



What's New in Blink® 2.0

Blink® 2.0 represents the continued advancement of eEye Digital Security's revolutionary, award winning approach to end-point intrusion prevention. In addition to several infrastructure improvements, the following is a partial list of feature enhancements that will be included in this new version, generally available at the end of February 2005.

Anti-Spyware Protection

Note: Spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or those engaging in nefarious activities. As such, spyware is cause for public concern about privacy on the Internet as well as performance impacts to infected machines.

Since its original release, Blink has always been able to preclude spyware from connecting out to the Internet to deliver surreptitiously acquired information, such as intellectual property, patient/customer data, financial and personal information, etc. With the advent of Blink 2.0, eEye now offers complete coverage from the impact of spyware, enhancing the performance of machines through security. This protection comes in two forms;

- *Real Time Malicious Code Protection* – Blink will actively block malware instances from being loaded into memory and give the option to quarantine or remove the suspected code. This is done by checking processes against a CRC (cyclical redundant check) database of spyware methods.
- *Disk Scanning and Removal* – As a 'last line of defense', Blink will also offer the capability to perform intelligent disk scanning and remove malware from disk, similar to traditional tools available today.

Blink's real time malware protection has a distinct advantage over competitive offerings which solely rely on disk scanning for the identification and removal of malware. Blink's active protection will preclude malware from loading into memory and its attempt to write to disk. Competitive offerings must resort to scanning disk, which is purely reactive in nature. This is also offered in Blink, but not as its primary method of protection.

Identify Theft Protection

Note: Phishing attacks use 'spoofed' and fraudulent communication methods designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

Leveraging its protocol analysis engine, Blink is now able to detect and classify phishing attempts made via the POP3, IMAP or HTTP protocols. This includes images used to convey these phishing attacks. Similar to how Blink is able to analyze the sessions of packets for methods of attack, it is also able to recognize malicious website images or redirects that may be used as part of phishing scams. The phishing attempt is replace by a Blink alert within the text and an event is logged.



Application Layer Protection

Blink's Application Layer Protection is the final layer in Blink's real-time defenses - it thwarts all buffered code execution exploits, by detecting when payload code executes in system resources belonging to another process (the process being attacked). Blink detects all payloads that attempt to run in memory (execute in the stack, heap, or BSS segment). These memory areas are designed to be used for program data, not for code execution, but an attack that causes the CPU to fetch instructions from these areas will result in the CPU evaluating and executing payload data. Upon detection of such violating actions, Blink will terminate the process instead of allowing for the execution of the malicious payload code.

Stateful Firewall Rules

Blink will dynamically create the necessary System Firewall rules to temporarily enable applications, allowed by Blink policy, to function. This will reduce the rule configuration process necessary to coexist with popular applications such as Outlook, and business applications such as SAP, and Oracle that need network firewall rules associated with them.

Advanced Central Policy Capabilities

For environments that require multiple deployment mechanisms (the Blink Console), users may now connect to a co-existing Blink Console and edit the policies stored at that remote location. This allows multiple administrators to manage a central a central policy or policies from multiple consoles.

Additionally, for organizations with large, distributed operations, connections to Blink-protected machines are not always constant, yet there may be the need to update policies on those machines. For this reason, policies can be downloaded from alternative locations, other than the traditional method, the Blink Console. Policies can now be downloaded from HTTP/S, FTP servers, as well as via the secure communications channel to a Blink Console.