



BLINK® Endpoint Vulnerability Prevention

Multi-layer Threat Mitigation and Intrusion Prevention

Networks have evolved from traditional desktop and server architectures to now include a myriad of platforms and components. These digital assets have multiple user profiles and configurations, including remote and mobile users, all of which must comply with corporate standards and policies. Many of these assets are links within critical business processes spanning geographies and enterprise applications. As network architectures have become more complex, so have the threats which security professionals face; rapidly propagating worms - such as Blaster and Sasser - and directed attacks causing tremendous costs to enterprises when these attacks spread across the infrastructure, within the perimeter.

To better combat these evolving threats, organizations must look beyond traditional firewalls and intrusion detection systems, which weren't designed for internal security threats. Each individual device must have non-intrusive, proactive protection to shield it from these attacks and ensure business continuity. We have reached the point where protection of the individual digital assets within the perimeter is a must.

A Unique Multi-Layered Security Solution

eEye Digital Security developed the Blink® Endpoint Vulnerability Protection system by integrating multiple layers of proven security technologies. Blink proactively shields assets from previously undetected vulnerabilities, making assets more resilient to attacks, even when patches aren't available or installed. Blink combines and extends the technologies of intrusion prevention and application firewalls, and eEye's Retina® vulnerability assessment scanner.

These integrated protection layers work hand in hand to provide the most powerful protection of individual digital assets from targeted and mass propagated attacks. Blink's protection is designed to protect assets from zero-day attacks that leverage unknown vulnerabilities where patching is not an option. Blink thus increases operational efficiency and ensures business continuity by:

- **Protecting from known and undefined vulnerabilities**, through periodic local vulnerability assessment and process activity monitoring, hosts protected by Blink are continuously scanned against Retina's vulnerability database as well as monitored by specialized analyzers which detect abuse or non-standard usage.
- **Extending the timetable to remediate**, allowing organizations to patch during normally scheduled maintenance windows, not in a frantic response to a worm or virus outbreak. This extended window allows for the rigorous testing of vendor patches and the prioritization of remediation activities.
- **Enforcing policy compliance**, constantly auditing corporate security standard configurations, reducing the risk associated with non-standard applications, such as outdated antivirus deployments, and increasing bandwidth efficiencies by eliminating peer-to-peer or file sharing usage.

To support large-scale deployments, eEye provides a comprehensive management infrastructure suitable for use across large, distributed networks. Through Blink's Security Console, administrators can perform comprehensive asset discovery, deploy Blink agents throughout an enterprise and administer customized configuration settings with no impact to end users. Additionally, Blink seamlessly integrates with Active Directory as a means to manage the identities and relationships that make up network environments, further leveraging enterprise investments.

Fast Facts

- Combines several best-of-breed threat mitigation technologies:
 - Intrusion prevention system
 - System-level firewall
 - Application-level firewall
 - Local vulnerability assessment scanner
 - Non-intrusive process activity monitors
- Protects from known and undetected vulnerabilities
- Enforces internal configuration standards
- Centralized management
- Rapid deployment and ease of administration
- Integrates with REM Security Management Console for enterprise-wide reporting and analysis



eEye Digital Security®

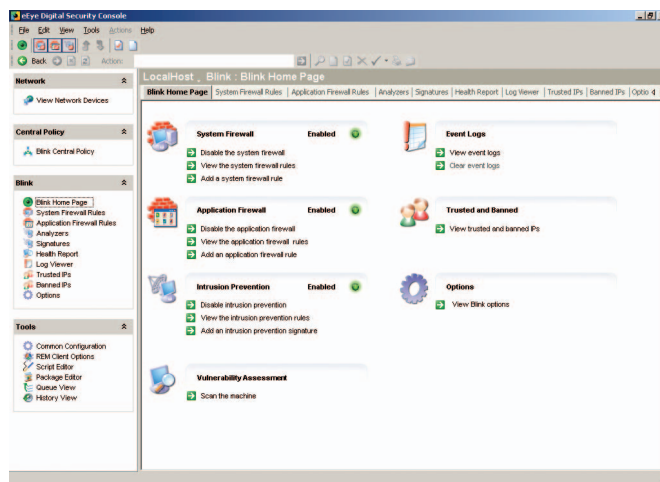
BLINK[®] Endpoint Vulnerability Prevention

Additional Features and Benefits

- **Unsurpassed Intrusion Prevention Technology**
Detection and blocking of unknown or very new attacks that are able to bypass signature checking solutions; detection and blocking of known attacks using pattern matching analysis against rule database; network traffic reconstruction and analysis by protocol.
- **System and Application Firewalls**
Analysis of each packet of network traffic entering the local system; allows/denies traffic based on a set of predetermined firewall rules; monitors the source of network traffic in real time; allows traffic only from authorized applications.
- **Local Vulnerability Assessment**
Based on award-winning Retina's network scanner technology; non-intrusive; provides a list of recommended remediation actions.
- **Logs and Captures**
Log firewall and IPS events; capture packets.
- **Works with IPSec and Supports OPSEC**
Ensures compatibility with VPN clients.
- **Automatic Updates**
Sync-It automated updates from eEye; updates from the management station(s).
- **Network Asset Discovery**
Discover network assets via Active Directory, ARP, and NetBIOS; multiple group views.
- **Remote Deployment**
Create customized Blink installation packages and push them out through the network using the eEye Console.
- **Centralized Management**
Centrally manage Blink installations through the Console; manage the network of Blink-protected hosts with the ability to drill down to an individual machine or group of machines.
- **Integration with REM Security Management Console**
Seamless integration with REM console for advanced reporting and analysis. Integration with eEye's vulnerability assessment and remediation workflow.

System Requirements

- **Blink:**
 - OS Workstation: Windows NT 4 (SP6), Windows 2000 (SP3) or Windows XP
 - OS Server: Windows NT Server, Windows 2000 Server, Windows 2000 Advanced Server or Windows Server 2003
 - 233 MHz or higher Intel Pentium II or compatible processor
 - 128 MB of RAM
 - 40 MB of free disk space
- **Console:**
 - OS Workstation: Windows 2000 (SP3) or Windows XP
 - OS Server: Windows 2000 Server, Windows 2000 Advanced Server or Windows Server 2003
 - 233 MHz or higher Intel Pentium II or compatible processor
 - 256 MB RAM
 - 50 MB hard-disk space required for installation
 - .Net Framework 1.1



About eEye Digital Security

eEye Digital Security is a leading developer of network security products that deliver unsurpassed levels of vulnerability protection before, during and after malicious attacks. Driven by the world-renowned eEye Research Team, the company has won numerous awards and recognition in the field of network security, including the recent top 10 recognition in the Red Herring Top 100 Innovators awards for 2004. A global company with offices, partners and distribution channels around the world, eEye helps protect the digital assets of major corporations, educational institutions, and government entities in over 80 countries.

eEye Digital Security
www.eEye.com

U.S. Tel: 1.866.339.3732
N. America: 1.949.900.4100
Geneva: +41 22.718.7700
London: +44 (0) 208.956.2270

N. America: sales@eeye.com
International: sales.eu@eeye.com



eEye Digital Security[®]

VULNERABILITY IS OVER