FireSphere™

Advanced Defense Against APTs and Evasive Infections

Today's advanced persistent threats (APTs), malware and data-stealing infections are using port evasive techniques to invade your network, where they can stay hidden for months. As a deluge of high profile data breaches illustrates, preventing 100% of malware is unrealistic. That's why you need a proactive approach, with cutting-edge technology and innovative features that not only block APTs, but also find infections already on the network, empowering you to respond and mitigate them in real time and prevent data loss.

iboss FireSphere is the only solution that combines the lean forward technologies of behavioral sandboxing, continuous infection monitoring, network anomaly detection, and the CISO Command Center, to deliver unmatched protection against the persistent, signatureless threats that plague modern networks.

FireSphere Features

Behavioral Sandboxing

While an AV signature/heuristic database provides an essential line of defense to your network security, it can only detect malware with known signatures. FireSphere proprietary Behavioral Sandboxing detects, isolates and dissects APTs, evasive malware, zero-day attacks and polymorphic viruses that signatures alone can't block. And while other security solutions are adding sandboxing, there is an increasing number of threats designed to circumvent standard sandboxes. FireSphere Behavioral Sandboxing technology was developed to detect and analyze the complex, signatureless threats designed to evade standard sandboxing solutions.

The FireSphere Advantage

- Combines signatureless malware defense and infection detection at the gateway
- Provides innovative network anomaly detection to identify evasive infections already on your network that are masking C&C communications
- Employs global threat cloudsourcing to deliver in-depth investigative and forensic malware intelligence via the exclusive CISO Command Center and Threat Intelligence Cloud
- Minimizes the time from infection to detection with continuous monitoring that delivers zero-second detection of malware hiding on your network
- Provides unrivaled security for mobile and BYOD environments by quarantining high-risk devices and users
- Easily scales to fit even the largest, distributed enterprise environments and is available as a standalone or will seamlessly integrate with any other security solution
- Delivers full web stream APT defense with layer 7 visibility across all 131K data channels, not just ports 80 and 443

- Auto-Deposit – Unlike standard sandboxing solutions, FireSphere scans across all files to detect and isolate signatureless malware, which is auto-deposited in a secure environment, where it can be executed and analyzed to determine its behavior and threat potential.

- On-Demand – You can also analyze suspicious files, URLs, USB flash drives and other objects with FireSphere's unique on-demand feature, giving you control that other solutions don't offer.

FireSphere Sandboxing provides deep file analysis via cutting-edge, innovative features such as Full System Emulation and File Baiting.

Auto-Quarantine

FireSphere contains the spread of infections by network-wide scanning for infected machines and high-risk user behavior, and immediately quarantining machines that are harboring malware or engaging in risky behavior. This protection extends across your organization to encompass all users whether on or off network, on mobile devices or BYOD.

Continuous Infection Monitoring

FireSphere continuously monitors and inspects all 131 thousand inbound/outbound data channels to find active infections on the network and contain them before data loss can occur. Data loss often occurs when a bot hiding on the network tries to contact C&C outside. FireSphere's continuous monitoring detects C&C attempts before they are successful, giving you time to respond and mitigate.

Network Anomaly Detection

FireSphere includes Network Baselining for data anomaly analysis, a critical protection layer that increases infection detection and identifies viruses that use evasive tactics to mask C&C communications.

Here's how FireSphere Baselining Prevents Data Loss:

- Employs iboss full Web stream visibility and dynamic indexing to access historical data logs, which are essential to establishing a connection baseline of normal network traffic for your organization.

- Continuously monitors a range of parameters including connection counts, destination, bytes In/out, and deviations in traffic, to pinpoint unusual behavior that can signify the network has been compromised.

- Stops data transfers and alerts you when a problem is revealed, giving you time to investigate and remediate before data loss occurs.

