# Axigen Antivirus & Antispam

## Real-time Email Protection with Premium Content Filtering

powered by

CYREN

# PREMIUM CONTENT FILTERING

When it comes to security, we put tremendous attention into making sure our customers benefit from the best tools. Therefore we've added the CYREN AntiVirus & AntiSpam premium security layer in our security solutions portfolio.

## WHY CYREN?

**Cyren's Expertise** in building efficient, mass-scale security services mitigate Internet threats for thousands of organizations and hundreds of millions of users in 190 countries.

**Cyren's RPD Technology,** a unique, patented technology that differentiate the Pattern Detection approach in the security industry.

**Cyren Global protection platform,** Cyren's service is powered by the GlobalView™ Cloud, the largest global security platform of its type.

**Cyren's Engine Flexibility** designed for high throughput but is also flexible allowing integration into the thinnest hardware platforms, as well as large-scale carrier-grade deployments.

**Cyren Recognition** Providing Internet security technology to more than 150 security companies and service providers, protecting over 550 million users.

### RECURRENT PATTERN DETECTION (RPD™) TECHNOLOGY

CYREN has developed a unique and highly successful response to email security challenges with its RPD™ technology, which focuses on detecting recurrent message patterns in outbreaks, rather than on a lexical analysis of the contents of individual email messages.

The aim of RPD™ is to identify and classify all types of email-borne threats and outbreaks. It is content-agnostic and can therefore detect spam and phishing in any language, format, or encoding method, while identifying patterns of new email-borne viruses and worms for which signatures have not been made.

### REAL-TIME. BECAUSE NOTHING ELSE IS GOOD ENOUGH.

Most attacks last a few hours. In order to be truly efficient, the solution has to work real-time to detect and block outbreaks proactively. Otherwise the intervention will be made late in the attack event when most of the damage has already been done.

Typically, within the first minutes of the release, CYREN has already proactively identified the outbreak and is able to classify and instruct the host application to block any messages from the outbreak before they reach recipients.

## HOW IS CYREN UNIQUE?

### REAL-TIME DETECTION AND BLOCKING

Because most attacks last only a few hours and involve the release of tens of millions of emails containing malicious content or spam.

If the solution does not work in real-time to detect and block outbreaks proactively, it will simply be reacting towards the end of the attack, when most of the damage has already been done.

### LANGUAGE AND CONTENT AGNOSTIC

Because damaging threats are often found in emails that do not contain English characters or messages that use images rather than text.

Solutions that focus on the content of a message are likely to miss these threats, decreasing their overall effectiveness and increasing instances of false negatives received by recipients.

### ADAPTIVE TO NEW METHODS AND TRICKS

Because malicious hackers and sophisticated spammers change their tactics of distribution and infiltration constantly in order to fool and evade current technologies.

CYREN's cloud based technology makes it easy to continuously adapt the detection and blocking technologies to the newest threats and spam methods.

## HOW IT WORKS

CYREN

# Threat Detection and Blocking

**1** A new massive attack is launched over the Internet. Within minutes, RPD has identified the threat pattern and forwarded it to the CYREN Datacenter, which classifies and stores the recurrent message patterns of the attack in a vast repository of message patterns.

