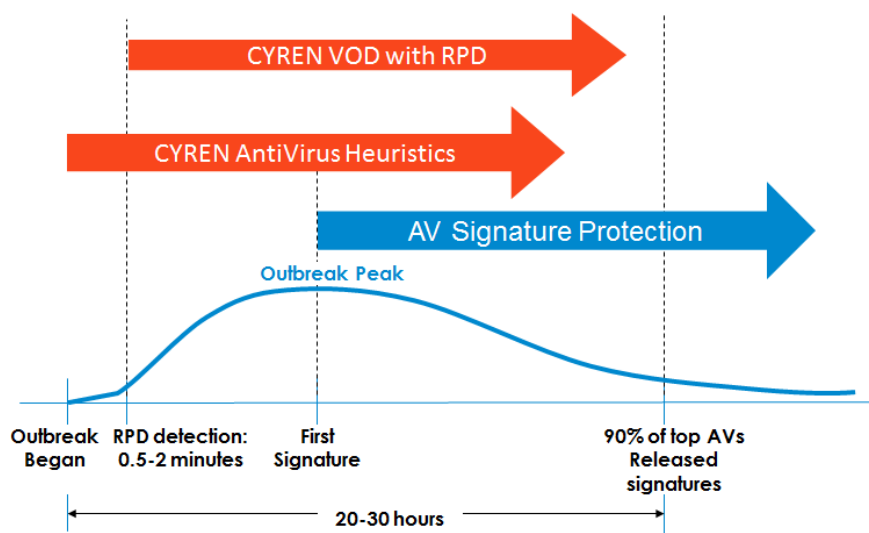# CYREN

⚡ VIRUS OUTBREAK DETECTION

Email-borne malware remains a real threat, with well executed social engineering convincing recipients to open and execute harmful attachments. While Heuristic antivirus (AV) detection technology such as that found in **CYREN AntiVirus** detects new malware as it emerges, other malware requires signature creation, which creates a detection time gap.

CYREN Virus Outbreak Detection (VOD) 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 VOD specifically to meet the technology and business needs of:

- Service Providers and Anti-Spam Vendors –offer virus outbreak 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

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 AntiSpam and AntiVirus detection

"CYREN has a long track record of consistently delivering top outbreak detection for spam and viruses. As the battle to make email safe heats up, I am confident with CYREN as our ally."

Peter Falck
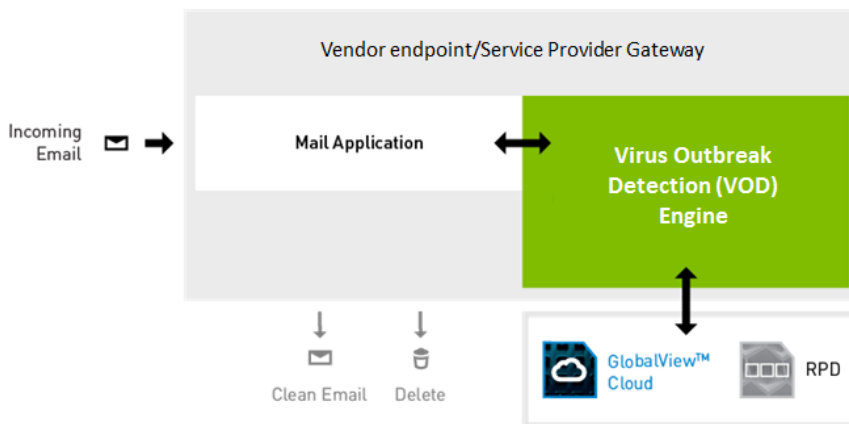**CEO**
Halon Security

HOW IT WORKS

The foundation is the CYREN GlobalView™ Cloud infrastructure, operational over 15 years across multiple worldwide high-availability data centers. CYREN patented cloud-based Recurrent Pattern Detection (RPD) technology analyzes billions of globally collected emails every day to detect malware outbreaks *at the zero-hour*.

Malware outbreaks distributed via email share identifiable patterns, such as: 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, 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 VOD 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™ Cloud 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