DATASHEET

DNSWatch

Inspects DNS traffic to block malicious connections on all ports and protocols

WatchGuard DNSWatch™ is a Cloud-based service adding DNS-level filtering to detect and block potentially dangerous connections and protect networks and employees from damaging attacks. WatchGuard analysts triage any critical alerts, following up with an easy-to-understand accounting that includes detailed insights about the potential infection. When the attack uses phishing, and an employee clicks the link, DNSWatch automatically redirects them away from the malicious site and offers resources that reinforce phishing education.

"Our antivirus was good. WatchGuard is better. WatchGuard was simple to deploy and immediately stopped attacks from impacting our business."

~ Mike Brooks, IT Manager, SEEPEX Inc.

EFFECTIVE DNS-BASED PROTECTION

Hackers need to use DNS to execute attacks over the Internet so examining DNS traffic is a great way to find and ultimately intercept attacks! DNSWatch brings DNS-level filtering into our Total Security Suite, providing an added layer of security to stop malware infections.

Malicious DNS requests are automatically detected and blocked, redirecting users to a safe place instead of to the attacker. Combining DNSWatch with complementary services like Reputation Enabled Defense reputation lookup service, WebBlocker content filtering, GAV and APT Blocker sandboxing melds their protective capabilities to block malicious connections on all ports and protocols – including those used with phishing and spear-phishing attacks.

LOW TCO CLOUD SERVICE

DNSWatch operates 100% from the Cloud, so there's no software to maintain, or any hardware beyond the Firebox you are already using with Total Security Suite services. Requiring no client-side configuration makes deploying DNSWatch a breeze to set up and manage, saving even more time and money.

TACKLE PHISHING WITH AUTOMATED TRAINING

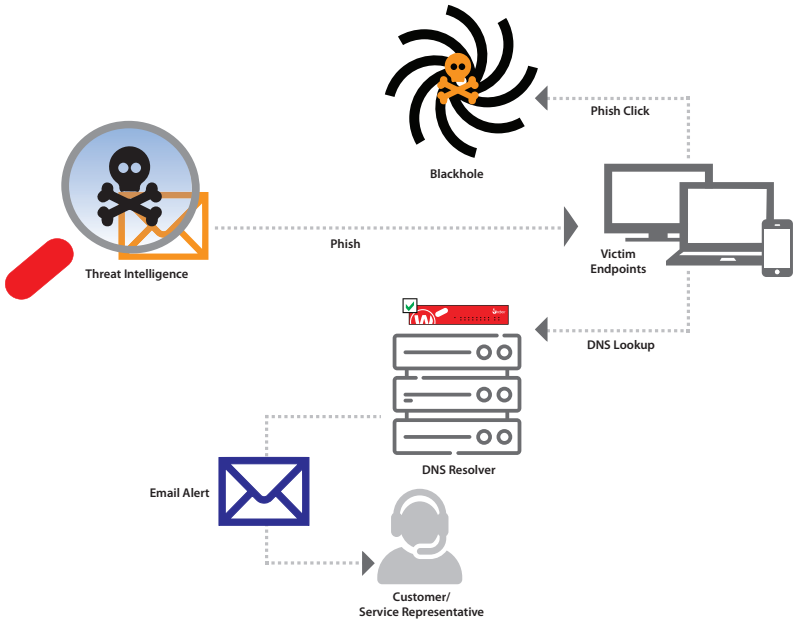
Educating users is an IT admin's first line of defense in protecting their organization, but it can be a challenge to provide timely training, when the mistake is fresh in the user's memory. DNSWatch increases an organization's resilience to phishing by automating employee education. When a user clicks on a phishing message, they are redirected to a safe page that offers education and games to reinforce the warning signs of a phishing attack. By automatically delivering training at the time of the infraction, DNSWatch provides the best opportunity for employee learning and reduces risks to the organization from repeated attacks.

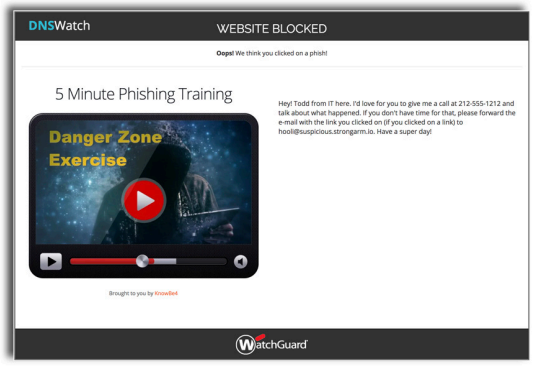
ACTIONABLE ANALYSIS IN YOUR INBOX

It sometimes takes a human to analyze data and enable true understanding. DNSWatch includes feedback from analysts for a personal touch not found in other DNS filtering solutions. When attackers strike, they are kept engaged in the DNSWatch Blackhole so that we can learn more about them. Then, our analysts draft a report with the details about infections detected and blocked by the service. No need to spend hours combing through logs or researching an alert as it comes through – the analysis arrives right in your inbox. This service allows companies to quickly and easily react to address any potential risks…doing what others can only do with an army of security analysts.

FEATURES & BENEFITS

- Detects and blocks malicious connections by inspecting traffic to the DNS for added security
- Provides immediate phishing education to users at the time of click for heightened end-user awareness after an attempted attack
- Personalizes analysis on detected infections with information on the attacker, type of attack and attacker goals, so that organizations can take quick action
- It's quick to install and easy to manage – saving time and costs and reducing the burden on busy IT staff
- Works in concert with other Total Security Suite services for effective, layered protection





HOW IT WORKS

WatchGuard DNSWatch 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.

TOTAL SECURITY SUITE

STRONG SECURITY AT EVERY LAYER

Uniquely architected to be the industry's smartest, fastest, and most effective network security products, WatchGuard solutions deliver in-depth defenses against advanced malware, ransomware, botnets, trojans, viruses, drive-by downloads, data loss, phishing and much more.

ONE PACKAGE. TOTAL SECURITY.

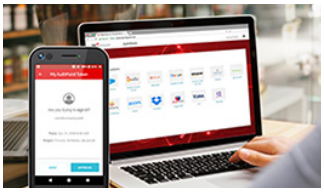
The flexibility of WatchGuard's integrated platform makes it easy to have exactly the security components your business network requires. Whether you choose to start with the security basics or deploy a comprehensive arsenal of network defenses, we have bundled security services to match your requirements.

	SUPPORT	BASIC SECURITY	TOTAL SECURITY
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal*	✓	✓	✓
Intrusion Prevention Service (IPS)		✓	✓
Application Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
DNSWatch			✓
IntelligentAV**			✓
ThreatSync (XDR)			✓
EDR Core			✓
WatchGuard Cloud			
Log Data Retention		90 Days	365 Days
Report Data Retention		1 Day	30 Days
Support	Standard (24 x 7)	Standard (24 x 7)	Gold (24 x 7)

*Not available on Firebox T20/T20-W, T25/T25-W, or T35-R. Total Security Suite required for M270, M370, M470, M570, M670, FireboxV and Firebox Cloud.
**Not available on Firebox T20/T20-W, T25/T25-W, or T35-R.

THE WATCHGUARD PORTFOLIO

Network Security



Multi-Factor Authentication

Secure Cloud Wi-Fi

Endpoint Security

Contact your authorized WatchGuard reseller or visit **www.watchguard.com** to learn more.

U.S. SALES +1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com WatchGuard Technologies, Inc.