

# FIREBOX CLOUD

Erweiterung des WatchGuard-Sicherheitsperimeters auf die Public Cloud



Immer mehr Unternehmen verlagern ihre Anwendungen von lokalen Servern in die Cloud – egal ob E-Mail- und Webserver, CRM-Systeme oder Datenspeicher, vieles wird auf Cloud Services umgestellt. Angesichts dieser Menge an sensiblen Daten, die jetzt in die Cloud wandert, ist Sicherheit ein absolutes Muss. Mit Firebox Cloud von WatchGuard können Netzwerkadministratoren den Schutz ihrer internen IT-Umgebung ohne Probleme auf Server in der Public Cloud ausweiten.

*Anbieter von Cloud Services sind zwar für die Sicherheit der Cloud verantwortlich, es ist allerdings die Aufgabe jedes einzelnen Unternehmens, die eigenen sensiblen Daten auf dem Weg dahin und zurück abzusichern. Entsprechend dieses Prinzips der geteilten Verantwortung müssen Administratoren jede Möglichkeit ausschöpfen, um die Daten bestmöglich zu schützen und Cyberangriffe abzuwehren. WatchGuard Firebox Cloud bietet für Public-Cloud-Umgebungen die gleiche erstklassige Sicherheit, die Anwender der Firebox® UTM-Appliances (Unified Threat Management) bereits gewohnt sind. Firebox Cloud ist im Handumdrehen installiert und schützt Server in Public Clouds vor Bedrohungen wie Botnets, standortübergreifenden Scripting-Angriffen, SQL-Injection-Versuchen und weiteren Gefahren.*

## KONZIPIERT FÜR DIE CLOUD

Unternehmen, die ihre Anwendungen und Dienste auf Public-Cloud-Dienste übertragen, müssen dasselbe Sicherheitsniveau bieten, das sie auch vor Ort bereitstellen. Die WatchGuard Firebox Cloud bietet UTM-Sicherheitsdienste gegen Angriffe, Malware und zur Filterung von Webinhalten, die nicht von Cloud-Dienstleistern bereitgestellt werden.

## AUSWEITUNG DES WATCHGUARD-SCHUTZES

Mit der Firebox Cloud können kleine bis mittlere Unternehmen und dezentral aufgestellte Organisationen, die ihre Infrastruktur zum Teil in die Cloud verlagert haben, ihre Konfigurations- und Wartungsaufgaben nachhaltig rationalisieren. Der Sicherheitsradius wird einfach erweitert. Dank des kombinierten Einsatzes von Firebox Cloud und physischen Firebox-Appliances muss man sich zudem gar nicht erst mit zusätzlichen Produkten zum Schutz einer virtuellen Public Cloud (VPC) auseinandersetzen.

## BIG-DATA-VISUALISIERUNG

WatchGuard Firebox Cloud fügt sich ebenfalls nahtlos in die Visualisierungslösung WatchGuard Dimension ein, die zum Standard-Umfang aller WatchGuard UTM- und NGFW-Lösungen gehört. Dank zahlreicher Big-Data-Visualisierungs- und Reporting-Werkzeuge lassen sich mit Dimension sicherheitsrelevante Probleme und Trends im Handumdrehen identifizieren. Aufgrund der detaillierten Einblicke steht der Umsetzung passgenauer Sicherheitsrichtlinien nichts mehr im Wege – und dies gilt für alle Systemumgebungen.

## VERSCHIEDENE KAUFOPTIONEN

WatchGuard bietet gleich mehrere Kaufoptionen, um Ihnen die Inbetriebnahme der Firebox Cloud zu erleichtern. So können Sie eine separate Lizenz nach dem BYOL-Modell (Bring Your Own License) von einem WatchGuard-Partner erwerben und sich damit den von Ihnen präferierten Dienstleister an ihrer Seite sichern. Oder Sie entscheiden sich im Direktkauf für eine nutzungsbasierte Abrechnung (z.B. pro Stunde).

