CYREN BY DATA443

Cyren Malware Detection Engine

Supercharging Detection of Advanced Threats

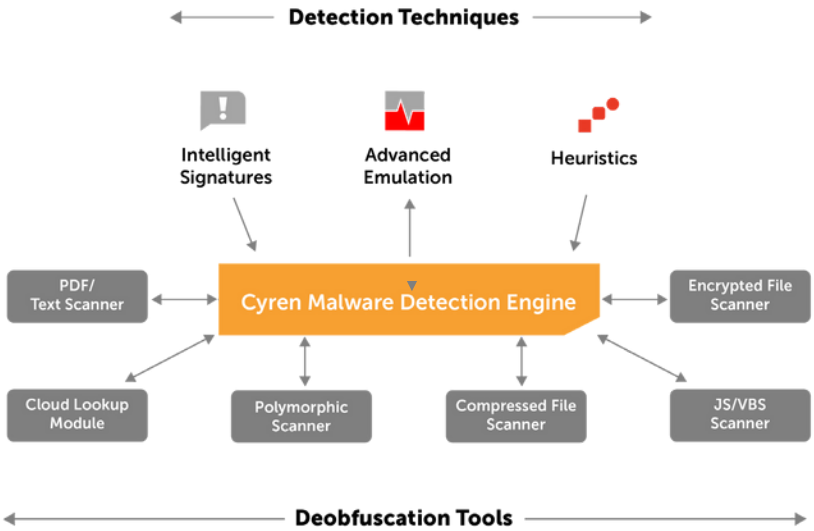
Organizational users rely on multiple tools and products to improve their productivity and collaboration. These tools allow them to share a large volume of files including documents, PDFs, spreadsheets, etc. – allowing for instant collaboration and communication. This increased reliance on email communication and cloud file-storage/sharing platforms has given rise to an increased number of incidents involving file-based malware and file-based phishing. Users and organizations trust your product/tool to provide a safe platform to share content and collaborate. Any breach of this trust can lead to unintentional spread of malware, infect your customers, and cause irreparable damage to your brand. Any embedded malware detection engine must provide product managers the confidence to reduce vulnerabilities to cloud-hosted, file-based malware. Additionally, any service providers that integrate malware detection capabilities in their email and web services must be able to rely on the detection capabilities to ensure protection against evolving advanced threats.

Benefits of Cyren Malware Detection Engine

- Focused on the latest outbreaks
- Rapid detection with/without network connectivity
- Effective detection of packed/ obfuscated files
- Powered by Cyren GlobalView™ Threat Intelligence Cloud

Cyren Malware Detection Engine

Cyren's Malware Detection Engine is the best solution for hardware/ software vendors, and service providers needing a security solution that combines superior detection with maximum performance. By employing several advanced microscanners (deobfuscation tools), Cyren's Malware Detection Engine offers multi-layered detection, modular architecture, and multi-platform support. Cyren Malware Detection Engine's fast and accurate detection relies on analytics and automation: heuristic analysis, advanced emulation, and intelligent signatures. The quality of detection stems from our ability to continuously refresh data stored in Cyren GlobalView™ and the way we integrate expertise and analytics to transform the data into actionable intelligence.



