DNSWatchGO

DNS-Level Protection for Users on the Go

Whether working from a home office, coffee shop, or conference hotel room, the modern employee relishes the opportunity to be productive where they feel most comfortable. Today, three-quarters of global employees work remotely at least one day a week. As a result, more and more of your business is being conducted off-network, and outside of your traditional security tools. WatchGuard DNSWatchGO provides DNS-level protection and content filtering that keeps your business safe from phishing, ransomware, and other attacks even when your user is outside of the network, without requiring a VPN.

Key Features

- DNS-level detection, providing an additional layer of security to block connections to the bad guys

- Automatically protects end users from phishing attacks and C2 connections

- Content filtering that limits access to risky areas of the web with 130 pre-defined blocking categories

- Provides immediate security education to heighten end user awareness after an attack

- Lightweight, always-on security - no VPN required!

- Supports Windows 7, 8, 10, and Chrome OS

Protection on the Go

Phishing, malware, and ransomware represent some of the most serious threats to a business's security, and your employees are more vulnerable when they are outside of your secure perimeter. The burden of

keeping your organization safe as employees roam free is daunting, but DNSWatchGO makes it easy to defend your business wherever your users go. By proactively identifying DNS requests bound for malicious content, DNSWatchGO stops risky clicks from becoming major security incidents. When your user clicks a link or enters a web address in their browser, DNSWatchGO monitors and correlates the DNS traffic against our intelligence feeds, identifying and blocking connections to domains owned by the bad guys.

Off-Network Visibility and Enforcement

As users become more mobile you lose visibility into their Internet activity, creating a significant blind spot in your defenses. You may also want to restrict your users from accessing certain types of content, like social media and adult sites, for productivity reasons. DNSWatchGO gives you instant visibility and control over the web activity occurring on devices both inside and outside of your network, allowing you to enforce web content policies to keep users away from the areas of the web that could threaten your business. Easily establish policies for your users based on 130 pre-defined blocking categories, and fine-tune access by individual users or groups.

Tackle Phishing with Automated Training

90% of attacks begin with a successful phishing email that tricks users into clicking a link or downloading a file they shouldn't. DNSWatchGO is the first security service to provide phishing protection and education wherever your users go, allowing you to take advantage of those teachable moments when the lesson is most likely to stick. When an end user clicks on an email or link that DNSWatch has identified as a phishing attempt, they are redirected to an interactive video that educates on the warning signs of a phishing attack and gives the user an action to take, such as reporting the offending email or speaking with a member of your IT team when they encounter a threat in the future.

Low TCO Cloud Service

DNSWatchGO, as a 100% Cloud-based solution, is easy to deploy and manage, saving you time and money. There's no hardware and no need to update software manually, while devices deploy in minutes, quickly providing visibility Into Internet activity wherever your user goes. Centrally manage DNSWatchGO policies for all of your users.

Lightweight Client

DNSWatchGO is a lightweight client application that you install on portable computers that leave your network, such as employee laptops or student notebooks. Once installed, DNSWatchGO forwards DNS requests to the DNSWatch service for comparison to a database of malicious domains. DNSWatchGO supports Chrome OS, Windows 7, 8, and 10.

How It Works

WatchGuard DNSWatchGO monitors outbound DNS requests, correlating them against an aggregated list of malicious sites. Requests that are determined to be malicious are blocked, redirecting the user to a safe site to reinforce their phishing training.

WatchGuard Security Experts

Centralized Policy

Simply point Firebox at DNSWatch

All Devices

DNSWatch behind Firebox

Client redirects DNS, adds company and group information

DNSWatchGO Off-Premises