DATENBLATT

DNSWatch

Durch die Untersuchung des DNS-Datenverkehrs werden schädliche Verbindungen über sämtliche Ports und Protokolle blockiert

WatchGuard DNSWatch™ ist ein Cloud-basierter Service, der mit Filtern auf DNS-Ebene potenziell gefährliche Verbindungen erkennt und blockiert und somit Netzwerke und Mitarbeiter vor schädlichen Angriffen schützt. Die Analyseexperten von WatchGuard beschäftigen sich mit allen wichtigen Warnmeldungen und dokumentieren potenzielle Infektionen in einfacher Sprache und mit detaillierten Informationen. Wenn ein Mitarbeiter bei einem Phishing-Angriff auf den Link klickt, wird er von DNSWatch automatisch von der schädlichen Site weggeleitet, und es werden Materialien zur Auffrischung der Kenntnisse zu Phishing-Angriffen angeboten.

„Unser antivirus war gut. WatchGuard ist besser. WatchGuard ließ sich einfach bereitstellen und sorgte sofort dafür, dass sich Angriffe nicht mehr negativ auf unsere Unternehmensabläufe auswirken konnten."

~ Mike Brooks, IT-Manager, SEEPEX Inc.

EFFEKTIVER DNS-BASIERTER SCHUTZ

Hacker müssen DNS nutzen, wenn sie ihre Angriffe über das Internet durchführen wollen. Daher ist die Überwachung des DNS-Datenverkehrs eine hervorragende Methode zum Auffinden und Abfangen von Angriffen! Mit DNSWatch wird unser Total Security Suite um die Filterung auf DNS-Ebene und damit um eine zusätzliche Sicherheitsebene zum Schutz vor Infektionen durch Malware ergänzt.

Bösartige DNS-Anfragen werden automatisch erkannt und blockiert, und die Benutzer werden auf eine sichere Website statt auf die des Angreifers weitergeleitet. Durch die Kombination von DNSWatch mit ergänzenden Services wie dem Reputations-Suchdienst Reputation Enabled Defense, der WebBlocker-Inhaltsfilterung und den Sandboxing-Lösungen GAV und APT Blocker verschmelzen die Schutzfunktionen zu einer Gesamtlösung, die schädliche Verbindungen über alle Ports und Protokolle blockiert – auch diejenigen, die bei Phishing- und Spear-Phishing-Angriffen genutzt werden.

CLOUD-SERVICE MIT GERINGEN BETRIEBSKOSTEN (TCO)

DNSWatch wird vollständig in der Cloud betrieben. Sie müssen also keine Software warten, und außer der Firebox, die Sie bereits für die Total Security Suite-Services nutzen, auch keine Hardware. Da auf Client-Seite keine Konfiguration erforderlich ist, sind die Einrichtung und das Management bei der Bereitstellung von DNSWatch ein Kinderspiel. Dadurch sparen Sie zusätzlich Zeit und Geld.

KAMPF GEGEN PHISHING MITTELS AUTOMATISIERTER SCHULUNGEN

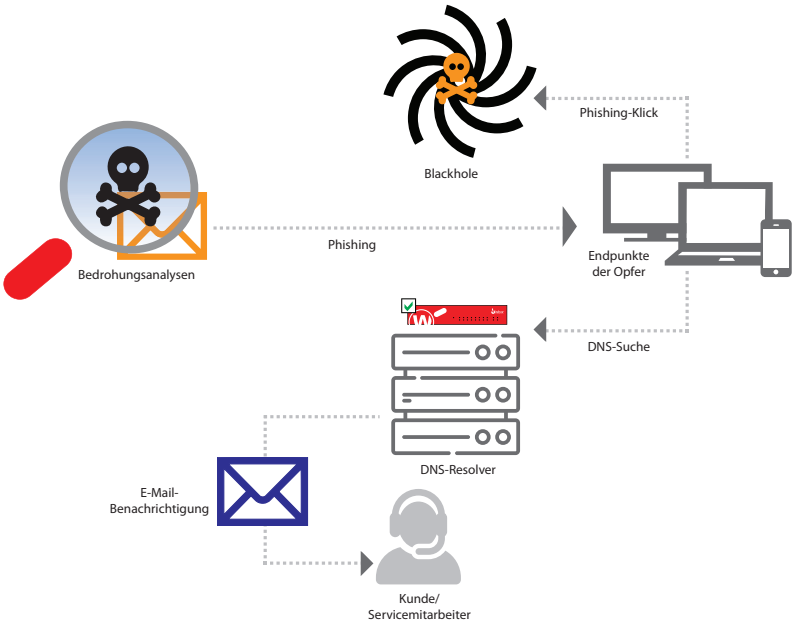
Eine erste Verteidigungslinie gegen Phishing-Angriffe ist für die IT-Administratoren das Wissen und Problembewusstsein der Benutzer. Rechtzeitig Schulungen anzubieten – also dann, wenn den Benutzern ihr Fehler noch frisch in Erinnerung ist, kann jedoch ziemlich kompliziert sein. DNSWatch steigert mit automatisierten Mitarbeiterschulungen die Widerstandsfähigkeit einer Organisation gegenüber Phishing-Versuchen. Wenn Benutzer auf eine Phishing-Nachricht klicken, werden sie auf eine sichere Seite geleitet, die mit Informationen und auf spielerische Art und Weise verdeutlicht, an welchen Warnsignalen Phishing-Angriffe zu erkennen sind. Durch die automatische Schulung unmittelbar nach dem begangenen Fehler nutzt DNSWatch das optimale Zeitfenster für einen Lernerfolg bei den Mitarbeitern. So sinkt das Risiko weiterer Angriffe auf die Organisation.

