INTRINSIC•SECURITY

FireBreak AntiWorm : Network Defense In Depth

Contact Us Today!

Phone: +1 (202) 330-1037

email: sales@intrinsicSecurity.com

FireBeak AntiWorm Benefits

- Instantly detect worm activity
- Detect and impede "Zero Day" worms without AntiVirus definitions
- Impede worm progress without complex "tuning" required by IDS/IPS and PC based firewalls
- Detect & suppress polymorphic worms, including worms & variants never before seen, never studied in any lab
- Detect & impede worms without definition files
- Detect impede and locate worms that get past IDS, IPS, firewalls & AntiVirus
- Slow the spread of worms on a network
- Instantly alert network and security staff to the worm activity
- Identify infected systems
- Identify the port or ports a worm is using to spread
- Network Appliance based - no software to install on the PC

FireBreak will reduce the damage caused by worms and save you money.

FireBreak is centrally managed via any modern web browser - network operators can use Windows, Linux, or Mac OS X.

FireBreak is easy to configure and deploy.

FireBreak Intrusion Suppression System

FireBreak provides uniquely effective anti-worm protection. It's the first ***Intrusion Suppression System*** for enterprise networks. FireBreak brings new depth to network defense-in-depth strategies.

FireBreak does not replace Firewalls, IDS (Intrusion Detection Systems), or AntiVirus products. FireBreak provides active suppression of worms, slowing the spread of a worm and instantly alerting you to an outbreak. FireBreak coexists with other network security products and helps them work better -- without custom integration or tuning.

With FireBreak, you can start protecting your network in days, not months.

Network AntiWorm Defense in Depth

APPLIANCE BASED • ZERO PC FOOTPRINT
SCALABLE & SECURE • UNIX FOUNDATION
WEB INTERFACE • EASY TO MANAGE
ZERO-DAY WORM DEFENSE
NO ANTIVIRUS DEFINITIONS REQUIRED

FireBreak AntiWorm

Intrusion Suppression System

FireBreak detects worms without definitions, immediately alerts responsible staff, and actively impedes the progress of worms on a network. FireBreak buys critical time to respond to a worm outbreak -- worms won't be able to sneak in and spread for two days before AntiVirus definitions arrive. FireBreak will identify which systems are infected on a network. The system can be deployed quickly, without extensive tuning.

NETWORK OPERATORS can inspect and update the configuration of sensors from a central location. FireBreak discovers networks connected to FireBreak Monitors and reports network topology information without time consuming configuration. No need to produce hundreds of pages of LAN diagrams to deploy the system -- just hook up the FireBreak Monitors and they will tell you about the network.

SECURITY ANALYSTS can monitor trends over time and identify the locations infected during an outbreak, and the other networks those worms probed. FireBreak helps identify how the worm got into the network -- did a network back door get hooked up? Is a VPN gateway or firewall configured incorrectly? When a worm hits, your security analysts will instantly know what ports the worm is using to spread -- no guesswork, and no need to capture worm "samples" for forensic analysis.

INCIDENT HANDLERS (CIRT/CERT) can be instantly alerted to the exact systems infected in the earliest moments of a worm outbreak. FireBreak slows the spread of a worm and buys response time for your Incident Response Team.

MANAGERS can see the effectiveness of incident response procedures. How quickly were infected systems isolated? FireBreak also provides managers with critical alerts, based on thresholds or other conditions. FireBreak supports large organizations -- each person can define the scope of the alerts based on segments of the network their team manages.

Contact us today!

FireBreak can be **managed via any modern web browser**.

FireBreak AntiWorm Monitors are hosted on a **robust, scalable and mature** UNIX foundation.

FireBreak AntiWorm Monitors are **self-configuring** on most networks. They **automatically discover connected networks**, find your enterprise FireBreak Server based on a simple DNS entry.

FireBreak AntiWorm Monitors are **not vulnerable to Windows**, Linux, Apache, SQL Server **nor other worms** because the sensors do not run other services. FireBreak provides a flexible alerting system that can notify incident handlers, network administrators, and managers about events in their area of responsibility. FireBreak can **deliver alerts** based on the alert type -- **email, pager, SMS, FAX and VXML** (synthesized voice) directly to a land line or cell phone.

Intrinsic•Security

FIREBREAK ANTIWORM

+1 (202) 330-1037

sales@intrinsicSecurity.com