PRODUCT USE RIGHTS SUPPLEMENT

FOR SYMANTEC NETWORK PROTECTION PRODUCTS (FORMERLY BLUE COAT)

This Product Use Rights Supplement ("Supplement") contains additional terms and conditions for the Licensed Software licensed under the Symantec License Agreement (or other manually or digitally signed agreement that references a "Product Use Rights Supplement") between Symantec Corporation and/or its affiliates and You as the individual, the company, or the legal entity that will be utilizing the Licensed Software (referenced below as "You" or "Your") (the "Symantec License Agreement"). The Symantec License Agreement and the Supplement are collectively referred to herein as the "License Agreement." Capitalized terms used in this Supplement but not defined herein will have the meanings given in the Symantec License Agreement. To the extent there is a conflict between the terms and conditions of the Symantec License Agreement and this Supplement, the terms and conditions of this Supplement will take precedence.

BY DOWNLOADING, INSTALLING OR USING THE LICENSED PRODUCTS, YOU AGREE TO COMPLY WITH THE PRODUCT USE RIGHTS IN THIS SUPPLEMENT, IN ADDITION TO THE TERMS AND CONDITIONS OF THE SYMANTEC LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE PRODUCT USE RIGHTS APPLICABLE TO THE LICENSED PRODUCTS, DO NOT DOWNLOAD, INSTALL OR USE THE LICENSED PRODUCTS.

For purposes of this Supplement, the Licensed Products are: See list set forth on Exhibit A.

1.   USE RIGHTS AND LIMITATIONS.

The applicable usage rights, restrictions, and terms are set forth in Exhibit B unless different terms are indicated in Exhibit A. In addition, an agreement other than the Symantec License Agreement may apply, as indicated in Exhibit A. In the event of a conflict between the usage rights, restrictions, and terms set forth in Exhibit B and a product-specific Product Use Rights Supplement or Service Description (each as available at: https://www.symantec.com/about/legal/repository), the product-specific Product Use Rights Supplement or Service Description shall govern.

2.   ADDITIONAL TERMS AND CONDITIONS.

Additional terms and conditions that may apply to the Licensed Products are available at: https://www.symantec.com/content/dam/symantec/docs/eulas/third-party-notice/blue-coat-products-third-party-en.pdf

In addition, the Licensed Products may come with or include files or documents containing additional terms and conditions, including separate hardware warranties.

Exhibit A

Symantec Network Protection Products
(formerly Blue Coat)

Product/Service	Usage Rights and Restrictions
Advanced Secure Gateway (ASG)	See Product Use Guide attached as Exhibit B.
CacheFlow	See Product Use Guide attached as Exhibit B.
Cloud Data Protection (CDP)	See Product Use Guide attached as Exhibit B.
Cloud Services	See Legal Repository https://www.symantec.com/about/legal/repository for applicable Service Agreement and Service Description for CloudSOC (CASB) and Web Security Service. For all other cloud services, please see Product Use Guide attached as Exhibit B.
CloudSOC (CASB) (formerly Elastica) - CloudSOC Audit - CloudSOC CASB for IaaS (formerly CloudSOC Security for IaaS) - CloudSOC CASB for SaaS (formerly CloudSOC Security for SaaS) - CloudSOC CASB Gateway - CloudSOC SpanVA - CloudSOC Reach Agent	See Legal Repository https://www.symantec.com/about/legal/repository for applicable Service Agreement and Service Description.
Content Analysis	See Product Use Guide attached as Exhibit B.
Data Loss Protection (DLP) (formerly Blue Coat)	See Product Use Guide attached as Exhibit B.
Director	See Product Use Guide attached as Exhibit B.
Hosted Reporting services	See Product Use Guide attached as Exhibit B.
Industrial Control Systems Protection (ICSP)	See Product Use Guide attached as Exhibit B.
IntelligenceCenter	See Product Use Guide attached as Exhibit B.
MACH5 VA	See Product Use Guide attached as Exhibit B.
Mail Threat Defense	See Product Use Guide attached as Exhibit B.
Malware Analysis	See Product Use Guide attached as Exhibit B.
Management Center (MC)	See Product Use Guide attached as Exhibit B.
Mobile Device Security (MDS)	See Product Use Guide attached as Exhibit B.
PacketShaper	See Product Use Guide attached as Exhibit B.

PolicyCenter	See Product Use Guide attached as Exhibit B.
ProxyAV	See Product Use Guide attached as Exhibit B.
ProxySG	See Product Use Guide attached as Exhibit B.
Reporter 10.x	See Product Use Guide attached as Exhibit B.
Reporter 9.x	See Product Use Guide attached as Exhibit B.
Reverse Proxy	See Legal Repository https://www.symantec.com/about/legal/repository for applicable agreement(s) and Product Use Rights Supplement.
Secure Web Gateway Virtual Appliance	See Product Use Guide attached as Exhibit B.
Security Analytics	See Product Use Guide attached as Exhibit B.
Security Analytics Central Manager	See Product Use Guide attached as Exhibit B.
SSL Visibility	See Product Use Guide attached as Exhibit B.
Web Security Service	See Legal Repository https://www.symantec.com/about/legal/repository for applicable Service Agreement and Service Description.
X-Series	See Product Use Guide attached as Exhibit B.
X-Series Management System (XMS)	See Product Use Guide attached as Exhibit B.