**2** New incoming messages arriving in the Axigen mail relay or front-end mail server are analyzed.

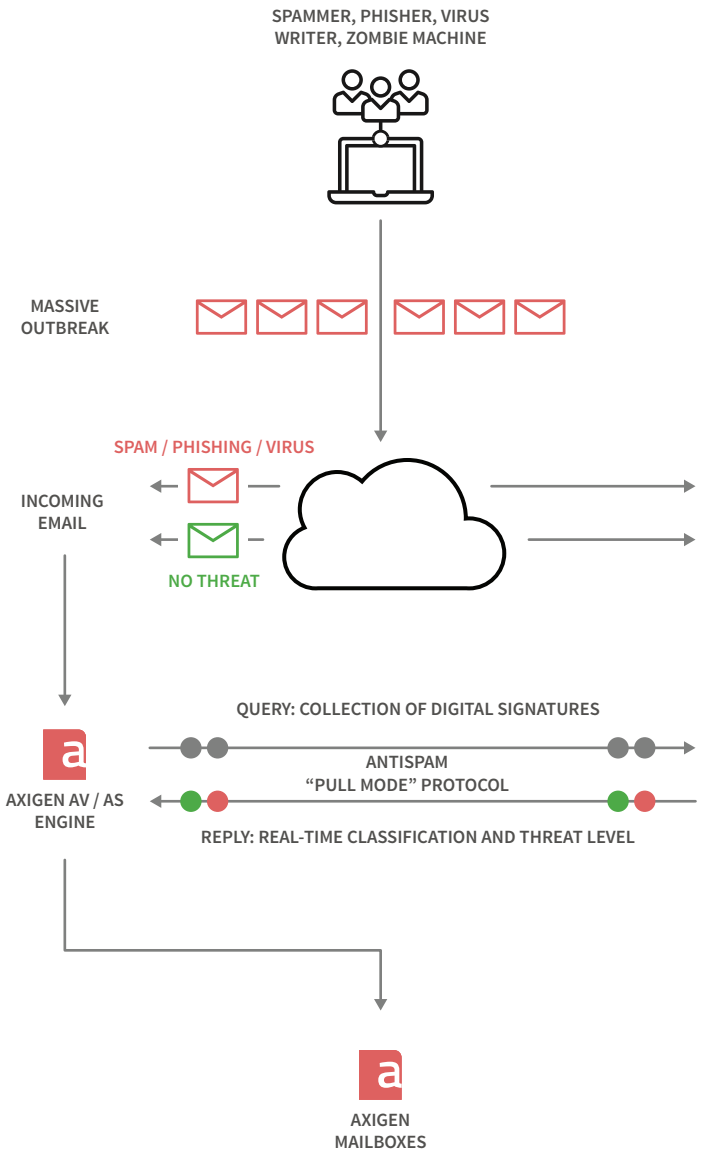
**3** Message patterns are then checked against Axigen policy and user rules (optional).

**4** A query containing a collection of digital signatures representing only patterns of the message is sent to the CYREN Datacenter.

**5** Within a few milliseconds, the CYREN Datacenter classifies the message patterns and sends a reply to Axigen. The size of the query is about 500 bytes and the total round-trip time is ~300 ms, excluding Internet latency.

**6** Axigen applies predefined, customizable blocking policies (delete, quarantine, or send to user's personal quarantine or Inbox folder, etc.).

**7** Axigen stores the information in a local detection cache, making future local classification even more efficient and especially effective if the communication with the CYREN Datacenter is temporarily unavailable while new messages continue to flow into the organization from other routes.




RECURRENT PATTERN DETECTION (RPD™)

DETECTION SERVICE CENTER

REDUNDANT CENTER

**TIP**

Because the CYREN approach does not focus on contents analysis, it is completely irrelevant whether malicious hackers vary the contents of the message, use non-English characters, images, single or double byte encoding, etc. Even when virus authors release multiple instances of the same virus within an attack, CYREN is able to track and block all variations.

axigen

# The Antivirus & Antispam

# SUPERSTRUCTURE

## ANTI-IMPERSONATION

- SPF
- DKIM

## DNS BLACKLISTS

- **DNSBL**
  IP BLACKLISTS
- **DBL**
  DOMAIN BLACKLISTS
  COMING SOON

## CONTENT FILTERING

- **KASPERSKY**
  ANTIVIRUS & ANTISPAM
- **CYREN**
  ANTIVIRUS & ANTISPAM

## THE TOOLBOX

- GREYLISTING
- COUNTRY FILTERING
- ATTACHMENT FILTERING
- IDENTITY CONFIRMATION
- BLACKLISTS
- WHITELISTS
- ACCEPTANCE POLICIES
- ...