## FUNKTIONEN UND VORTEILE

- Schnelle und unkomplizierte Absicherung von Virtual Private Clouds gegenüber Bedrohungen wie Botnets, standortübergreifenden Scripting-Angriffen, SQL-Injection-Versuchen und weiteren Gefahren
- Zeitsparend dank angepasster Benutzeroberfläche für jede Cloud-Plattform
- Reibungsloser Aufbau sicherer Verbindungen in die Public-Cloud-Umgebung
- Hohe Transparenz dank der Netzwerkvisualisierungslösung WatchGuard Dimension
- Verschiedene Kaufoptionen für unterschiedliche Anforderungen



	KLEIN	MITTEL	GROß	EXTRA GROß
<b>LEISTUNGSBESCHREIBUNG <sup>1</sup></b>				
Max. Anzahl CPU-Kerne	2	4	8	16
Benutzer	50	250	750	1.500
EDR-Core Lizenzen	50	150	250	250
Firewall	2 Gbit/s	4 Gbit/s	8 Gbit/s	Unbegrenzt
VPN	0,4 Gbit/s	1,5 Gbit/s	3,0 Gbit/s	Unbegrenzt
VPN-Nutzer	50	600	6.000	10.000
<b>CLOUD-FUNKTIONEN</b>				
Unterstützte Umgebungen	Amazon Web Services (AWS), Microsoft Azure (Nur BYOL)			
Abonnementmodelle	Bring Your Own License, On-Demand			
<b>SICHERHEITSFUNKTIONEN</b>				
Firewall	Stateful packet inspection, deep packet inspection, proxy firewall			
Anwendungsproxies	HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3, POP3S, SMTP, y IMAPS			
Angriffsschutz	DoS-Attacken, fragmentierte Pakete, komplexe Bedrohungen und vieles mehr			
Filteroptionen	Browser Safe Search, YouTube für Schulen, Google for Business			
<b>NETZWERKFUNKTIONEN</b>				
QoS	8 priority queues, DiffServ, modified strict queuing			
IP-Adresszuweisung	DHCP (client)			
NAT	Statisch, dynamisch, 1:1, IPSec traversal			
Weitere Funktionen	Statisches Routing, Port-Unabhängigkeit			
<b>VPN UND AUTHENTIFIZIERUNG</b>				
Verschlüsselung	DES, 3DES, AES 128-, 192-, 256-bit			
IPSec	SHA-2, IKE Pre-shared Key, Drittanbieterzertifikatimport, IKEv1/v2, Suite B			
Authentifizierung	RADIUS, LDAP, Windows Active Directory, RSA SecurID, interne Datenbank, SAML 2.0			
<b>MANAGEMENT</b>				
Protokollierung und Benachrichtigungen	WatchGuard, Syslog, SNMP v2/v3			
Benutzeroberflächen	Weboberfläche, skriptfähige CLI			
Reporting	WatchGuard Dimension enthält über 100 vordefinierte Berichte sowie Übersichtsdarstellungen und Visualisierungswerkzeuge.			

<sup>1</sup> Die Werte in dieser Spezifikationsübersicht gelten nur für das BYOL-Abonnementmodell.



### 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.

	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		90 Tage	365 Tage
Aufbewahrung von Reportdaten		1 Tag	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, FireboxX und Firebox Cloud.  
 \*\* Nicht erhältlich auf Firebox T20/T20-W, T25/T25-W, oder T35-R.

### VERSCHIEDENE KAUFOPTIONEN

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.

### BERATUNG UND SUPPORT DURCH EXPERTEN

Mit jedem Firebox-Modell erhalten Sie ein Startabonnement für den Support. Der in der Basic Security Suite enthaltene Standard-Support bietet technischem Support rund um die Uhr und Software-Updates. Ein Upgrade auf den Gold-Support ist Bestandteil der Total Security Suite von WatchGuard.

## 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](http://www.watchguard.de).