CISO Command Center

FireSphere's exclusive CISO Command Center goes beyond logging events to translate them into actionable intelligence by correlating and prioritizing real-time threat intelligence from FireSphere and the iboss Threat Intelligence Cloud. The results are correlated across a wide range of parameters, giving you the compete context of zero-day threats and evasive malware. Getting hundreds of alerts from one piece of malware generating multiple callbacks could quickly overwhelm your resources. FireSphere eliminates noise and false positives, by delivering prioritized alerts, showing which machines need remediation and why.

Here's how the CISO Command Center shortens time to remediation and saves IT resources:

- Correlates alert information to directory user/machine name, along with a snapshot of global historical outbreaks.

- Eliminates noise and reduces false positives with in-depth real-time forensic analyses allowing CISOs to focus on valid threats.

- Prioritizes threat severity by aggregating data from millions of global endpoints and over 55 different malware engines.

- Detects evasive malware already on the network by monitoring and mapping infection callbacks.

- Inoculates against future attacks by identifying IP aliases and malicious hosted files.

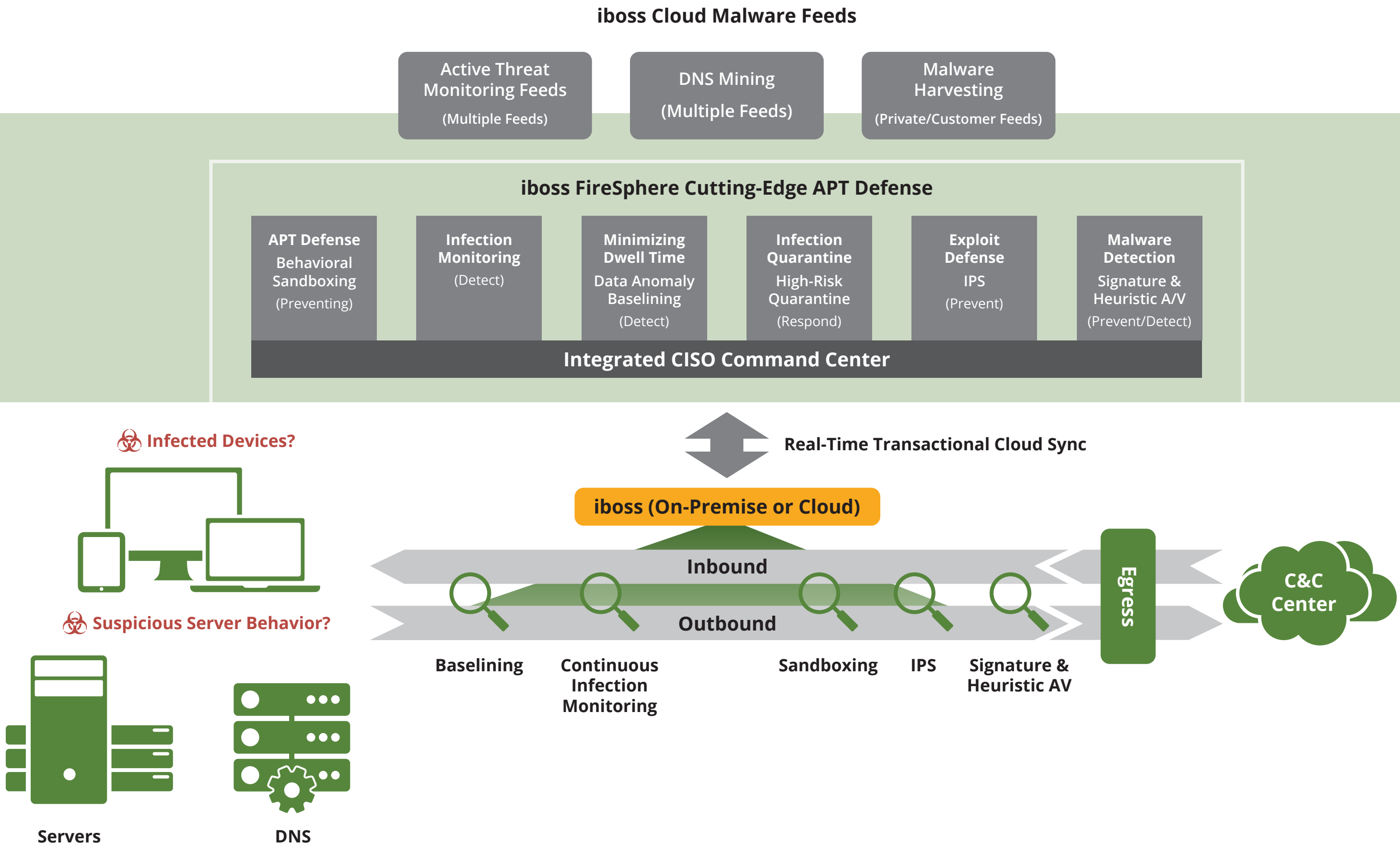
Threat Intelligence Cloud

FireSphere collects global threat intelligence in the cloud from millions of iboss endpoints and over 55 advanced global malware engines, correlating it to deliver comprehensive zero-day threat information to the CISO Command Center. The Threat Intelligence Cloud analyzes how a threat is acting globally and what patterns it is displaying, which can predict future behavior. This forensic intelligence gives you the complete context you need to quickly remediate problems without having to deal with the noise and false positives generated by other solutions. By analyzing and prioritizing threats, the Threat Intelligence Cloud helps accelerate remediation, increase IT efficiency, shorten dwell time and reduce data loss.

