Data Sheet

Data Loss Prevention Package

ibOSS®
THE DISTRIBUTED GATEWAY PLATFORM

The iboss Distributed Gateway Platform

Packaging Overview

iboss offers three different 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 12-hour LIVE support. This data sheet discusses the Data Loss Prevention package, which offers essential web gateway features, advanced data loss prevention capabilities, and more.
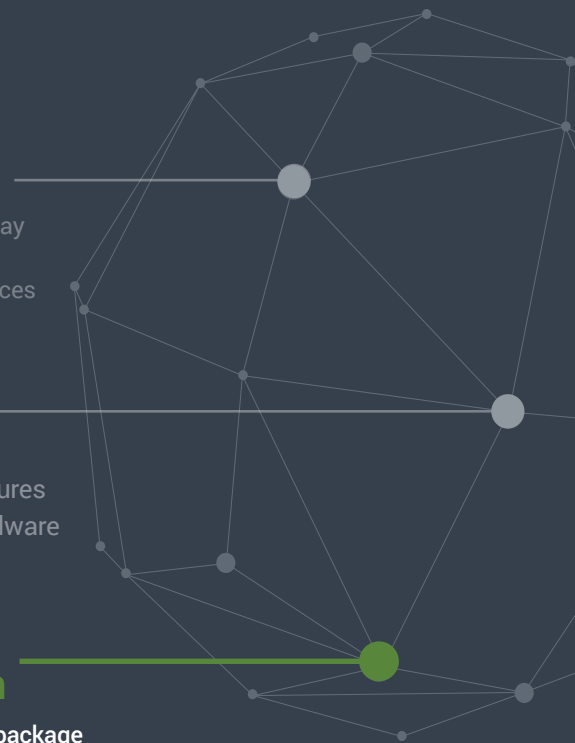
Core
Essential web gateway features for both on- and off-network devices

Malware Defense
Core package features plus advanced malware defense & more

Data Loss Prevention
Malware Defense package features plus advanced data loss prevention capabilities

Data Loss Prevention Package Features

The Data Loss Prevention (DLP) package is our most comprehensive offering. It includes all the standard security features from our Core package, all advanced malware defense features from our Malware Defense package, plus deep file-based data loss prevention capabilities.

Deep File-Based Data Loss Prevention Capabilities

The DLP package offers comprehensive file-based data loss prevention capabilities that detect and stop the transfer of sensitive data to and from the cloud while keeping security teams informed with automated alerts. This provides protection against unauthorized cloud use and sensitive data loss protection for the use of the cloud, ensuring sensitive data is secured and maintained within organizationally approved cloud services.

Advanced Detection Capabilities

- Screen content to prevent unintended loss of sensitive information
- Capable of scanning: Credit card numbers, Personally Identifiable Information (PII), email addresses, GPS map data, AES encryption keys, credit card stripe data, phone numbers, KML map data, Windows directories

Advanced Content Analysis Engines

- Process and parse targeted files, ensuring that even compressed content is accessible to the detection engines
- Set compressed file max scan depth to search for content deep within zip files
- Analyzes numerous file types including: Base16, GZip, PDF, Outlook data files, SQLLite Database , Windows PE Executables, Zip files, RAR files, Windows Hibernate Files, Windows LNK files, Windows PE Files

The DLP Package Also Includes:

All Core and Malware Defense Features

Complete web and content filtering across all ports and protocols, with a dynamic, real-time URL database.

Compliance with industry regulations for data privacy and protection, including HIPAA and CIPA.

Fastest and most scalable SSL traffic management, with microsegmentation to selectively decrypt based on content, device, user, or group.

Cloud application and social media controls for content-aware management of social media applications like Facebook, Twitter, LinkedIn, and Pinterest.

Mobile device protection for extending cybersecurity coverage across all iOS, Android, Windows, Mac, and Chromebook devices.

Protection for out-of-date browsers and operating systems for extending protection of deployed technologies after EOL.

Signature-based malware prevention and breach detection leveraging best-of-breed industry signature databases for up-to-the-minute threat information.

Command and Control (CnC) callback monitoring across all ports and protocols, including domain, URL, and blacklisted IP monitoring.

Behavioral Malware Sandboxing Defense for real-time auto- or manual-deposit of user downloaded files for behavioral sandboxing analysis.

SDN integration for threat isolation, including infected machine auto-locking to block internet communication.

Global cloud threat intelligence to analyze and predict threat behavior using crowd-sourced threat intelligence.

Time-saving Incident Response Center for real-time translation and prioritization of security event logs into incidents, reducing noise.

Intrusion Detection and Prevention Real-time intrusion, malware and virus 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

iboss also offers add-on features and services that can be added to any package. Those include: bandwidth optimization and network anomaly detection & containment, as well as Mission Critical Support.

About iboss

The iboss Distributed Gateway Platform is a web gateway as a service that is specifically designed to solve the challenges of securing distributed organizations. Built for the cloud, iboss leverages a revolutionary, node-based architecture that easily scales to meet ever-increasing bandwidth needs and is managed through a single interface. The iboss Distributed Gateway Platform is backed by more than 110 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

DATA SHEET / Data Loss Prevention Package / PAGE 4

LN-02-18