

# CYREN

## CYREN ctasd product description

---

*Version 5.00, 13 December 2015*

© 2015 CYREN Inc.

All rights reserved

## Trademark and Copyright Statement

CTT20-800-112-088-R2

© CYREN Inc. 2015 All rights reserved.

The information contained in this document is subject to change without notice. CYREN makes no warranty of any kind. CYREN will not be liable for any direct, indirect, incidental, consequential or other damage alleged in connection with the furnishing or use of this information. Except as allowed by copyright laws or herein, reproduction, adaptation or translation without prior written permission is prohibited. RPD™, ctasd™, and ctengine™ are trademarks of CYREN Inc. All other trade/service marks or names that may be referenced and/or mentioned in this document belong to their respective owners. Microsoft is a trademark and/or registered trademark of Microsoft Corp. Linux is a trademark of Linus Torvalds. Red Hat is a trademark of Red Hat, Inc. in the United States and other countries. Debian is a registered trademark of Software in the Public Interest, Inc.

**COPYRIGHT AND PERMISSION NOTICE** Copyright (c) 1996 - 2015, Daniel Stenberg, <daniel@haxx.se>. All rights reserved. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

## Contacts

Any technical questions you or your developers have about using the ctasd should be addressed to [support@cyren.com](mailto:support@cyren.com).

## About CYREN

CYREN™ provides proven Internet security technology to more than 150 security companies and service providers including 1&1, Check Point, F-Secure, Google, Microsoft, Panda Security, Rackspace, US Internet, and WatchGuard, for integration into their solutions. CYREN's GlobalView™ and patented Recurrent Pattern Detection™ (RPD™) technologies are founded on a unique cloud-based approach, and protect effectively in all languages and formats. CYREN Antivirus utilizes a multi-layered approach to provide award winning malware detection and industry-leading performance.

CYREN technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, enabling our partners to protect end-users from spam and malware, and ensure safe, compliant browsing. The company'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, formerly known as Commtouch, was founded in 1991, is headquartered in the US in McLean, Virginia, with offices in Palo Alto, California, Herzliya, Israel, Berlin, Germany, and Reykjavik, Iceland.

For more information about enhancing security offerings with CYREN technology, visit our website at [www.cyren.com](http://www.cyren.com), see our blog at <http://blog.cyren.com> or write to [info@cyren.com](mailto:info@cyren.com).

## ctasd™ Product Description

CYREN Advanced Security Daemon (a.k.a. ctasd™) is a plug-n-play email-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. The daemon adds a layer of email filtering to your mail delivery system in order to provide real-time classification, already in the first minutes after a new outbreak is launched.

ctasd is a cross-platform detection engine for integration with third-party applications using a simple-to-implement communication protocol that offers the most accurate threat detection available. It was designed to minimize the exposure of users to the high magnitude of email-borne threats and to deliver nearly 100% protection against massive spam and virus attacks.

When analyzing new email messages, ctasd uses CYREN's classification methodology, known as the Recurrent Pattern Detection (RPD™) technology to identify threat patterns in real-time as they are released to the Internet within an outbreak. ctasd can be used to offer incoming email protection that enables CYREN OEM and ISP partners to prevent their customers or users from receiving spam. It can also be used to enable service providers the ability to detect and block outbound spam messages, thereby protecting their business reputation and avoid being blacklisted by other servers.

Typically, CYREN partners are vendors and integrators of messaging and messaging security appliances, Service Providers, developers of anti-virus programs, firewalls, routers, modems, mail servers, security gateways, desktop applications, etc. who wish to offer inbound email-borne threat detection services in their product or enhance their already-existing anti-spam or anti-virus capabilities. Other partners use CYREN's Outbound Spam Protection to ensure that no one is abusing their infrastructure to send spam and/or viruses out to unsuspecting recipients, thereby damaging the reputation of the partner's services.

When ctasd is integrated into a service provider environment to detect outbound spam, CYREN Outbound Spam Protection monitors outbound traffic by listening to the service provider's traffic. Using CYREN's patented RPD technology, adjusted for the specific requirements of outbound spam, the solution is able to determine in realtime if an email message is spam and/or a virus and to identify the origin of its sender.

## Anti-Spam Solutions

While most current anti-spam solutions rely on a form of lexical analysis, ctasd offers detection services that are content-agnostic and therefore able to detect spam in all languages, message formats and encoding (singlebyte and double-byte), even in messages containing only images.

