



# BLINK® 4.0 Endpoint Protection Platform

## Integrated Threat Management Enhances Endpoint Security.

## SOLUTION OVERVIEW

- Integrated virus, spyware, identity theft, and malware protection
- Combines multiple security products into one solution
- Protects against both known and zero-day vulnerabilities
- Advanced network and application protection with host-based intrusion prevention and buffer-overflow protection technologies
- Allows organizations to maintain protection outside of change control windows
- Highly scalable with the REM® Security Management Console for centralized policy control and enterprise-wide reporting



## Product Overview

Blink® Professional Edition is the only complete multi-layered endpoint protection solution to provide organizations with a single, low-footprint endpoint protect platform solution that replaces their multiple, bloated, desktop and server security agent implementations. Designed for any size organization from small businesses to large enterprises, Blink Professional delivers integrated anti-virus, anti-spyware, protocol-based host-intrusion prevention, application and system firewalls, patented sandbox technology, buffer-overflow protection, system-change and application-execution control, and host vulnerability assessment capabilities in a single installation and more importantly, with a single agent. This allows Blink Professional to protect against zero-day attacks better than any other solution. Blink Enterprise provides centralized and dynamic policy enforcement, centralized event management, and centralized vulnerability management through the REM Security Management Console for unprecedented scalability.

## Benefits and Features

### 1. Protects against Viruses, Spyware, Trojans, Keystroke Loggers, and other Malware

Blink protects from malicious applications in real time, as well as providing full disk scanning capabilities by using three layers of protection: signatures, heuristics, and sandbox engine technology.

### 2. Stops the Propagation of Worms and Viruses

In addition to protecting from attacks, Blink stops new or current infections by slowing or stopping the attack as it moves across the network and protecting one trusted host on the network from infecting another.

### 3. Protection for (and from) Mobile Users

Mobile users are outside the corporate firewall and must be protected when they connect at airports, hotels, partner sites, and even at home. Once they return to the corporate network, Blink dynamically changes policies to provide maximum protection while away, and trusted connections while in the office, ensuring proper protection where ever they go.

### 4. Policy and Regulatory Compliance Enforcement

Blink regulates the use of non-approved applications and report any changes to a host that would impact compliance. In addition, the local Retina vulnerability assessment engine built into Blink reports health and status for all regulatory compliance initiatives.

### 5. Scalable and Centralized Control with the REM Security Management Console

Using the REM Security Management Console, Blink can be managed with little or no end-user intervention as part of your entire threat management strategy. REM provides the ability to deploy agents, maintain policies, and report on all of the Blink agents from a single web-based interface. In addition, REM is available as an appliance or software to meet the individual business requirements of any organization.



eEye Digital Security®

# BLINK® 4.0 Endpoint Protection Platform

## Key Advantages

- o Anti-Virus, Anti-Spyware, and Anti-Malware (signature, heuristics, and sandbox engines)
- o System and Application Firewalls (Port, IP, and Application Based)
- o Host Intrusion Prevention System (Protocol Based)
- o Identity Theft Protection (Removable Storage Protection and Phishing)
- o Zero Day Exploit Protection (Buffer Overflow and API Protection)
- o Local Vulnerability Assessment powered by Retina
- o Non-intrusive protection does not disrupt applications and business functions as a means of protection
- o Blink does not require resource intensive “learning mode” to initiate protection
- o Completely transparent, no end-user intervention or behavioral training required
- o Easily create and enforce central policies and publish to selected users, groups, or hosts
- o The REM Security Management Console provides complete policy, control, and reporting for Blink Enterprise users.

## Product Requirements

- o Microsoft Platform Support: Windows 2000, XP (32 bit), 2003, and Vista and 2008 (32 and 64 bit)
- o Blink can be deployed from the REM Security Management Console or by using third-party software distribution systems using the 3rd Party Package Wizard
- o Blink is capable of removing other antivirus and security products on a host using the Software Removal Tool prior to deployment allowing for rapid migration from one vendor to another.

## Why Use Blink Professional

### 1. Complete end-point protection or an antivirus replacement

Blink secures critical Microsoft-based assets against intrusion and from being leveraged as attack vectors by providing anti-malware (anti-virus and anti-spyware), firewall, intrusion prevention, vulnerability assessment, and system protection above and beyond any traditional Anti-Virus deployment.

### 2. Policy and standard configuration enforcement

Blink can be configured to block the execution of any rogue applications and even prohibit the installation of new programs; even if the user is a system administrator. Blink can also be configured to limit certain applications or network traffic in connection with regulatory requirements.

### 3. Protection for/from mobile users or remote workforces

Blink protects mobile users, or remote employees when they connect to the network and from activities when not connected to the organizations firewall and IPS/IDS systems. Blink also protects other internal users from any infection that may propagate through the network from unprotected systems and devices. Any organization with a large number of mobile users, VPN access, or remote office and consultants/contractors will understand the benefit of protecting their devices while working remotely and upon their return to the corporate environment.

