

# Web Application Firewall

## Complete Security for Enterprise Applications

### At a glance

The Symantec Web Application Firewall enables you to secure and accelerate your web applications.

The WAF:

#### Delivers Next-Generation Application Security

- Protecting against the OWASP Top 10 Risks and more

#### Accelerates Application Performance

- Ensuring you can scale your deployment to meet your needs

#### Provides Flexible, Granular Policy

- Protecting and enforcing regulations and corporate policy around web applications and web properties

## Introduction

Web servers are often targeted by attackers to help them host and deliver malware; Verizon's 2015 Data Breach Investigation Report found attacks on web applications were one of the most common threats enterprises faced.

To mitigate the risks a compromise poses to their reputation and ongoing operations, enterprises are implementing Web Application Firewalls (WAF) to protect their web properties and enforce the security and privacy of their web applications. To ensure the security they implement does not adversely affect the performance of the web, many enterprises are choosing the Symantec Web Application Firewall, which is capable of both securing and accelerating web applications for optimal productivity.

The Symantec WAF is a component of Symantec's Web Application Security solution, making it easier and more efficient to leverage and secure web-based applications to support your business requirements. With the Symantec WAF, you can safely set policies and protections around your applications to enable your employees, vendors and customers to get work done. Built on the industry-leading ProxySG, the Symantec WAF addresses today's security concerns including the Top Ten risks identified by the Open Web Application Security Project (OWASP), providing the most advanced policy, control, accountability and performance features available in a WAF solution.

## The Symantec Difference – WAF Delivery

Symantec has been providing security for the web since 2001 and is trusted by most of the world's most respected and demanding organizations. A WAF is a natural extension to Symantec's proxy deployments, enabling enterprises to benefit from all the security, performance and control features already available in our industry-leading ProxySG. The Symantec Web Application Firewall is offered as a licensed enhancement to the ProxySG and is enabled with the purchase of the Web Applications Protection license.

## Next-Generation Application Security

The Symantec WAF delivers advanced, next-generation protection that addresses today's critical security concerns including the OWASP Top 10 vulnerability concerns for web applications. The WAF conducts advanced threat analysis on both inbound and outbound content to detect and protect your infrastructure from attacks. Protection is provided through both signature-based engines capable of blocking known attack patterns and advanced signature-less engines designed to uncover unknown and zero-day attacks in the web traffic.

Symantec's next-generation Content Nature Detection Engines understand the context of the content, representing a fundamental shift in attack detection technology that improves the overall accuracy and reliability of attack identification. The Content Nature Detection Engines can be used to combat many of today's web application attacks, including code injection, HTML injection, directory traversal, command injection, JSON validation, SQL injection and cross-site scripting. Administrators have the ability to set flexible policies to take advantage of all the WAF's advanced protection capabilities.

The WAF also protects the web infrastructure by isolating origin servers from direct Internet access. In addition, the WAF monitors your web servers and other proxy-related devices, conducting strict HTTP/HTML protocol validations from the server and client to ensure activity is legitimate. You can also secure user access to web applications by using the WAF as a SSL/TLS termination point. The WAF provides both server and client-side certificate support, with web services encryption/decryption and digital signature verification to ensure the integrity of the communications. As a SSL/TLS termination point, the WAF offloads the decryption/encryption of SSL from the web servers to improve overall performance and mitigate the risks of man-in-the-middle (MITM) attacks.

## Granular Policy Controls

The Web Application Firewall enables administrators to create policies as needed for compliance, regulatory, and security needs. The powerful policy engine in the ProxySG allows administrators to create extensive and flexible policies as needed including URL rewriting, SSL/TLS validation and enforcement. You can set policies based on the geographic location of the end-user accessing the enterprise's website to help mitigate risks and support your regulatory, corporate and compliance requirements.

Using Geo-IP enables you to identify the country location of a specific client's IP address to understand where they are coming from, so you can make appropriate decisions around their access. The Geo-IP database is automatically updated through the Symantec Global Intelligence Network, so any changes will be immediately reflected in the IP address. A real IP address of the client is required, which can be attained from a source IP address or a HTTP request header (e.g. x-forwarded-for).

## Accelerated Application Performance

The Symantec WAF enables you to accelerate the delivery of your web applications and content to ensure a consistent, satisfactory experience that maximizes your users' productivity. The WAF provides integrated caching, stream splitting and bandwidth controls for optimal performance.

In addition, you can improve the scalability of your web farms by off-loading potentially resource intensive functions to the WAF, such as user authentication, SSL termination and web content optimization. The WAF also performs health checks for HTTP, HTTPS, TCP, ICAP and ICMP, helping you monitor your web content servers and overall environment, and alerting you to issues as soon as they occur quickly address and resolve them.