iboss™
CYBERSECURITY

FireSphere™

Delivers Powerful Features that Defend Against APTS, Evasive Malware, Polymorphic Viruses and Data Loss



iboss Cloud Malware Feeds

Active Threat Monitoring Feeds (Multiple Feeds)

DNS Mining (Multiple Feeds)

Malware Harvesting (Private/Customer Feeds)

iboss FireSphere Cutting-Edge APT Defense

APT Defense	Infection Monitoring	Minimizing Dwell Time	Infection Quarantine	Exploit Defense	Malware Detection
Behavioral Sandboxing		Data Anomaly Baselining	High-Risk Quarantine	IPS	Signature & Heuristic A/V
(Preventing)	(Detect)	(Detect)	(Respond)	(Prevent)	(Prevent/Detect)

Integrated CISO Command Center

Real-Time Transactional Cloud Sync

iboss (On-Premise or Cloud)

Infected Devices?

Suspicious Server Behavior?

Inbound

Outbound

Egress

C&C Center

Baselining

Continuous Infection Monitoring

Sandboxing

IPS

Signature & Heuristic AV

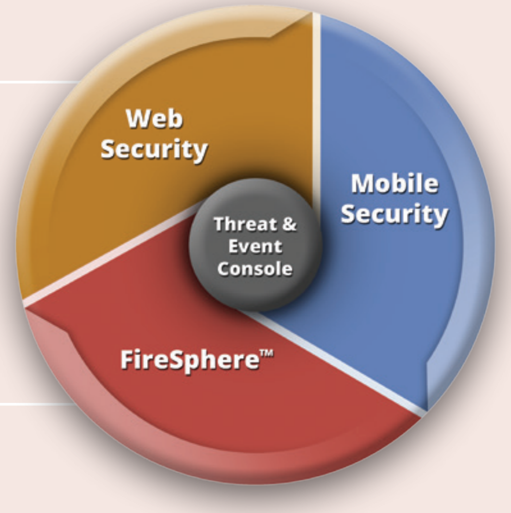
Servers

DNS

iboss Next-Generation Solutions

iboss patented technology protects organizations from APTs, targeted attacks and data loss with innovative Web Security, Mobile Security and FireSphere advanced APT defense solutions. All iboss solutions are integrated to provide real-time dashboards and single-pane-of-glass reporting.

- **Web Security with integrated BYOD and Bandwidth Management**
- **FireSphere for advanced defense against APTs**
- **Mobile Security with integrated MDM**



www.iboss.com | +1 877.742.6832

iboss, Inc. (P) 877.742.6832 Sales@iboss.com U.S. HQ 9950 Summers Ridge Rd., Bldg. 160 San Diego, CA 92121