WatchGuard

6 WESENTLICHE FUNKTIONEN EINER MODERNEN FIREWALL

1. LEISTUNGSSTARKE SSL-/TLS-ANALYSE

Wenn Sie HTTPS-Entschlüsselung und Inhaltsanalyse nicht nutzen, entgehen Ihnen wahrscheinlich **zwei Drittel der Malware**, die in Ihr Unternehmen eindringt.

Mehr als 80 % des geschäftlichen Datenverkehrs findet über verschlüsselte Kanäle statt, und 50 % der Phishing-Sites verbergen ihre Angriffe mit HTTPS. Durch die HTTPS-Analyse können Sie HTTPS-Datenverkehr entschlüsseln, den Inhalt auf Angriffshinweise überprüfen und ihn dann wieder mit einem neuen Zertifikat für eine sichere Übermittlung verschlüsseln.

OHNE ENTSCHLÜSSELUNG:
Keine Einblicke in Datentyp, Anwendung, Einhaltung von Richtlinien, Dateityp oder Datenabgriffsversuche über HTTPS.

TIPPS

Suchen Sie nach einer Firewall mit leistungsstarker HTTPS-Analyse, wenn ALLE Sicherheitsdienste aktiv sind.

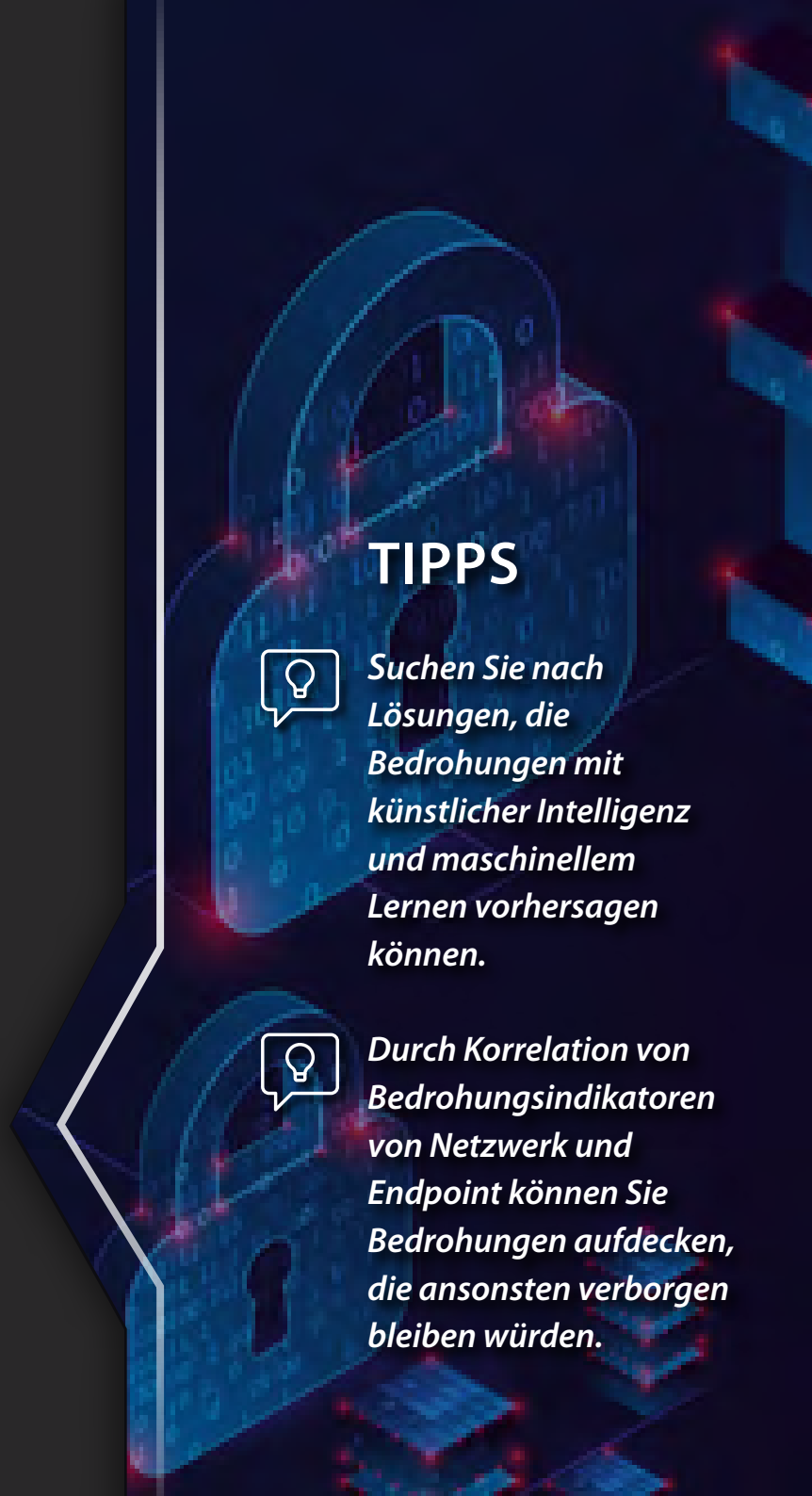
Suchen Sie nach einer Lösung, die eine VOLLSTÄNDIGE Analyse von TLS 1.3 unterstützt.

