iboss™
CYBERSECURITY

FireSphere™

Advanced APT Defence

- Continuous Network Monitoring
- Exclusive Network Baselining for anomaly detection
- Behavioural Sandboxing: auto-deposit and on-demand
- Actionable threat intelligence and fast remediation

www.iboss.com

iboss CYBERSECURITY

FireSphere™

Advanced Defence 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 behavioural sandboxing, continuous infection monitoring, network anomaly detection, and the CISO Command Centre, to deliver unmatched protection against the persistent, signatureless threats that plague modern networks.

FireSphere Features

Behavioural Sandboxing

While an AV signature/heuristic database provides an essential line of defence to your network security, it can only detect malware with known signatures. FireSphere proprietary Behavioural 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 Behavioural Sandboxing technology was developed to detect and analyse the complex, signatureless threats designed to evade standard sandboxing solutions.

The FireSphere Advantage

- Combines signatureless malware defence 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 Centre and Threat Intelligence Cloud
- Minimises the time from infection to detection with continuous monitoring that delivers zero-second detection of malware hiding on your network
- Provides unrivalled 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 defence 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 analysed to determine its behaviour and threat potential.

- On-Demand – You can also analyse 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:

- Full System Emulation – By employing multiple machine emulators and file types, FireSphere can identify malicious code, thwart evasion techniques and help prevent future exploits. This results in actionable threat intelligence that is immediately synchronised across the entire iboss database, offering real-time protection against threats, standard security solutions miss.

- File Baiting – FireSphere offers unique File Baiting technology to uncover threats that use evasive techniques, or polymorphic viruses that evade detection by constantly changing. FireSphere intercepts suspicious files and tests their behaviour on bait files in a controlled environment, generating actionable intelligence reports.

Auto-Quarantine

FireSphere contains the spread of infections by network-wide scanning for infected machines and risky behaviour, and immediately quarantining machines that are harbouring malware or engaging in risky be ha vi or. This protection extends across your organisation 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 the CISO Command Centre 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 analysis allowing CISOs to focus on valid threats