Exhibit B

Product Use Guide – Product-Specific Usage Rights and Restrictions
February 10, 2016

Blue Coat Systems, Inc.

Product Use Guide –

Product-Specific Usage Rights and Restrictions

This Use Guide includes and replaces Use Guides and Use Guide Addenda prior to the release date.

Released: 10 February 2016

Table of Contents

Blue Coat Product Usage Rights & Restrictions

General Comments

Subscription Software with Loaned Hardware. Some physical appliances (e.g. some CacheFlow appliances) may be available under a subscription software license with loaned hardware. At the end of the subscription term, customer must renew its subscription. Upon expiration or termination of the subscription, the customer's right to use the appliance terminates, and customer shall return the physical appliance and software thereon promptly upon request.

Subscriptions purchased on a term basis. Standard support is included as part of a subscription. For clarification, but without limitation, if a customer's usage (such as number of users) increases in the middle of a subscription term, the customer must purchase subscription(s) for the additional usage. At the end of the subscription term, customer must renew its subscription. If a subscription expires, services may cease to function or lose functionality, depending on the applicable subscription.

The customer is responsible for supplying the hardware for standalone software and virtual appliances.

Common Definitions and Terms

"Instance" means an instance of software created by executing the software's setup or install procedure or by duplicating an existing Instance. To "run an Instance" means to load an Instance of the software into memory and execute one or more of its instructions. Once running, an "Instance" is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.

Use of Blue Coat Product Data

Blue Coat data services and data feeds are licensed content and are restricted for use only with Blue Coat products and services.

Any attempt to extract, mine or reconstruct this licensed content is strictly prohibited.

Blue Coat's enrichment, including but not limited to application classifications, URL categories, risk levels, risk factors and other analysis of data generated from customer traffic is proprietary to Blue Coat ("Proprietary Data") and may not be shared, extracted or reconstructed for non-end-customer use or commercial purposes. Proprietary Data may not be disclosed to any third party except solely in furtherance of customer's internal purposes, and then only to the extent necessary to fulfill the stated internal purpose, with no other rights granted to such third party.

ProxySG

The ProxySG is an appliance ("ProxySG") sold with a perpetual software license. The ProxySG is available as either MACH5 Edition or Proxy Edition. The Proxy Edition includes the MACH5 capabilities, with additional functionality. Certain ProxySG models (SG-S200-10, SG-S200-20, SG-S200-30, SG300-5, SG300-10, SG600-10, SG600-20, SG900-10, SG900-10B, SG900-20, SG510-5, SG510-10, SG510-20, SG810-5, SG810-10, SG810-20) are restricted by maximum concurrent client IP addresses as set forth in the product descriptions. For these platforms, when the maximum number of client IPs is reached, the appliance will (depending on the user configuration) either bypass new connections or queue new connections for later handling. The platforms not specifically listed above will not cap the number of client IPs, but will process traffic from devices until the appliance exhausts available resources.

Several optional add-on features are licensed separately for additional fees. The following options are for use only on the specific ProxySG for which the option is licensed unless otherwise noted.

- Blue Coat WebFilter (BCWF). BCWF is available as either a perpetual or a subscription license as set forth below. Both license types are granted on a per user basis (or under certain circumstances, licensed specifically to a physical Proxy Edition appliance model). BCWF may be used for no more than the licensed number of BCWF users (or specific appliance for which the license applies). A user means, for purposes of BCWF, any end user that may access (through any number of devices such as a mobile device and desktop), at any time, the Internet via one or more ProxySG or SWG VAs that utilizes BCWF. End users without Internet access need not be counted. BCWF per user licenses for ProxySG may be used on one or more licensed Blue Coat Proxy Edition appliances provided that usage is in compliance with the above user restriction (BCWF is not available on the ProxySG MACH5 Edition).
    - o A perpetual license provides a one-time download of the BCWF database on the ProxySG, but this license does not allow database updates or use of Blue Coat's WebPulse service. Database updates and dynamic ratings using Blue Coat WebPulse service require a valid BCWF support contract in addition to the BCWF perpetual license.
    - o Subscription licenses are for the applicable term and must be renewed prior to expiration of the term for continuous service.
- Blue Coat Intelligence Services (IS). IS are a family of data services, each sold with a subscription license as set forth below. IS may be used for no more than the number of IS users for that service. A user means, for purposes of IS, any end user that may access (through any number of devices such as a mobile device and desktop), at any time, the Internet via one or more ProxySG, ASG or SWG VA that utilizes IS. End users without Internet access need not be counted. IS per user licenses for ProxySG may be used on one or more licensed Blue Coat Proxy Edition appliances provided that usage is in compliance with the above user restriction (IS are not currently available on the ProxySG MACH5 Edition).
    - o Subscription licenses are for the applicable term and must be renewed prior to expiration of the term for continuous service.
- Flash Capability Option. The Flash option, offered with a perpetual license, enables the ProxySG to control, cache and/or split Adobe Flash RTMP, RTMPT, and encrypted RTMP/T traffic.
- Encrypted Tap. The Encrypted Tap option, offered with a perpetual license, enables the ProxySG to process encrypted traffic and output the decrypted content for inspection by separately-purchased external system(s). Encrypted Tap is not available on the ProxySG MACH5 Edition.
- CachePulse. The CachePulse option, offered on a subscription basis for a specific term, provides caching rules and instruction updates. The CachePulse updates require that the ProxySG appliance has a valid support contract in addition to a CachePulse subscription license.
- Web Applications Protections (WAP). WAP, offered on a subscription basis for a specific term, allows

the ProxySG to automatically utilize updated signatures, rules and data for the purposes of securing and protecting web application and content servers from direct Internet threats. WAP is not available on the ProxySG MACH5 Edition. WAP updates require that the ProxySG appliance has a valid support contract in addition to a WAP subscription license.