2. MEHRSTUFIGER SCHUTZ VOR ZERO DAY MALWARE

64 % aller Malware-Bedrohungen in einem typischen Geschäftsnetzwerk sind auf Zero Day Malware zurückzuführen.

Ein Zero-Day-Angriff versucht, eine Sicherheitslücke in Computersoftware oder Geräten auszunutzen, bevor diese Sicherheitslücke erkannt und behoben wurde. Der Schutz vor Zero-Day-Angriffen wehrt derartige Bedrohungen ab, obwohl die genauen Methoden des Angriffs unbekannt sind.

SCHICHT FÜR MAXIMALEN SCHUTZ:
KI-gestützte Erkennung, Sandboxing in der Cloud, integrierte Endpoint-Erkennung und -Reaktion



TIPPS

Suchen Sie nach Lösungen, die Bedrohungen mit künstlicher Intelligenz und maschinellem Lernen vorhersagen können.

Durch Korrelation von Bedrohungsindikatoren von Netzwerk und Endpoint können Sie Bedrohungen aufdecken, die ansonsten verborgen bleiben würden.

3. SCHUTZ VOR PHISHING UND UNÜBERLEGTEN KLICKS

83 % der Unternehmen sind bereits einem Phishing-Angriff zum Opfer gefallen.

Hacker setzen auf DNS, um ahnungslose Opfer zu täuschen. Eine genaue Untersuchung von DNS-Anforderungen trägt also enorm dazu bei, Angriffe zu erkennen und letztendlich abzuwehren. Wenn Anwender unwissentlich auf schädliche DNS-Adressen zugreifen, können diese Zugriffe automatisch blockiert werden. Dabei werden Anwender nahtlos zu einer sicheren Landingpage umgeleitet.

DIE ERSTE VERTEIDIGUNGSLINIE:
Blockieren Sie bösartige Clickjacking- und Phishing-Domains unabhängig von Verbindungstyp, Protokoll oder Port.

TIPPS

Suchen Sie nach Lösungen, die sowohl Phishing-Versuche als auch Command-and-Control-Kanäle blockieren.

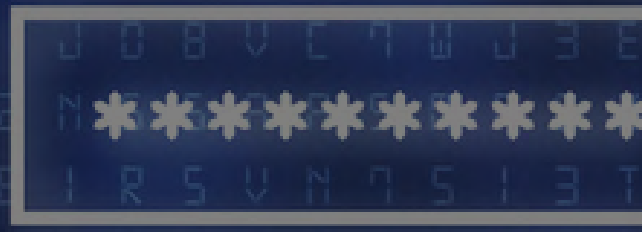
Suchen Sie nach Lösungen, die Anwender, die einem Phishing-Versuch zum Opfer fallen, in Echtzeit informieren.

4. WEBBASIERTES PORTAL FÜR SICHEREN ZUGRIFF

Anwender verbringen im Schnitt **36 Minuten pro Monat** damit, ihre Anmeldedaten manuell einzugeben. Das bedeutet eine Verschwendung von fast einem ganzen Arbeitstag pro Mitarbeiter und Jahr.

Mit Single Sign-On können Mitarbeiter sich mit ihren Anmeldedaten einmalig anmelden, um auf alle Anwendungen, Websites und Daten, die sie brauchen, zuzugreifen. SSO verbessert die Sicherheit, da Anwender sich weniger Passwörter merken müssen, und entlastet die IT-Teams, bei denen ansonsten zahlreiche Anfragen für Passwortrücksetzungen eingehen.

BEST PRACTICE:
Kombinieren Sie SSO mit MFA, um RDP-(Remotedesktop-), SSH- und Webzugriffsverbindungen zu sichern.



TIPPS

Stellen Sie sicher, dass das Portal die gängigen Identitätsanbieter unterstützt, wie AuthPoint, Shibboleth, OneLogin, ADFS oder Okta.

