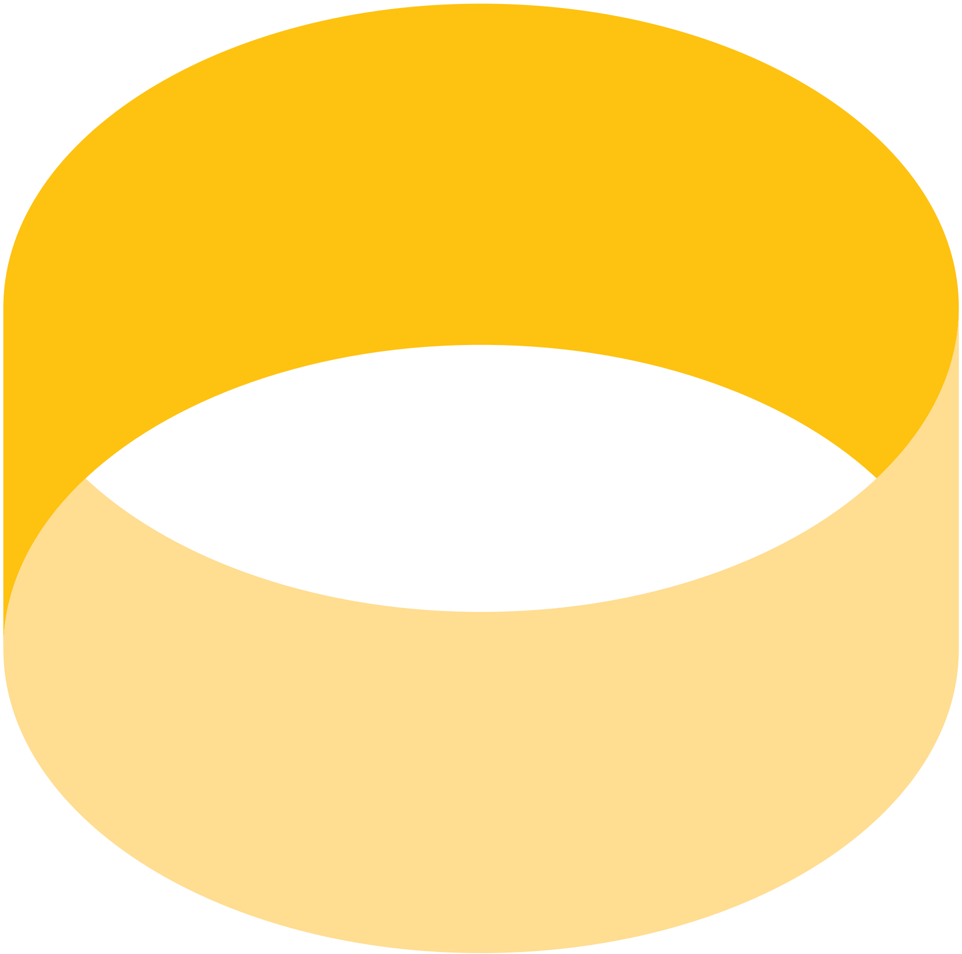


Three Reasons a Secure Web Gateway is Vital for Your Security Stance

White Paper | July 2017

Table of Contents

Executive Summary

If your organization is like most, the web is essential for your ongoing operations. This reliance on the web is only going to grow, as more workers go mobile, and more workloads move to the cloud. Unfortunately, the web is also increasingly risky, as more and more cyberattacks use the web to target business resources and operations. To protect your business, you need visibility and control over all web traffic.

Secure Web Gateways (SWGs) can deliver the insights and controls you need to mitigate the risks of the web. They pick up where Next-Generation FireWalls (NGFWs) leave off, providing Layer 7 termination and in-depth inspection of web and encrypted web traffic required to uncover and protect against the increasingly sophisticated web threats targeting your business.

This white paper describes what a SWG offers and the three main reasons it is a vital component of your layered defense strategy. It then details how the Symantec SWG delivers the web security you can rely on to confidently adopt cloud apps and move more workloads to public and private cloud environments.