Secure Web Gateway Virtual Appliance

The Secure Web Gateway Virtual Appliance (SWG VA) is sold with a subscription license for the applicable term. SWG VA is licensed based on maximum concurrent client IP addresses. A SWG VA may not be used for more than the number of concurrent client IP addresses for which the subscription has been purchased, and only one Instance of SWG VA may be run per subscription license. When the maximum number of client IP addresses is reached, the virtual appliance will (depending on the user configuration) either bypass new connections or queue new connections for later handling. Unlike the Proxy Edition of ProxySG, the SWG VA does not contain some Proxy Edition (MACH5) optimization features and cannot be upgraded to Proxy Edition. BCWF is included as part of a SWG VA subscription during the applicable SWG VA subscription term for use only on the applicable SWG VA.

Several optional add-on features are licensed separately for additional fees. The following options are for use only on the specific SWG VA for which the option is licensed.

- Flash Capability Option. The Flash option, offered on a subscription basis for a specific term, enables the SWG VA to control, cache and/or split Adobe Flash RTMP, RTMPT, and encrypted RTMP/T traffic.
- Encrypted Tap. The Encrypted Tap option, offered with a perpetual license, enables the SWG VA to process encrypted traffic and output the decrypted content for inspection by separately-purchased external system(s).
- CachePulse. The CachePulse option, offered as a subscription basis for a specific term, provides caching rules and instruction updates.
- Web Applications Protections (WAP), offered on a subscription basis for specific term, allows the SWG VA to automatically utilize updated signatures, rules and data for the purposes of securing and protecting web application and content servers from direct Internet threats.
- Blue Coat Intelligence Services (IS). IS are a family of data services, each licensed as set forth below. IS services are licensed specifically to a virtual appliance (or under certain circumstances, licensed on a per user basis). IS may be used for no more than the number of licensed virtual appliances or number of IS users for that service. A user means, for purposes of IS, any end user that may access (through any number of devices such as a mobile device and desktop), at any time, the Internet via one or more ProxySG, ASG or SWG VA that utilizes IS. End users without Internet access need not be counted. If available, IS per user licenses for SWG VA may be used on one or more licensed appliances provided that usage is in compliance with the above user restriction.
  - o Subscription licenses are for the applicable term and must be renewed prior to expiration of the term for continuous service.

MACH5 VA

The MACH5 virtual appliance (M5 VA) is sold with a subscription license for the applicable term.
M5 VA is licensed based on maximum concurrent client IP addresses. An M5 VA may not be used for more than the number of concurrent client IP addresses for which the subscription has been purchased, and only one Instance of MACH5 may be run per subscription. When the maximum number of client IP addresses is reached, the appliance will (depending on the user configuration) either bypass new connections or queue new connections for later handling. Unlike the MACH5 Edition of ProxySG, the M5 VA is not upgradeable to Proxy Edition or Secure Web Gateway VA.

The following optional add-on features are licensed separately for additional fees. The following options are for use only on the specific MACH5VA for which the option is licensed.
- Flash Capability Option. The Flash option, offered on a subscription basis for a specific term, enables the proxy to control, cache and/or split Adobe Flash RTMP, RTMPT, and encrypted RTMP/T traffic.
- CachePulse. The CachePulse option, offered on a subscription basis for a specific term, provides caching rules and instruction updates.

Advanced Secure Gateway (ASG)
The Advanced Secure Gateway (ASG) is sold as a physical appliance with a perpetual software license. ASGs are restricted by maximum concurrent client IP addresses as set forth in the purchased license. When the maximum number of client IPs is reached, the appliance will (depending on the user configuration) either bypass new connections or queue new connections for later handling. The highest sold level of each platform (e.g., ASG-S400) will not cap the number of client IPs, but will process traffic from devices until the appliance exhausts available resources.

