

# BLINK<sup>®</sup> Endpoint Vulnerability Prevention

## Multi-layer Threat Mitigation and Intrusion Prevention

**N**etworks 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. 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' Blink<sup>®</sup> Endpoint Vulnerability Protection system integrates 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, personal firewalls, anti-spyware, identity theft protection and eEye's Retina<sup>®</sup> 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 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 using Retina's vulnerability database as well as protected through Blink's innovative approach to protocol analysis.
- **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.
- **Securing unsupported platforms**, as vendors end support for legacy platforms, organizations are left with little recourse to protect assets running critical applications. Blink's innovative IPS technology protects these systems without requiring a reduction in functionality.

To support large-scale deployments, eEye provides a comprehensive management infrastructure suitable for use across 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
  - Anti-Spyware Technology
  - Identity Theft Protection
  - System and Application Level Firewalls
  - Local Vulnerability Assessment Scanner
- Protects from known and undetected vulnerabilities
- Enforces internal configuration standards
- Centralized deployment and management
- Rapid deployment and ease of administration
- Integrates with REM Security Management Console for enterprise-wide reporting and security event analysis

*"The time for a more complete approach to host-based intrusion prevention is here. Traditional antivirus and personal firewall solutions are no longer sufficient to protect endpoint systems against targeted application-level attacks, and we can't keep our systems patched as quickly as new vulnerabilities are announced"*

- Gartner, 2005



eEye Digital Security<sup>®</sup>

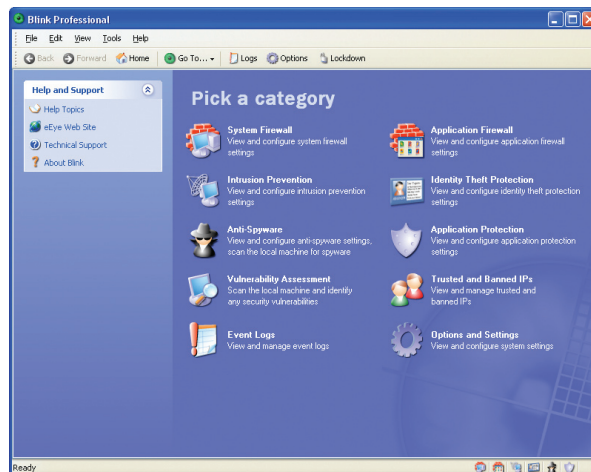
# BLINK® Endpoint Vulnerability Prevention

## Additional Features and Benefits

- **Unsurpassed Intrusion Prevention Technology**  
Detection and blocking of known or 'zero day' 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 policies; monitors the source of network traffic in real time; allows traffic only from authorized applications.
- **Anti-Spyware Technology**  
Blink will actively block malware instances from being loaded into memory and give the option to quarantine or remove the suspected code, as well as the ability to scan the disk for existing spyware instances.
- **Identity Theft Protection**  
Leveraging its protocol analysis engine, Blink is able to detect and classify phishing attempts made via various protocols. This includes images used to convey these phishing attacks.
- **Vulnerability Assessment**  
Based on the award-winning Retina Network Security Scanner; comprehensive, non-intrusive vulnerability auditing, provides a list of recommended remediation actions.
- **Remote Deployment**  
Create customized Blink installation packages and deploy them out through the network using the Blink Console, with no impact to end users.
- **Centralized Management**  
Centrally manage Blink installations through the Blink Console; manage the network of Blink-protected hosts with the ability to drill down to an individual machine or group of machines.
- **Integration with eEye's REM™ Security Management Console**  
Seamless integration with REM for risk analysis, event consolidation and enterprise reporting. Additionally, REM's remediation management workflow provides a collaborative approach to vulnerability management.

## 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
  - Internet Explorer 5.0 or higher
- **Console:**
  - OS Workstation: Windows 2000 (SP3) or Windows XP
  - OS Server: Windows 2000 Server, Windows 2000 Advanced Server or Windows Server 2003
  - 400 MHz or higher Intel Pentium II or compatible processor
  - 256 MB RAM
  - 50 MB hard-disk space required for installation



## About eEye Digital Security

eEye Digital Security is a leading developer of network security software, and the foremost contributor to security research and education. eEye's award-winning software products provide a complete vulnerability management solution that addresses the full lifecycle of security threats: before, during and after attacks. eEye protects the networks and digital assets of more than 8,400 corporate and government deployments worldwide, including Avon, Continental Airlines, Dow Jones, Prudential, University of Miami, Viacom, Vodafone, Warner Music and Wyeth. Founded in 1998, eEye Digital Security is a privately held, venture-backed firm with headquarters in Orange County, California. For more information, please go to [www.eEye.com](http://www.eEye.com).

eEye Digital Security  
[www.eEye.com](http://www.eEye.com)

U.S. Tel: 1.866.339.3732  
N. America: 1.949.900.4100  
U.K.: +44 (0) 1784.224.205  
N. America: [sales@eeye.com](mailto:sales@eeye.com)  
International: [sales.eu@eeye.com](mailto:sales.eu@eeye.com)



eEye Digital Security®