dynamic filtration technology

The Shape of Things

Today, most anti-virus solutions employ static, signature-based security technology that is highly successful at detecting and defending against known threats. Each day, the leading antivirus vendors devote considerable global resources to discover, research, and write signatures for new viruses. They then distribute these signatures to their customers, who in turn, must deploy and activate them to properly insulate their network.

This traditional approach allows for a critical window of vulnerability from the moment the virus is released into the wild until it is detected, diagnosed, distributed, and deployed – leaving users exposed and vulnerable for attack. At the current rate at which viruses emerge and propagate across the Internet, businesses are assuming a significant amount of risk. This is a liability that businesses cannot afford to ignore.

The DyVax™ Difference

DyVax™ takes a radically different approach. It completely eliminates the need for static signatures by utilizing dynamic filtering techniques. Dynamic filtering means no window of vulnerability – new viruses and malicious attacks are prevented before they are even written. Users are secure and businesses can rest easy knowing that viruses will automatically be thwarted. DyVax has successfully blocked zero-day worms and viruses at customer sites, including multiple variants of the Stration Worm and the Storm Trojan. In laboratory testing, DyVax has proven more successful than the leading commercial and open source antivirus solutions.

The Technology

DyVax™ works on the premise of two important values while scanning traffic – threat level and threshold level. For all incoming traffic, DyVax establishes the immediate threat level posed by the traffic and compares it against a threshold level. If the threat level exceeds the threshold level, the incoming traffic is identified as malicious, triggering automatic pre-selected protection. DyVax can attach warnings to email traffic, remove malicious content, or quarantine or terminate malicious traffic.

Beyond Prevention

DyVax™ is a complex algorithm and inspection engine that has been effectively deployed to dynamically filter email traffic, including POP3, SMTP and IMAP, to differentiate benign and malicious traffic. DyVax serves as a powerful malware vaccine by proactively shielding the user's networks, servers, and workstations from malicious threats and offering the industry's first true and unparalleled, zero-day threat protection.

DyVax is currently being developed to filter network traffic in order to build a true, signatureless Intrusion Prevention System capable of monitoring and protecting application level channels such as Web, FTP, and Instant Messaging. Additional capabilities will include protection from spam and other malware.

The underlying technology for DyVax has endured years of rigorous testing and refinement. DyVax has been combined in the AccessEnforcer™ to provide a comprehensive security solution including a stateful deep packet inspection firewall, complete intrusion detection and prevention system, spam protection, email filtering, instant messaging filtering and other beneficial solutions.