Core Package

iboss
™
THE DISTRIBUTED GATEWAY PLATFORM

The iboss Distributed Gateway Platform

Packaging Overview

iboss offers three different feature packages for customers to choose from, based on their specific gateway security needs. All Distributed Gateway Platform™ packages include advanced, real-time reporting; centralized management and administration in the cloud; flexible data redirection for any device, anywhere; and LIVE 12-hour support. This data sheet discusses the Core Package, which offers essential web gateway features for both on- and off-network devices.

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

Core Package Features

The Core Package is our entry-level offering and provides essential Web Gateway features for both on- and off-network devices. It includes all standard web gateway features and much more:

Complete web and content filtering – **for blocking access to online content that is harmful or objectionable**.
- Stream-based protection, including all ports and protocols (TCP & UDP)
- Granular category- and user-based filtering
- Real-time alerts based on keywords, events, and other customizable triggers
- File extension, domain extension, and content MIME type blocking
- Port access management
- Dynamic real-time URL database
- Proxy-based deep file analysis and inspection

Compliance with industry regulations for data privacy and protection – **for ensuring your organization is compliant with data privacy and protection policies and regulations.**
- Supports HIPAA compliance with Business Associates Agreement (BAA)
- CIPA-compliant content filtering for students and staff

SSL traffic management – **for monitoring and managing the growing amount of encrypted traffic, especially attempts to use SSL to bypass control measures.**
- Fastest, most scalable SSL decryption available
- Micro-segmentation to selectively decrypt based on content, device, user, or group

Cloud application and social media controls – **for closely managing which cloud-based apps and social media sites can be accessed and used.**
- Advanced application scanning and deep packet inspection (DPI)
- Content-aware management of social media applications like Facebook, Twitter, LinkedIn, and Pinterest
- Granular control over evasive cloud applications like TOR, BitTorrent, SnapChat, Skype, and more
- Safe Search enforcement for Google, Bing, and Yahoo
- Clean Image Search and Translation Filtering for Google Services

Mobile device protection – **for extending cybersecurity coverage for all of an organization's mobile devices, regardless of where or when they're used.**
- Complete content filtering for iOS, Android, Windows, Mac, and Chromebook devices
- BYOD and guest Wi-Fi policy management

Protection for out-of-date browsers and operating systems – **for extending protection of deployed technologies after end-of-life (EOL), when vendors stop issuing security updates and patches for them.**
- Browser EOL protection
- Operating system EOL protection

All Packages Include:

Customized, real-time reporting
for streamlining the process of producing timely, accurate, and professional reports for a range of compliance and internal management purposes. Reporting capabilities include comprehensive, drill-down reports; live, historical, and statistical reports; plus report scheduling and customization. Administrators can instantly pinpoint and lock users attempting to circumvent security via evasive protocols, and can auto-trigger Video Desktop Recording (DMCR). The iboss Distributed Gateway Platform also offers seamless SIEM integration for forensic-level reporting, as well as native Splunk integration.

Centralized management and administration in the cloud
for seamless policy management across all locations and users from a single pane of glass. The iboss Distributed Gateway Platform provides a cloud-based admin console with a fully responsive web UI. Regardless of the gateways an organization deploys, all features, functions, and policies are consistent across the distributed enterprise and all its devices and locations. Capabilities include complete bi-directional policy management, system-delegated administrators and reporting groups, location-based policies, and custom branding on end user sign-in and block pages.

Flexible traffic redirection for any device, anywhere to ensure the protection of all devices, no matter the operating system. Includes Windows, Mac, iOS, Android, Chromebook, and Linux devices.

Unmatched LIVE 12-hour support
is included in all packages at no additional charge, so any technical problems or questions can be quickly and easily addressed.

Additional Features

Check out the iboss Advanced and Premium Packages if you'd like to add other features, like advanced malware defense and data loss prevention.

Additionally, iboss offers other features and services that can be added onto any package. Those include: bandwidth optimization, mobile device management, network anomaly detection and containment, and cyber risk scoring, as well as Premier and Mission Critical Support.

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