DATA443

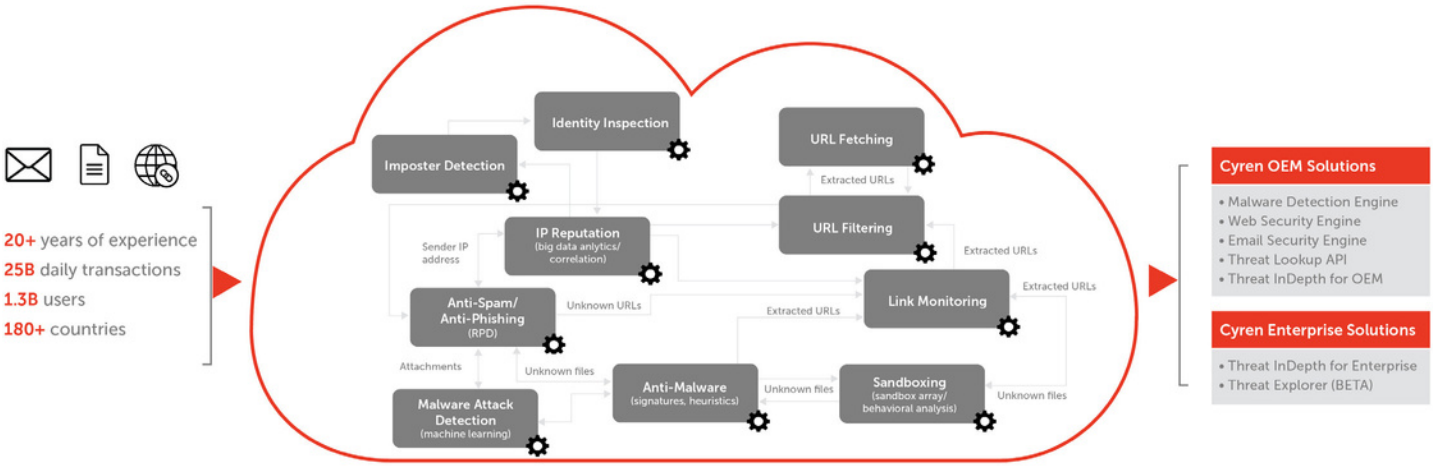
4000 Sancar Way, Suite 400
Research Triangle, NC 27709

Website: www.data443.com
Email: info@data443.com

US: +1 919 526 1070
UK: +44 203 7693 700

What Powers Cyren Malware Detection Engine?

Cyren gathers actionable intelligence by analyzing and processing billions of daily transactions in Cyren GlobalView™ Threat Intelligence cloud. By correlating insights gathered across email content, web traffic, and suspicious files; Cyren provides product owners with a multi-dimensional presentation of critical threat characteristics. Cyren GlobalView applies machine analytics to automatically transform data into actionable insights. Cyren's Malware Detection Engine leverages GlobalView to ensure rapid threat detection and analysis.



Benefits of Cyren Malware Detection Engine

Focused on the Latest Outbreaks - With new malware files being consistently shared via email, instant communication, and file-sharing platforms, it is critical to ensure that your product can protect user-trust by ensuring a safe environment to communicate and collaborate. With email being the primary threat vector responsible for more than 90% of breaches, information about the latest outbreaks can be gathered by analyzing email traffic. By monitoring billions of emails daily and leveraging multiple detection techniques including intelligent signatures, advanced emulation, and heuristics, Cyren analyzes and correlates email-based threats with those found in web traffic and suspicious files allowing for comprehensive protection against new outbreaks.

Rapid Detection with/without Network Connectivity - Cyren's Malware Detection Engine offers best-of-breed detection
capabilities regardless of network connectivity and does not solely rely on cloud-based lookups to provide accurate detection. When installed in an offline environment, the customer can download the latest definitions (hourly or as needed) directly to ensure detection against the latest threats. Alternatively, when installed with network connectivity, our new Cloud Assist capability allows you to rapidly address new threats as they materialize.

Effective Detection of Packed/Obfuscated Files - Threat actors have often used packing or obfuscation to make their files difficult to detect and analyze. Cyren's advanced Malware Detection Engine can quickly breakdown a large file into it's smallest components and rapidly scan them individually for malicious artifacts. This allows it to detect packed/ obfuscated files like scripts inside a PDF, macros inside an office document, or a file within a zip file.

Features of Cyren's Malware Detection Engine

- **Multi-layered detection** - using heuristics, emulation, and signatures
- **Modular architecture** - fast reaction to new threat types
- **Fast clean file processing** - over 90% of files scanned by AV are clean, optimized to make fast decisions about clean files
- **Full support for all types of compression techniques including** ZIP, Bzip2, RAR, 7zip, NSIS and CAB compression techniques
- **Multi-platform** (Windows, Linux, UNIX, etc.)
- **Award-winning technology** - with certifications from Virus Bulletin

DATA443

4000 Sancar Way, Suite 400
Research Triangle, NC 27709

Website: www.data443.com
Email: info@data443.com

US: +1 919 526 1070
UK: +44 203 7693 700