## Requirements

To take advantage of all the security and performance of the Symantec WAF, you need:

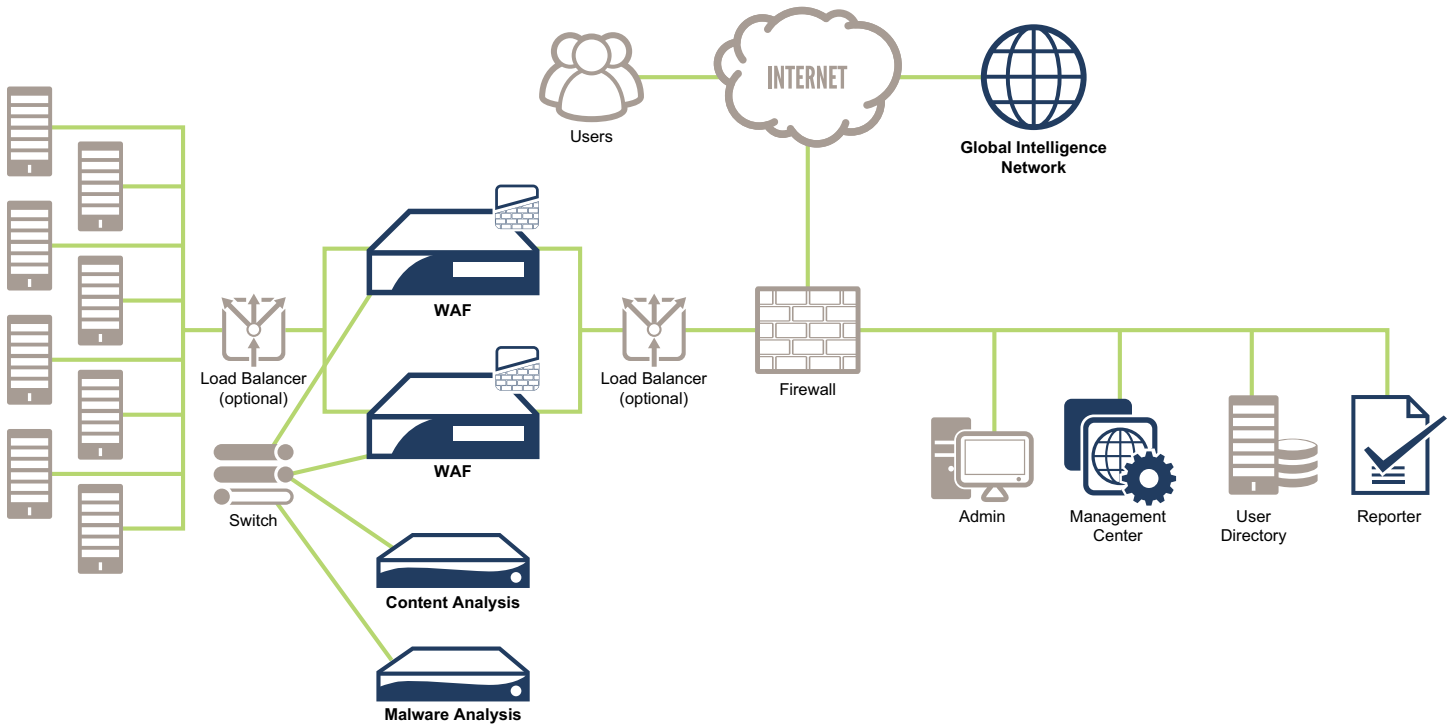
- Symantec Reverse Proxy (hardware or virtual), Proxy SG, with Proxy Edition or Symantec SWG Virtual Appliance (SWG Edition); MACH5 Editions are not supported
- Web Application Protections License - available as a yearly subscription, per appliance SKU
- Minimum of SGOS 6.5.3 to use base features of Application Protection; full Application Protection requires SGOS 6.6.2 and higher
- Minimum of SGOS 6.5.1 to take advantage of Geo-IP capabilities

It is highly recommended that you use Symantec Management Center and Reporter solutions to optimize the management of the WAF and get WAF-specific reporting.

## For More Information

Visit us online for additional resources at [Symantec.com](http://Symantec.com). To get started now or for help designing your WAF solution, contact your Symantec channel partner or Symantec Systems Engineer.

# Typical WAF Deployment



## About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit [www.symantec.com](http://www.symantec.com) or connect with us on [Facebook](#), [Twitter](#), and [LinkedIn](#).



350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | [www.symantec.com](http://www.symantec.com)