

## MALWARE AM WEBGATEWAY STOPPEN

Blue Coat ProxyAV™ erkennt Malware am Gateway und ist somit ein wichtiger Bestandteil der ADN-Infrastruktur (Application Delivery Network), die für umfassende Anwendungstransparenz, -beschleunigung und -sicherheit sorgt. Die ProxyAV-Appliances sind auf die Verwendung mit Blue Coat ProxySG Full Proxy-Appliances ausgerichtet und tragen so zum mehrschichtigen Sicherheitssystem von Blue Coat bei, das sowohl Schutz vor Inline-Bedrohungen als auch die Malwareprüfung von Webinhalten am Gateway umfasst. Die einzigartige High-Performance-Architektur von ProxyAV wird mit führenden Anti-Malware-Engines kombiniert, um auf effiziente Weise den Webverkehr zu sichern und Benutzer vor webbasierter Schadsoftware zu schützen. Gemeinsam bieten ProxyAV und ProxySG höchste Leistung bei minimalen Anforderungen an Hardware-Ressourcen und stellen somit eine umweltfreundliche und kostengünstige Lösung dar. Schützen Sie Ihre Benutzer und das gesamte Netzwerk vor Viren, Trojanern, Würmern, Spyware und anderen schädlichen Inhalten. Sogar Benutzer, die keine Virenschutzsoftware verwenden, sind damit in Sicherheit.

### LEISTUNGSMERKMALE

#### Inline-Bedrohungsanalyse

ProxyAV unterstützt führende Malware-Engines von Kaspersky, Sophos, Trend Micro, Panda und McAfee mit Updates im Intervall von 5 Minuten und bietet so besseren Schutz als Desktop-Virenschutzlösungen.

Die Engines zur Bedrohungserkennung umfassen Mechanismen wie den Abgleich von Signaturen mit bekannten Bedrohungen, eine Befehls- und Inhaltsverhaltensanalyse zur proaktiven Erkennung und den Emulationsmodus für die detaillierte Analyse von Skripten und ausführbaren Programmen.

Das nur von Blue Coat verwendete zeitversetzte Scannen schließt Objekte mit langer Ladedauer, wie Webradio und andere Medien, von der Threadverarbeitung aus, wodurch die Performance am Webgateway optimiert wird.

ProxyAV unterstützt vier Modi für die Inhaltsanalyse: herkömmliche Objektanalyse, Trickle-First- oder Trickle-Last-Stream-Analyse und verzögerten Scan.

Bei der Configuration von ProxyAV können Sie festlegen, ob eingehender und ausgehender Datenverkehr analysiert werden soll und

ob Dateien weitergeleitet werden sollen, wenn bei der Erkennung Fehler auftreten. Außerdem können Sie den Wert für die Zeitüberschreitung bestimmen und vertrauenswürdige Sites definieren. Für Zulassungs- und Sperrlisten können Richtlinien erstellt werden, die auf Dateierweiterungen sowie Größen- und Inhaltstypbeschränkungen basieren. Auch Warnungen und Protokolldateien sind individuell anpassbar.

#### Performance und Skalierbarkeit

ProxyAV wurde speziell für die effiziente Malware-Analyse am Gateway entwickelt. Lastverteilungs- und Clustering-Technologien erzielen eine höhere Effizienz – mit weniger Hardware als bei separaten Einzellösungen.

ProxyAV kommuniziert mit ProxySG über ICAP(S), ein standardisiertes Hochleistungsprotokoll.

#### Umfassender Scan

ProxyAV steht für erstklassige Malware-Scans – für Performance und Sicherheit.

ProxyAV kann Dateien mit einer Größe von bis zu 2 GB scannen und komprimierte Archive mit bis zu 99 Ebenen analysieren.

ProxyAV ist mit verschiedenen Clouds zur Bedrohungserkennung integrierbar, darunter Blue Coat WebPulse und Drittanbieter-Clouds. So kann der Cloud-Schutz am Gateway mehrere Anbieter umfassen.

#### ProxyAV 1400 und 2400

ProxyAV 1400 und 2400 wurden für große Unternehmen und Service Provider mit 10.000 oder mehr Benutzern entwickelt und sind 1:1 mit ProxySG 9000 integrierbar.

Integrierte Hardware-Servicefunktionen wie Montage-Gleitschienen reduzieren den Wartungszeitaufwand. Die doppelte, redundante Stromversorgung sichert hohe Verfügbarkeit.

