Modernize your Symantec Edge Secure Web Gateway without surrendering local control

Organizations running Symantec Edge Secure Web Gateway (formerly Blue Coat) face a narrowing set of choices as Broadcom consolidates its portfolio around cloud-only delivery. For organizations whose compliance, sovereignty, or operational requirements demand local data control, there is now a modern path forward that doesn't force a trade-off.

Skyhigh Security
Hybrid SSE Mesh

Zero trust, finally inside the building.

WHY NOW

Three reasons to modernize this year

01

AI agents have created a zero trust gap inside your perimeter

Autonomous AI agents inherit user-level access, query internal systems, chain APIs together, and move sensitive data — at machine speed, continuously. Many operate over persistent WebSocket connections that conventional cloud proxy inspection cannot reach.

If Zero Trust Network Access (ZTNA) is non-negotiable — and for highly regulated organizations it is — and your AI agents operate inside the network, zero trust enforcement cannot live exclusively in the cloud. That is an architectural requirement, not a product preference.

02

Administrative complexity and Broadcom licensing are driving up your total cost of ownership

Achieving full web, data, and cloud security on the Broadcom platform means managing separate consoles for Edge SWG (Secure Web Gateway), Cloud SWG, and Symantec DLP (Data Loss Prevention) — each with its own policy engine, licensing SKU, and renewal cycle. Policy drift between environments creates audit risk and engineering overhead.

Broadcom's per-user, per-module licensing charges the same rate whether a capability is used daily or once a year. Organizations are effectively funding multiple architectures while receiving the benefit of none.

03

Broadcom has ended support for on-premises components your architecture depends on

Broadcom formally ended support for all versions of on-premises Web Isolation as of January 1, 2024, and announced end-of-life for SGOS 7.3 (the prior long-term release) effective December 31, 2024, with no new features delivered beyond that date.[1]

Broadcom's strategic direction is consolidation onto cloud-only delivery. Organizations that require local data control — for compliance, sovereignty, latency, or OT/SCADA compatibility — face a binary choice: stay on a platform being commercially wound down, or move to a pure-cloud architecture that reintroduces the problems on-premises was chosen to solve.

WHY SKYHIGH TO MODERNIZE YOUR SECURITY

Security that lives where your data does

Skyhigh Security Hybrid SSE Mesh unifies on-premises Secure Web Gateway (SWG) appliances with advanced cloud-delivered security. Gain Zero Trust Network Access (ZTNA) and inline, agentless Secure Browser Controls on-premises and extend with Cloud Access Security Broker (CASB), Data Security Posture Management, (DSPM), Data Loss Prevention (DLP), and Remote Browser Isolation (RBI) from the cloud — all under a single console. Your data plane stays physically on premises. You get modern security capabilities and the unified policy, alerting, and administration your team needs, without surrendering the local control your compliance requirements demand.

★ #1 in Data Protection
Gartner Critical Capabilities for SSE², outpacing Broadcom and other SSE / SWG alternatives in the same evaluation.

◆ Leader and Outperformer
GigaOm Radar for SSE — converged policy framework specifically cited for reducing administrative complexity across hybrid environments.

✓ FedRAMP High Authorized
Enabling US federal agencies and defense industrial base organizations to deploy modern zero trust without waiting on cloud-native authorization timelines.

■ 3,000+ customers trust Skyhigh
Including 80% of the largest global banks and nearly half of the Fortune 100, to protect their most sensitive data.

Copyright © 2025 Musarubra US LLC. All rights reserved. Skyhigh Security is a registered trademark of Musarubra US LLC.

THE SKYHIGH SECURITY DIFFERENCE

A modernization, not a migration

Skyhigh Security Hybrid SSE Mesh replaces aging Symantec Edge Secure Web Gateway hardware with modern, scalable Secure Web Gateway (SWG) appliances that optionally extend to a full Security Service Edge (SSE), all through a unified policy and management console. Your CPL (Content Policy Language) policies and the fine-tuning your team has invested in them are preserved and extended through Skyhigh's unified policy console, not rebuilt from scratch in a new engine.

CONTROL WITHOUT COMPROMISE

Zero trust where your network actually is.

