

CYREN

CYREN AntiMalware SDK

OEM Cyber Intelligence



The Best Defense against Zero-Day Malware

Internet connectivity is now an essential element of many new technologies and cyber threats continue to evolve to explicitly target these new platforms. Designed to proactively combat these new threats and trusted by many of the largest technology brands in the world, the CYREN AntiMalware SDK is the best solution for hardware, software, and service providers needing a security solution that combines superior detection with maximum performance.

CYREN operates the world's largest threat intelligence network—GlobalView™—with 500,000 points of presence processing the traffic of over 600 million users in 200 countries, a global data collection and automated detection capability which delivers actionable malware intelligence globally on a nearly real-time basis. Our security cloud analyzes over 17 billion transactions per day across multiple security vectors to deliver an unmatched view of malware outbreaks as they emerge.

Superior Detection

- **Multi-layered detection**—using heuristics, emulation, and signatures
- **Modular architecture**—fast reaction to new threat types
- **Award-winning technology**—with certifications from Virus Bulletin
- **Secondary engine**—if you have conventional antivirus (AV), add CYREN AntiMalware SDK for a proactive approach to catching web and email malware

Maximum Performance

- **Fast clean file processing**—over 90% of files scanned by AV are clean, so our engine is optimized to make fast decisions about clean files
- **Low resource consumption**—low CPU and memory usage delivers deployments using only half the hardware of competitors
- **Small footprint**—our engine is <2MB, and definition files can be 35MB
- **Low bandwidth**—updates <2mb mean lower bandwidth requirements

Anti-malware for any platform

The CYREN AntiMalware SDK is an ideal foundation for a range of hardware and software security applications and offerings, including:

SecaaS vendors

- Messaging security services
- Web security services

Security appliance vendors

- Gateways, firewalls, UTMs
- Network Attached Storage

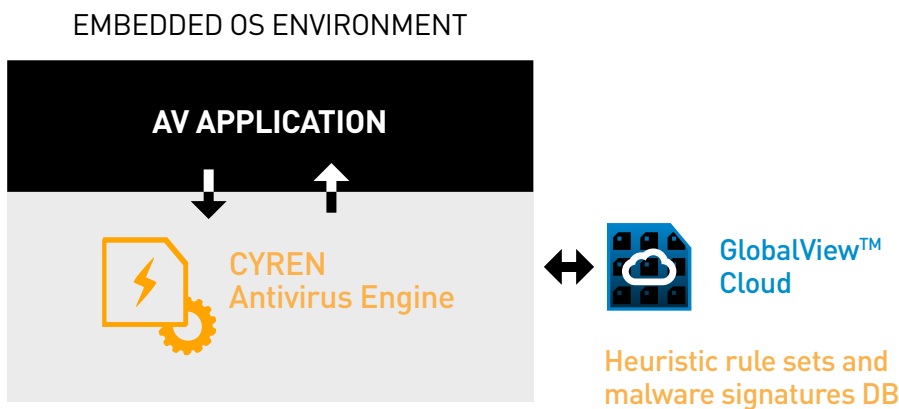
Internet of Things

- Embedded operating system devices



How it Works

The CYREN AntiMalware SDK engine uses a modular framework. Each Threat Protection Module within the framework scans specific objects (e.g., PDF files) or searches for specific virus types (e.g., polymorphic viruses). This architecture is more flexible than the monolithic engines of competitors—new modules can be added quickly to combat new threats without having to change existing ones—giving faster protection from evolving threats.



Fast Deployment

The modular architecture also means faster deployment for partners. Quality assurance testing of the engine is completed far more rapidly after module updates or additions since existing modules are left untouched. We use a minimal number of function calls for integration of the engine, speeding integration time. Also, new features are exposed by adding parameters without changing the basic function call set, ensuring backward compatibility and easier management of deployed products.

Your One-Stop Shop for Internet Security

- **Full Internet Security**—our Unified Engine provides AntiMalware, AntiSpam, URL Filtering, and Malware Attack Detection
- **Dual engine protection**—Virus Outbreak Detection enhances our AntiMalware by blocking email-borne malware threats without scanning

“CYREN detection technology enables industry-leading catch rates in our Forefront server security products. CYREN helps Microsoft deliver on its Business-Ready Security strategy to enable customers to manage risk and empower their people.”

- JOHN CHIRAPURATH, IDENTITY AND SECURITY GROUP, MICROSOFT



Specifications

- Full anti-malware SDK detects worms, Trojans, spyware, adware and other potentially unwanted application types
- Full support for all types of ZIP, Bzip2, RAR, 7zip, NSIS and CAB compression techniques
- Mature and optimized i386, x86_64 and ARM emulator
- 32-bit, 64-bit; little and big Endian
- Multi-platform (Windows, Linux, UNIX, etc.)
- Detailed threat feedback through simple API, including detection accuracy and type
- Native windows COM interfaces for easy integration with .NET or script interfaces
- Small definition file size
- Multi-core, multi-threading safe libraries
- Milter plugin for Sendmail or Postfix based servers

