Synoptek®

Web Content Filtering

Service Definition

Table of Contents

1 INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Web Content Filtering (the "Service").

The service definitions found herein reflect Companies standards at the time the Service Order(s) was issued. Company reserves the right to change any particular standard herein to reflect the current company's best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERING

Synoptek's Web Content Filtering Service is designed to reduce your exposure and shrink your organization's attack surface. Our Web Content Filtering Service prevents advanced threats before they can infiltrate your organization. With our centralized approach, Synoptek provides coverage for a range of devices, including laptops, desktops and iOS devices. Our Security personnel will continue to advise on ever changing threats and recommended actions.

Synoptek's Web Content Filtering, or WCF, not only blocks malware, botnets and phishing over any port, protocol or app, but also detects and contains advanced attacks before they can cause damage to your end-user's endpoint devices. This service uses big-data analytics and machine learning to automate protection against both known and unknown threats. Synoptek's WCF stays always-up-to-date with no hardware to install, no software to maintain, and is fully managed by your Synoptek technical service team.

Key Features and Benefits	
1. Category-based Filtering 2. Supports Compliance 3. Allow or Block specific domains 4. Block Page Bypass 5. Whitelist-Only	1. Quick Deployment 2. Predictive Intelligence 3. No Added Latency 4. Proven Reliability 5. Comprehensive Threat Protection

3 SOLUTION PURPOSE

Unlike other solutions that react to known threats and add latency by re-routing every internet connection through proxy or VPN gateways, Synoptek's Web Content Filtering uses predictive intelligence to discover unknown threats and adds no latency.

4 HOW IT WORKS

Synoptek's Web Content Filter integrates security features into one of the most fundamental protocols that underlies the internet, DNS (Domain Name System). The result is a robust service that enables SMBs to protect their networks and network resources using their existing infrastructure with no additional equipment, software or on-going upgrades and maintenance involved. Because no new hardware or software is required, deploying Synoptek's Web Content Filter is fast and non-intrusive to your staff.

5 WHAT'S INCLUDED

Your subscription to Synoptek's Web Content Filter includes the following:

1. Blocking of content and websites related to the following:
   - a. Adware
   - b. Alcohol
   - c. Dating
   - d. Drugs
   - e. Gambling
   - f. Hate/Discrimination
   - g. Lingerie/Bikini
   - h. Nudity
   - i. Pornography
   - j. Proxy/Anonymizer
   - k. Sexuality
   - l. Tasteless
   - m. Weapons
2. Blocking of traffic related to malware, drive-by downloads/exploits, mobile threats, botnets and phishing attempts.
3. Installation of 'Roaming Clients' for mobile devices such as laptops to protect assets that may connect to networks outside of the organization's control (each Roaming Client is considered a single seat for billing purposes).
4. A customized block page that displays whenever an asset attempts to visit a page that has been blocked by Synoptek's Web Content Filter. This block page will show your company logo and a message that reads:
   - a. "Sorry, [The page the user was trying to reach] has been blocked by your network administrator."

A 'seat' is defined as any end-point where an instance of Synoptek's Web Content Filter is deployed. This includes, but is not limited to, desktops, laptops, tablets, smart phones, etc.

6 SERVICE LIMITATIONS

Synoptek's Web Content Filter is an excellent addition to an organization's strategy of defense in depth. Synoptek's Web Content Filter is not an all-in-one solution for preventing all threats, attacks or variations of malware that may be leveraged against your organization. As a result, it should be expected that this service alone cannot detect or prevent *all* threats and is best used in conjunction with other security tools and resources.

Web-born threats are prevalent and broad. Synoptek's Web Content Filter is an always-on solution that blocks connections to these web-born threats and restricted websites. Synoptek's WCF delivers piece-of-mind without the need for reporting. As such and by default, WCF reporting is not enabled.