



CyberDefender Argus network

Last Modified on: August 24th, 2010



CyberDefender Corporation

617 West 7th Street, Los Angeles, CA 90017

www.CyberDefender.com | Phone: (213) 689-8631

The purpose of this document is to provide an introduction and key differentiators of the patent pending CyberDefender Argus network.

Proprietary and Confidential: This document is proprietary and confidential information of CyberDefender Corp., and is covered by copyright and trade secret protection. Unauthorized adaptation, distribution, use, or display is prohibited and may be subject to civil and criminal penalties. Disclosure to others is prohibited.

Contents

1	Overview	3
2	Background	3
3	The security challenge.....	3
4	Our solution	4
5	Argus network Work Flow	7
6	Improvements in Argus network	8
7	Cost benefit of using the Argus network.....	8
8	Summary.....	9
9	CyberDefender anti malware network on cloud platform patent application...9	

CyberDefender Argus network–Collaborative Internet Security Network Version 3.0

1 Overview

CyberDefender Corporation has implemented Version 3.0 of its ^patent pending Argus network platform powered by the Secure-Peer Network (SPN) technology and the Threat Protection Network (TPN) technology, cloud computing, and conventional computing practices. The Argus network has already been used by seven million users. The TPN technology automates the primary data exchange and management mechanisms used by Threat Research and Development TR&D to leverage automated engines, utilities, analysis tools, human engineering, to identify and neutralize new threats in real-time; providing near-instant protection to end users against malware. Combined, this set of technology and process is called Threat Protection Network (TPN). SPN and TPN leverage the power of the user community by treating each client as a node and the Secure Peer Network to create a Collaborative Internet Security Network (CISN).

2 Background

All Antivirus and Antispyware companies utilize proprietary threat protection systems and processes to enable them to discover new and repurposed threats. These systems need to identify, detect, analyze, create countermeasures, test for false positive and false negative patterns, deploy new non-disruptive countermeasures, and monitor the effectiveness of their actions to ensure containment and removal of threats. **The entire threat lifecycle, from a threat's first detection, its isolation, effective countermeasure and eradication needs to happen quickly, accurately and be deployable globally to all users across the Internet.**

3 The security challenge

Effective Identification and eradication processes present many challenges which must be overcome by any successful security provider. These challenges push the envelope of security industry capabilities by the constantly changing nature and evolving nature of threats. There are a growing number of online transactions from all segments of computer users and, a rise in new social networking interactions (Second life, Face-book, MySpace) being conducted with strangers, as users of younger and older generations are utilizing computers more than ever. New threats are growing exponentially as the maturity and profile of the malicious authors move from disgruntled employees or fame seekers to independent and well organized thieves who are monetizing the theft of **personally** identifiable information and diverting consumer and corporate monies.

Security companies are challenged to identify new and more robust threats from organic sources through social networking sites, shared videos, domain stealing, and website technology injections (SQL, .net, URL injections). Injections take advantage of vulnerabilities in website technology or system configurations allowing hackers to create attacks, then leverage this information to modify or create imposter sites which result in identity theft and financial losses. These threats are very elegant and difficult to detect even by security experts and leaves the under protected computer user little chance of avoiding a well planned and executed attack.

These changes in technology drive the frequency and amount of data that must be analyzed by security experts; all of which have some form of Threat Research Center needing to apply its resources to:

- Locate and isolate new threats
- Retrieve threat data and programs to analyze
- Characterize and define threat danger levels
- Create and test new counter measures and repairs
- Provide rapid distribution of counter measures

4 Our solution

CyberDefender's SPN network has a clear advantage over other security companies when it comes to exchanging data between the TPN and the users. CyberDefender has proven and reliable data exchange using redundant and dynamically tunable automated delivery mechanisms leveraging the latest cloud computing and secure peer-to-peer technologies.

The primary mechanism utilizes multiple, redundant configurable exchange systems. SPN can retrieve potential threats and deploy neutralization and countermeasures quickly using secure peer-to-peer, cloud computing and Alert Server protocols for failover.

