Barracuda's Antivirus Technology

White Paper

The Barracuda Networks anti-malware technology is purpose-built to solve the unique needs of email and Web security appliances. Unlike traditional antivirus technologies designed to work on desktop computers, Barracuda Networks anti-malware technology is specifically designed for:

- Speed of response
- Prioritizing malware threats that propagate quickly
- Low false positives
- Leveraging the resources of the free and open source (FOSS) security research community for maximum breadth

With this combination of technologies specifically designed to meet these criteria over SMTP and HTTP protocols, Barracuda Networks is able to provide best-of-breed protection for customers of the Barracuda Email Security Gateway and Barracuda Web Security Gateway. In addition, Barracuda Networks also incorporates these technologies into Barracuda Message Archiver, Barracuda SSL VPN, and Barracuda Web Application Firewall.

Speed of Response

Like other antivirus research centers, Barracuda Labs, Barracuda Networks' 24x7 threat operations center, maintains traps (or "honeypots") on the Internet to collect threats and threat data. In addition, Barracuda Networks leverages aggregated and anonymous data from over 150,000 customer systems worldwide to collect and respond to data about the latest threats. These systems span small-to-medium businesses, educational institutions, government agencies, enterprises, and service providers that contribute to a diverse corpus of email and Web threat data on the Internet, representing over 1.5 billion emails and 75 billion Web requests per day.

This threat data enables Barracuda Labs engineers to continually update the virus, spyware, and spam definitions that are offered as part of the Barracuda Energize Updates subscriptions on Barracuda Networks appliances.

The Barracuda Email Security Gateway leverages Barracuda Real-Time Protection for instantaneous protection against the latest threats as they attempt to propagate. While email remains the fastest and dominant method of rapid propagation, other Barracuda Networks products update themselves automatically with latest virus definitions at hourly intervals.

Prioritizing Malware Threats that Propagate Quickly

While some may measure antivirus efficacy based on size of signature database, Barracuda Labs measures itself on preventing virus propagation. Barracuda Labs has developed backend systems specifically designed to:

- Identify email propagation useful for both spam and email-borne viruses
- Measure outbound spyware phone-home activity from honeypot and customer systems
- Identify new or hacked Web sites that may host malware content

Barracuda Labs engineers can react more quickly than many other researchers by analyzing how viruses propagate. Binaries that are propagated by known spam bots or that are hosted on known bad Web sites can be prioritized above other binaries for analysis. In addition, unknown binaries that communicate via known spyware phone-home protocols or that communicate with known spyware destinations can also be prioritized. As such, by leveraging Barracuda Labs' specialized knowledge of IP and domain reputation of traffic sources and destinations, Barracuda Networks can uniquely prioritize those threats capable of propagating most quickly.

Moreover, Barracuda Labs' technology investment in Predictive Sender Profiling informs Barracuda Labs of suspicious behaviors from even those sources and destinations that have not yet established negative reputations. Examples of these cases include hacking of legitimate Web sites by hackers or potentially newly infected bots on otherwise legitimate computers.

Low False Positives

The requirements of a gateway security product form factor differ from a desktop anti-virus software package. When a desktop anti-virus program falsely classifies a harmless file as a virus, users can generally retrieve the suspicious file from a local quarantine through a graphical interface on their computers without involving IT. However, when a gateway product strips and prevents a file from being delivered to an email server or stops a Web download session, retrieval of the file is often more difficult or sometimes impossible.

With a heritage in gateway security, Barracuda Labs has prioritized low false positive rates in its analysis. While some antivirus vendors may look for simple signatures (e.g., a long string value in a macro) to gain coverage, Barracuda Labs works to restrict signatures to only harmful sequences (e.g., a long string value in macro that actually attempts to exploit a buffer overflow to run malicious code).

The focus of Barracuda Labs is to reduce threats without interrupting legitimate work whether this applies to spam, viruses, or other threats.

Leveraging and Extending on Free and Open Source Software (FOSS)

Barracuda Networks is known in the security industry for its use of ClamAV, the world's leading free and open source anti-virus project. Select Barracuda Networks appliances include the ClamAV engine, and Barracuda Labs leverages the ongoing updates contributed by the open source security research community.

With this relationship, Barracuda Labs rounds out its coverage of proprietary rapid-response threat data with the world's largest open source collection of common malware vulnerability data. ClamAV excels in identifying viruses which are not well covered by rapid-response techniques, including those that are wellknown but that do not propagate quickly. The combination of Barracuda Networks proprietary antivirus protection with ClamAV open source protection has proven to be a powerful one in the marketplace.

Summary

Barracuda Networks can offer unique value to its customers by utilizing anti-virus technology purpose-built for its products. By leveraging open source, Barracuda Networks can offer similar performance of commodity anti-virus products for common threats. However, unlike anti-virus engines for desktop computers retrofitted for gateway usage, Barracuda Networks offers industry leading rapid response and protection to the threats that propagate most aggressively - all without affecting legitimate work.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com