Several optional add-on features are also available for additional fees. The following options are for use only on the specific licensed ASG for which the option is purchased unless otherwise noted.
- ASG appliances come with software with the capability to run on-box Content Analysis functions. Content Analysis requires a separately purchased applicable File Inspection subscription to provide the additional Content Analysis on-box functionality. A File Inspection subscription (designed to provide virus protection and file whitelisting functionality) provides updates to pattern files containing information to identify viruses or malicious software and is sold on a per user basis. File Inspection subscriptions may not be used for more than the number of users for which the subscription has been purchased. A user means, for purposes of File Inspection, any person that may access the internet via one or more Blue Coat gateway devices (such as ProxySGs, SWG VAs and/or ASGs) that are configured to utilize any File Inspection functionality. End users without Internet access need not be counted. If a File Inspection subscription expires or terminates, services will cease to update and the File Inspection functionality will be lost. Content Analysis includes the capability to direct files to off-box sandbox technologies but such technologies must be separately purchased and are subject to additional restrictions.
- Blue Coat WebFilter (BCWF). BCWF is sold with either a perpetual or a subscription license as set forth below. Both license types are granted on a per user basis (or under certain circumstances, licensed specifically to a physical Proxy Edition appliance model). BCWF may be used for no more than the licensed number of BCWF users (or specific appliance for which the license applies). A user means, for purposes of BCWF, any end user that may access (through any number of devices such as a mobile device and desktop), at any time, the Internet via one or more ASG, ProxySG or SWG VAs that utilizes BCWF. End users without Internet access need not be counted. BCWF per user licenses for ProxySG may be used on one or more licensed Blue Coat Proxy Edition, ASG or SWG VA appliances provided that usage is in compliance with the above user restriction.
  - o A perpetual license provides a one-time download of the BCWF database on the ProxySG,

but this license does not allow database updates or use of Blue Coat's WebPulse service. Database updates and dynamic ratings using Blue Coat WebPulse service require a valid BCWF support contract in addition to a BCWF perpetual license.

- o Subscription licenses are for the applicable term and must be renewed prior to expiration of the term for continuous service.

- Blue Coat Intelligence Services (IS). IS are a family of data services, each sold with a subscription license as set forth below. IS may be used for no more than the number of IS users for that service. A user means, for purposes of IS, any end user that may access (through any number of devices such as a mobile device and desktop), at any time, the Internet via one or more ASG, ProxySG or SWG VA that utilizes IS. End users without Internet access need not be counted. IS per user licenses for ASG, ProxySG, or SWG VA may be used on one or more licensed appliances provided that usage is in compliance with the above user restriction.

  - o Subscription licenses are for the applicable term and must be renewed prior to expiration of the term for continuous service.

- Flash Capability Option. The Flash option, offered with a perpetual license, enables the ASG to control, cache and/or split Adobe Flash RTMP, RTMPT, and encrypted RTMP/T traffic.

- Encrypted Tap. The Encrypted Tap option, offered with a perpetual license, enables the ASG to process encrypted traffic and output the decrypted content for inspection by separately-purchased external system(s).

- CachePulse. The CachePulse option, offered on a subscription basis for a specific term, provides caching rules and instruction updates. The CachePulse updates require that the ASG appliance has a valid support contract in addition to a CachePulse subscription license.

Data Loss Protection (DLP)

DLP is an appliance sold with a perpetual software license. The DLP appliance requires a Network DLP and/or Discovery DLP license. Network DLP (designed to inspect and apply policy on network communications such as HTTP, FTP, SMTP and Webmail) and Discovery DLP (designed to scan workstations and file services for sensitive data) are each sold on a subscription per user basis. Network DLP and Discovery DLP may not be used for more than the number of users for which the subscription has been purchased. For Network and Discovery DLP purposes only, a user means any unique log-in ID (employees, contractors, guests, etc.).

Cloud Services

Blue Coat offers multiple cloud services, such as the Web Security Service (WSS), Mobile Device Security (MDS), and Hosted Reporting services, subject to the terms and conditions set forth in the separate Cloud Services Agreement.

ProxyAV

ProxyAV is an appliance sold with a perpetual software license. ProxyAV requires a separately purchased anti-virus (AV) subscription to function. AV subscriptions include updates to pattern files containing information to identify viruses or malicious software. A ProxyAV (and the applicable AV subscription) may be used for no more than the number of users for which the subscription has been purchased. A user means, for purposes of ProxyAV, any person that may access the Internet via one or more ProxySG(s) that are configured to send traffic to the applicable ProxyAV appliance for services. If a subscription expires or terminates, services will cease to update on the ProxyAV appliance.

Content Analysis

Content Analysis (CA) is sold as a physical appliance or as a virtual appliance (CA VA). The CA physical appliance is sold with a perpetual software license. The CA VA is licensed on either a perpetual or subscription basis.
CA requires a separately purchased File Inspection (FI) subscription to function. A File Inspection subscription (designed to provide virus protection and file reputation functionality) provides updates to pattern files containing information to identify viruses or malicious software as well as known good files. A CA appliance (and applicable subscription) may not be used for more than the number of users for which the subscription has been purchased. A user means, for purposes of CA, any person that may access the Internet where such person's traffic is sent through the applicable CA appliance for services. If an FI subscription expires or terminates, services will cease to update on the CA appliance.
CA includes the capability to direct files to other products but such technologies must be separately purchased and are subject to additional restrictions.

Mail Threat Defense
Mail Threat Defense (MTD) is sold as a physical appliance or as a virtual appliance (MTD VA). The MTD physical appliance is sold with a perpetual software license. The MTD VA is licensed on either a perpetual or subscription basis.
A MTD appliance may not be used for more than the number of e-mails per day (24 hour period) for which the appliance has been purchased. E-mail means, for purposes of MTD, the SMTP messages distributed by electronic means from one computer user to one or more recipients via a network and scanned by MTD. E-mail not scanned by MTD need not be counted by MTD licensing.
MTD requires a separately purchased Email Inspection (EI) subscription to function. An Email Inspection subscription (designed to provide virus protection and file reputation functionality) provides updates to pattern files containing information to identify viruses or malicious software as well as known good files. EI may not be used for more than the number of users for which the EI subscription has been purchased. A user means, for purposes of EI, any person that may access email via an email service that is protected/scanned via MTD. If an EI subscription expires or terminates, services will cease to update on the MTD appliance.