## Organizations

Organization with predominantly Microsoft-based assets

Large-scale enterprise organizations

Small and Medium sized businesses (SMBs)

Regulated organizations (healthcare, financial and manufacturing, for example)

Educational institutions where internet access is unregulated

## User Environment

### PRIMARY

Security, desktop, and network managers with responsibility for a LAN or WAN with 50 to 5,000 hosts (workstations or servers).

### VERTICAL

Security and operation managers in industries with strong mandates and government regulations, including PCI, SOX, GLB, FDCC and HIPAA, for example



# BLINK<sup>®</sup> 4.0 Endpoint Protection Platform

## Questions to Consider

1. How do you currently protect your endpoints (workstations, servers, laptops)?
2. What antivirus protection do you currently use? When does your subscription expire?
3. How many security products do you currently use to protect your endpoints? Which products do you use for firewall protection? Anti-spyware? Vulnerability Assessment?
4. Do you patch in response to outbreaks, or do you have regularly scheduled patching windows? Have you been able to adhere to those windows? Do you have strict change control procedures?
5. Do you have network policies regarding application usage, configuration standards, or regulatory compliance?
6. Do you rely primarily on perimeter protection for your network?
7. How do you protect mobile users and remote employees, contractors, and consultants?

## Key Features

### ◦ Firewall Protection

Blink performs traditional firewall duties, allowing or denying traffic based on a set of predetermined common applications. Blink also monitors the source of network traffic in real time and only allows traffic from authorized applications, preventing unauthorized programs from making illegal outbound connections. Users or administrators can add custom rules for any application, port, or IP address to customize the solution to meet an organizations business needs.

### ◦ Virus and Spyware Protection

Blink provides complete signature, heuristics, and sandbox-based protection using three anti-malware engines. Blink's patented sandbox technology actively blocks malicious activity from unidentified and zero-day threats. Heuristics provide an additional protection and can stop new attacks as they are released without the need for updates for signatures.

### ◦ Intrusion Prevention

Blink provides protocol-based protection that inspects network traffic to and from the host, and protects against vulnerabilities inherent in the applications and operating system communicating through the network. Blink blocks "zero-day" attacks that bypass traditional security solutions, by reviewing the network traffic at the host and determining attacks by deviations in acceptable TCP/IP protocols. These deviations are outside of documented specifications or contain content that could cause malicious behavior. Blink's intrusion prevention solution can protect all Windows hosts, regardless of patch level, from worms that could gain unauthenticated control over a host.

### ◦ System Protection

Blink provides control over which applications are acceptable by authorizing or denying program file execution. In addition, Registry Protection prevents specific registry settings from being modified, stopping malicious programs from infecting or modifying systems. Storage Protection prevents data leakage by regulating USB and Firewire storage devices. Finally, Blink System Protection provides complete buffer overflow and Windows API protection for the entire operating system and any application.

### ◦ Vulnerability Assessment

Blink contains a local copy of eEye Digital Security's award winning Retina Network Security Scanner. The scanner is configured to provide local authenticated scans of the host and eliminate the need for network-based vulnerability assessment of the host. When Blink is used with REM, all attacks, virus, and vulnerability data is centrally stored for management and reporting.

### ◦ REM Security Management Console

Combined with REM, the integrated solution provides event and state analysis capabilities along with security and compliance reporting. The REM Security Management Console integrates attack-related information with local and network vulnerability assessment data, providing a complete security solution.



eEye Digital Security®

# BLINK® 4.0 Endpoint Protection Platform

## Other eEye Solutions

### BLINK ENTERPRISE

Do you need to centrally manage and report on a distributed network?

Blink Enterprise (includes Standard Support and REM Management Console):

25 Asset Pack \$1400 (each additional unit \$30) per year  
100 Asset Pack \$2500 (each additional unit \$25) per year

### RETINA

Blink protects critical Windows machines, but what about the remainder of your infrastructure? You should always have a network-based vulnerability scanning component as part of their overall security process. Do you have non-Windows machines you want to protect, or do you have the concern of rogue machines appearing on your network? How do you protect your web based applications?

## Reviews

*“Blink can provide a superb breadth of power in a single well-designed and solid package.”*  
-VB100, May 2008

*“eEye performed best in detecting exploits. It was the clear leader in identifying client-side attacks, alerting on all of our tests.”*  
-Information Security Magazine, November 2007

*“We’re pleased with the anti-virus capabilities that eEye has built into the product, as well as with Blink’s integration with eEye’s REM event manager and central policy management component.”*  
-eWeek, May 2007

## About eEye Digital Security

eEye® Digital Security is pioneering a new class of security products: integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise’s key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. eEye’s research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. **For more information, please visit [www.eEye.com](http://www.eEye.com).**