



FOR IMMEDIATE RELEASE

eEye® Digital Security Eliminates the Threat of Zero-Day Attacks with Blink® – The Industry's Most Comprehensive End-Point Security Solution

Blink Revolutionizes Enterprise Security By Protecting Against Unknown Vulnerabilities and Socially Engineered Security Threats While Allowing Enterprises to Patch on Their Own Schedule

ALISO VIEJO, Calif., July 26, 2004 – eEye® Digital Security, a leading developer of vulnerability management software solutions for enterprise security, today announced Blink – the most powerful and comprehensive end-point security software product introduced to date. Designed to be implemented on individual assets such as servers, PCs and laptops, Blink is the first end-point product to combine multiple layers of security technologies to protect enterprises from “zero-day” attacks that leverage yet unknown vulnerabilities within enterprise networks. This comprehensive security solution allows enterprises to defer patching vulnerable machines until regularly scheduled maintenance cycles, thereby saving millions of dollars in lost business disruption and the associated IT resource drain caused by “panic” patching. Additionally, Blink eliminates the problem of so-called “socially engineered” security threats in which hackers trick individuals into downloading malware or otherwise making their own machines vulnerable to attack. As a result, Blink uniquely protects assets from vulnerabilities, as opposed to only thwarting attacks.

“We expect the exploitation of vulnerabilities before enterprises can remediate them to rise steadily. It is imperative that businesses implement some means to protect themselves from unpatched and rapidly developing new vulnerabilities,” said Paul Proctor, vice president at META Group, a leading provider of IT research, advisory services and strategic consulting. “Multi-layered security solutions that incorporate capabilities like intrusion prevention, vulnerability mitigation and firewall technologies can help enterprises better protect their digital assets.”

These trends have created an imperative for enterprises to protect individual digital assets within the network perimeter by applying protection layers on the assets themselves. Blink provides this level of protection and is the culmination of three years of development by the industry's most successful security vulnerability research team. Over the last five years, eEye has been recognized as the preeminent organization in the discovery of the most critical vulnerabilities in various platforms and applications, including the vulnerabilities subsequently leveraged by Sasser, Witty, Code Red and Sapphire worms, as well as the Microsoft ASN vulnerability and hundreds of other important discoveries. This expertise gives eEye a distinct advantage in designing software solutions for the assessment, remediation and prevention of vulnerabilities and the attacks that leverage them. The end result is Blink - the most powerful and effective vulnerability and intrusion prevention software in the industry.

Blink leverages multiple layers of protection to shield individual digital assets from intrusion. The primary layer is an intrusion prevention mechanism that protects from attacks leveraging yet unknown vulnerabilities. While most IPS technologies use the known signature of the virus or worm to detect and stop attacks, Blink focuses instead on the methods of exploitation that such attacks utilize. This enables Blink to stop intrusion without having to identify the unique signature of the attack itself.

The layers of protection within Blink include:

- **A Protocol-Based Vulnerability Protection System that shields the asset from unknown attacks without the use of signatures**
- **A Rule-Based Vulnerability Defense System to pinpoint and shield the asset from known vulnerabilities**



- **A Systems-Level Network Firewall to control unauthorized connectivity to the asset from others**
- **An Application-Level Network Firewall to prevent unauthorized programs from running on the asset**
- **A Host-Level Vulnerability Assessment scanner to detect and report security issues and policy non-compliance on the asset**

These capabilities are delivered in the form of a software agent that is managed from a centralized console and implemented on each device – such as a laptop, server or PC – running any Microsoft® Operating System (OS). Designed to be completely non-intrusive, Blink can be installed, updated and managed in a transparent manner without requiring end-user intervention so as not to impact productivity.

Why Does the Industry Need Blink?

Unknown vulnerabilities represent the greatest threat to enterprises' digital assets. Contrary to popular belief, many hackers do not wish for worms to be released, as this galvanizes enterprises to patch machines that could otherwise be used as doors into a network. This will continue to be a growing issue as enterprises become more successful at proactive vulnerability assessment and remediation – hackers will focus on ways to compromise systems in a “zero-day” fashion. Since Blink operates by stopping the activity that results from an attack rather than the signature of the attack itself, this technology is able to stop even unknown vulnerabilities from being exploited.

Additionally, as the window continues to shrink between the time vulnerabilities are announced and when enterprises are able to patch their systems, the costs incurred by companies through patch management will continue to grow. A company with thousands of machines in its network can expect to experience millions of dollars in lost productivity and business disruption when patching is immediately required. As a result, enterprises need the ability to defer patching to scheduled maintenance cycles, as well as intermediate protection from attacks that intend to leverage the unpatched vulnerability. By protecting individual machines, Blink allows corporations to patch their systems on a less disruptive, more cost-effective schedule.

