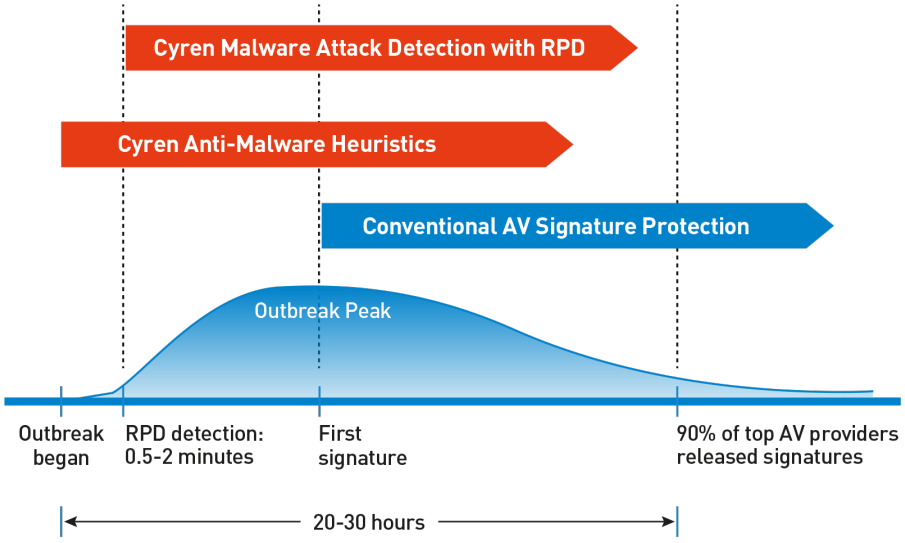
CYREN

Malware Detection Engine

Email-borne malware remains a real threat, with well-executed social engineering attacks convincing recipients to open and execute harmful attachments. Conventional anti-virus (AV) detection technologies rely on time-consuming signature generation and propagation, while Cyren's heuristic anti-malware detection technology detects new malware as much as 30 hours earlier than 90% of signatures released by the top AV providers, catching malware outbreaks at the very beginning.



Cyren Malware Detection Engine provides a complementary shield to conventional AV technology, providing protection in the earliest moments of malware outbreaks, continuing as each new variant emerges. Cyren designed the service to specifically meet the technology and business needs of:

- **Service Providers and Anti-Spam Vendors**—offer malware attack protection as a powerful value-added feature, broadening and differentiating your offerings from competitors
- **Security Appliance Vendors**—with full automation, a tiny footprint and easy implementation, the Cyren solution is a perfect extra layer for any security appliance
- **AV Vendors**—provide better service by protecting customers from new viruses. Use Cyren alerts to accelerate signature production

Cyren's Malware Detection Engine Differentiators

- High malware detection rates from the very start of email- attached outbreaks
- Enhanced customer satisfaction due to real-time protection from email-borne malware with almost zero false positives
- Increased revenue by adding a premium messaging security solution to your current offerings
- Simplified operations & improved TCO by working with a single vendor for Internet security services – the same engine can provide Anti-Spam and Anti-Malware detection

CYREN

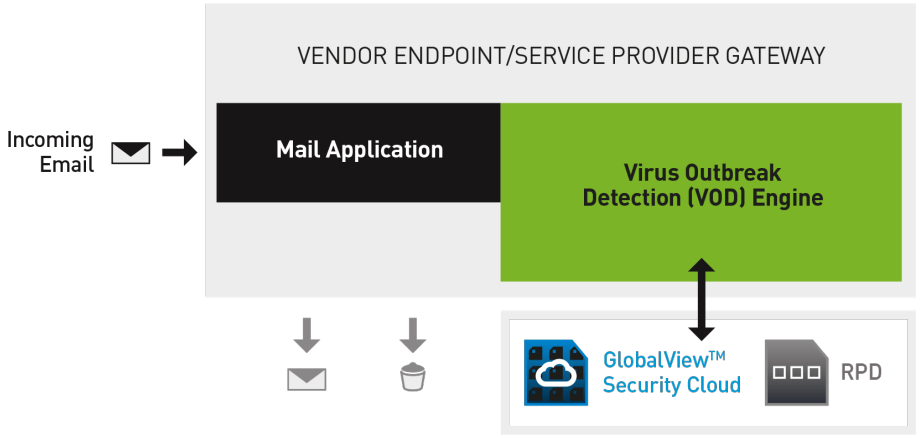
Malware Detection Engine

How it Works

The foundation is the Cyren GlobalView™, operated globally across 19 high-availability data centers. Cyren's patented cloud-based Recurrent Pattern Detection (RPD) technology analyzes billions of globally collected emails every day to detect malware outbreaks the moment they emerge.

Malware outbreaks distributed via email share identifiable patterns, such as: the sender IP address; the same malicious code in attached malware; or combinations of characters from the subject and body of the email. RPD does not rely on file scanning like conventional AV technology, instead complementing AV with detection based on:

- Email distribution patterns—such as senders (how many, location) and the volume of the emails sent over a period of time
- Structure patterns—in the email messages and attachments



Vendors and service providers integrate the Malware Detection Engine into their email security solution. The engine queries a local cache of detection signatures to determine if the scanned attachment is malware. If the signature is not found locally, a small query signature (not the attachment) is sent to the GlobalView™ for further analysis.

If the query signature is diagnosed as malware, the email and attachments are flagged as such. If it is not, the email is cleared for transmission to its recipient.

Functionality

- Based on market-proven RPD technology
- Fully automated real-time solution—zero human intervention
- Easy integration gets your product to market fast
- Comprehensive SDK (daemon or shared library)
- Supports any version of Linux, FreeBSD, Solaris, Windows, and others
- Very low CPU and Memory load
- Efficient processing: hundreds of messages per second per processor

www.cyren.com/contact
sales@cyren.com