When ctasd's Anti-Spam service is integrated with a third-party messaging application to handle incoming messages, ctasd analyzes messages that are passed to it and returns accurate spam classifications to the querying application to apply an action (such as release to the recipients, delete the message at the entry point before it drains further corporate resources, quarantine for second opinion or delayed decision, etc.).

CYREN has developed two engines to provide the highest levels of detection and protection:

- RPD Engine – proven Recurrent Pattern Detection engine
- LocalView Engine – score-based engine enhancing RPD detection.

### RPD Engine

The RPD engine is responsible for identifying message patterns in spam attacks as they emerge on the Internet. Any message containing one or more of these unique patterns can be assumed with a great deal of certainty to be part of the same mass-mailing and the CYREN Recurrent Pattern Detection distinguishes solicited from unsolicited bulk emails patterns.

### LocalView Engine

CYREN LocalView Engine was designed as an additional engine supporting CYREN's efforts to provide solutions for identifying and neutralizing malware and threats in the areas of email messages. The LocalView engine was designed to further enhance CYREN's patented Recurrent Pattern Detection technology.

For those customers who have already adopted a dual-engine, anti-spam strategy, CYREN's LocalView offers an ideal solution as the second, SpamAssassin-like engine. Like SpamAssassin, an open source project by the Apache Software Foundation, LocalView works using similar terminology and rule-based scoring.

### Virus Outbreak Detection

In the case of email-borne malware outbreaks or new instances of already-known viruses, ctasd delivers Zero- Hour Virus Protection services detecting if and when new unknown viruses and worms have

infiltrated through the defenses of existing signature-based or heuristics/sandboxing-based anti-virus scanner. CYREN's Zero-Hour Virus Protection service protects enterprises and end-users during the first critical hours of the outbreak before new signatures or heuristics rules have been prepared and distributed by the anti-virus vendors to their customers.

## Command Antivirus Protection

ctasd also offers virus detection via its Command Antivirus capabilities. When enabled, ctasd's antivirus protection offers superior, efficient detection with a small footprint. It is appropriate for integration into a wide variety of products or services and is configured to block malware of all types, including worms, Trojans and spyware. The Antivirus Protection service can be used to scan objects including email messages, individual files or entire folder locations.

When Command Antivirus functionality is enabled and integrated, each query sent by the querying device to the CYREN Datacenter (by ctasd) will result in an additional classification in the response. For instances in which a virus is detected, the response will include the virus type, accuracy, virus name and scan result. An important element of the antivirus solution is the creation and maintenance of definition files that contain information about known viruses. ctasd downloads updated definition files on a predetermined schedule. These definition files enable CYREN to provide the most up-to-date, effective antivirus protection available.

Command Antivirus uses heuristic rules or signatures to identify malware email attachments as well as files stored on PC or network drives and can return detailed information about the type of threat, the virus name, and more.

## CYREN Inbound and Outbound Services

ctasd can be integrated to deliver one or more of the following services:

---

**Note:** *Separate license keys are required for enabling Inbound and Outbound services.*

---

### Inbound

- Inbound Spam Detection
- Inbound Virus Outbreak Detection
- Inbound Command Virus Protection

### Outbound

- Outbound Spam Protection
- Outbound Virus Outbreak Detection
- Outbound Command Virus Protection

## Licensing Options

A single ctasd daemon can provide single or multiple Inbound Services without affecting performance and accuracy. However, another ctasd daemon is required to provide single or multiple Outbound services (and vice versa). Once provisioned, the CYREN partner may choose to disable one or more services locally for testing purposes and then enable the service or services for actual production use.

## ctasd Benefits

ctasd was designed to integrate easily to offer immediate benefits, including the following:

