



# BLINK<sup>®</sup> SERVER

## Endpoint Protection Platform



### Fast Facts

o **Blink Provides Complete Server Protection Security by Combining:**

- Application and system firewall
- Virus and spyware protection
- Protocol-based intrusion prevention
- Vulnerability assessment
- Patented system protection
- Zero-day attack protection
- Web Application Firewall featuring SecureIIS
- Configuration Management Enforcement
- Enable Regulatory Compliance Initiatives

**Secure  
Your Business.**  
[www.eEye.com](http://www.eEye.com)  
866-282-8276

While signature-based anti-virus security solutions continue to be the primary for servers to meet regulatory compliance and business continuity requirements, a major shift is developing toward integrated threat management to enhance server security. Server administrators are constantly struggling to prevent attacks against server-based applications, mis-configurations, and zero-day threats. Successful exploits can leverage anything from network services to web applications and signature based anti-virus solutions are not enough on their own to repel these threats. Each time a new vulnerability, remote exploit, or other application threat is identified, organizations need to assess the risk to the critical server infrastructure and take appropriate mitigation steps. Ignoring the new threat or relying on outdated defenses only increases the risk of a successful breach.

Further complicating the server security equation is the breakdown of client-server network architectures. Mainstream adoption of virtualization, mobile, cloud, SaaS and remote access technologies force the traditional network perimeter to provide filtered access to critical servers. Application exploits for web servers, databases, and other vulnerabilities represent an easy opportunity for malware and data loss to propagate through trusted connections. In response, perimeter and network security capabilities are increasingly important on servers and endpoints to secure the connection.

### **Integrated Threat Management: Complete Server Protection**

To enhance server security and combat threats in real-time, organizations are migrating from a standalone server anti-virus software and adopting integrated threat solutions in its place. Blink Server 4, from eEye Digital Security, combines multiple-layers of server security capabilities and leverages an intrusion prevention engine that dynamically protects against new threats, in real time, even when vendor patches are not available. Since Blink Professional 4 was launched in 2006, it has successfully thwarted 100% of remote intrusion attempts on endpoints. Blink Server 4 builds on that technology and provides a complete server protection platform with full-featured integrated threat management capabilities. Blink Server 4 delivers a host of positive business benefits:

- Layered security protection that optimizes defenses against viruses, spyware, worms, trojans, cross-site scripting, SQL injection, email server protection, mis-configurations, and other malicious zero-day exploits
- The ability to consolidate 7+ discrete server security agents into a single Blink Server 4 agent and reap significant administrative time savings in the process
- Reduce system resource requirements compared to the memory footprint of maintaining 7+ discrete security products for everything from anti-virus to vulnerability assessment
- Combine Blink 4 with REM, eEye's Security Management Console, to obtain centralized attack, risk, vulnerability and overall security management
- Reduce server security costs more than 70% by eliminating the licensing and support costs associated with buying and maintaining multiple security solutions

Please visit [www.eeye.com](http://www.eeye.com) to request an evaluation copy of Blink Server 4 or to download a free copy of Blink Personal and find out for yourself why Blink garners the highest praise in independent product reviews.

**"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

The endpoint to vulnerability starts here.

# BLINK<sup>®</sup> SERVER

## Additional Features and Benefits

### - System, Application, and SecureIIS Web Application Firewall

Blink performs traditional firewall duties, allows or denies traffic based on a set of predetermined rules and it monitors the source of network traffic in real time allowing traffic only from authorized applications. Blink's Web Application Firewall featuring SecureIIS works as an ISAPI filter protecting against the latest threats from cross site scripting to SQL injection and meets the strict regulatory compliance of PCI DSS v1.2 Section 6.

### - Virus and Spyware Protection Servers

Blink Server provides complete signature and heuristics-based attack protection. Using patented sandbox technology, Blink Server can stop new attacks as they are released without the need for updates on the server. Signatures provide an additional layer of protection for known malware. Blink Server virus and spyware protection protects the host and processes as required for regulatory compliance.

### - Intrusion Prevention and Zero-Day Protection

Blink Server provides protection where a vendor has not yet created signatures or patches to protect against vulnerabilities in their operating system or application. Blink Server blocks zero-day attacks that bypass traditional signature-based solutions, protecting critical servers and their data.

### - System Protection

Blink Server provides control over which applications are allowed to function by authorizing or denying program file execution. Registry Protection prevents specific registry settings from being modified, stopping malicious programs or errand users from infecting or modifying systems. Storage Protection prevents data leakage by regulating USB and Firewire storage devices.

### - REM<sup>™</sup> 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 picture of server and endpoint security.

## About eEye Digital Security

eEye Digital Security is the global leader in the next generation of security solutions: comprehensive vulnerability management and zero-day endpoint security protection. eEye enables secure computing through world-renowned research and innovative technology, supplying the world's largest businesses with integrated and research-driven vulnerability assessment, intrusion prevention, asset security and compliance solutions. eEye's research team is consistently the first to identify new threats in the wild and our products leverage that research to deliver the tools necessary to protect our customers' environments. The endpoint to vulnerability starts here.

eEye's customers represent the largest deployments of vulnerability assessment and prevention technology in the private and public sectors. eEye protects the networks and digital assets of a growing network of more than 9,000 corporate and government deployments worldwide. Founded in 1998, eEye Digital Security is an award-winning CA internet security company headquartered in Orange County, California.

U.S. Tel: 1.866.282.8276

N. America: 1.949.333.1900

Germany: +49 (0) 8031 2227 432

U.K.: +44 (0) 20 8432 3490

N. America Sales: [sales@eEye.com](mailto:sales@eEye.com)

International Sales: [sales.eu@eEye.com](mailto:sales.eu@eEye.com)



## System Requirements

### Blink<sup>®</sup> Server Edition:

- Windows 2000 and 2003
- Windows 2007 (32-bit or 64-bit)
- Windows 2008 (32-bit or 64-bit)
- 1GHz or higher (or compatible) CPU
- 512 MB of RAM
- At least 150 MB of free disk space
- SecureIIS Web Application firewall requires IIS 5.0, IIS 6.0, and IIS 7.0 (32 and 64 bit)

### REM<sup>™</sup> Security Management Console 3.7.x:

- Windows 2000 Server SP4 or higher
- Windows 2003 Server SP2 or higher (32-bit)
- Microsoft SQL Server 2000 SP4 or higher
- Microsoft SQL Server 2005 SP1 or higher
- Microsoft SQL Server 2008
- Intel Pentium IV 2.0GHz (or compatible)
- 1 GB of RAM
- 300MB (software install) 20GB (database)
- Network Interface Card (NIC) with TCP/IP enabled
- Microsoft .Net Framework 2.0
- Microsoft IIS 6.0 or higher ASP.Net

The endpoint to vulnerability starts here.