MTD includes the capability to direct files to other products but such technologies must be separately purchased and are subject to additional restrictions.

Malware Analysis

The Malware Analysis (MA) is sold as an appliance with a perpetual software license. MA requires a separately purchased MA Content Subscription license to function. MA Content Subscription is licensed per specific MA appliance and requires that the MA appliance have a valid support contract.

As part of its functionality, third party applications can also be installed on a VM profile on the MA. Blue Coat provides third party applications as detailed in the Section Appendix below with full redistributable rights provided. Except for the applications and versions described below, the user is solely responsible for procuring and licensing properly any third party applications.

The MA appliance is provided with a Microsoft Product Identifier Card that includes Microsoft Certificates of Authenticity (COAs), with the COAs provided based on the customer's representation to Blue Coat as to whether or not it has in place a valid Microsoft Volume Licensing Agreement that includes Software Assurance.

For customers purchasing the Blue Coat Malware Analysis appliance with a valid Microsoft Volume Licensing Agreement that includes Software Assurance
User must have a valid Microsoft Volume Licensing agreement and must purchase Software Assurance for each COA provided.
The user is licensed to use any combination of the following Microsoft Windows Operating System products running in simultaneous Instances, provided that in no event may the number of simultaneously running Instances exceed the number of COAs provided on the Microsoft Product Identifier Card.

- Microsoft® Windows® XP Professional for Embedded Systems ESD (Virtualization Only)
- Windows® 7 Professional for Embedded Systems ESD (Virtualization Only)
- Windows® Embedded 8 Pro ESD (Virtualization Only)

For customers purchasing the Blue Coat Malware Analysis appliance without a valid Microsoft Volume Licensing Agreement that includes Software Assurance
If the user is not party to a valid Microsoft Volume Licensing agreement that includes Software Assurance, the COAs provided on the Microsoft Product Identifier card will be product-specific, with the same number of COAs provided for each available product. In this case, the user is licensed to use any combination of Microsoft Windows Operating System products running in simultaneous Instances, provided that in no event may the number of simultaneously running Instances exceed a number equal to the number of COAs provided for each relevant product. (That is, if, for example, the Microsoft Product Identifier card shipped with the product includes 12 COAs for Windows XP Professional and 12 COAs for Windows 7 Professional, the product may run up to 12 total Instances of any combination of products).

For these purposes, the following definitions apply:
- "Operating System Environment" or "OSE" means all or part of an operating system Instance, or all or part of a virtual (or otherwise emulated) operating system Instance which enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and instances of applications, if any, configured to run on the operating system Instance or parts identified above. There are two types of OSEs, physical and virtual. A physical hardware system can have one Physical OSE and/or one or more Virtual OSEs.
- "Physical OSE" means an OSE that is configured to run directly on a physical hardware system. The operating system Instance used to run hardware virtualization software (e.g. Microsoft Hyper-V or

similar third-party technologies) or to provide hardware virtualization services (e.g. Microsoft virtualization technology or similar third-party technologies) is considered part of the Physical OSE.

- "Virtual OSE" means an OSE that is configured to run on a virtual hardware system.

Section Appendix

Windows Embedded Desktop Operating System Products

Licensed Product Name and Version

- Microsoft® Windows® XP Professional for Embedded Systems ESD (Virtualization Only)
- Microsoft® Windows® XP Professional 64 Bit Edition for Embedded Systems ESD (Virtualization Only)
- Windows® Vista Business for Embedded Systems ESD (Virtualization Only)
- Windows® Vista Ultimate for Embedded Systems ESD (Virtualization Only)
- Windows® 7 Professional for Embedded Systems ESD (Virtualization Only)
- Windows® 7 Ultimate for Embedded Systems ESD (Virtualization Only)
- Windows® Embedded 8 Pro ESD (Virtualization Only)

Office Viewer Products

Licensed Product Name and Version

- Microsoft Office 2007 Viewers – Word, PowerPoint, Excel

PacketShaper

The PacketShaper is an appliance sold with a perpetual software license. Depending on the platform, the options, requirements and restrictions vary.

Without any separately-purchased options, the PacketShaper 900, PacketShaper 1700, PacketShaper 3500, PacketShaper 7500, PacketShaper 10000 and PacketShaper 12000 appliances run in monitor only mode. In this mode, the PacketShaper only provides visibility functionality. Additional functionality is available for additional fees. The following options are for use only on the specific PacketShaper for which the option is purchased.