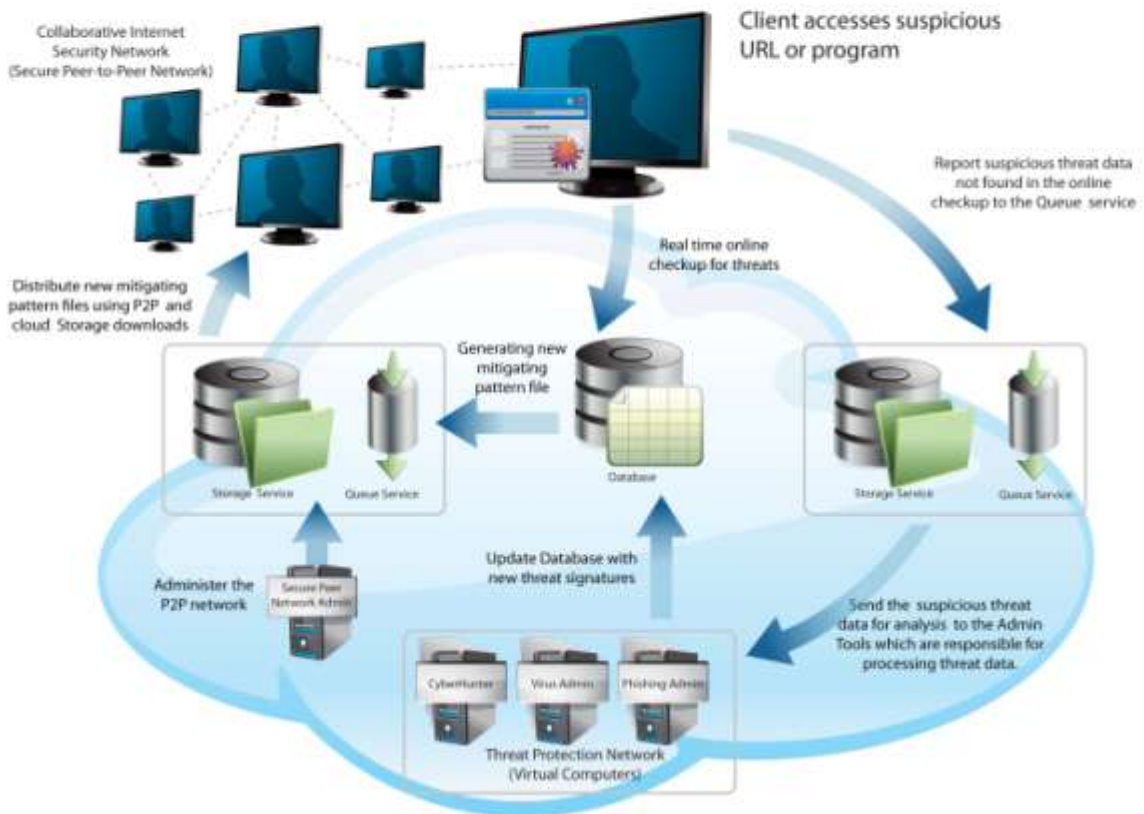


Figure 1.0

In addition to redundancy against rare SPN component outages, this allows for different consumer connectivity options. For example, small businesses, which have more IT management over computing environments, may opt to schedule protection as opposed to using near real-time secure peer-to-peer protection.

The maturity of Cloud Computing creates benefits, including encapsulating computing services from the outside world, and simplifying the hardware scalability challenges of storage, database and system services. CyberDefender recognized these benefits early on and spent significant time in 2008 to integrate Cloud Computing into the SPN data exchange mechanism, and re-deployed its TPN utilities to the cloud computing platform. This enables a nearly endless ability to increase automated capacity as our client base increases and quickly address the increase in frequency and maturity of security threats.