The Web Gap in Today's Defenses

More and more of your traffic runs over the web, as more people and devices connect, and more data and workloads move to the cloud. Gartner predicts cloud computing will grow 18% in 2017 to $246.8 billion in total worldwide revenue. They estimate software as a service (SaaS) is around 18.5 percent of the public cloud market, growing at 20.3 percent annually.

There is no sign this growth is going to slow or our reliance on the web is going to taper off any time soon. Given that cyber attackers go where the money is, it follows that as businesses invest more in web infrastructure and services, hackers will invest in ways to exploit this web usage. This makes the web more dangerous than ever. Just look at recent headlines on the ransomware, malware and phishing attacks that disrupted organizations around the world, such as WannaCry, the exPetr virus and Google Docs attack.

Motivated attackers are targeting web sites, public networks and cloud applications to disrupt operations, tamper with and steal valuable data, and infiltrate corporate resources. In the Verizon 2016 Data Breach Investigations Report, web application attacks held the number one spot for data breaches. Google estimates that more than 760K sites are compromised annually; in 2016, they saw the number of hacked sites go up by approximately 32%.

In 2017, organizations in the U.S. and outside have budgeted, on average, $1.77 million and $1.30 million, respectively, for cloud spending. *(IDG)*

The shared, on-demand expansive nature of the web makes it hard to keep up with all the different threats you're facing and shut down all the different attack vectors. The fact that web traffic is opaque to most of your security infrastructure, because cloud applications use HTTPS by default for transport layer encryption, doesn't help. In addition, security solutions often put the onus on you to predict what is coming. They assume you can define what is 'good' and 'bad' in your environment with policies, whitelists and blacklists. They are rooted in the static concept of a perimeter, with firewalls as the anchor, inspecting and controlling the traffic that comes in and out of the network.

As ESG recently noted, "Next-generation firewalls (NGFWs) proved to be a stop-gap at best… It's time for CISOs to stop thinking about network perimeters and security appliances, and envision network security built upon a proxy-based architecture composed of distributed network services." Networks don't have perimeters. Networks are boundless and constantly changing, with workers on the move, applications in the cloud, and services hosted by SaaS/IaaS/PaaS/etc. providers that are outside your direct control.

Mobile Growth Stats:

- By 2020, there will be 105.4 million mobile workers — IDC
- For 2017, the number of mobile phone users is forecast to reach 4.77 billion — Statista

This leaves a gap in your defenses. You need to keep up with the dynamic nature of the web and stay ahead of all these threats targeting your organization. This requires monitoring EVERY web transaction, so you can see exactly what is going on, with Layer 7 termination and inspection capabilities, and effectively find and shut down web attack vectors to protect your assets and operations. You need a Secure Web Gateway (SWG).

Secure Web Gateway as a Solution

Secure Web Gateway (SWGs) provide full and comprehensive protection for your defense-in-depth strategy. With the ability to terminate and emulate traffic as a control point, it allows you to add the capabilities needed to control and protect web traffic. Key capabilities include visibility and classification of web traffic, decryption and re-encryption of traffic, policy enforcement, data loss prevention and compliance, and threat protection.

Gartner IT Glossary defines a secure web gateway as:

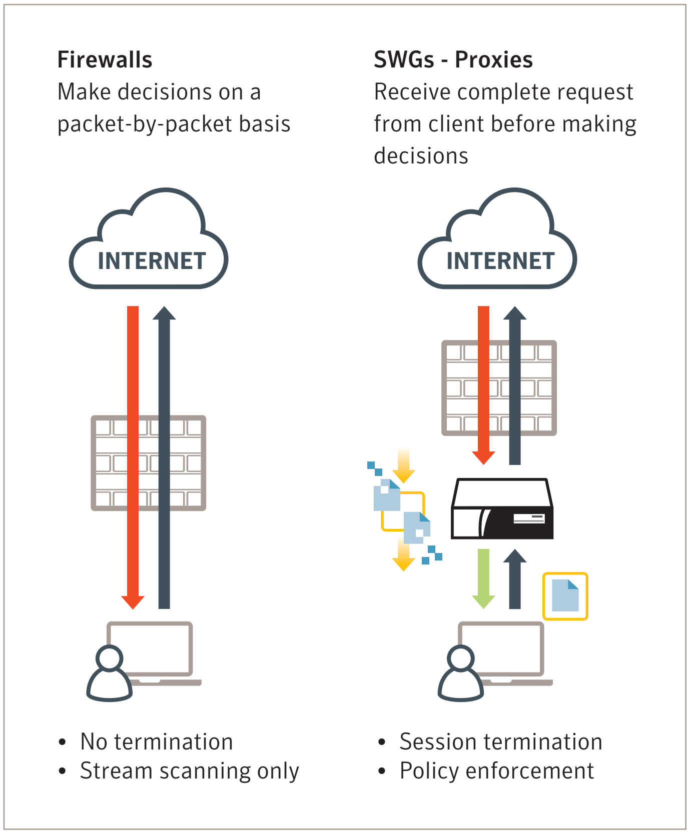
> “A solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. At a minimum, these gateways include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype. Native or integrated data leak prevention is also increasingly included.”