- Priorities 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

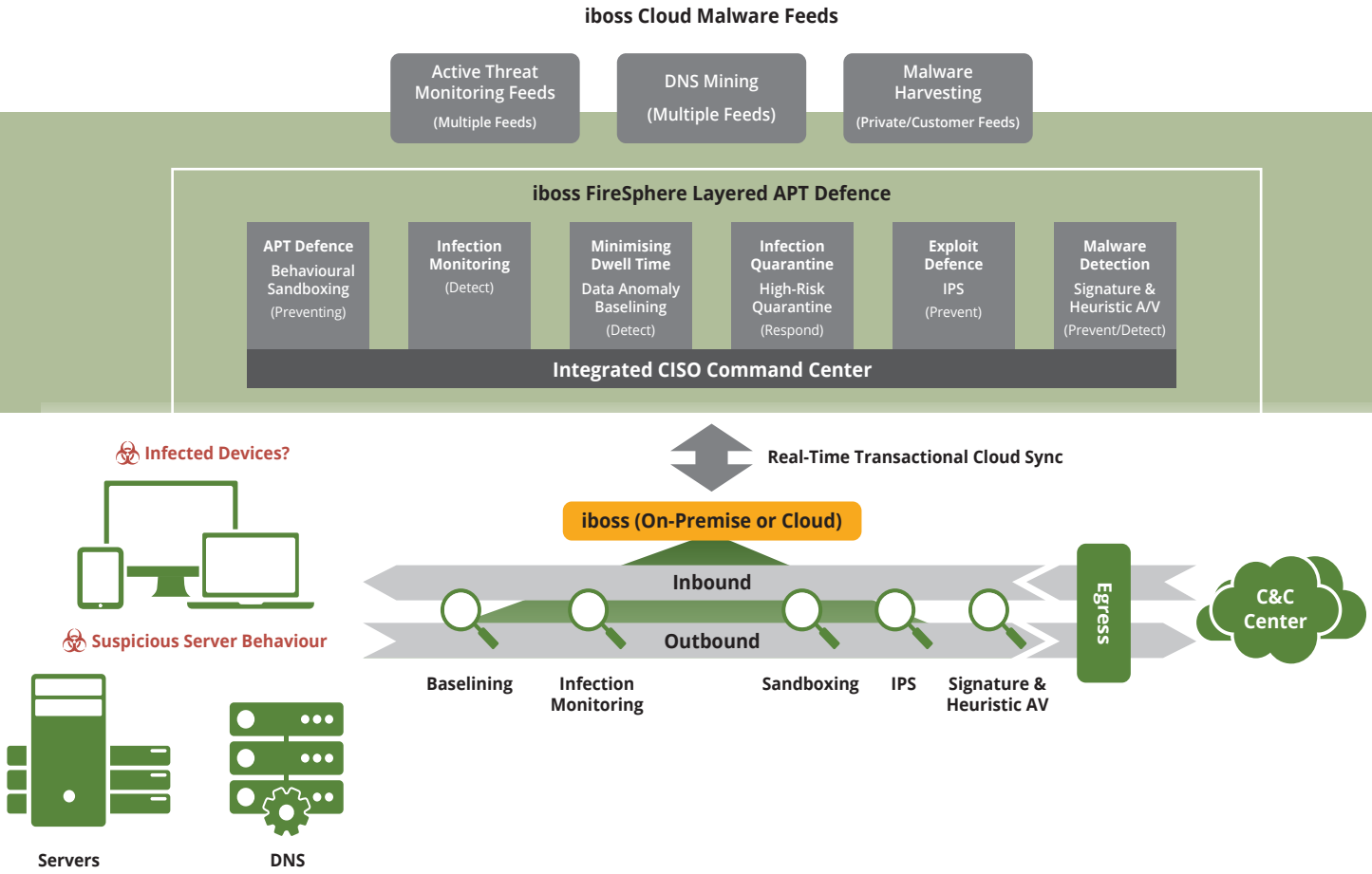
Fire Sphere collects global threat intelligence in the cloud from millions of iboss endpoints and over 55 advanced global malware engines, correlating it to deliver comprehensive zero-day threat information to the CISO Command Centre. The Threat Intelligence Cloud analyses how a threat is acting globally and what patterns it is displaying, which can predict future behaviour. 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 analysing and prioritiing threats, the Threat Intelligence Cloud helps accelerate remediation, increase IT efficiency, shorten dwell time and reduce data loss.

FireSphere™

iboss CYBERSECURITY

FireSphere™

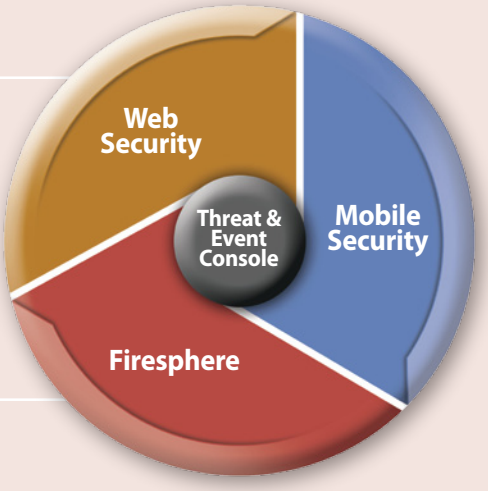
Delivers Powerful Layered Defence Against Apt, Evasive Malware, Polymorphic Viruses and Data Loss



iboss Next-Generation Solutions

iboss patented technology protects organisations from APTs, targeted attacks and data loss with innovative Web Security, Mobile Security and FireSphere™ advanced APT defence solutions. All iboss solutions are integrated with our exclusive advanced threat SIEM single-pane-of-glass reporting.

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



emeia@iboss.com | **+ 44 (0)20 3713 0470**

iboss · ICS House · Hall Road · Maldon · Essex · CM9 4LA

www.iboss.com | +1 877.742.6832