- **Minimal integration time:** enabling you to integrate and instantaneously begin benefiting from ctasd's email-borne threat protection. ctasd already embeds the CYREN ctEngine™ (detection engine), which means that you are not required to apply a long series of API calls to initiate communication between your client application and an embedded detection engine. Instead, you will only need to implement a small script that either streams the messages or points to their location on your network for filtering. This also enables your application to interface in any language (for example, C, C++, Perl, etc.). Additionally, because ctasd was completely developed and tested to work with CYREN's detection engine, your resources for testing this module after integration is spared and thus shortening the time-to-market.
- **Platform independency:** ctasd includes all the system dependencies required to run on all popular platforms such as Linux, Solaris, FreeBSD and Windows in a separate `chroot` environment. This means that ctasd is generic for each platform and can be used for all versions of the same platform.
- **Robustness:** ctasd is implemented out-of-process, meaning that if you are currently calling (or plan to call) other 3<sup>rd</sup>-party applications, there should not be any conflicts with the embedded detection engine by CYREN. ctasd continues to maintain communication, even if one of these other processes goes down. ctasd's ability to maintain communication and continue to function and deliver classifications means that it will deliver better and faster diagnostics of reported problems because it offers an independent client environment, isolated from other interferences that might negatively impact on performance or functionality. Uptime of the solution is also improved because CYREN's ctasd includes a self-monitoring mechanism to detect and report problems in communication or functionality.
- **Usage:** ctasd allows implementation as a separate process or on separate machines serving multiple clients. This flexibility in deployment can improve usability and performance.
- **Commitment** to support and development: CYREN has an aggressive support and development process, committing to develop new versions and functionality for its Service Provider and OEM partners on an ongoing basis. Each new ctasd build includes all updates and changes, thus enabling CYREN's partners to easily integrate updated versions and re-integrate smoothly. Once you integrate an auto-upgrade procedure, newer ctasd builds can be integrated seamlessly and transparently.

## ctasd Solution Components

The ctasd solution involves the following components:

- CYREN Datacenter
- ctasd daemon
- ctasd protocol
- Querying devices

### **CYREN Datacenter**

The CYREN Datacenter monitors global email traffic in real-time (24\*7\*365) from various sources on an ongoing basis and maintains a vast database of classifications that are determined based on numerous dynamically changing parameters.

### **ctasd**

The CYREN Advanced Security daemon (ctasd) performs various functions, from receiving and processing incoming queries from query devices, to determining the Spam and/or virus outbreak detection classifications of incoming messages and quickly responding to the querying device with details on several key data types.

### **ctasd Protocol**

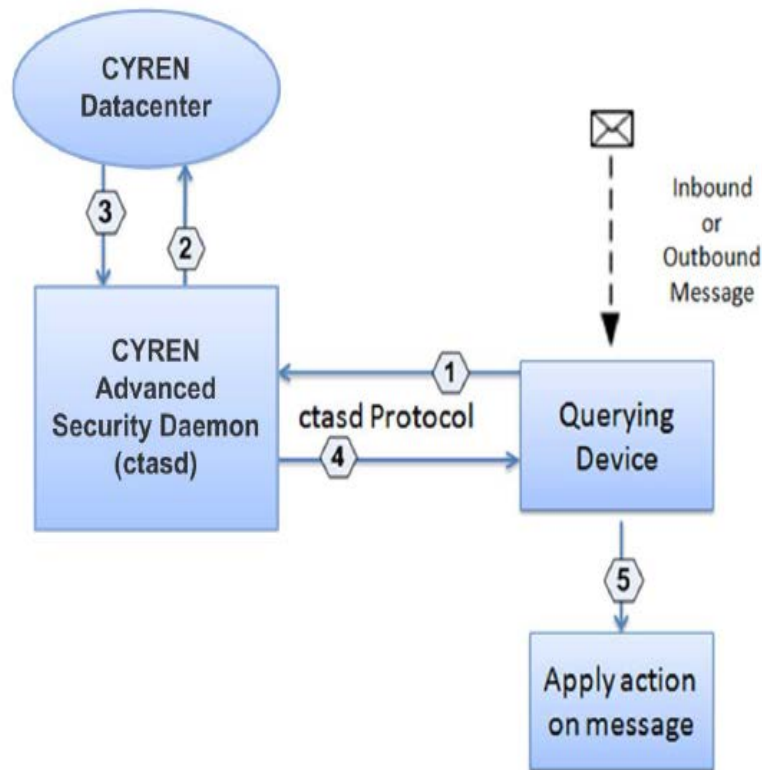
In order to enable communication between a querying device and ctasd, CYREN has developed a simple protocol for its OEM and Service Provider partners. This enables CYREN partners to provide advanced anti-spam and virus outbreak detection services to their users. Communication between the ctasd and the querying device is accomplished over HTTP. The ctasd protocol for all ctasd services is documented in the *CYREN Anti-SpamDaemon (ctasd) Integration Manuals* (separate documents for inbound and outbound).

### **Querying Device**

For the purposes of this document, the term “querying device” is used as a generic term for OEM/Service Provider applications or MTA mail filter plug-ins (e.g. Postfix Milter plug-in) responsible for email filtering. These applications are integrated with ctasd to provide anti-spam and virus outbreak detection by sending queries to ctasd over HTTP. Once a response is received from ctasd, the querying device is responsible for applying connection management decision and flow control actions based on ctasd’s response.