A Proxy Architecture is the Key

The reason that SWGs can deliver this web control and protection is due to their ability to terminate and emulate traffic with their proxy architecture. As a proxy, the SWG is an intermediary, sitting between a client and server – it doesn’t matter where that client is or what device is being used. The SWG terminates the inbound connection and emulates the client to originate a separate outbound connection to the server. Since the SWG has proxied the connection, it can wait to receive and assemble the entire communication, buffering an entire request, including headers and body, if needed, so they can figure out exactly what the server response trying to do. Proxies can even decrypt and reassemble encrypted traffic (SSL/TLS), which makes up more than half of all web traffic and has represented a massive blind spot for most organizations, to give you 100 percent visibility of your traffic.

Once the entire communication is reassembled, the SWG will decide whether it should be sent to its destination or if it requires further inspection. It may analyze the communication itself or send it to other solutions or services, such as data loss prevention (DLP) solution, sandbox, etc., for additional analysis and policy enforcement. This ensures nothing gets by uninspected and that security and corporate policies are consistently applied to all communications, including mobile and cloud traffic.

This differs from stream-based security devices, such as next-generation firewalls. Instead of looking at the entire content payload to see the full picture, these solutions look at the traffic packet-by-packet and decide whether it should be allowed to go to its destination. They typically don’t buffer an entire file, due to memory and processing constraints, so they make decisions based on incomplete information.



When something suspicious is identified, the firewall may be able to stop the file from being completely transferred and prevent the full impact of the attack, but, for all practical purposes, it is too late. You still need to investigate what got through and potentially remediate any malicious data that reached its destination before the attack was identified. A proxy, on the other hand, creates completely independent sessions between the client and the proxy, and the proxy and the server, which ensures nothing reaches the destination until it’s explicitly allowed.

> A quick Google Search on “How to Evade a Firewall” turns up dozens of ways to mess with traffic to sneak by undetected.

If there are any ambiguities such as conflicting content-type headers, a proxy can resolve them. Because the proxy is terminating TCP – parsing and reconstructing the segments as if it were the destination server – it is easy for the proxy to change, insert or modify messages as needed to ensure the communication is 'clean.' Proxies generally don't forward original requests as-is to the server. Instead, they generate a new request based on the data they read from the client. As a result, the proxy stops attackers who play games with TCP segments – dropping segments, sending segments out of order, or sending overlapping segments – to attempt to confuse and evade detection by next-generation firewalls.

Note, there are instances when the next-generation firewall will buffer to try and get more context before forwarding the traffic. Unfortunately, there are natural limits to how much they can do without terminating TCP. For example, they can't do more than a 'window's worth' of TCP data unless they generate a TCP acknowledgement, which then makes them more of a proxy. If a client and server negotiate a 16 KB window and the firewall wants to look at something that is 32 KB into the stream before it forwards any of the client's data through to the server, it will have a problem. The same will apply when trying to buffer data coming back from the server. Because of this limit, packet-based firewalls can't integrate with other systems, such as Data Loss Prevention (DLP) for enforcement, as that requires the full content stream, not just the first few packets, to inspect. Since proxies terminate TCP and always send their own TCP acknowledgements to the client and server, this problem doesn't apply to them. The proxy works with DLP and other systems that need the full content stream to do complete their analysis and provide a verdict for enforcement.

