

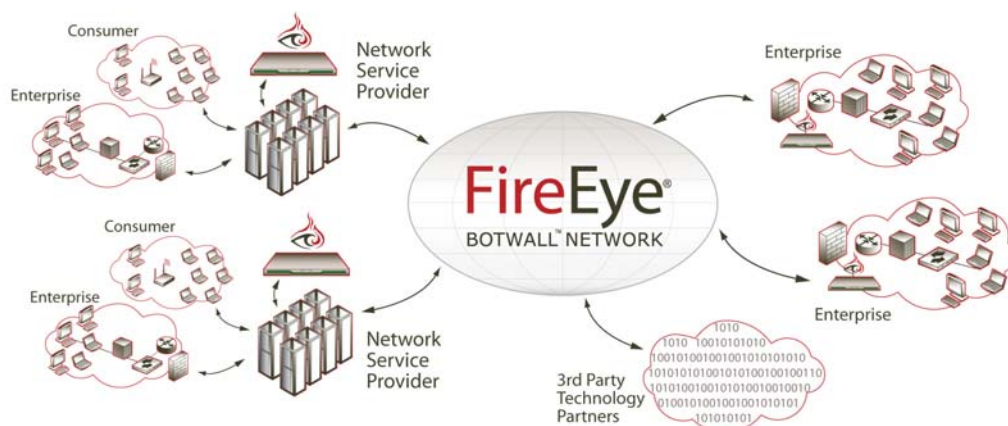
The FireEye Botwall Network gives enterprises and service providers a real-time view into botnets around the world. By pinpointing command and control (C&C) locations, identifying botnet propagation tactics, and diagnosing malicious bot activities, the FireEye Botwall Network is an “in-the-cloud” service that provides customers pre-emptive protection against the real and escalating botnet threat. Customers are connected to the Botwall Network by simply enabling their FireEye Botwall appliances to communicate with the Botwall Network. Once connected, Botwall appliances receive real-time botnet intelligence enhancing their ability to:

- Identify compromised machines on the network
- Block bot communications to botnet C&C servers
- Prevent bot proliferation attacks on the network

### Global Proliferation of Botnets

Botnets are massive groups of compromised, remotely controlled machines and are used to take customer data, perpetrate online fraud, and steal intellectual property. Botnets are a widely dispersed threat making them particularly difficult to combat solely in the service provider ‘cloud’ or only locally within organizational networks and endpoints.

Bot masters living in one country connect to botnet command & control (C&C) infrastructure located in another remote location that in turn commands bots located around the world. It takes a combined global intelligence coupled with local analysis to uncover bots and prevent them from trafficking in valuable enterprise data and resources.



### FireEye Botwall Network: Global Analysis & Intelligence

- Analysis of global Internet traffic
- Continuous discovery of botnet whereabouts & activities
- Real-time dissemination of botnet analysis to participants
- Botnet malware inspection & classification
- Ability to participate in Botwall Network analysis

### Botnets Exhibit Dynamic, Evolving Attack Tactics

While legacy network and host security technologies have remained fundamentally stagnant, botnets are rapidly adopting new penetration attacks, including botnet worms, new social engineering tactics, zero-day exploits, and Web-based malware. Botnet worms, for example, have penetrated millions of PCs forming some of the largest botnets known presently. They are stealthy, targeted malware designed to mutate rapidly and spread quietly circumventing traditional security technologies, like antivirus and IDS/IPS. Bot infiltrations are largely undetectable by traditional means because techniques to bypass them are readily available in open-source malicious code examples.

“Annual loss due to computer crime was estimated to be \$67.2 billion for U.S. organizations”

- 2005 Federal Bureau of Investigation survey

## Using Global Intelligence to Protect Local Assets

FireEye provides anti-botnet protection through FireEye Botwall appliances connecting into the FireEye Botwall Network service. The FireEye Botwall Network is a globally deployed botnet discovery and analysis service offering subscribers with the most current botnet intelligence to complement on-premise anti-botnet Botwall security appliances. The Botwall Network analyzes and disseminates:

- Botnet C&C fully qualified locations (IP address, protocol, ports)
- Botnet malware attack profiles (signatures, network behaviors)
- Bot activity notifications

The FireEye Botwall Network is formed from interconnected FireEye Botwall appliances deployed at service providers around the world. These intelligent devices receive and share malware analysis intelligence. This systematic approach prevents botnets before they infiltrate to exploit customer data, intellectual property, and enterprise resources for profit.

The global intelligence feeds FireEye Botwall appliances to prevent local botnet infiltrations ensuring customer data, intellectual property, and network resources remain safe from compromise.

## FireEye Analysis & Control Technology (FACT)

FireEye uses patent-pending security virtualization technology to uncover C&C servers and the ever-morphing botnet infiltration techniques used to expand botnet armies. The FireEye Analysis and Control Technology, or FACT, is built into each FireEye Botwall appliance, which form the Botwall Network. FACT uses advanced network security combined with state-of-the-art virtualization technology to combat botnets and network malware. FACT protects against botnet malware by analyzing real-time network traffic flows in which botnet malware attacks virtual victim machines. When an attack is confirmed within a virtual victim machine, FireEye Botwall appliances instantly takes protective measures against the attack as well as records and catalogues attack details.

With FACT deployed to analyze Internet traffic, FireEye can:

- Pinpoint botnet command & control coordinates
- Discover small- and large-scale botnets before they infiltrate customer networks
- Automatically create zero-day signatures based on malware code
- Eliminate false alerts, complex setup rules associated with behavioral heuristic techniques
- Utilize in-the-network security avoiding any chance for host security compromise

FireEye now offers the first anti-botnet protection system to integrate global awareness with local network analysis to precisely identify, understand, and stop emerging botnet and malware threats.

The FireEye Botwall Network is a global, multi-enterprise alliance of enterprises, services providers, and research organizations fighting against botnets and targeted malware. IT professionals can benefit from FireEye's global network and technology visibility to help identify and understand emerging botnet and malware threats. FireEye increases network visibility and restores IT control over the network by discovering and blocking botnet communications as well as derailing botnet proliferation attempts.

## About FireEye, Inc.

FireEye, Inc. is the leader in anti-botnet protection, enabling organizations to protect critical intellectual property, computing resources, and network infrastructure against bot infiltration. Today's most damaging attacks originate from and through highly organized botnets, or networks of remotely controlled, compromised machines. FireEye delivers a complete solution that is designed from the ground up to detect and protect organizations from botnets through global and local intelligence and analysis. The company is backed by Sequoia Capital, Norwest Venture Partners, and JAFCO.

[www.fireeye.com](http://www.fireeye.com)

FireEye, Inc.  
1390 McCarthy Blvd.  
Milpitas, CA 95035  
+1 (877) FIREEYE (347.3393) [info@fireeye.com](mailto:info@fireeye.com)

© 2008 FireEye, Incorporated. All rights reserved.

FireEye, Botwall and the FireEye logo are registered trademarks of FireEye Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners. BNDS031708 03/08