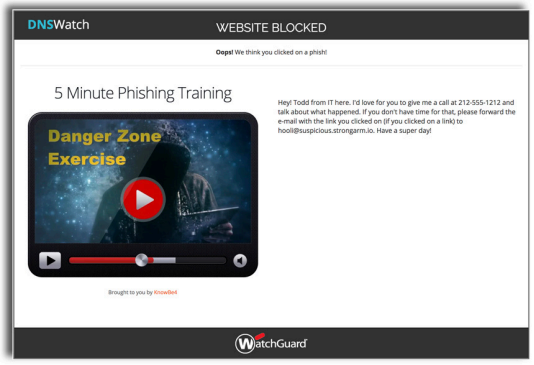
HANDLUNGSORIENTIERTE ANALYSE IN IHREM POSTFACH

In manchen Fällen kommt die wahre Tragweite von Informationen nur nach eingehender Datenanalyse durch Experten zum Vorschein. DNSWatch umfasst Feedback von Analyseexperten und ergänzt die DNS-Filterung damit um einen persönlichen Aspekt, der bei anderen Lösungen nicht verfügbar ist. Wenn Angreifer zuschlagen, halten wir sie im DNSWatch Blackhole fest, um sie eingehender untersuchen zu können. Anschließend fertigen unsere Experten einen Berichtsentwurf mit Details zu den vom Service erkannten und blockierten Infektionen an. Sie müssen nicht stundenlang Protokolle durchsuchen oder sich sofort mit eingehenden Warnmeldungen beschäftigen – die Analyse kommt verlässlich in Ihrem Posteingang an. Der Service ermöglicht es Unternehmen sogar, schnell und einfach auf potenzielle Risiken zu reagieren und damit Schritte zu unternehmen, die andere nur mit einem Heer an Sicherheitsanalysen bewerkstelligen können.

FUNKTIONEN UND VORTEILE

- Schädliche Verbindungen werden bei der Prüfung von DNS-Datenverkehr erkannt und blockiert
- Benutzer werden sofort nach einem vom System vereitelten Phishing-Angriff mit entsprechendem Schulungsmaterial für das Thema sensibilisiert
- Personalisierte Analysen zu erkannten Infektionen und Informationen zum Angreifer sowie zur Art und Zielsetzung des Angriffs ermöglichen Organisationen ein schnelles Handeln
- Die einfache Installation und Verwaltbarkeit erspart den Unternehmen Zeit und Kosten und entlastet die IT-Mitarbeiter von zeitraubenden Aufgaben
- Gemeinsam mit anderen Services der Total Security Suite entsteht ein effektiver, mehrstufiger Schutz





FUNKTIONSWEISE

WatchGuard DNSWatch überwacht ausgehende DNS-Anforderungen und stellt sie einer zusammengestellten Liste böswilliger Sites gegenüber. Als schädlich erkannte Anforderungen werden gesperrt. Die Benutzer werden auf eine sichere Site weitergeleitet, auf der sie ihre Kenntnisse zum Thema Phishing auffrischen können.

TOTAL SECURITY SUITE

UMFASSENDE SICHERHEIT AUF ALLEN EBENEN

Aufgrund ihrer einzigartigen Architektur und fundierten Abwehrmechanismen gegen Malware, Ransomware, Botnets, Trojaner, Viren, Drive-by-Downloads, Datenverlust, Phishing und mehr gelten die Netzwerksicherheitslösungen von WatchGuard als die intelligentesten, schnellsten und leistungsfähigsten auf dem Markt.

EIN PAKET. TOTALE SICHERHEIT.

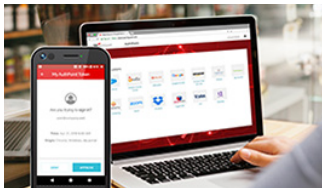
Die Flexibilität der integrativen WatchGuard-Plattform macht's möglich: Stellen Sie einfach die Sicherheitskomponenten zusammen, die Ihr Unternehmensnetzwerk tatsächlich benötigt. Dabei spielt es keine Rolle, ob Sie mit einer Grundsicherung beginnen oder umfassendere Maßnahmen zum Schutz Ihres Netzwerks etablieren möchten – wir stimmen unsere Sicherheitsdienste genau auf Ihre jeweiligen Anforderungen ab.

	SUPPORT	BASIC SECURITY	TOTAL SECURITY
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal*	✓	✓	✓
Intrusion Prevention Service (IPS)		✓	✓
Anwendungskontrolle		✓	✓
WebBlocker (URL-/Inhaltsfilterung)		✓	✓
spamBlocker (Anti-Spam)		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
DNSWatch			✓
IntelligentAV**			✓
ThreatSync (XDR)			✓
EDR Core			✓
WatchGuard Cloud Aufbewahrung von Protokolldaten Aufbewahrung von Reportdaten		90 Tage 1 Tag	365 Tage 30 Tage
Support	Standard (24 x 7)	Standard (24 x 7)	Gold (24 x 7)

* Nicht erhältlich auf Firebox T20/T20-W, T25/T25-W, oder T35-R.
Total Security Suite erforderlich für M270, M370, M470, M570, M670, FireboxV und Firebox Cloud.
** Nicht erhältlich auf Firebox T20/T20-W, T25/T25-W, oder T35-R.

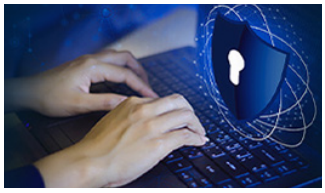
DIE WATCHGUARD PORTFOLIO

Netzwerksicherheit



Multifaktor-Authentifizierung

Sicheres, cloud-verwaltetes WLAN



Endpoint Security

Weitere Informationen erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter **www.watchguard.de.**

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1 206 613 0895 WEB www.watchguard.de WatchGuard Technologies, Inc.