Likewise, although the vast majority of enterprises have network-level security elements in place (e.g., firewalls, IDS/IPS, etc.), many remote workers, such as mobile workers, teleworkers, contractors and others, unintentionally acquire vulnerabilities “in the wild” and introduce these vulnerabilities to the corporate network once they reconnect. This internal attack vector is becoming a frequent cause of worms and virus outbreaks. Blink provides the means to isolate and evaluate each machine prior to its reconnection to the network. If any of Blink's security mechanisms detect unusual behavior, the machine is isolated via its application and system-level firewalls, and the attack is prevented.

Blink also helps enterprises enforce policy compliance by constantly auditing corporate security standard configurations to reduce the risk of compromise. Finally, traditional security measures offer no defense against socially engineered security threats that attack from inside the organization. Even if a user unwittingly downloads a virus or worm, Blink is able to recognize the harmful activity, shut down the offending application, and isolate the machine from the rest of the network.

“The scramble to patch thousands or more systems in the wake of announced software vulnerabilities is costing enterprises up to tens of millions of dollars a year – even if the vulnerability remains unexploited,” stated Firas Raouf, eEye's COO. “Moreover, the most malicious hackers are using unknown vulnerabilities in specific, targeted attacks against these enterprises – often without their knowledge. While our large enterprise customers have successfully used eEye's Retina Security Scanner to identify and fix known vulnerabilities, it was clear they also needed a mechanism to both protect against undiscovered vulnerabilities and to better manage the time-consuming and costly patching process.”



eEye® Digital Security

eEye Digital Security
One Columbia, Suite 100
Aliso Viejo, CA 92656

Toll Free: 1.866.339.3732
Tel: 1.949.900.4100
Fax: 1.949.349.9538
Web: www.eeye.com

Unlike other host-based intrusion prevention technologies, Blink does not rely on anomaly-based protection. Anomaly-based solutions must first learn normal machine processes and the typical calls these processes make to the OS. Once activated, such solutions protect from attacks by looking for anomalies in the processing of the potentially malicious traffic, and blocking the calls to the OS that are generated by that processing. Such solutions tend to require repeated learning stages as processes evolve over time, including having to be turned off when new applications – including patches – are deployed. This process requires ongoing human intervention and diminishes IT productivity. Another drawback to anomaly-based solutions is they must wait until the attack is actually processed, forcing either disruption of the process or restarting it as the only ways to block attacks, which negatively impacts end-user productivity. In contrast, Blink requires no administrator intervention to be effective and operates in a completely non-intrusive fashion, blocking attacks *before* they are processed by the targeted applications.

Designed for Large Enterprise Deployments

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 Microsoft's Active Directory as a means to efficiently manage the identities and relationships that make up network environments, further leveraging enterprise investments.

Blink does not require on-site installation for each device, but can instead be deployed, installed, maintained and upgraded from a centralized location, making it particularly easy to manage for enterprises with thousands of devices. In addition, many end-point security products shut down systems that exhibit offensive activity, which usually results in administrators having to manually reboot the entire system. For a large enterprise network, this can cost thousands of dollars in IT resources and end-user downtime. By comparison, Blink is able to isolate individual applications, thus allowing the system to continue running even while the rest of the network is protected.

Blink is available and operating in production networks today. To find out more, contact eEye or visit the company's Website at: <http://www.eeye.com/blink>.

About eEye Digital Security

eEye Digital Security is a leading developer of security software and an active contributor to network security research and education. eEye provides complete vulnerability management solutions that address the full lifecycle of security threats: before, during, and after attacks. eEye's award-winning products include vulnerability assessment, remediation management, intrusion prevention and network forensics solutions. eEye protects the networks and digital assets of more than 2,500 corporate and government entities in over eighty countries, including AT&T Wireless, Avon, Citigroup, Continental Airlines, US Department of Defense, Dow Jones, Ernst & Young, Prudential, Viacom, and Wyeth. Founded in 1998, eEye is a privately held, venture-backed firm with headquarters in Orange County, Calif. For more information visit www.eeye.com.

Contacts

Jay Nichols, Sterling Communications, 1.408.395.5500 | email: jnichols@sterlingpr.com
Joe Repetti, 1.949.900.4100 x243 | email: press@eeye.com

Europe: Tony Brookes, +41 22 718 7700 | email: tbrookes@eEye.com

All trademarks contained within this press release are the sole property of their respective owners and are hereby acknowledged.