



## eEye® Digital Security Technical Brief

# Remote and Mobile User Protection

In today's interconnected and dynamic workplace, organizations rely on a large part of their workforce working remotely from corporate offices. This creates a situation where networks are driven by computing assets flowing in and out of network perimeters, with the need to provide remote assets access to the internal network. Such fluidity in computing assets has rendered perimeter-based security solutions inadequate in protecting all aspects of computing activities.

Remote and mobile users require multiple access and configuration profiles to fulfill their job duties. For example, providing access to email or sales force applications from hotel rooms, airports, or customer offices. Another remote worker profile is that of the telecommuter working from home. Often, these users access the corporate network via the Internet rather than a secure connection. What these user scenarios have in common is the exposure to possible compromise and attacks from the Internet, and insufficient protection by corporate firewalls. Such unprotected access points are veritable playgrounds for would-be attackers and worms that propagate with little or no user interaction. Remote users whose workstations become compromised provide attackers with multiple vectors into a corporate network, once reconnected.

Mobile and remote employees thus require a tailored approach to securing their assets and ensure they are not susceptible to attacks or are harboring malicious malware applications that could infect the entire corporate network upon re-connection of the mobile device. Traditionally, a common measure many companies employ to address these usage scenarios is to install a personal firewall onto these end-point assets in order to mitigate potential attacks and infections.:

Unfortunately, attacks have become more sophisticated than what a traditional personal firewall can effectively address. When resources are protected by traditional personal firewalls, the protection typically ends at the network – hence, if an attack compromises an application, the host device becomes completely vulnerable. If a personal firewall then allows a service to execute, the software providing the service must be up-to-date and configured properly. Once the application is accessed over the network, the personal firewall cannot protect the application, nor can it control application usage of the network beyond simple port/IP address control.

Another clear illustration of the shortcomings of personal firewalls is their inability to stop “blended threats”. The NIMDA worm illustrates this type of risk. NIMDA was a multi-faceted attack that used multiple attack vectors: HTTP, email, and shared folders. Systems that were protected at the network level from HTTP attacks were often vulnerable via email, or via vulnerable web browsers. A personal firewall would not be able to combat these multiple avenues of attack. If a mobile worker became unknowingly infected with the NIMDA worm – or any worm for that matter – and re-connected with the corporate network, he would immediately give that worm access to a new group of targets for widespread infection.

## Blink End-Point Vulnerability Prevention

The Blink End-Point Vulnerability Prevention solution is comprised of several proven security technologies, including system and application firewalls, intrusion prevention systems, non-intrusive protocol analysis, and local vulnerability assessment scanning technology – based on eEye’s award winning Retina® Network Security Scanner and. With this comprehensive protection, Blink repels all classes of attacks, including known vulnerabilities and exploits, as well as undetected vulnerabilities, which could result in ‘zero-day’ attacks.

In the case of the NIMDA, systems protected by Blink would not have been susceptible to any of NIMDA’s attack vectors, nor would they have allowed a computer to be used to infect other workstations on a network. Blink is also able to control attack propagation and damage even after if an attack has successfully entered a network by limiting communication between particular applications, IP addresses, or, if warranted, by shutting down a network connection altogether. This last example is increasingly relevant considering the damage that can be done by a workstation once it re-enters the corporate network, in essence bypassing the network level firewall at the front door. Precluding an asset to attack from within the perimeter has quickly become a critical business requirement.

Furthermore, Blink allows users to remain protected, regardless of how frequently they re-connect to the corporate network, as there are no signatures to update. Blink’s ability to protect against classes of attack, rather than relying on a database of attack signatures translates into the utmost in protection for critical digital assets.

For the added protection of mobile and remote users, Blink includes the following features:

- **Malicious Application Control Prevention** protects against application hijacking via DLL control hooking
- **Application Policy Control** prevents abusive user behavior within applications, such as downloading files via p2p or Instant Messenger applications
- **Non-Signature Based Attack Prevention** detects and blocks attacks without the need or use of attack signatures. This translates into complete protection, even when an attack is circulating, but the vendor has not yet created signatures or provided patches. This also obviates the administrative burden associated with updating signatures files.
- **Inbound and Outbound port blocking:** Blink controls all aspects of network traffic including all inbound and outbound connections. Blink also controls traffic based on protocol, port, and communicating host address
- **Operating System Hardening:** Blink acts as Windows hardening solution, preventing attacks from modifying critical OS binary files or configuration settings

Securing mobile and remote employees requires a specialized approach to adequately ensure the security of not only those particular assets, but also, the corporate network. To meet this challenge requires creates comprehensive, multi-layered solution. Leveraging multiple elements of proven security technologies, the Blink Vulnerability Prevention solution is uniquely suited for this challenge.

To learn how the Blink Vulnerability Prevention solution can help **Maintain Scheduled Patching Cycles**, [click here](#).

To request more information regarding Blink, [please click here](#).