This is also why a proxy is best positioned to handle encrypted traffic. Decrypting SSL requires negotiating and completing a full SSL handshake, which we just noted can create issues for non-proxy solutions. Furthermore, to ensure robust encryption, the intermediary should no reduce SSL security by downgrading or presenting weak ciphers. There may also be privacy concerns with decrypting specific categories of traffic, such as traffic that contains Personally Identifiable Information (PII) from financial and healthcare site, so a good solution will be able to categorize content before committing to decryption. Selective and granular control for SSL decryption decisions allows the proxy to integrate with corporate and legal compliance policies.

A proxy is also necessary for strong authentication, such as issuing an auth challenge, or sending redirects to other services used for do authentication. A next-generation firewall's authentication is often limited to more passive forms, such as asking another device to provide a mapping from IP address to username. This type of authentication is only 'best-effort' identification – it's not true authentication. In addition, it can be extremely problematic in environments where IP addresses are shared, or where they are dynamically assigned and change hands frequently.

Combined it's easy to see why a Secure Web Gateway is quickly becoming one of the most vital components of an organization's security infrastructure.

Top Three Benefits of a Secure Web Gateway

> "Secure web proxies complement other network security controls by safeguarding common threat vectors, while enabling data loss prevention, regulatory compliance, and protection from internal and external threats."
> — ESG

A Secure Web Gateway provides a much-needed layer of defense that protects you from ubiquitous, emerging and advanced web threats, empowering you to safely support mobile users and devices and confidently move more applications and workloads to the cloud. To maximize the value of a SWG, you should look for a solution that:

1. Detects and Prevents Evasive Cyberattacks

By virtue of being a proxy, most SWGs can identify threats concealed in web traffic that would otherwise evade detection by firewalls and other stream-based security solutions. As described in the previous section, a SWG proxy will eliminate any ambiguities and look at the entire session before deciding what to do next. This is often the only way to uncover and stop attacks before they can do any damage and prevent policy violations that put your compliance and ongoing operations at risk. While this enhanced security is inherent to proxies, you should also look for a SWG that can:

- **Stay on top of new and emerging threats** – constantly monitoring and incorporating new attack signatures into detection capabilities. Up-to-date web intelligence is a must. Intelligence that is augmented and correlated with the latest file, email and endpoint threat intelligence will give you a holistic approach, with superior efficacy, to uncover attacks targeting your organization.

The search giant Google reports that 77% of all its traffic is encrypted. — Google

You should look for SWGs that can do file extraction and orchestration to ensure traffic is appropriately inspected and handled. Ideally, the SWG will send content and files to other relevant systems (DLP, EDR, CASB, etc.) to improve the ability of the overall security infrastructure to identify attacks and coordinate an effective response, while maintaining compliance.

- **Remove the SSL blind spot** – exposing threats hiding in encrypted traffic. The memory and processing required to decrypt SSL traffic can cripple the performance of most security solutions – NSS found next-generation firewalls that enabled SSL decryption averaged an 81% performance loss. As a result, most security solutions let SSL traffic pass through uninspected. Given the prevalence of SSL, with half the web encrypted, that's a lot of traffic not being analyzed for attacks or policy violations. A Ponemon Study found that nearly half of cyberattacks over a 12 month period used encryption to sneak into organizations undetected.

Because proxies are built to efficiently decrypt and reassemble traffic, they can handle encrypted traffic to eliminate the SSL blind spot. But not all SWGs are the same – a US CERT Advisory warned that many HTTPS inspection products do not properly verify the certificate chain of the server before re-encrypting and forwarding client data, which means they could be enabling a Man-in-the-Middle (MiTM) attack. To combat, the SWG must reconstruct "the SSL connections to the same standards clients and servers negotiated." It should have strong, "modern" cipher coverage, supporting the most recent TLS versions (e.g. v1.2), and not allow weak ciphers.

The SWG should also provide visibility into all SSL traffic, even the traffic from clients leveraging cloud services. To support corporate privacy policies and regulatory requirements, the SWG should allow you to dictate exactly which traffic to decrypt, via rules and policies. To meet performance needs, you may want a separate dedicated appliance to intercept and decrypt all combinations of TLS versions and ciphers in your environment. If you choose this route, the appliance should help you get maximum benefit from the decryption, completing it once and then sending it to all appropriate systems for deeper inspection and enforcement.

