UPGRADE BRIEF

Symantec® SGOS 7

The Benefits of Upgrading to the Latest Edge SWG Operating System

Top Five Reasons to Upgrade

1. Harness the Evolving Internet
2. Protection from Advanced Threats
3. Monitor and Control Cloud Application Growth
4. Increase Security Effectiveness with Cloud Integration
5. Keep in Step with the Latest Updates

Why Upgrade?

Symantec, a division of Broadcom, is the leader in proxy-based Secure Web Gateway (SWG) security solutions that global leaders have relied on for years. This trusted technology continues to protect the largest organizations and most demanding security teams. As security threats have evolved, so too has our ability to protect against the most sophisticated adversaries. Ongoing advancements, innovations, and fixes to our award-winning SWG solution are only realized if customers are running the latest and greatest version.

If you are running an older version of SGOS, official support may end soon or has already ended. It may be time to upgrade to ensure you are getting the most out of your investment. SGOS 7 delivers the most advanced SWG capabilities, new features and is the platform for further development and innovation. Now is the time to upgrade!

Top Five Reasons to Upgrade

1. Harness the Evolving Internet

Internet web standards continue to evolve, and there has been a significant shift to new technologies and protocols to ensure security, increase performance, and maintain customer privacy.

Why Upgrade: *SGOS 7 has native support for these standards, including TLS 1.3, HTTP/2, and DNS over HTTP (DoH). If you want to ensure complete visibility and policy controls of these new protocols without downgrading security or impacting performance, it's time to upgrade.*

2. Protection from Advanced Threats

Maintaining a comprehensive security posture, protecting against new risks, and making policy updates can be time consuming and complex. New threats might evade detection if you are not prepared.

Why Upgrade: *The Symantec® curated Proxy security policy in SGOS 7 applies a strong security posture that is easy to deploy and manage. High-risk isolation for unknown, uncategorized, and potentially risky traffic (risk levels > 5) reduces operational overhead and ensures secure user access to unknown sites.*

3. Monitor and Control Cloud Application Growth

Cloud Application adoption continues to rise, and with it comes a huge challenge to identify and manage the risk of unsanctioned cloud applications.

Why Upgrade: *SGOS 7 (with Intelligence Services) has built-in capabilities for real-time discovery of over 45,000 cloud applications. Cloud application traffic traversing through the proxy can use existing policy controls plus new cloud application attributes to allow/deny/coach users, ensuring enforcement of acceptable cloud use policies. No additional license is needed!*

4. Increase Security Effectiveness with Cloud Integration

Any advanced security requires real-time updates, centralized reporting, and management for all deployments (on-premises and in the cloud) and access to a global network of threat intelligence.

Why Upgrade: *SGOS 7 leverages the cloud for real-time threat intelligence and updates, centralized reporting for unified threat identification, and CASB shadow IT discovery (proxy automatically sends logs to the cloud). Manage common policy between all SWG deployments, on-premises and cloud.*

5. Keep in Step with the Latest Updates

SGOS 7 is the long-term release of the Symantec industry-leading SWG solution to maintain effective security and to achieve the complete set of advanced feature capabilities; it's critical to be on the latest, supported release.

Why Upgrade: *SGOS 7 incorporates over 20 years of Symantec leadership in proxy-based SWG solutions. The long-term supported release includes numerous upgrades, fixes, and integration to the Symantec security products portfolio including SSL Inspection, CASB, Content Analysis/Sandboxing, Isolation, DLP, and more.*

Why Transition from BCIS to More Advanced Intelligence Services?

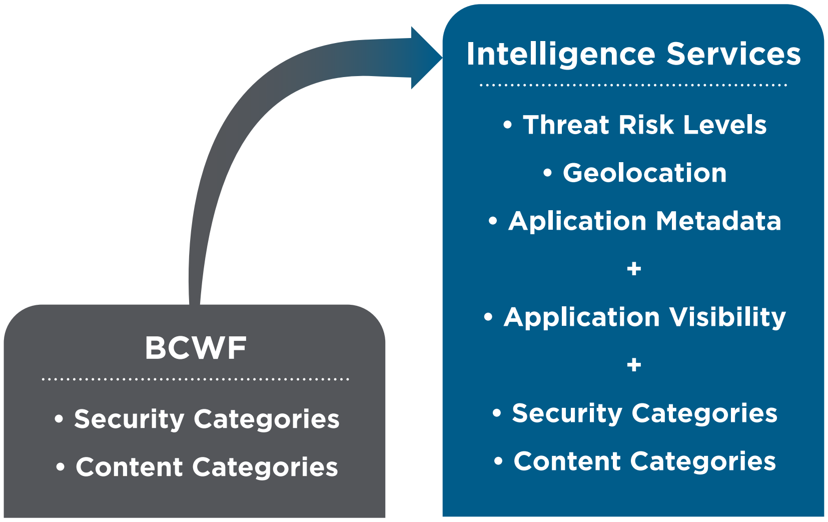
Blue Coat WebFilter (BCWF)