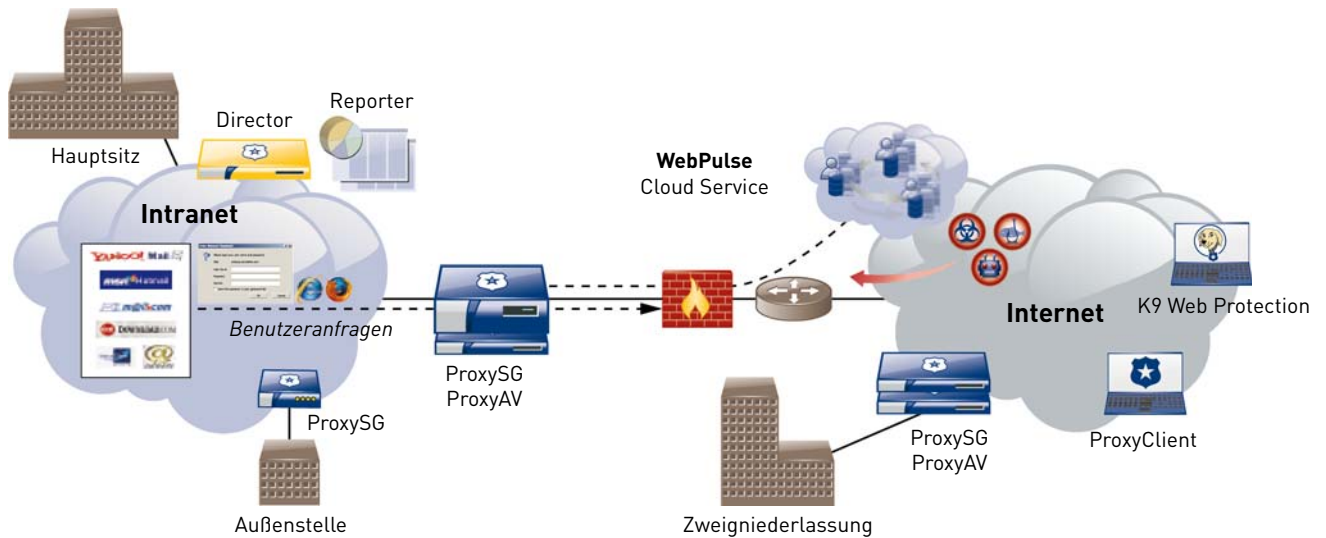
#### ProxyAV 1200

ProxyAV 1200 für die Mittelklasse fügt sich 1:1 in mittelgroße ProxySG-Plattformen ein – kostengünstig und als einheitliche Plattform, die auf einem Rack Platz findet. Dank ökonomischerem Prozessor umfasst die Lösung dieselben Hardwarefunktionen wie ProxyAV 1400.

#### Vorteile im Überblick

- > Weniger Appliances bedeuten weniger Verwaltung und Platzbedarf und letztlich einen besseren ROI.
- > Integrierter Investitionsschutz wird mit 4- oder 5-jährigen Serviceverträgen erzielt.
- > Cloud-Schutzsysteme von verschiedenen Anbietern verstärken die Malware-Analyse um zusätzliche Ebenen.
- > Sicherheit und Performance schließen einander nicht aus.





	AV1200-A	AV1400-A	AV2400-A
<b>System</b>			
Prozessoren	1 Quad-Core-CPU	1 Quad-Core-CPU	2 Quad-Core-CPU's
Laufwerke	1 x 500-GB-SATA	1 x 500-GB-SATA	1 x 500-GB-SATA
RAM	3 GB	3 GB	6 GB
Netzwerkschnittstelle	(2) integrierte 10/100/1000Base-T-Netzwerkkarten		
<b>Umgebungsbedingungen</b>			
Stromversorgung	Netzbetrieb 100-120/200-240 V~, 50/60 Hz, 6,0-3,0 A		
Max. Leistungsaufnahme	225 Watt	225 Watt	320 Watt
Wärmeleistung	325 W	325 W	375 W
Temperatur	5 °C bis 35 °C		
Luftfeuchtigkeit	Bis 90 % relative Luftfeuchtigkeit (nicht kondensierend)		
Höhe	Bis zu 3.048 m		
<b>Abmessungen und Gewicht</b>			
Gehäuse	Montierbar in 19-Zoll-Rack		
Abmessungen (L x B x H)	697 x 430 x 43 mm		
Gewicht (maximal)	16,5 kg		
<b>Technische Standards</b>			
Emissionen	FCC/CISPR 22 Klasse A, EN 55022/CISPR 22 Klasse A, IEC 61000-3-2/EN 61000-3-2, IEC 61000-3-3/EN 61000-3-3, CISPR 24/EN 55024, VCCI Klasse A Nr. 1706609, CE, BSMI, CCC, C-Tick, KCC/RRL, Dictamen		
Sicherheit	UL 60950-1, UL 94, IEC 60950-1/EN 60950-1, CSA C22.2 Nr. 950 M95, TÜV-GS, TÜV-S, BSMI, CCC, KCC/RRL, Dictamen		
Normen	UL/CSA, TÜV-GS, TÜV-S, BSMI, C-Tick, KCC, CCC, CE, GOST-R		
<b>Gewährleistung</b>	Es besteht für ein (1) Jahr ab Versanddatum eine beschränkte Gewährleistung, die nicht übertragbar ist. BlueTouch Support-Verträge für Software-Support rund um die Uhr und Optionen für Hardware-Support separat erhältlich.		