New Product

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Security Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Version</td>
<td>Security Analytics S500 Hardware</td>
</tr>
<tr>
<td>Previous Version</td>
<td>Security Analytics Gen. 6 Hardware</td>
</tr>
<tr>
<td>Platforms</td>
<td>S500</td>
</tr>
<tr>
<td>Language</td>
<td>English, French, Japanese, Korean</td>
</tr>
</tbody>
</table>

**Note:** Media will be offered via electronic download from [Symantec Software Downloads](https://www.symantec.com) from 4th December 2017.

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>5th February 2018</th>
</tr>
</thead>
</table>

**Disclaimer**

Any information regarding future Symantec offerings, future updates or other planned modifications is subject to ongoing evaluation by Symantec and therefore subject to change. This information is provided without warranty of any kind, expressed or implied. Customers who purchase Symantec offerings should make their purchase decision based upon features that are currently available.

Product Information

Symantec™ Security Analytics is a turnkey, pre-configured appliance that harnesses the Symantec™ Security Analytics software to capture, index, classify and enrich all network traffic (including full packets) in real time. This data is stored in an optimized file system for rapid analysis, instant retrieval and complete reconstruction to support all of your incident-response activities. The appliances can be deployed anywhere in the network: at the perimeter, in the core, in a 10 GbE backbone, or at a remote link to deliver clear, actionable intelligence for swift incident response and resolution and real-time network forensics. Symantec™ Security Analytics components include:

- **2 Gbps appliances**—High-performance analytics, massive scalability, and centralized management
- **10 Gbps appliances**—Enterprise-proven capabilities via more interfaces, storage, and memory
Notification of Status Change

Symantec™ Security Analytics
1st January 2018

- **Storage modules**—Storage capacity through direct-attach modules or high-density, Fibre Channel modules that support up to 1.5 PB of storage per capture appliance
- **Central Manager**—Manage over 200 Security Analytics appliances or VMs from a central location

What’s New

Symantec™ Security Analytics capture and management models are now available on the common hardware platform of other Symantec (formerly Blue Coat) products. Security Analytics 2G, 10G, 10GHD, and Central Manager appliances now all share the common S500 platform.

End of Life Policy

In the course of developing and delivering innovative and functionally richer products that address customer needs, Symantec may from time to time discontinue certain products, platforms and models. Symantec Product End-of-Life Policy for Network Protection Products is intended to provide information to help customers plan the evolution of their environment and make more informed purchase, support and upgrade decisions.

Definitions

- **Appliance**: The Equipment with the operating-system software (OSS).
- **Symantec Network Protection Software Products**: Network Protection Products offered by Symantec only in software form.
- **End of Life (EOL)**: The last date support is available for the applicable product. This is the last date Symantec will respond to any issues with the product. After this date, all support services for the product are unavailable, and the product becomes obsolete.
- **End of Maintenance (EOM)**: The last date defects will be fixed for an OSS release. After this date, Symantec will no longer commit to develop, repair, maintain or test the OSS.
- **End of Sale (EOS)**: The last date the applicable Equipment may be purchased.
- **Equipment**: The physical product or platform and its physical components.
- **Long Term Release (LTR)**: Minor Release of OSS that will be supported for a minimum of 3 years from designation as an LTR or a minimum of 2 years after EOM notification, whichever date occurs later.
- **Operating System Software (OSS)**: Symantec™ Network Protection Appliances Products operating system software.
- **Standard Release**: Minor release of OSS that will be supported for a minimum of 1 year after EOM notification.
OSS Release Nomenclature

- **Major Release (x)** Significant new functionality or major architectural change to the previous version of the OSS.
- **Minor Release (x.y)** New features added to the OSS to enhance capabilities, improve usability and serviceability.
- **Maintenance Release (x.y.z)** Primarily meant to fix bugs and OSS defects, although limited OSS enhancements may be included.
- **Patch Release (x.y.z.a)** Resolves one or more specific OSS defects, made available to a limited set of customers.

Policy

This policy applies to Symantec™ Network Protection Appliances that reach End of Sale date after April 30, 2010 and does not apply to Symantec™ Network Protection Software Products.

Symantec reserves the right to modify this policy for specific products as business demands justify. This policy and any modifications to this policy including notices and information regarding EOS, including the last date to order new Appliances, renew support contracts and suggested migration path(s) for the affected Appliances will be posted on the Support Policies section of the Symantec web site.

a. Symantec™ Network Protection Appliances are typically supported for at least five years from the Appliance purchase date for customers under active maintenance agreements. The actual EOL date for each Appliance may vary and will be the later of 5 years from the purchase date, if the purchase is made prior to the end of the fiscal quarter in which an EOL notification is issued and the EOL date, which date shall always be issued by Symantec with two years’ advance notice. The five years of support availability for Appliance purchases made after the Symantec fiscal quarter in which the EOL notification was made will be prorated and will relate back to the last day of that fiscal quarter in which the EOL notification was made. In order to achieve full support availability, customers must have continuous support with no gaps in coverage. Commencing on the EOL notification date and during the period until EOL date, Symantec will continue to provide:

   (i) technical support;

   (ii) spares or replacement parts for Equipment in accordance with the Return Materials Authorization (RMA) process. If an identical appliance or component is not available, Symantec will replace with a similar or better; and

   (iii) a supported version of OSS that is compatible with the Equipment, subject to (b)(iv) below.
b. OSS support will be as follows:

(i) In general, Symantec will support a given Major or Minor Release of OSS for a minimum of 180 days from EOM notification, unless the Release is designated as a Standard or Long Term Release.