- **Local ZTNA on your own on-premises and branch gateways** — not only through a vendor-owned edge node in someone else's cloud.
- **Inline, agentless browser security on-premises:** WebSocket-aware AI agent and messaging app inspection and protection directly at the local network edge with no enterprise browser replacement.
- **Decryption and inspection performed locally** — sensitive payloads never cross third-party or jurisdictional boundaries.
- **Dark data center architecture** with no inbound listening ports, blocking external scanning and lateral movement.
- **Segmentation for industrial environments:** enforces strict network segmentation in OT/SCADA environments operating under layered industrial architectures, stopping ransomware from propagating from corporate IT into operational systems.

ONE POLICY. EVERYWHERE.

Your CPL investment, extended — not replaced.

- **CPL policy preservation:** Skyhigh's unified policy console supports migration and re-expression of existing CPL (Content Policy Language) policies — the rules your team has refined over years carry forward, rather than being rebuilt in a new engine.
- **Policy-as-code architecture:** policy authored once and pushed automatically across physical appliances, virtual systems, and cloud nodes — no manual reconciliation, no drift.
- **Single cloud console** governing every environment. No split-brain admin panes.
- **Bi-directional failover** between local appliances and cloud PoPs — internet outages do not take down in-office users.
- **50%+ reduction in admin overhead** from unified policy authoring across all environments.

PAY FOR WHAT YOU USE

License capability, not seat count.

- **Flexible consumption-based token model** — option to allocate security dynamically across on premises and cloud based on actual demand.
- **No re-procurement to activate a new capability** — deploy advanced capabilities like DLP or browser controls the day you need them.
- **Up to 60% of inspection volume** offloaded from cloud services to on-premises hardware, converting a recurring cloud cost into a fixed asset.
- **Enterprise Browser Controls** bring inline DLP and AI prompt-level governance to any standard browser — agentless, immediate, no rollout required.
- **Base-tier DSPM (Data Security Posture Management) included natively** — not a separate, premium-priced module.

Designed for the industries where local control is non-negotiable

Financial services & insurance	Government & defense	Healthcare & pharmaceuticals	Manufacturing & critical infrastructure
Local SSL/TLS decryption with full PKI sovereignty. Decrypted PII never touches third-party infrastructure. Aligns with DORA, FCA, MAS, and equivalent mandates.	Air-gap capable. Comply-to-Connect posture checking for DoD Zero Trust mandates. Deployable with or without optional cloud-native FedRAMP High authorized cloud security – all with common policy and management.	Patient data never exits the physical perimeter. Medical device and OT isolation. HIPAA and national health data regulation alignment.	No internet dependency for in-plant operations. Enforces segmentation in OT/SCADA environments without disrupting physical processes — stopping ransomware from spreading from corporate IT into operational systems.

Copyright © 2025 Musarubra US LLC. All rights reserved. Skyhigh Security is a registered trademark of Musarubra US LLC.

MODERNIZATION PATH

Four phases. Your pace. No forced rip-and-replace.

PHASE 1	PHASE 2	PHASE 3	PHASE 4
Assess & plan	**Deploy in parallel**	**Adopt new unified capabilities**	**Rationalize & optimize(Ongoing)**
Inventory existing CPL policies. Map data sovereignty zones, OT/SCADA environments, and SSL inspection performance. Identify CPL rules to preserve and extend.	Deploy Skyhigh SWG appliances alongside existing Symantec Edge SWG. Import and validate CPL policy baselines. Run parallel traffic — zero disruption to operations.	Enable ZTNA and agentless Secure Browser Controls in SWG appliances. Extend with cloud CASB, DSPM, and DLP. Retire legacy appliances on your schedule.	Consume token budget dynamically. Retire unused Broadcom entitlements. Continuous policy-as-code optimization under one console with full audit visibility.

Your next security architecture should be built on your terms.

Request a personalized assessment of your current Symantec Edge Secure Web Gateway environment and see exactly what a modernization — not a migration — would look like for your organization.

REQUEST YOUR ASSESSMENT

skyhighsecurity.com/blue-coat-displacement

skyhighsecurity.com

1. Sources: (a) Broadcom formally ended support for all versions of on-premises Web Isolation as of January 1, 2024 (knowledge.broadcom.com/external/article/215429). (b) Broadcom announced end-of-life for SGOS 7.3 effective December 31, 2024, with no new features delivered beyond that date (knowledge.broadcom.com/external/article/151102). Customers should verify the current support status of their specific hardware models and software versions directly with their Broadcom account team.

2. Source: Gartner Critical Capabilities for Security Service Edge, 2024. Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner research organization and should not be construed as statements of fact.

Copyright © 2025 Musarubra US LLC. All rights reserved. Skyhigh Security is a registered trademark of Musarubra US LLC.