The TPN consists of a suite of engines and utilities known VirusAdmin, PhishingAdmin and CyberHunter. The SPN consists of the utility called SPNAdmin. These tools allow the TR&D staff to manage automation exceptions, provide manual intervention when new threats require it, and allow for the most flexible and optimized methods to be used to counter malware attacks. CyberDefender has put a focus on the ability to scale hardware capacity, create flexibility to quickly acquire threat data directly and indirectly, optimize threat research staff, and focus on current, new and relevant and immediate threats.

SPNAdmin – a system that manages the overall performance of the cloud computing capacity needs, secure peer-to-peer and alert server. SPNAdmin automatically creates new virtual engines and work queues to address increased capacity along with shutting off virtual cloud computing services when not used to reduce costs. It also provides operations data for the TR&D staff.

VirusHunter – an engine that manages the server side logic which is directly used by automated and real time analysis engines (fed by our CISN network as well as by our CyberHunter); takes in new uncategorized threats from customer service and support groups where some of the newest mature threat variants are identified; and allows for the quick automation and integration of new malware detection techniques that the industry and CyberDefender are constantly creating.

PhishingAdmin – a system that consolidates phishing and malware URLs from the CISN. It provides the capabilities to monitor trends, automatically sort and prune URLs, translating them into near real time threat protection via MyIdentityDefender toolbar, provides web messaging on latest outbreaks of threats, and updates the master blacklist and whitelist for TPN data.

CyberHunter – a server side engine that strategically crawls the internet based on proprietary taxonomy of priorities scans sites for malware URLs and vulnerabilities, and updates CISN customer base in near real-time.

