SOLUTION BRIEF

Benefits of a Unified Endpoint Agent and Cloud SWG

OVERVIEW

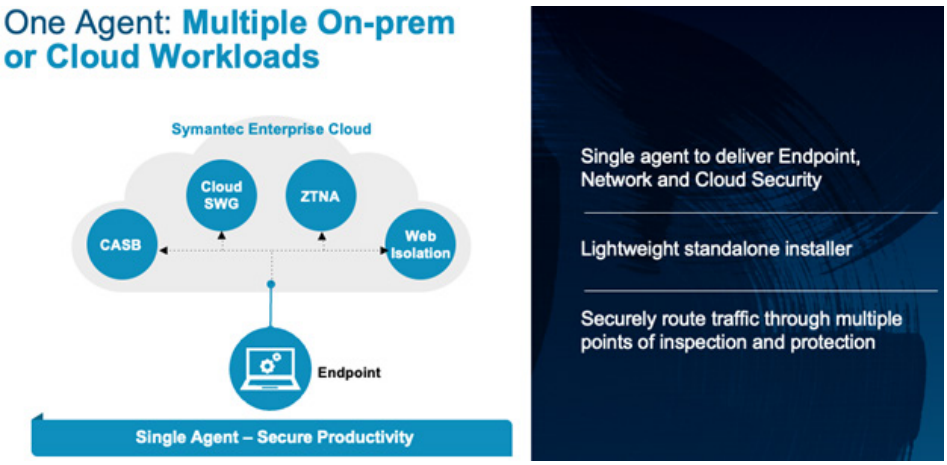
The Symantec Endpoint Security Agent now brings network and web security to Symantec Endpoint Security (SES) customers. It delivers significant advantages across security, operations, and user experience. Customers who use SES to deliver industry-leading endpoint protection and have licensing for Cloud SWG now have access to full network traffic inspection and security policy enforcement, without needing to install another agent.

Enhanced Security and Policy Consistency for Endpoint and Network

The combined solution ensures comprehensive protection, regardless of user location.

- **Consistent security everywhere:** Symantec® Endpoint Security Agent enforces the exact same Symantec Cloud Secure Web Gateway (SWG) policy, whether the user is in the office, at home, or traveling. This behavior eliminates security gaps that often occur when users bypass corporate proxies through personal Wi-Fi or home networks, and it enables swift detection of a threat before it reaches the endpoint.
- **Deep, full-proxy inspection:** The agent steers all web traffic (HTTP/S) to the Cloud SWG, enabling full SSL/TLS decryption and inspection. With over 95% of web traffic encrypted, the Cloud SWG is critical for detecting malware, phishing, and command-and-control callbacks hidden within encrypted sessions.
- **Zero Trust enforcement:** By residing on the endpoint, the agent can continuously verify user identity and device posture (such as, device patch status and firewall configuration). The Cloud SWG then uses this context to enforce granular Zero Trust Network Access (ZTNA) policies to ensure secure access to private applications, without the need of a VPN.
- **Data loss prevention (DLP) at the edge:** The agent extends corporate DLP policies to all web traffic, preventing sensitive information (financial data or customer PII) from being uploaded to unauthorized personal cloud storage or webmail accounts.
- **Unbypassable protection:** The enterprise-grade agent is designed to be tamper-proof, preventing users from easily disabling or uninstalling the security software to bypass web filtering or threat controls.

