CYREN

ANTIVIRUS FOR EMAIL

Malware threats continue to grow in both volume and complexity. Email-borne malware remains a considerable threat, with social engineering convincing recipients to open and execute harmful attachments. CYREN Embedded AntiVirus for Email provides the ultimate defense with a dual-detection approach: Cloud-based pattern detection combined with multi-layer file scanning. This dual approach ensures malware detection from the zero-hour of an outbreak through any stage of the malware lifecycle.

CLOUD-BASED PATTERN DETECTION

Our patented cloud-based Recurrent Pattern Detection (RPD) technology analyzes billions of emails every day to detect malware outbreaks at the zero-hour. Outbreaks distributed via email share identifiable patterns such as: sender IP addresses; 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, instead detecting 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

MULTI-LAYER FILE SCANNING

CYREN Embedded AntiVirus provides multiple layers of file-based malware detection including:

- Heuristics – basic and emulator-based
- Algorithmic scanning methods – using an internal detection language
- Signature-based scanning – for exact malware file identification
- Emulation – for encrypted and polymorphic virus detection
- Several Threat Protection Modules use the above detection techniques to accurately detect malware hidden in PDF files, HTML and Java scripts, archive files and many more

CYREN Embedded AntiVirus for Email customers include:

Google Microsoft McAfee

BENEFITS

- **High catch-rates** - for email-borne malware with our dual detection approach
- **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
- **Lower TCO** - by working with a single vendor for your Internet security services

"We strive to provide industry-best products and support, and our partnership with CYREN extends our ability to satisfy customers. CYREN's dual-detection antimalware approach keeps our customers safe from malware and their mailboxes free of unwanted email."

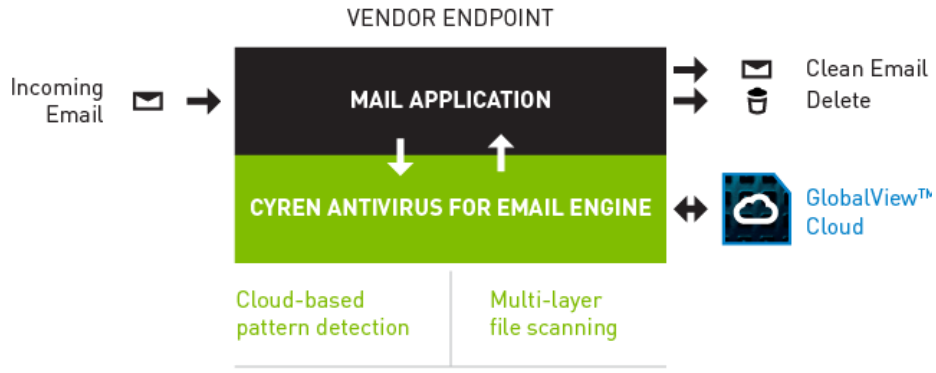
John "Tripp" Allen
President, Messaging Division
IPSwitch

CYREN

CLOUD-BASED ARCHITECTURE

All CYREN solutions are built on the CYREN GlobalView™ Cloud. GlobalView™ Cloud collects and analyses billions of internet transactions daily to build unmatched insight into Internet security threats. This data is instantly available to endpoints that implement CYREN Email Security, Web Filtering, and Antivirus solutions.

CYREN Embedded AntiVirus for Email can be integrated into vendor devices or service provider environments. An email attachment query is sent by the Mail Transfer Agent (MTA) or security device to the CYREN engine. The result is a combined response from the pattern detection and file scanning services. This enables the requester to delete malware attachments and emails and forward clean emails to their intended recipients. Integration options include comprehensive SDKs, daemons, and a range of plugins and milters.



The CYREN Engine is designed for high throughput but is also flexible allowing integration into the thinnest hardware platforms, as well as large-scale carrier-grade deployments. The same engine can be expanded to include additional services such as AntiSpam, or URL Filtering.

By combining multiple security services into a single engine and framework, our partners gain important technological, operational and financial benefits.

SPECIFICATIONS

- Full anti-malware SDK detects worms, Trojans, spyware, adware and potentially unwanted application types
- Full support for all types of ZIP, Bzip2, RAR, 7zip, NSIS and CAB compression techniques
- Comprehensive SDK (daemon or shared library) as well as industry-standard milters and plugins
- Multi-platform (Windows, Linux, UNIX, etc.)
- Detailed threat feedback through simple API, including detection accuracy and type
- Small definition file size
- Efficient processing – hundreds of messages per second, per processor
- Very low CPU and memory load