Suchen Sie nach einer Lösung, die die gängigsten Softwaretoken unterstützt, darunter AuthPoint, Okta Mobile, Google Authenticator, OneLogin Protect, Duo Mobile, RSA SecureID.

5. NEUESTE VPN-TECHNOLOGIE UNTERSTÜTZEN

68 % der Unternehmen haben ihre VPN-Nutzung infolge der COVID-19-Pandemie ausgeweitet.

Virtuelle private Netzwerke (VPNs) bieten einen sicheren Tunnel von Remotestandorten zur Hauptniederlassung. Anwendern stehen verschiedene Typen von VPN-Technologie für die mobile oder Remotenutzung zur Verfügung. Einige Firewall-Anbieter verkaufen zusätzliche VPN-Lizenzen mit der Firewall, während andere die vollständige Lizenzkapazität mit jedem Modell beinhalten.

VPN-TECHNOLOGIEN FÜR REMOTEANWENDER:
IKEv2 (neueste, schnellste Technologie), IPSec (aber keine Pre-Shared Keys verwenden), SSL (am häufigsten genutzt), L2TP (veraltet, vermeiden)

TIPPS

Für Anmeldungen bei in der Cloud gehosteten Anwendungen (SaaS) sowie den VPN-Zugriff auf Unternehmensnetzwerke sollte MFA angewendet werden.

Suchen Sie nach Plattformen, die einen Standard-Routentunnel unterstützen, bei dem der Datenverkehr für eine vollständige Sicherheitsprüfung zurück zur zentralen Firewall geleitet wird.

6. NATIVE AUTOMATISIERUNG

Durch die Automatisierung konnten **die Personalstunden für die Verwaltung der Sicherheit um beachtliche 80 % verringert werden**.

Sie benötigen einen hohen Automatisierungsgrad, um mit Bedrohungen Schritt zu halten, Zeit- und Geldverschwendung zu reduzieren sowie die Transparenz einer modernen Netzwerkumgebung zu erhöhen. Einheitliche Sicherheitsplattformen sind von Grund auf mit Automatisierung konzipiert und können die Sicherheit Ihres Netzwerks nicht nur aufrechterhalten, sondern auch über den traditionellen Perimeter hinaus erweitern.

4 EBENEN DER AUTOMATISIERUNG:
Verwaltung, betrieblich, reaktionsschnell und vorausschauend

TIPPS

Integration in RMM- und PSA-Tools kann schnellere Supportreaktionen ermöglichen.

KI-gestützter vorausschauender Schutz kann die komplexen Bedrohungen abwehren, die ansonsten ein internes Expertenteam erfordern würden.

Firebox®

1. Führende SSL/ TLS-Entschlüsselung
2. 3 Ebenen von Zero-Day-Schutz
3. Cloudbasierte DNS-Filterung
4. Standardmäßiges Zugriffsportal
5. 4 Arten mobiles VPN, einschließlich IKEv2
6. Stellt alle 4 Ebenen der Sicherheitsautomatisierung bereit

Weitere Informationen finden Sie unter www.watchguard.com/de/wgrd-products/firewall-appliances

250
Netzwerkangriffe

1.300
schädliche Dateien

~ durchschnittliche Anzahl blockierter Bedrohungen pro Firebox 2019

WatchGuard erzielte eine hohe Sicherheitseffektivität und niedrige Gesamtbetriebskosten und ist **eines von nur zwei Produkten, die 100 % der Ausweichmanöver blockierten.**

- NSS Labs

DAS WATCHGUARD-SICHERHEITSPORTFOLIO

Netzwerksicherheit

Netzwerksicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

Sicheres WLAN

Die Secure Wi-Fi Solution von WatchGuard ist eine richtungsweisende Neuerung für den Markt von heute: Sie schafft eine sichere, geschützte WLAN-Umgebung, eliminiert den Verwaltungsaufwand und ermöglicht beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint® können Sie die passwortbasierende Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach schließen. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Smartphones" als Identifizierungsfaktor genutzt. Auf diese Weise erhält nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen.

Endpoint-Sicherheit

WatchGuard Endpoint Security ist ein Cloud-natives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Seine auf künstlicher Intelligenz basierende Flagship-Lösung Panda Adaptive Defense 360 verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

ÜBER WATCHGUARD

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Weitere Informationen finden Sie unter **WatchGuard.de**.

WatchGuard®

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 **INTERNATIONALER VERTRIEB:** +1 206 613 0895 **WEB** www.watchguard.com/de