- Shaping Keys provide Quality of Service (QoS) and packet shaping. Shaping is licensed per appliance by the throughput managed. For example, if a customer wants to manage a 10 Mbps WAN link they would purchase a 10M Shaping license that may manage 10 Mbps inbound and 10 Mbps outbound or 20 Mbps of total bandwidth.
- Compression Keys allows the PacketShaper to compress traffic on the customer's network and is licensed per appliance.
- The PacketShaper 12000 offers an "ISP 10000" option allowing the creation and use of up to 10,000 classes when using the ISP build of software. Without this license the system will limit to 5,000 classes with the ISP build or 2048 when running the standard build.
- WebPulse Services. WebPulse Services query Blue Coat's WebPulse cloud service for URL category and web application classification information. Currently, use of WebPulse services on a PacketShaper requires a valid support contract for the specific PacketShaper. The PacketShaper must be able to regularly query Blue Coat's support servers to verify entitlement. If the system is unable to confirm a valid support contract within any 30 day (24 hours per day) period the PacketShaper will cease to query for URL categories and applications until an entitlement check returns the presence of a valid support contract. In the future, WebPulse functionality on PacketShaper may require a separate subscription license.

The PacketShaper S500, S400 and S200 (PS-S500, PS-S400, PS-S200) require a separately purchased Shaping license to function (unlike other PacketShapers which have monitor only option). Shaping is licensed per appliance by the throughput managed. For example, if a customer wants to manage a 5 Gbps WAN link they would purchase a 5G Shaping license that can manage up to 5 Gbps inbound bandwidth and 5 Gbps outbound bandwidth. Increasing the licensed bandwidth also increases certain other specifications of the unit including dynamic partitions as well as managed hosts and flows.

The following optional add-on feature may be available and licensed separately for the PS-S500, S400 and S200. The option is for use only on the specific PacketShaper for which the option is licensed.

- WebPulse Services. WebPulse Services query Blue Coat's WebPulse cloud service for URL category and web application classification information. Currently, use of WebPulse services on a PacketShaper requires a valid support contract for the specific PacketShaper.

Notes: the PS-S500, PS-S400 and PS-S200 do not offer compression options or varying class levels.

SSL Visibility

SSL Visibility is an appliance sold with a perpetual software license.

- Host Categorization is an optional add-on that allows customers to set policies based on host category. Host Categorization is a separately licensed subscription per specific SSL Visibility appliance. Host Categorization requires that the SSL Visibility appliance has a valid support contract.

CacheFlow

CacheFlow is an appliance sold with a perpetual software license. The following options are available for CacheFlow appliances.

- Blue Coat WebFilter (BCWF). BCWF is available as a perpetual license as set forth below. Licenses are granted on a per user basis (or under certain circumstances, licensed specifically to a physical CacheFlow appliance model). BCWF may be used for no more than the licensed number of BCWF users (or specific appliance for which the license applies). A user means, for purposes of BCWF, any end user that may access (through any number of devices such as a mobile device and desktop), at any time, the Internet via one or more CacheFlow(s) that use BCWF. End users without Internet access need not be counted. BCWF per user licenses for CacheFlow may be used on one or more licensed CacheFlow appliances provided that usage is in compliance with the above user restriction. This license is offered for a one-time download of the BCWF database on the CacheFlow device, but this license does not allow database updates or use of Blue Coat's WebPulse service. Database updates require a valid BCWF support contract.
- CachePulse. The CachePulse service provides caching rules and instruction updates. CachePulse service is provided for the CacheFlow appliance with a valid support contract for such appliance.

Other CacheFlow Notes: CacheFlow appliances are configured to send information consisting of aggregated statistics to Blue Coat. This functionality cannot be disabled. Such information includes, but is not limited to, basic network configuration for each network interface; bandwidth used by HTTP services; HTTP request/response attributes (e.g. cacheable, non-cacheable, non-cacheable reasons); operation of the object cache (per-disk and overall); raw system resources such as: per-cpu usage and memory pressure, and calculated resources such as: resource load, bandwidth savings; hardware diagnostics reporting (disks, memory, networks interfaces, and power supply); and CachePulse feedback consisting of domain popularity and caching effectiveness. Blue Coat will also collect health information for appliances that are currently or was recently in a 'Warning' or 'Critical' state.

If BCWF is enabled, a summary containing content filter configuration details (including the database provider, last upload time, and services in use) is included. Following a reboot of the appliance, the following information will also be sent to Blue Coat: the reason for the restart; software traceback information, in case of an unexpected software crash (this data allows for preliminary software crash analysis, before a more detailed (and larger) context core file is uploaded to Blue Coat); core image summary, specifically detailing the number of core images on the appliance.

Security Analytics

Security Analytics (SA) is sold as a physical or virtual appliance or as standalone software. Physical appliances are sold with a perpetual software license. Software and Virtual Appliances are licensed on either a perpetual or subscription basis.

Several optional add-on features are licensed separately for additional fees. The following options are for use only on the specific Security Analytics platform instance for which the option is licensed.

- Retention. Security Analytics includes a base amount of indexed data retention. Retention defines the amount of aggregate metadata and packet storage data a Security Analytics appliance will be able to address and is enforced in the system. Additional storage expansion licenses must be purchased to increase retention. Storage devices purchased from Blue Coat require the purchase of a storage expansion license unless the product description clearly indicates that a storage expansion license is included. Storage purchased from a third-party always requires the purchase of a storage expansion license in order to be used with SA.