2. Provides Visibility Into Web Traffic

The web is hard to keep up with - there are new web sites, new content, new links, etc. constantly being added. All represent new attack vectors that threat actors can use to infiltrate the organization and compromise its operations and assets. With a firewall, a lot of web traffic bypasses the controls and security measures in place, because users go directly to web services to get their work done. In addition, most organizations are in the dark about what applications users are using. Unfortunately, it's impossible to secure or control the unknown, so the first thing you should look for is a SWG solution that can:

- **Monitor and log everything** – keeping track of what is happening throughout the environment, not only on-premises, but also in all your public and private clouds. EVERY web transaction should be monitored, so you have the visibility and information you need to understand who is using the web and how it's being used. This helps you understand how you are being attacked and create better security and use policies in line with your data protection and compliance objectives.

- Nearly 75% of all legitimate websites have unpatched vulnerabilities. — Symantec
- The typical organization thinks they are using 30-40 cloud apps, but are actually using 841–95% of those apps are not SOC-2 or GDPR compliant. — Symantec

- **Support compliance efforts** – offering the granularity that's essential to effectively control usage and apply policies aligned with regulatory requirements. It is not enough to see and control usage based on HTTP and HTTPS or the application name and a simple subset of fields. You need a SWG that understands and can categorize different web traffic, based on its many attributes, to support more precise policy enforcement. Granular control over app usage will improve the efficacy of your risk management and compliance efforts.

Regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), International Traffic in Arms Regulations (ITAR), Gramm-Leach Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI), European Union's General Data Protection Regulation (GDPR), which is set to take effect in May 2018, have strict data guidelines around how the data can be handled and where it can reside. The SWG should be able to hone in on relevant traffic and apply policies, such as ‘save data within xx country,’ to maintain compliance.

3. Optimizes the Total Cost of Ownership (TCO)

To be effective, a SWG can’t be too complicated to deploy, implement or maintain. It should be easy to integrate and able to adapt to effectively protect against new and emerging threats in web traffic, applications and environments. You should look for a SWG that can:

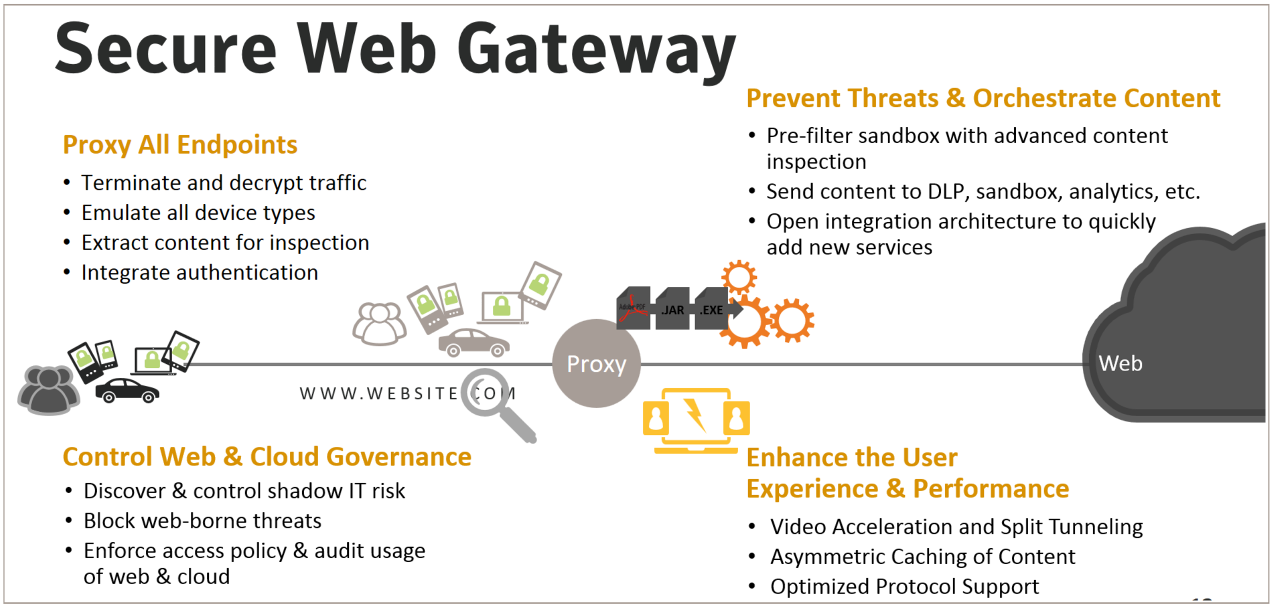
- **Maximize existing investments with a robust ecosystem** – integrating with other solutions in the ecosystem and extending the security stance across all the organization’s environments, both on-premises and in the cloud. The solution should be able to forward traffic to other services, so they can appropriately inspect or apply policies to it that adhere to the organization’s overall business and security objectives.
- **Perform ‘as advertised’** – inspecting all web transactions, without degrading performance or causing significant delays. Processing and inspecting traffic adds latency, but the delay must be imperceptible to your end-users. Make sure the solution can deliver the performance you need, when everything is turned on, even SSL decryption, not just when a few features are enabled. Better yet, look for a solution that can enhance the user experience.
- **Minimize management** – ensuring the solution is easy to deploy, manage and maintain, while being flexible enough to meet the unique needs of the organization. It should be able to easily extend consistent protection across all on-premises and cloud environments.