5 Argus network Work Flow

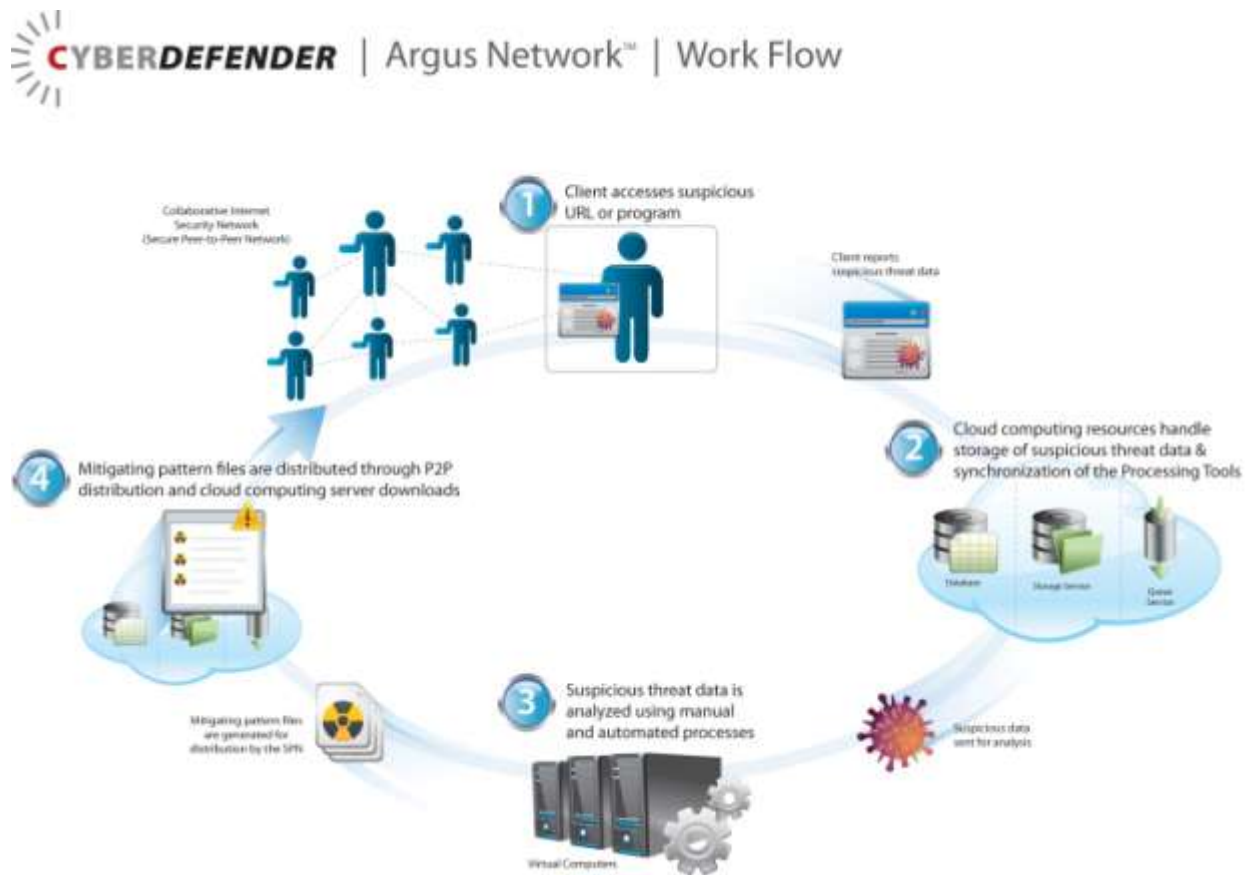


Figure 3.0

1. Client Accesses a suspicious URL or program:

User with a CyberDefender Client opens a URL or program that is suspicious. The Client program checks the cloud databases to see if this has been already been reported and identified by another user. **This check is called the "online checkup" and is done in real time.** If this is not the case then the threat data is reported to the cloud Queue service.

2. Storage of suspicious threat data:

All the threat data reported to the Queue service is stored in the cloud storage. This threat data is then sent to the processing tools or admin tools that are run in a virtual environment.

3. Processing of suspicious threat data:

Suspicious threat data is analyzed using manual and automated processes. The automated analysis is performed by multiple processing tools or admin tools depending on the kind of data reported. The automated analysis uses both behavioral and signature based analysis. The suspicious threat data that is identified as malware is then added to the cloud databases as a signature. These newly added signatures are then incorporated into mitigating pattern files and stored in the cloud.

4. P2P distribution of mitigating pattern files:

The mitigating pattern files are distributed by initial client downloads from the cloud storage. When the network is seeded the P2P distribution is responsible for majority of the client updates.

6 Improvements in Argus network

The main benefit of upgrading to the TPN in the Argus network 3.0 as compared to the TPN in Argus network1.0 is that threat data and its access has been transferred from dedicated servers into cloud storage and cloud database services. There is no central server to manage the threat data distribution or online threat data access. Instead, preparatory systems have a set of admin/processing tool programs running on the cloud machines which use online cloud queue service to sync the secure peer network, threat reporting and threat data automated analysis.

7 Cost benefit of using the Argus network 3.0

Complete detection and removal of threats requires signature distribution. CyberDefender uses its Argus network Secure Peer Network (Peer-to-Peer architecture) to distribute signature data and engine updates to its users by leveraging cloud storage and synchronization services. Most of the current day AntiVirus companies use client-server architecture for signature and engine update distribution enhanced by cloud computing detections. This makes the cost of each update more affordable to CyberDefender as its number of users grow. This consequently makes greater frequency of updates affordable and improves end user protection. Currently the TPN tools generate on an average 4 mitigating pattern files daily for phishing/malware URLs and virus/malware threats. The SPN tools check for new updates to distribute every hour.

8 Summary

CyberDefender has harnessed the **power of today's stable Cloud Computing environment and have** deployed the Threat Protection Network within the Cloud platform, augmenting its already powerful, fast and secure peer-to-peer (Argus network). These combined methodologies can automatically scale on-demand, provide near real-time, end to end threat analysis and ultimately, deploy timely and effective threat neutralization and protection to our users.

CyberDefender is committed to remain the thought leader for creative and innovative security counter measures meeting the needs for scalability, speed and quality of threat neutralization, today and in the future.

9 ^ CyberDefender anti malware network on cloud platform patent application

CyberDefender has already filed a USPTO patent application number **61,221,477** which is titled "System and method for operating an anti-malware network on a cloud computing platform."