- Intelligence Services for Security Analytics (IS for SA). Formerly called ThreatBLADES, a data subscription providing real time updates to threat intelligence used by Security Analytics. Subscriptions allow access to the applicable threat intelligence service for the subscription term. Data subscriptions are available in two forms:
    - o Intelligence Services for Security Analytics. Intelligence Services subscriptions provide all threat intelligence required for a single instance of a Security Analytics platform across all ports and protocols. IS for SA is licensed per specific SA appliance or software and requires that the SA appliance or software have a valid support contract.
    - o ThreatBLADE Subscription. Per user, per protocol ThreatBLADE subscriptions may not be used for more than the number of users for which subscriptions have been purchased. For purposes of ThreatBLADES, a "user" means any person that may have their activity recorded, at any time during the subscription period, in the Security Analytics platform(s).
        - ▪ WebThreat BLADE provides URL category information as well as file information for content traversing Web protocols, i.e., HTTP and decrypted HTTPS.
        - ▪ FileThreat BLADE provides file information for content traversing File Transfer protocols, e.g., FTP, tFTP, NFS, SMB.
        - ▪ MailThreat BLADE provides URL category information as well as file information for content traversing the E-Mail protocols, e.g., SMTP, POP3 and IMAP.
    - o ThreatBLADE updates require a valid support contract for all Security Analytics appliances or software.

Security Analytics Central Manager

The Security Analytics Central Manager is sold as a physical or virtual appliance or as standalone software. Physical appliances are sold with a perpetual software license. Software and Virtual Appliances are licensed on either a perpetual or subscription basis.

X-Series

- The X-Series system consists of a chassis and separately purchased hardware modules and hardware accessories. The minimum X-Series configuration for a functioning system requires the purchase of at least one of each of the following modules which are offered on a perpetual basis for use on an X-Series chassis: Application Processor Module (APM). APMs provide the capability to run applications on the X-Series chassis. X-Series systems require at least one APM. APMs run additional software applications from third parties (such as Checkpoint, Imperva, Cisco (Sourcefire) or McAfee) that must be separately licensed from the applicable third party and have separate license restrictions.
- Network Processor Module (NPM). NPMs provide network connectivity to the external network and within the X-Series system. X-Series systems require at least one NPM.
- Control Processor Module (CPM). CPMs provide a variety of controls the X-Series system. X-Series systems require at least one CPM.

In addition, the following option is licensed separately for an additional fee and is used only on the specific X-Series for which the option is licensed.

- X-Series Routing Software (RSW). The RSW application is licensed on a perpetual basis and is a set of dynamic routing protocol features that can be applied to an X-Series system. RSW may only be used on a single X-Series system. An additional RSW license must be purchased for each X-Series system on which the RSW will run.

X-Series Management System (XMS)

The X-Series Management System (XMS) is software offered with a perpetual license for managing X-Series systems. Customers may not run more than one Instance of XMS for each XMS license purchased. XMS may be used to manage no more than the number of X-Series systems for which licenses(s) have been purchased.

Management Center (MC)

Management Center (MC) is available as a physical appliance or as a virtual appliance (MC VA). The MC physical appliance is sold with a perpetual software license. The MC VA is licensed on either a perpetual or subscription basis. Licensing for both platforms is based on the number of Target Assets. A Target Asset is defined as anything that can be registered as a distinct, single, manageable component in MC.

An MC appliance or MC VA may be used to manage no more than the number of Target Assets purchased or licensed. These may include Blue Coat products of various types (for example: VAs, appliances, licensed software, services, SaaS or cloud licenses), and specific functionality in multi-product bundles or systems (each treated as a distinct asset) or other manageable components (for example, sensors, enforcement points or collectors).

Only one Instance of MC VA may be run per license.

Reporter 10.x

Reporter is sold as a physical appliance or as a virtual appliance (Reporter VA). The Reporter physical appliance is sold with a perpetual software license. The Reporter VA is licensed on either a perpetual or subscription basis. Licensing for both platforms is based on the maximum number of terabytes (TBs) allowed for storing logs or other metadata by the Reporter.
Customers may not run more than one Instance of Reporter for each Reporter license purchased.

Reporter 9.x

Reporter 9.x is software sold with a perpetual license for reporting on access logs from other Blue Coat appliances (e.g., ProxySG). Reporter has three versions with different licensing restrictions:
- Standard Edition. Reporter Standard Edition is available without an additional fee with a valid ProxySG support contract and may not be used to report on more than 50 million log lines.
- Enterprise Edition. Reporter Enterprise Edition may not be used to report on more than 2.5 billion log lines and has a perpetual software license.
- Premium Edition. Reporter Premium Edition may not be used to report on more than 20 billion log lines and has a perpetual software license.

Customers may not run more than one Instance of Reporter for each Reporter purchased.

Director

Director is sold as a physical or virtual appliance, with a perpetual software license (for both the physical and virtual appliance), for managing ProxySGs, MACH5 VAs and/or SWG VAs. Director may only be used to manage a maximum of 300 (physical and/or virtual) appliances at any time. Only one Instance of Director virtual appliance may be run per license.

IntelligenceCenter

IntelligenceCenter (IC) is software sold with a perpetual license for reporting on PacketShapers. The IC base license includes the IC application and a single Data Collector. With the base license, a customer may report on only a single device. Only one Instance of IC may be run per license.
- Additional Devices. Additional device upgrade license(s) must be purchased to report on additional devices. Device upgrade licenses require a base license. The number of devices configured to be reported on by IC may not exceed the number of devices for which license fees have been paid.
- Data Collector (DC). Additional DC licenses are required to collect data in more than one database. A customer may run no more than one Instance of DC per DC license.