> “When next-generation firewalls turned on client-side SSL decryption, 2048 ciphers caused a mean average of 81% in performance loss across all vendors tested.”
> — NSS Labs “SSL Performance Problems

Sometimes vendors will try to deliver on requirements to protect the web through partnerships. This adds complexity for customers, forcing you to deploy, manage, maintain and integrate multiple products, from multiple vendors who have varying service level agreements, objectives and roadmaps. You should look for an integrated, comprehensive web security solution that requires minimal time and resources to keep current.

How Symantec Delivers

Symantec’s secure web gateway enables you to monitor, control and secure web traffic, so you can confidently embrace mobile initiatives, move workloads to the cloud, and adopt cloud apps. The Symantec Secure Web Gateway strengthens your security stance, providing a single, powerful security solution that can be deployed on-premises, in the cloud or in hybrid environments for real-time



Secure Web Gateway

Proxy All Endpoints

- Terminate and decrypt traffic
- Emulate all device types
- Extract content for inspection
- Integrate authentication

Prevent Threats & Orchestrate Content

- Pre-filter sandbox with advanced content inspection
- Send content to DLP, sandbox, analytics, etc.
- Open integration architecture to quickly add new services

Control Web & Cloud Governance

- Discover & control shadow IT risk
- Block web-borne threats
- Enforce access policy & audit usage of web & cloud

Enhance the User Experience & Performance

- Video Acceleration and Split Tunneling
- Asymmetric Caching of Content
- Optimized Protocol Support

web protection and control. It integrates with your ecosystem to enhance the performance and security of your overall security infrastructure, while delivering users a superior web experience.

Symantec's approach gives you the visibility, attack prevention and simple management you need to protect your web traffic and enable your mobile users:

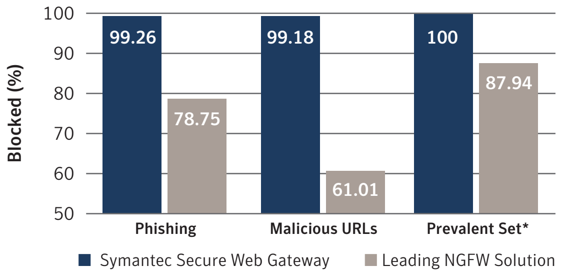
1. Cyber Attack Detection and Prevention

The Secure Web Gateway terminates and reassembles the web traffic, so it can be processed by multiple layers of security, in a single efficient pass. This means that traffic is fully inspected and validated before it reaches its destination. This protection can be extended to your cloud environments with the Symantec Web Security Service (WSS). With Symantec, you can:

- **Stay on top of new and emerging threats** – Symantec's extensive, up-to-date web protection gives you the holistic approach you need to identify and mitigate the risks posed by the web. A recent Tolly report documented the attack detection benefit the Symantec's SWG had over a leading next-generation firewall solution. The chart below shows how effective Symantec was at preventing phishing, malicious URLs and prevalent attacks.