## System Architecture and Data Flow

Although the data flow of ctasd can vary depending on configuration settings and deployment scenarios, a typical data flow is detailed below:



### Typical ctasd data flow:

1. An inbound or outbound message is received by the querying device. In an Outbound message, the SenderID is included in the message. The querying device uses the CYREN ctasd protocol to generate a query to ctasd requesting spam and virus outbreak classifications.
2. ctasd prepares and forwards a query to a CYREN Datacenter to retrieve the most up-to-date information based on known message patterns.
3. The CYREN Datacenter responds to ctasd with current information regarding the message patterns in the query.
4. ctasd then prepares a response, collating all current information into a pre-determined format and sends the response back to the querying device. In an Outbound implementation, SenderID counter values and alerts are included in the response message.
5. The querying device, upon receiving the response from ctasd, may apply a predefined action to the message (i.e., for inbound messages: reject the message, approve the message and pass it to the recipient, etc.). For Outbound implementations: a predefined action may be applied based on the sender (i.e. Sender ID lockout, placing Sender ID behind a walled garden, sending the Sender ID a warning message etc.).

ctasd automatically stores spam classifications received in responses from the CYREN Datacenter to a local cache to optimize the detection and classification process.



ctasd analyzes message patterns against this local cache as the first step in spam detection and filtering. If a match is found based on previous queries, a similar classification is assigned and the querying device can then apply an appropriate action without sending a new query. If no match is found, ctasd will then prepare and send a query to the CYREN Datacenter. The local cache is updated regularly each time a response is received from the Datacenter and older or expired classifications are deleted.

In addition to the local cache, ctasd maintains a persistent cache, which is automatically reloaded when ctasd is stopped and restarted. This helps improve overall response time because it restores the local cache with the most up-to-date classifications, as well as previously stored classifications that are still relevant.

## ctasd Deployment Options

ctasd can integrate with a wide variety of applications and devices to enable spam, Zero-Hour Virus Protection detection services, and/or Command Antivirus Protection. Each deployment option is adaptable to the individual requirements and infrastructure of the CYREN OEM partner and its customers or the environment of the Service Provider.

Following is a partial list of some of the ways in which ctasd can be deployed:

- A single ctasd standalone daemon (running on either a dedicated box or one of the existing machines within the organization) can be used to serve one or more querying devices simultaneously.
- Multiple ctasd daemons running on multiple machines can serve one or more querying devices.
- One or more ctasd daemons can run on the same machine.
- ctasd may also run as a fully-embedded daemon that is tightly integrated with the OEM partner's solution.

---

**Note:** When providing both Inbound and Outbound Mail Flows, separate license keys are required for each.

---

ctasd can be deployed on the customer's premises, thus requiring no authentication between ctasd and the querying devices. Nonetheless, ctasd will require authentication of communication between ctasd and the CYREN Datacenter. Alternatively, ctasd can be deployed over WAN and remotely from the querying devices.

## ctasd Protocol

The querying device is developed and implemented by the OEM partner or Service Provider according to the published ctasd protocol in the *ctasd Integration Manuals (one for inbound services and one for outbound)*.

ctasd is integrated with the host product and customer's messaging network according to one or more of the scenarios detailed in [ctasd Deployment Options](#).

The querying device receives messages from the messaging network and for each message it generates and posts a request to ctasd to classify the message.

Communication between the querying device and ctasd is made over HTTP. CYREN uses and requires standardrfc822 headers structure. The querying device connects to a TCP port on the ctasd daemon as defined in ctasd.conf and sends one of several types of requests. These include:

- A query which points to a specific file from a specified location. This instructs ctasd to access the file and determine whether it represents an email-borne threat such as spam or a virus.
- A query which includes streaming message data for ctasd to analyze.
- A query reporting either a false negative or a false positive in a previous classification, thus enabling ctasd to further improve its performance and detection rate.

ctasd also supports a SpamAssassin-compatible protocol, referred to as Spamd. The Spamd protocol should be used when a Mail Server has built-in integration to SpamAssassin. In these cases, it may be easier to integrate with ctasd using the spamd protocol, which is compatible for use with the Exim Mail Server.