PolicyCenter

PolicyCenter (PC) is software sold with a perpetual license for managing PacketShapers. With the PC base license, a customer may manage only a single device. A customer may run no more than one Instance of PC per base license.
- Additional Devices. Additional device upgrade license(s) must be purchased to manage additional devices. Device upgrade licenses require a base license. The number of devices configured to be managed by a PC may not exceed the number of devices for which license fees have been paid.

Cloud Data Protection (CDP)

Cloud Data Protection (CDP) is software sold with a subscription license. CDP is offered for multiple cloud applications, each licensed separately.
- Cloud Data Protection for Salesforce. CDP for Salesforce may be used for no more than the number of Salesforce users purchased for CDP functionality. A Salesforce user means, for purposes of CDP for Salesforce,--a Salesforce Professional Edition, Enterprise Edition, or Unlimited Edition user as licensed from Salesforce.com. CDP for Salesforce users may not necessarily be purchased to the customer's total count of Salesforce users.
- Cloud Data Protection for ServiceNow. CDP for ServiceNow may be used for no more than the number of ServiceNow users purchased for CDP functionality. A ServiceNow user means, for purposes of CDP for ServiceNow, a requestor, approver or fulfiller user as licensed by ServiceNow-. CDP for ServiceNow users may not necessarily be purchased to the customer's total count of ServiceNow users.
- Cloud Data Protection for Yammer. CDP for Yammer may be used for no more than the number of

Yammer users purchased for CDP functionality. A Yammer user means, for purposes of CDP for Yammer,-a Yammer Enterprise user license, activated as part of a Microsoft Office 365 Enterprise, Office 365 Education, Office 365 Nonprofit, SharePoint Online + Yammer Enterprise, Yammer Enterprise Standalone, Enterprise Cloud Suite or Power BI plan. CDP for Yammer users may not necessarily be purchased to the customer's total count of Yammer Enterprise users.

- Cloud Data Protection for Xactly Incent. CDP for Xactly Incent may be used for no more than the number of Xactly Incent users purchased for CDP functionality. A Xactly Incent user means, for purposes of CDP for Xactly Incent,-a sales user as licensed from Xactly in either the Xactly Incent Enterprise or Xactly Incent Express products. CDP for Xactly Incent users may not necessarily be purchased to the customer's total count of Xactly Incent users.
- Cloud Data Protection for Oracle CRM On Demand. CDP for Oracle CRM On Demand may be used for no more than the number of Oracle CRM On Demand users purchased for CDP functionality. An Oracle CRM On Demand user means, for purposes of CDP for Oracle CRM On Demand,-a CRM user as licensed from Oracle for Oracle CRM On Demand. CDP for Oracle CRM On Demand users may not necessarily be purchased to the customer's total count of Oracle CRM On Demand users.

Each application product above has add-on servers for additional functionality
- Cloud Data Protection Integration Server. CDP Integration Server is licensed per each CDP application user purchased from any and all CDP application products above.
- Cloud Data Protection Communication Server. CDP Communication Server is licensed per each CDP application user purchased from any and all CDP application products above.

The following optional products are also licensed with separate subscriptions:
- Cloud Data Protection Policy Builder. CDP Policy Builder may be used for no more than the number of Policy Builder application purchased for CDP functionality. A Policy Builder application means, for purposes of CDP Policy Builder,-either:
  o a single production instance of a business application that is individually and discretely licensed from an application provider, or,
  o if used for an internally developed application, a single production instance of a business application with a single physical or logical database instance.

- Cloud Data Protection for Salesforce Communities. It is licensed based the number of annual logins or the number of users. CDP for Salesforce Communities may be used for no more than the number of Salesforce Communities annual logins or named users purchased for CDP functionality. A Salesforce Communities user means, for purposes of CDP for Salesforce Communities, a Salesforce Customer, or Partner or Employee Community user as licensed from Salesforce.com. Salesforce Communities annual logins means, for purposes of CDP for Salesforce Communities, the quantity of Customer, Partner or Employee Community user authenticated sessions (logins) that have been licensed from Salesforce.com. CDP for Salesforce Communities users may not necessarily be purchased to the customer's total count of Salesforce Communities annual logins.

Section Appendix
Cloud Data Protection has operating prerequisites. These include:
Operating Systems. The following operating systems are supported:
- Ubuntu versions 12.04 or greater
- CentOS 5.x or greater
- RHEL 5.x or greater

Industrial Control Systems Protection (ICSP)

ICSP is an appliance sold with a perpetual software license. ICSP requires an additional anti-virus (AV) subscription to function. Subscriptions include updates to pattern files containing information to identify viruses or malicious software. An ICSP (and the applicable subscription) may be used for no more than the number of Windows Driver Agents (Agents) that have been licensed. An Agent, for purposes of ICSP, means any Windows ™ system running the applicable driver that restricts access to data contained within a USB drive which has not been scanned and certified by the ICSP appliance.

END

![Symantec]

PROD_USE_RIGHTS_SUPP_(License Agreement 9/01/2016)_Network.Protection.Products_25August2017