Symantec Secure Web Gateway vs. Leading NGFW Solution Web Security Effectiveness

Malware Tests (Higher numbers are better)



Notes: "Blocked" categories configured as similarly as possible.
Symantec allowed for more granular blocking.

Source: Tolly, March 2017
*Prevalent Set refers to known malware that has been in use in the last 4 weeks.

Symantec is constantly learning and incorporating new attack vectors into its detection capabilities, leveraging the real-world data collected by Symantec's Global Intelligence Network, which provides the broadest and deepest set of threat intelligence in the industry. This intelligence can also be correlated with the latest file, email and endpoint threat intelligence.

The Symantec Content Analysis (CA), which is embedded in the SWG, uses dual anti-malware engines to detect malicious activity and eliminate well-known threats to reduce the amount of traffic that requires deeper analysis. It can broker inspections to sandboxes, which detonate suspicious files in multiple sandbox environments to determine their risk level and uncover zero-day threats. It can also run the traffic through multiple security engines, such as:

- **Whitelists and Blacklists**, which identify known good and bad files.
- **File Reputation Analysis**, which looks at hash reputations, based on ratings and risk scores in its up-to-date reputation database, to identify threats.
- **Predictive File Analysis**, which uses static code analysis and machine learning to identify files that exhibit malicious behaviors.

You can also take advantage of:

- **Symantec CloudSOC/CASB** – providing threat detection, data governance, DLP, security controls and post-incident forensic analysis for both sanctioned and un-sanctioned apps.
- **Other devices within the security infrastructure** – enabling additional analysis and orchestrating a response, as needed, to minimize the impact of an attack. Because Symantec SWG terminates and reassembles the entire communication it can integrate with other systems that require the full stream to complete their inspection. Symantec Secure Web Gateway will extract and send content and files to other solutions, including:
  - Data loss prevention (DLP) systems to monitor and protect sensitive data
  - Endpoint detection and response (EDR) systems, such as the Symantec Endpoint Protection (SEP) Manager) – to accelerate verification and remediation of infections
  - Malware analysis engines. For example, Symantec Content Analysis (CA), Symantec Malware Analysis (MA), and third-party anti-virus and sandboxing products
  - Content delivery networks (CDNs)
- **Remove the SSL blind spot** – Symantec Secure Web Gateway can decrypt and reassemble SSL traffic to uncover attacks and ensure your corporate and security policies are consistently enforced across ALL traffic. You control what to decrypt to ensure alignment with corporate privacy policies and regulatory requirements.

Symantec with the Blue Coat ProxySG, was the only vendor to get an "A" for SSL inspection in the report "The Security Impact of HTTPS Interception," based on research by contributors from the University of Michigan, the University of Illinois Urbana-Champaign, Mozilla, Cloudflare, Google, the University of California Berkeley, and the International Computer Science Institute, which triggered the US-Cert Advisory. The Report verified that Symantec maintains the TLS/SSL security level, correctly verifying the certificate chain and mirroring both the client and browser ciphers, with strong, "modern" ciphers, such as those supported by TLSv1.2, to prevent MiTM attacks.

If you have multiple devices that want decrypted traffic, the Symantec SSL Visibility Appliance can offload the decryption to maximize the performance and lower the TCO of your security infrastructure. The Visibility Appliance takes a 'decrypt once - feed all' approach to enable the rest of the security infrastructure to focus on delivering what they do best.

2. Visibility into All Web Traffic

Symantec gives you visibility into your web traffic, so you can start to implement controls to manage your risks and meet your security and compliance requirements. With Symantec, you can:

- **Monitor and log everything** – Symantec SWG can be deployed to monitor every web transaction, both HTTP and HTTPS, so you know exactly what is going on in your environment and can create better use and data loss prevention policies. This visibility forms the basis of good threat intelligence and the implementation of effective corporate and security policies that align with your business requirements and tolerance for risk.

  The Secure Web Gateway can integrate with the Symantec CloudSOC platform, the industry's leading Cloud Access and Security Broker (CASB), to give you visibility and governance over your data in more than 21,000 cloud apps. CloudSOC delivers insightful visualizations and intuitive controls that protect against non-compliant activityand threats targeting cloud accounts. It can even discover access that you may not know about, uncovering Shadow IT that can be brought into your organization's domain and control.

