

SYMANTEC

Product Name: Symantec Proxy Secure Gateway¹

Main Website: <https://www.symantec.com/>

Product Website: <https://www.bluecoat.com/products-and-solutions/on-premise-secure-web-gateway>

Product Integration Type

Web Proxy

Integration Objective

Integrates with Symantec Proxy Secure Gateway to help with URL mitigation. Symantec periodically retrieves bad web URLs from SmartCore to block them. The list of bad URLs is found under Cyphort Manager mitigation tab -> Secure Web Gateways.

Customer Value Proposition

Integrates with existing third party security devices such as Symantec to automatically block malicious web URLs.

Tested Vendor Versions

Symantec Proxy SG 6.5.1.1

Integration Classification

Blocking: Firewall, Web Proxy

Integration Details

Enterprise. Can work in large environments with a variety of integration points.

Integration Method

Vendor Pull: Symantec polls SmartCore periodically to get the list of bad URLs to block. By default, Symantec polls every 5 minutes, but this is configurable on the Symantec product

¹Integration was tested with Symantec Proxy SG Virtual Appliance 100. Integration works with any Symantec Proxy SG.

Integration Detail Summary (API, CLI)

- ▶ Under mitigation -> Secure Web Gateway, the Cyphort Manager lists the bad URLs that need mitigated. It compiles the list based on the web URLs of malware downloads that SmartCore has seen. To avoid false positives, SmartCore ensures that the domain reputation of a bad URL is also low
- ▶ Under the Cyphort Manager Environmental settings, the administrator can generate a unique Cyphort URL where Cyphort posts the list of bad URLs. Symantec polls the Cyphort URL periodically to obtain the list
- ▶ Before Symantec pulls the bad URLs from Cyphort, it checks if Cyphort's certificate is trusted and if the Subject Name in Cyphort's certificate matches the domain of the Cyphort device. If this check fails, Symantec will not be able to retrieve the URL list.
- ▶ For more information, please refer to the detailed joint solution brief at: http://go.cyphort.com/rs/181-NTN-682/images/CYPHORT_SB1-bluecoat.pdf

Cyphort Manager GUI Component

- ▶ Yes
- ▶ Cyphort Manager configuration: Symantec settings can be configured under Settings -> Environmental Settings.

GUI Operational Use Case

Operational Use Case: The Symantec UI is used to check if the Web URLs are blocked.

Threat Score Impact

No

Integration Documentation

N/A

Integration Demo

No

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

