



PANDA CLOUD INTERNET PROTECTION

Simply... Evolution

WHAT IS PEER - TO - PEER (P2P)?



PANDA CLOUD
OFFICE PROTECTION



PANDA CLOUD
EMAIL PROTECTION



PANDA CLOUD
INTERNET PROTECTION





INDICE	1
What is P2P?	2
P2P THREATS	3
DATA LEAKAGE	3
COPYRIGHT INFRINGEMENT	3
RESOURCE CONSUMPTION.....	3
ACCESS CONTROL ENFORCEMENT	3
DATA RETENTION.....	3
MALWARE	3
TIME INEFFECTIVENESS.....	3
LA SOLUCIÓN PANDA CLOUD INTERNET PROTECTION (PCIP)	3
GNUTELLA / GNUTELLA2.....	3
BITTORRENT.....	3
PANDO	3
EDONKEY	3
TOR / HTTP TUNNEL.....	3
SKYPE	3
GOOGLE TALK DESKTOP CLIENT	3
GIZMO	3
SUITE PANDA CLOUD PROTECTION	4



WHAT IS P2P?

Peer to peer (P2P) technologies denote a type of application communication architecture that allows individuals to communicate and share data with other individuals without necessarily needing a central server to facilitate the communication. It is important to note that “P2P” refers to a type of application architecture and not specific end application functionality; i.e. P2P is a technical means to a some greater end. However, “P2P” is often used synonymously to mean “file sharing”, as that is one very popular use of P2P technology.

There are other application purposes beyond file sharing that leverage P2P—for example, Skype uses hybrid P2P architecture to provide VoIP services and Tor uses a P2P architecture to provide anonymous network routing functionality. The primary advantage of a P2P approach is that it le

verages the resources (e.g. bandwidth, storage, etc.) of the many clients/peers to provide the overall application and network services rather than relying on the resources of one or more central servers—thus preventing those central servers from becoming a bottleneck for the entire network.

A secondary advantage of a P2P approach is that there is no single central authority that can be blocked or removed and cause the collapse of the whole P2P network; this provides a certain “self-surviving” and robustness quality that may be desired for various reasons.



Figure 1 – Traditional client/server network

(<http://en.wikipedia.org/wiki/Peer-to-peer>)



Figure 2 - P2P network

(<http://en.wikipedia.org/wiki/Peer-to-peer>)



P2P THREATS

P2P applications in use within an enterprise network can pose many threats and concerns:

- **Data leakage:**
Corporate information or files are knowingly or unknowingly being uploaded.
- **Copyright infringement**
Users are downloading illegal / copyrighted content.
- **Resource consumption:**
Excessive bandwidth consumption, including potential extra bandwidth consumed while servicing other peers not related to direct user use.
- **Access control enforcement:**
The decentralized nature of P2P technologies make it difficult to utilize traditional network access control mechanisms to block usage.
- **Data retention:**
Properly logging and auditing P2P communication data can be difficult to impossible.
- **Malware:**
virus, Trojans, or other malware could potentially be downloaded by the user.
- **Time ineffectiveness:**
Time spent using P2P applications is time not spent working

THE PANDA CLOUD INTERNET PROTECTION (PCIP) SOLUTION

The PCIP solution can identify various popular P2P applications. Once identified, a location's policy can dictate whether specific P2P traffic types are allowed, blocked, or throttled by a bandwidth limitation. As of Q3/2010, the PCIP solution offers support for the following P2P applications:

- **Gnutella/Gnutella2:**
File sharing networks used by the popular Limewire and BearShare clients.
- **BitTorrent:**
File sharing method that relies on certain web sites (called "trackers") to index all peers that have pieces of a certain file; there are many popular BitTorrent clients available on the Internet.
- **Pando:**
A single-vendor commercial and proprietary derivative of BitTorrent that is friendlier to use over HTTP.
- **eDonkey:**
File sharing network used by the popular eMule client.
- **Tor / HTTP Tunnel:**
An anonymous routing network used to hide where a user is coming from and where they are going to.
- **Skype:**
A single-vendor commercial and proprietary VoIP network.
- **Google Talk Desktop Client:**
Voice over IP protocols and applications.
- **Gizmo:**
Voice over IP protocols and applications.



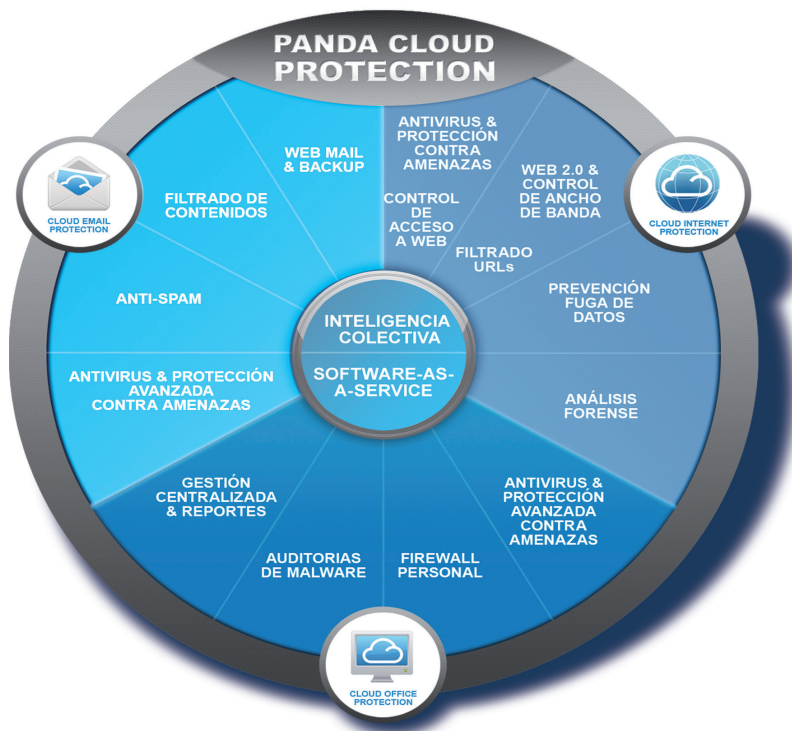
PANDA CLOUD PROTECTION SUITE

Panda Cloud Internet Protection is part of the Panda Cloud Protection suite which is a complete SaaS security solution that protects all the main threat entry points: endpoint, email and Web traffic, against malware, spam, phishing, cross-site scripting and other advanced Web 2.0 attacks, through a light, secure and simple solution.

As the security suite is based in the cloud it offers maximum protection, while optimizing costs and productivity. Startup is immediate and the solution is simple to manage through an intuitive Web console.

The Panda Cloud Protection suite harnesses the power of Collective Intelligence. Panda's cloud-based Collective Intelligence leverages 21 terabytes of knowledge and experience drawn directly from millions of users to deliver comprehensive, instantaneous, non-intrusive real-world protection against known and unknown malware to all users.

Panda Cloud Protection leverages the power of the cloud to not only provide up-to-the-minute protection against known and unknown threats but also to streamline the delivery of that protection through the anytime, anywhere power of the Cloud Management Console.



PANDA SECURITY

EUROPE

Ronda de Poniente, 17
28760 Tres Cantos. Madrid. SPAIN

Phone: +34 91 806 37 00

USA

230 N. Maryland, Suite 303
P.O. Box 10578. Glendale, CA 91209 - USA

Phone: +1 (818) 5436 901

www.pandasecurity.com

© Panda Security 2010. All rights reserved. 0810-WP-Outdated Browsers

PANDA
SECURITY