CYREN

IP Reputation Service

Threat Intelligence (SDK)

CYREN CyberIntelligence

The challenge to keep unwanted network traffic outside the network perimeter is never-ending. Spammers and hackers continually evolve and change their methods to evade traditional perimeter security solutions.

Messaging security vendors can now achieve unprecedented performance and detection levels, blocking zombie traffic before it enters customer networks. Utilizing the world's most comprehensive email security network—Cyren's GlobalView™ Security Cloud—our embedded IP Reputation real-time analysis will:

- Identify hundreds of thousands of new zombies (compromised accounts and host computers) everyday
- Continuously track traffic from tens of millions of IP addresses
- Accurately classify billions of email messages per week in real-time

A Global View Of Reputation

Cyren's GlobalView Security Cloud compiles both historical and up-to-the-minute sender reputation data from highly diverse traffic sources in every country, with coverage from managed services and network hardware devices to desktop software. Our patented Recurrent Pattern Detection™ technology automatically aggregates
this high-level view of all senders, distinguishing in real time between legitimate corporate senders, valid publishers, zombies, and spammers/malware distributors.

The Scale Of The 'Zombie' Problem

The following illustrates the scale and scope of the challenge posed by compromised (zombie) host computers:

- Zombies send 85% of all spam, an estimated 120 billion messages a day
- Around 200,000-500,000 zombies 'come alive' everyday
- A typical zombie botnet sends up to 1 billion messages in a few hours
- There are typically 10,000–200,000 zombies in a single botnet
- 5–10 million zombies are active on any given day

Why Use Cyren's IP Reputation Service?

- Quickly and easily expand your messaging security solution breadth and value
- Maintain customer loyalty by improving service levels
- Improve sales margins by adding solution value
- Reduce your customers' operational overhead and enable higher throughput for their systems

> "Every enterprise and service provider should seriously consider incorporating a reputation service as part of its spam and virus control strategy. Cyren's combination of global monitoring and real time analysis offers a competitive edge to its licensees."

- RICHI JENNINGS, FERRIS RESEARCH

Google Microsoft Check Point SOFTWARE TECHNOLOGIES LTD. DELL Deutsche Telekom

CYREN

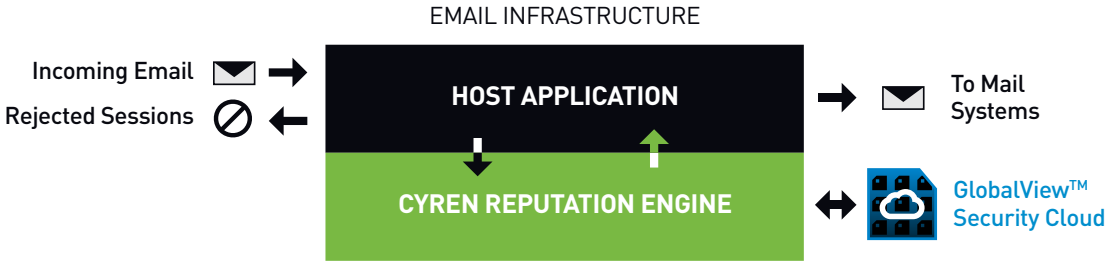
IP REPUTATION SERVICE

Threat Intelligence (SDK)

CYREN CyberIntelligence

How It Works

A partner device identifies an incoming SMTP connection request. The device then queries IP Reputation for information about the sending IP address. Based on the results from the GlobalView Security Cloud, the connection is accepted, tempfailed, perm-failed, or throttled.



Capabilities

- Real-time botnet detection—under a minute from start of attack
- High accuracy assessment based on Cyren's GlobalView Security Cloud: - 80+ vendor networks, spanning 180 countries
  - Sources: firewalls, messaging appliances, desktop software, xSPs
- Aggregate attributes: DNS info, geography, dynamic IPs, public RBLs, etc.
- Decision Manager increases zombie protection, minimizes False Positives:
  - Dynamic time windows for temp—failing and accepting connections
  - Built-in rate limiting
- Rich data set provided per IP, including:
  - Recommended action: block, throttle, allow
  - IP class—classifies IP into actionable classes
  - IP Risk level—Likelihood of message being unwanted: 0–100
  - Volume and volume spikes
  - Spam ratio and spam ratio spikes
  - Valid bulk data (e.g. newsletters)

Specifications

- Supports standard Mail Transfer Agent (MTA) platforms
- Designed for high-scalability—over 4000 messages/second
- Multiple deployment options: local daemon for built-in caching and failover (Linux, FreeBSD, Solaris and Windows)
- HTTP, UDP, and RBL/RBL+ interfaces available
- Cloud access via UDP—no software installation required

Benefits For Your Customers

- **Lower Resources**—Reduced second-tier resource requirements, e.g. hardware, network,
- **Save Bandwidth, Enhance Performance**—By blocking >85% of unwanted traffic at the perimeter, bandwidth and resource use is substantially reduced, improving the Quality of Service for remaining traffic
- **Increase Security**—Filtering the majority of email-borne viruses, worms and trojans before they enter the network, increases overall security
- **Eliminate False Positives**—Using rate-limits and temporary rejects, a measured response virtually eliminates false positives
- **Improve Detection**—Overall detection rate is improved

www.cyren.com/**contact**

sales@cyren.com