(ii) In the event Symantec designates a specified Release as a Standard Release, such release will be supported for a minimum of 1 year from EOM notification.

(iii) In the event Symantec designates a specified Release as a Long Term Release, such release will be supported for a minimum of 2 years from EOM notification.

(iv) Customers may be required to upgrade to the latest OSS release in order to correct a reported problem.

For some software releases (Symantec™ Network Protection Software Products or OSS), the EOM and EOL date will be the same. If the EOM date is not specified on the Support Policies section of the Symantec Network Protection Products web site, the EOM date is the same as the EOL date.

Customers are advised to move to the most current Maintenance Release (x.y.z) for the given Minor Release (x.y). For purposes of clarification, bug fixes and limited enhancements (if applicable) will be provided on the most current Maintenance Release only during the applicable notice period.

The Symantec support services outlined above require a current support contract for the Symantec Network Protection Product. Support contracts that have not been renewed timely or have lapsed after 12 months of the EOS date are not renewable. Renewal of support contracts will generally be available until the last year of support, but will not extend beyond the EOL date. Please contact your Symantec sales representative or Symantec channel partner regarding fees payable during the period between EOS and EOL.

Security Analytics – Marketing Descriptions

Short:
Like a security camera and DVR for the network, Symantec™ Security Analytics arms incident response and security teams by delivering a proactive and complete network traffic recording — a “system of record” — for full security visibility, advanced network forensics, and real-time threat detection.

Medium:
Like a security camera and DVR for the network, Symantec™ Security Analytics arms incident response and security teams with a proactive and complete network traffic recording — a “system of record” — for full security visibility, advanced network forensics, and real-time threat detection. This enables organizations to identify and detect advanced malware, analyze and contain zero-day and targeted attacks, conduct comprehensive forensic investigations, efficiently respond to incidents, and swiftly resolve security breaches.
Long:
Like a security camera and DVR for the network, Symantec™ Security Analytics arms incident-response and security teams with a proactive and complete network traffic recording — a “system of record” — for full security visibility, advanced network forensics, and real-time threat detection. This enables organizations to identify and detect advanced malware, analyze and contain zero-day and targeted attacks, conduct comprehensive forensic investigations, efficiently respond to incidents, and swiftly resolve security breaches.

Symantec™ Security Analytics delivers complete network security visibility with the automated network traffic capture and evidence retention necessary to uncover the full source and scope of an attack. Symantec’s Intelligence Services and 3rd-party reputation providers enrich Security Analytics for automated real-time detection and insight against targeted attacks, advanced malware, and zero-day threats. Symantec™ Security Analytics enables swift analysis and incident resolution through advanced forensics and correlated analytics.

US Government Encryption Controls
Symantec and its partners must comply with the import and export laws of both U.S. and non-U.S. jurisdictions. Symantec and its partners, along with individuals involved in any unauthorized import or export activity, could suffer serious legal consequences if software, hardware, or services are released to anyone without the appropriate government approvals. Distribution of these products may require action on your behalf prior to sale and/or distribution into certain countries and to persons or entities within those countries, including government offices. It is your responsibility to comply with all U.S. and applicable local legal requirements. Further information on U.S. export regulations can be found by visiting the websites for the U.S. Bureau of Industry and Security (http://www.bis.doc.gov/) and the U.S. Office of Foreign Assets Control (https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx).

After Symantec completes its trade compliance review of a product, the product’s import and export classification and licensing information can be found at: https://www.symantec.com/content/dam/symantec/docs/other-resources/web-product-matrix-en.xlsx

A product listed under the link above can be exported to all countries, except as follows:

- No release to embargoed countries (e.g., the Crimea region of Ukraine, Cuba, Iran, North Korea, Sudan, and Syria)
- No release of beta or trial ware to embargoed or restricted countries (e.g., Belarus, the Crimea region of Ukraine, Cuba, Iran, North Korea, Sudan, and Syria)
- No transactions involving entities or people listed on U.S. and foreign government Restricted Parties Lists (RPLs) or Denied Parties Lists (DPLs)
- No transactions involving end-users associated with nuclear, missile, chemical, or biological weapon proliferation
Notification of Status Change

Symantec™ Security Analytics

1st January 2018

- No transactions involving end-uses or users that require an individual validated export license
- No release and/or use of a product within China, France, Hong Kong, Israel, or Russia, if the product is restricted by the laws of that country and its government has not yet issued an applicable license

Disclaimer: Symantec makes import and export data available for informational purposes only. It may not reflect the most current legal developments, and Symantec does not represent, warrant or guarantee that it is complete, accurate or up-to-date. This information is subject to change without notice. This information is not intended to constitute legal advice or to be used as a substitute for specific legal advice from a licensed attorney. You should not act (or refrain from acting) based upon this information without obtaining professional advice regarding your particular facts and circumstances.