## ctasd Reports and Logging

ctasd features many SNMP counters that monitor its performance and activities. The counters report on a variety of values, for example:

- The length of the current session.
- The total number of ClassifyMessage queries.
- The number of ClassifyMessage queries currently being processed by ctasd..
- For each spam or virus classification, the total number of messages classified to date for either inbound or outbound services per license key.

A list of these counters can be found in the ctasd Integration Manuals (one for inbound spam/virus detection and one for outbound spam/virus protection).

## ctasd Minimum Requirements

The ctasd package includes all its necessary system dependencies and can therefore be run on any Windows, Solaris, Linux or FreeBSD platform. Make sure you install the specific ctasd package that was compiled for your platform.

Following is a list of recommended hardware requirements:

- Single CPU, 2.8 GHz
- 1 GB RAM
- 80 MB free disk space
- 100 Mbps Network interface

## ctasd Package

The ctasd package contains the following:

- ctasd daemon and associated binary
- ctasd documentation
- Sample files for quick evaluation and testing
- SNMP script for counters
- Operating system binaries for compatibility with multiple platforms

## Supported Platforms

ctasd is compiled for the following platforms:

- Windows 32 Bit
- Linux
- FreeBSD
- Solaris 9/10 32bit over SPARC
- Solaris 9/10 32bit over x86

## CYREN RPD™ Technology

CYREN ctasd is powered by CYREN's renowned Recurrent Pattern Detection (RPD) technology. RPD is a patented technology which identifies massive outbreaks in the first instances that they are released to the Internet.

Massive outbreaks which distribute spam, phishing, and email-borne viruses or worms, consist of many millions of messages intentionally composed differently in order to evade commonly-used filters. Nonetheless, all messages within the same outbreak share at least one and often more than one unique, identifiable value which can be used to identify messages connected with this outbreak. By identifying these distinguishing values, also known as message patterns, CYREN's technology is able to identify whether a message should be classified as spam, suspected spam, non-spam, etc.

The objective of spam is often to lead the recipient to the same commercial websites. Different spam attacks are often launched from the same network of zombie machines that can be suspected or blacklisted by their unusual monitored behavior. In the case of phishing, the goal is to lure the recipient to voluntarily disclose personal and confidential information via clever social engineering methods. As with spam, the objective is often to lead the victims to some faked URLs. Each email-borne virus can be classified because no matter what message contents or source, it always contains the same malicious code (otherwise, it is a different virus or amutation of the same virus). These factors produce recurring values of typical outbreaks. Any message containing one or more of these unique patterns can be assumed with a great deal of certainty to be part of the same outbreak.

The identification of one message pattern may often lead to incriminating an entire series of other message patterns discovered in other outbreaks. For example, an unknown IP address of a machine that started sending out confirmed-spam messages in a consistent and quantifiable method can be classified as a new zombie, while the messages are classified to be spam based on different message patterns.

Message patterns are extracted from the message envelope during the SMTP session and from the message headers and body with no reference to the lexical meaning of the content. Thus pattern analysis can be used to identify outbreaks in any language, message format, and encoding type. Message patterns can be divided into:

- Distribution patterns, which determine if the message is "good" or "bad" by analyzing the way it is distributed to the recipients.
- Structure patterns, which determine the volume of the distribution.

Pattern matching and detection represents a new and greater understanding of how email-borne threats are created and propagated. Because tactics for distributing spam, phishing, and email-borne viruses and worms are constantly evolving, it is necessary to proactively identify new and unique patterns in real-time to determine new outbreaks as they are released to the Internet and begin targeting recipients.

RPD, a technology based on CYREN's patent #6,330,590, extracts and then analyzes relevant message patterns, which are used to identify massive email-borne outbreaks and suspected sources of spam and malicious code.

The analysis results are stored in a vast warehouse of classifications of each message pattern and replicated to several CYREN Datacenters deployed worldwide. Therefore, RPD is not only used to identify new patterns, it is also used to reconfirm and enhance the classification of already-identified message patterns and source IP(s) on an ongoing basis.

RPD is designed to distinguish between the distributions of solicited bulk emails which represent legitimate business correspondence from those of unsolicited bulk emails by applying a reverse analysis. The results of this analysis are 'bleached' message patterns belonging to "good" messages and source IP(s) such as popular newsletters, mailing lists, etc.

CYREN uses the RPD technology in a highly scalable environment to deliver extremely high performance and detection rates by analyzing many millions of new patterns each day (24x7x365). On average, new outbreaks

## Contacts

Any technical questions you or your developers have about using the ctwsd should be addressed to [support@cyren.com](mailto:support@cyren.com).