

No one gets in unless we say so.



Broadview FrontLineSM Managed Firewall

Expert security policy enforcement and 24x7 monitoring and management.

Less than 5%
of network attacks
are detected.

The majority of network break-ins and security breaches go undetected. Attacks have an 88% success rate, but are detected by less than one in 20 of the target organizations. And of those organizations that detect these threats, only 5% actually react to them.

Broadview FrontLine Managed Firewall delivers active protection for your networks – 24x7x365 monitoring, reporting, maintenance and fault resolution proactively provided by Broadview security experts. And Broadview optimizes your configuration through regular security policy reviews and recommendations.

On an ongoing basis, Broadview handles OS patches, log files, upgrades and hack attempts – reporting to you at your option. You're empowered by real-time visibility into performance and attempted security violations with end-user management through Broadview's FrontLine customer portal. The result? You get the peace of mind of achieving peak network security without having to worry about owning, programming or maintaining equipment.

Key Benefits of Broadview FrontLine Managed Firewall

- Protects against the most current and advanced network attacks including denial of service attacks
- Broad range of world class features from the Cisco[®] Catalyst platform
- Stateful inspection technology ensures the highest levels of security as opposed to standard packet filters or NAT
- Memory and throughput aren't capped by the capacity of a premise-based firewall
- No capital investment
- No end user licenses
- Attacks are blocked at the core of the Broadview network, ensuring a clean connection to the customer premise
- "SIP-aware" – seamlessly accommodates VoIP traffic



INFRASTRUCTURE | SECURITY | PRODUCTIVITY





Broadview monitors all customer activity around-the-clock from its secure, state-of-the-art Network Command Center. Best-of-breed firewall technology and Broadview security experts provide **a one-two punch that knocks out potential threats.**

www.broadviewnet.com/frontline

Mission-critical Functionality

Broadview FrontLine Managed Firewall protects your network or networks from intruders on an outer, unprotected network. This critical layer of security forms a boundary so traffic between protected and unprotected networks flows through your firewall, limiting access to only your authorized users.

Common Attacks

- **Buffer overflow:** Hacker sends an oversized file to the system causing a buffer overflow
- **Backdoor:** A mechanism covertly installed on a victim's system to gain unauthorized access
- **Trojans:** A malicious piece of code installed by a hacker to serve a purpose other than the authorized users' original intent
- **Blind spoofing:** Hacker crashes servers and steals IP addresses by predicting a sequence of numbers

Other Types of Attacks

- SYN flooding
- Non-blind spoofing
- Reset attack
- FIN attack
- Teardrop attack
- Application layer attack
- Cross site scripting
- CGI abuses
- Port scan
- Web defacement (graffiti)
- Denial of service
- Distributed denial of service
- Password cracking
- War dialing



Additional elements of the Broadview FrontLine suite:

- E-mail Security
- Secure Virtual Private Network
- Data Backup and Recovery (Coming Soon)
- Internet Policy Management (Coming Soon)

Broadview Networks, the Broadview Networks logo, and "Think about it" are registered marks of Broadview Networks, Inc. All other marks are property of their respective owners. © 2006, all rights reserved.

Broadview FrontLine. Active protection against threats to your data...your network...your business.