- BCWF reached End-of-Life (EOL) status on August 31, 2023.
- BCWF is over 15 years old and is only supported on older platforms. While it is a good solution, it is out of date. No new features will be added to BCWF.
- BCWF is not supported on SGOS 7 and later. SGOS 7+ leverages the more advanced Intelligence Services.

Intelligence Services

- Intelligence Services is more advanced than BCWF, has more features, and offers greater integration opportunities.
- Intelligence Services provides Risk Levels for threat assessment, regardless of category (or uncategorized).
- Intelligence Services delivers expanded application visibility: application groups, identification, attributes, and operations.

Figure 2: Transitioning from BCWF to Intelligence Services Provides Advanced Services



Intelligence Services

- Threat Risk Levels
- Geolocation
- Aplication Metadata

+

- Application Visibility

+

- Security Categories
- Content Categories

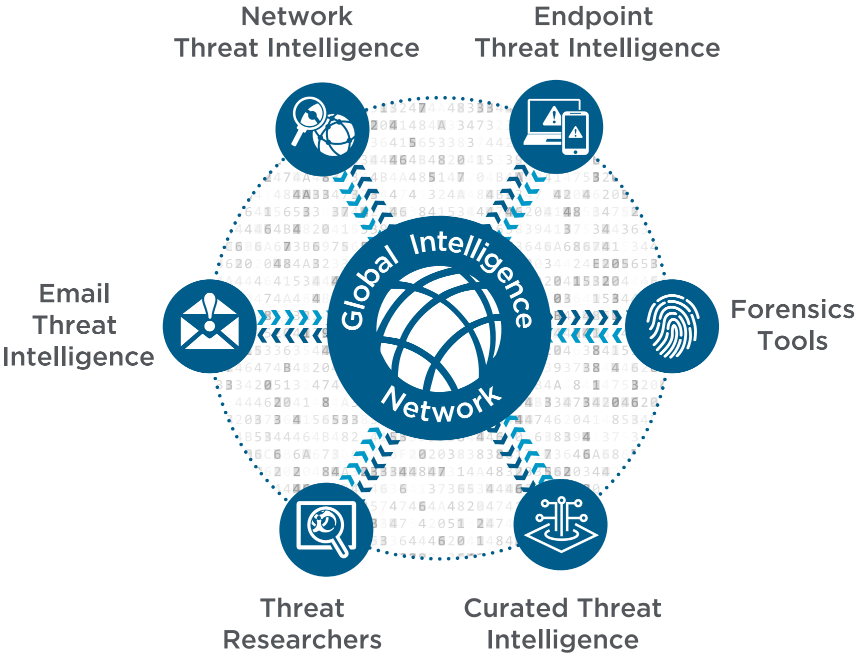
BCWF

- Security Categories
- Content Categories

Symantec
by Broadcom

Proof: Symantec Leads in Threat Intelligence

Global Intelligence Network Backs Every Symantec Network Security Solution


Network Threat Intelligence
Endpoint Threat Intelligence
Email Threat Intelligence
Global Intelligence Network
Forensics Tools
Threat Researchers
Curated Threat Intelligence

Advanced intelligence, Delivered Everywhere it Matters

- **The world's largest civilian threat intelligence network:**
  - Employs more than 1000 engineers and researchers and 123 million attack sensors across 157 countries.
  - Analyzes threat telemetry from over 15,000 enterprises and 175 million users.
  - Employs more than 200 analytics engines.
  - Processes more than 1 billion web and file requests daily, in over 60 languages.
- **Effective:** Blocks 99.99% of known and emerging threats.
- **Cross-product support:** Supports Symantec network, data, and endpoint protection solutions, and more.
- **Cloud-delivered:** Identifies and isolates traffic to risky and unknown sites.
- **Authoritative:** Symantec Enterprise Blogs and Symantec Threat Research Team reports.
- **Trusted:** Subscribers include 15,000 enterprises globally, including over 70% of the Fortune 500.

Additional resources are available online:

- Recommended Releases
- How to Upgrade your SGOS
- Recommended SGOS Upgrade Path

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SGOS7-UGB-PB100 January 8, 2024