, user, group, or other user-defined parameters.

BYOD and guest Wi-Fi management – Reduces the risks presented by BYOD devices and guest Wi-Fi users with integrated BYOD management that extends security across all the devices using your network. Capabilities include: identification of BYOD users not using a NAC and automated binding to the network directory or LDAP, advanced application controls, and automatic high-risk quarantine.

Single-platform orchestration – Provides single-pane-of-glass management with real-time visibility across all locations and devices. Capabilities include: cloud-based admin console with responsive web UI, bi-directional policy management, seamless directory integration and group management, and system-delegated administrators.

Customized, real-time reporting – Streamlines the production of timely, accurate, and professional reports for a range of compliance and internal management purposes. Automated reporting capabilities include: comprehensive drill-down reports; live, historical, and statistical reports; and easy report scheduling and customization. Also includes native Splunk integration and SIEM integration for forensic-level reporting.

Intrusion detection and prevention – Delivers highly effective, real-time detection and prevention of network breaches by viruses, worms, and other categories of malware. Includes an automated data feed of threat signatures with frequent updates. Provides instantaneous views of event details, including source and destination IP addresses, and easy rules creation and editing.

Incident response center – Analyzes and prioritizes security incidents to enable faster and more effective responses. Automatically translates and correlates data from security event logs in real-time to identify the most serious incidents that require prioritized and expedited remediation.

Behavioral malware sandboxing – Leverages file detonation for signatureless malware detection. Suspicious downloads or other untrusted files can be safely inspected, and if necessary, neutralized.

Package Add-ons Customize the platform to fit your needs

Bandwidth monitoring and shaping – Gives organizations complete visibility into their bandwidth utilization, ensuring availability by spotting problems and curbing misuse. Capabilities include: centralized policy and threshold setting and monitoring, and controls for ensuring bandwidth availability at critical times and locations.

Network anomaly detection and containment Monitors packets, bytes, and connections across all 131K data channels to establish baselines of normal network traffic. Automatically detects anomalous behavior, contains the malware that is causing it, and stops the activity before data loss occurs. Includes data flow restrictions by country, organization, or subnet, with fully configurable thresholds. Delivers full-stream protection, including TCP and UDP ports, and provides real-time alerts and drill-down forensics for anomalous traffic.

Cyber risk scoring – Powered by industry-leading analytics technology from FICO, this feature automatically identifies and scores the cyber risks posed by specific users and devices. This feature provides real-time cyber threat quantification and remediation by leveraging proprietary algorithms to quickly spot breaches other systems miss, including attacks using TOR.

Mobile device management – Provides the ability to monitor, manage, and secure mobile devices anywhere, any time. Includes granular application management, application locking or pushing, and live device location GeoMapping.

About iboss

iboss has created the first and only Distributed Gateway Platform specifically designed to solve the challenge of securing distributed organizations. Built for the cloud, iboss leverages an elastic, node-based architecture that provides advanced security for today's decentralized organizations and scales to meet the ever-increasing bandwidth needs of tomorrow. The iboss Distributed Gateway Platform is backed by more than 100 patents and protects over 4,000 organizations worldwide, making iboss one of the fastest growing cybersecurity companies in the world.

To learn more, visit www.iboss.com or contact iboss at sales@iboss.com