Data Sheet

Malware Defense 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 Malware Defense package, which offers essential web gateway features, plus advanced threat protection 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 plus deep file-based data loss prevention capabilities

More than Core

The Malware Defense package is our mid-level offering. It includes all standard gateway security features from our Core package, plus advanced threat protection capabilities. The following Core package features are included:

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

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

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.

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

Malware Defense Features

Signature-based malware prevention and breach detection

- Malware identification and mitigation from best-of-breed signature databases and iboss proprietary malware registry
- Up-to-the-minute threat information with synchronous database updates

Command and Control (CnC) callback monitoring across all ports and protocols

- Domain, URL, and blacklisted IP monitoring
- Geolocation identifies where callbacks are originating from

Behavioral Malware Sandboxing Defense

- Real-time auto- or manual-deposit of user downloaded files for behavioral sandboxing analysis
- Blended AV scanning
- Malware rules for more granular control over malware content analysis

Malware Defense Features *Continued*

Global cloud threat intelligence to analyze and predict threat behavior

- Crowd-sourced threat intelligence for signatures and samples
- Malware origin and behavior pattern investigation

Time-saving Incident Response Center

- Real-time malware detection for prioritized response
- Translation and prioritization of security event logs into incidents, reducing noise
- Actionable to-do list for remediation and auditing of top security incidents
- High risk/infected user and device identification
- Deep forensic analysis to reduce false positives
- Identification of IP aliases and malicious hosted files
- Dwell time infection measurement
- Snapshot of global historic outbreaks

Intrusion detection and prevention

- Real-time intrusion, malware, and virus protection
- Quickly and easily view event detail, including source and destination IP addresses
- Automatic signature threat feed subscriptions
- Category-based malware rules
- Visual rule creation and editing

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.

Ready to learn more? Request a demo.

Additional Features

Check out the iboss **Data Loss Prevention package** if you'd like to advanced deep file-based data loss prevention capabilities. 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 Premier and 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