Figure 1: Unified Endpoint Agent and Cloud Security

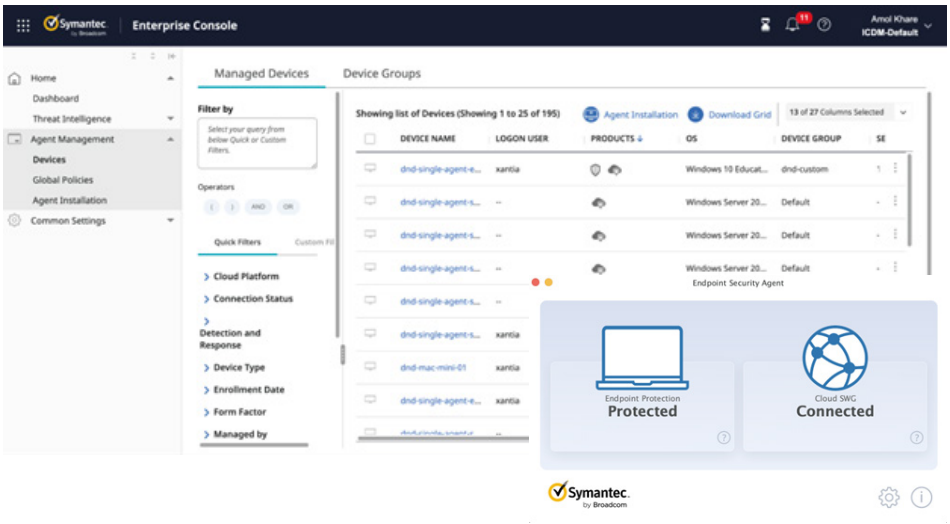


Operational Simplicity and Centralized Management

Consolidating endpoint and network security functions significantly reduces administrative overhead and complexity. The consolidated agent architecture provides shared services across products that can be managed through the agent UI for a simplified, consistent experience across multiple domains. Shared agent services include LiveUpdate, LiveUpdate server settings, restart scheduling, and tamper protection.

- **Unified policy console:** Instead of managing separate Cloud SWG features, endpoint security, and remote access tools, administrators use a single cloud console to define all policies. This console simplifies management, reduces the chance of misconfiguration, and ensures policies are instantly applied globally.
- **Reduced tool sprawl:** Using this single agent for endpoint security, traffic steering, and SWG connection minimizes the number of individual software agents needed on a device, reducing conflicts and management overhead.
- **Simplified deployment:** IT teams only have to deploy and maintain one piece of software, the unified agent, to provision multiple security services (SWG, CASB, ZTNA, and so on).
- **Centralized visibility:** All web traffic logs, threat detections, and policy violations are aggregated into one dashboard that delivers comprehensive insights for faster incident response and easier compliance reporting.

Figure 2: Endpoint Security Agent Management



Improved Performance and User Experience

The Cloud SWG model is built for the modern, distributed workforce.

- **Optimized, low-latency access:** Instead of *backhauling* remote users' Internet traffic through a central data center firewall, which adds latency, the agent connects users to the geographically closest Cloud SWG point of presence (PoP) that runs on the high-performance Google Cloud backbone. This architecture provides a faster, more direct path to cloud applications and the public Internet.
- **Intelligent traffic steering:** The agent intelligently distinguishes between corporate and personal traffic. It can also route specific, high-bandwidth traffic, such as video conferencing, directly, or steer traffic to the cloud proxy only when inspection is necessary. The routing provides a smooth, interruption-free user experience.
- **Global scalability and reliability:** Cloud SWG leverages Google's global infrastructure to deliver scale and high availability across numerous data centers worldwide. This architecture eliminates the capacity constraints and failure points of many traditional on-premises hardware appliances.
- **Consistent administrative experience:** The agent's administrative UI is completely redesigned and simplified across all supported components to ensure administrators can intuitively manage the agent and policy's deployment and upkeep.

The integrated solution of SES and Cloud SWG provides the foundation for modern security architectures like SSE and Zero Trust. This approach delivers consistent, high-efficacy protection by steering all traffic to the Cloud SWG for deep encrypted traffic inspection, website classification and categorization, security policy enforcement, and DLP protection, regardless of where the user is located. The solution also achieves operational simplicity by consolidating multiple security functions, visibility, and policy management into a single, centralized console. By connecting users to the nearest global PoP instead of backhauling traffic, this solution ensures optimized, low-latency performance for a robust, secure, and positive experience for the distributed workforce.

BROADCOM
connecting everything®

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

BUEA-SWG-SB100 December 9, 2025