

DyVax Under the Hood

Achilles' Heel of Traditional Security

Traditional security products rely on static rule sets to function. For example, firewalls use static policies set by the administrator to allow select IP addresses access into the network. Antivirus products rely on signatures or virus definitions to identify viruses while spam filters rely on content "fingerprints" or lists of known spammers called blacklists.

This traditional reliance on static rule sets can provide very accurate results for known threats whose unique "fingerprints" have been identified, they are powerless when addressing brand new "zero-day" attacks due to the manual, time-consuming process required to create signatures. This is time that most businesses cannot afford. Antivirus vendors require anywhere from 24 hours to 3 days to create a signature for a new virus after first identifying the new threat. In January 25, 2003, the SQL Slammer worm propagated around the Internet and caused massive damage to bank ATMs, airline systems and even the Internet infrastructure for entire countries - in just 10 minutes. This is certainly not enough time for any vendor to create a signature for the new threat, distribute the signature to their customers and then allow the customers to activate the new virus definitions. The damage has been done.

It is clear that the "all-or-nothing" static rule set approach is insufficient for today's high speed threats. New threats are discovered at an increasingly alarming rate, and numerous viruses and threats now morph or mutate into polymorphic forms thus evading the traditional signature based security solutions.

"The firewall is dead," says Google security specialist Niels Provos.
May 5th, 2007, <http://themoderatevoice.com>

How DyVax™ Works

To address this widening gap in security, the founders of Calyptix Security developed DyVax, an advanced inspection engine that does not rely on a static rule set to identify threats.

To understand how DyVax operates, the banking industry's credit model provides an excellent real world example. When a home buyer applies for a mortgage loan, the lender reviews the home buyer's creditworthiness by checking his credit rating. The credit score reflects the creditworthiness of the buyer and allows the lender to make an informed decision to approve or deny the proposed loan. If the risk of repayment is too great, the lender will deny the loan. Lenders apply this same scoring methodology in different environments, including home equity loans, credit cards, car loans and small business loans, to reduce their risk for repayment.

DyVax, Calyptix Security's patent-pending inspection engine, uses a similar dynamic approach when analyzing threats. DyVax does not use static rule sets like signatures or blacklists since they are inadequate for today's threats. Instead, DyVax uses a risk-scoring model to identify threats. In the process of building DyVax, the authors have analyzed large datasets consisting of legitimate and malicious data, and implemented risk-scoring algorithms to detect classes of threats, instead of individual threats themselves. This ensures that new threats in those classes are rapidly detected without requiring signatures.

"In the face of a rapidly evolving threat landscape, the firewall - the fundamental tool for managing network security today - is no longer adequate. A better approach is security that is based on policy. With policy-based security, the rules that govern access to networks, resources, and information can be enforced seamlessly across platforms and devices."

*February 6, 2007, Bill Gates, Chairman, Microsoft Corporation
<http://www.microsoft.com/mscorp/execmail/2007/02-06secureaccess.mspx>*

DyVax Under the Hood

DyVax has other built-in benefits that are especially useful to counter today's threats:

1. **Flexibility** – DyVax is written to be flexible, and so it has the ability to address a wide variety of threats on different network protocols (e.g. network layer, email, web, etc.). This flexibility enables DyVax to be extended to multiple protocols as malware authors use different protocols to achieve their aims.
2. **Environment awareness** – Different sites experience different kinds of threats. Because DyVax was designed to be sensitive to its operating environment, the inspection engine can react differently depending on where it is deployed.
3. **Internet awareness** – DyVax can obtain live feeds from the Internet to respond to and stop rapidly emerging threats. For example, it can customize itself to be more sensitive to threats during global worm outbreaks.

Demonstrated Success of DyVax

DyVax has undergone rigorous lab testing and has proven to be more effective than leading antivirus vendors in internal testing with a virus population in excess of 1,000 viruses. Given its flexibility and feature-rich foundation, DyVax is the perfect inspection engine for a Unified Threat Management (UTM) appliance. DyVax has been deployed on email traffic, executable files and Microsoft Office files to block viruses and malware in those sources.

In addition to success in the lab, DyVax has also outperformed leading anti-virus vendors in the field at live customer sites. Listed below are several examples where DyVax has successfully defended customers from previously unknown viruses before leading vendors were able to release protection.

Timeline of Events

	Calyptix Security		Traditional Vendors	
	Software Release Date	Virus Captured	Virus Identified	Signature Released
Stration Worm	7/31/06	9/10/06	9/10/06	9/11-20/06
Storm Trojan	1/9/07	1/17/07	1/17/07	1/18-22/07
Nuwar Worm	1/9/07	1/21/07	1/21/07	1/21-27/07
Valentine's Day Bug	1/9/07	2/13/07	2/13/07	2/14/07

The Future of DyVax

DyVax already protects networks from unknown threats in email, executable files and Microsoft Office files such as Word, Excel and PowerPoint. Calyptix is extending the reach of DyVax to provide even more protection by applying the same proven technology to web traffic, network traffic and instant messaging protocols.