- **Support compliance efforts** – With Symantec, you control how cloud apps are used to protect against data loss to ensure ongoing compliance. The Symantec Secure Web Gateway receives an app feed from the Symantec Global Intelligence Network, which contains attributes of more than 21,000 cloud apps, and growing. Most apps have about 90 attributes each that describe the business-readiness of the application. These attributes help you understand the risks of the app and determine whether it meets your compliance requirements. An attribute may identify where data resides, whether two-factor authentication is used, etc. You can use these attributes to build granular policies that provide exacting control over the application to manage and mitigate your risk. For example, you can 'allow' employees to use Box for enterprise file sharing, but 'block' files containing credit card numbers from being shared externally.

In addition, to adhere to specific data sovereignty and residency requirements, the Symantec Cloud Data Protection (CDP) solution can be easily integrated with the Secure Web Gateway to enable you to encrypt or tokenize sensitive traffic before it goes to the cloud. This ensures data, whether it's in-transit, stored or being processed in the cloud, remains private and accessible only to authorized users.

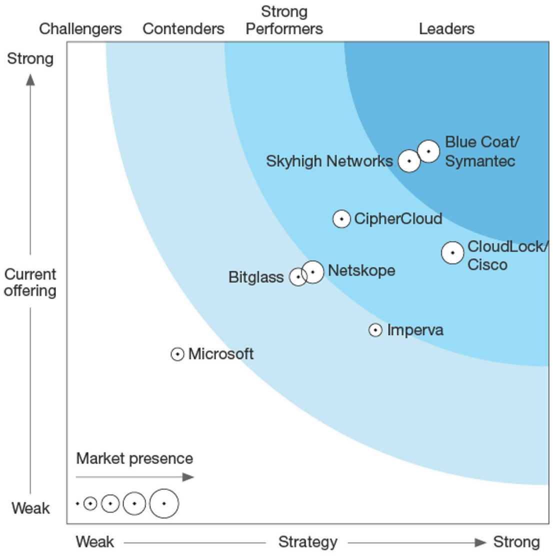
Integrated Cyber Defense for unparalleled visibility and protection

The Symantec Global Intelligence Network, which feeds Symantec's solutions with the broadest, deepest threat intelligence in the industry, uses artificial intelligence (AI) to analyze activity across endpoints, email and web traffic. It allows Symantec to identify advanced targeted attacks that would otherwise go undetected, with:

- 1,000 cyber warriors in nine global SOC centers around the world for response that never sleeps.
- 175,000,000 endpoints and 50 million consumer users protected.
- 8 billion security requests processed across products daily.

Symantec can encrypt or tokenize application fields or files, inline, in real-time, based on your policy to protect sensitive data in your applications. For example, if you want to use ServiceNow as your HR platform in Germany, you can tokenize employee data classified as Personally Identifiable Information (PII) to ensure it doesn't leave the country/EU's borders. This level of control enables you to adopt cloud apps while maintaining compliance with relevant regional and industry regulations.

Forrester Research identified Symantec as a Leader in their recent *Wave Report on Cloud Security Gateways*



Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable ratings

3. Low Total Cost of Ownership (TCO) for the Security Infrastructure

Symantec offers a comprehensive solution that gives organizations all the capabilities they need to protect their web traffic. Symantec devices are purpose-built to deliver high performance and low latency, while scaling to meet the varied security needs of your enterprise. With Symantec, you can:

- **Take advantage of open ecosystem to maximize investment value** – Symantec works with a robust ecosystem to give you the choice and flexibility you need to create an environment that meets your unique security and business requirements.

  Built with an open architecture, Symantec Secure Web Gateway integrates with your other systems, using standards and common protocols, to simplify integration with third parties that extend and enhance their capabilities.

  For example, you can use Secure Web Gateway to terminate, reassemble, inspect and apply policies itself and to extract and send content/files to other devices for additional analysis and enforcement actions. The Secure Web Gateway can work with your Active Directory database to identify a user, authenticate them, apply appropriate policies, and then coordinate additional inspections or responses aligned with business and security objectives.

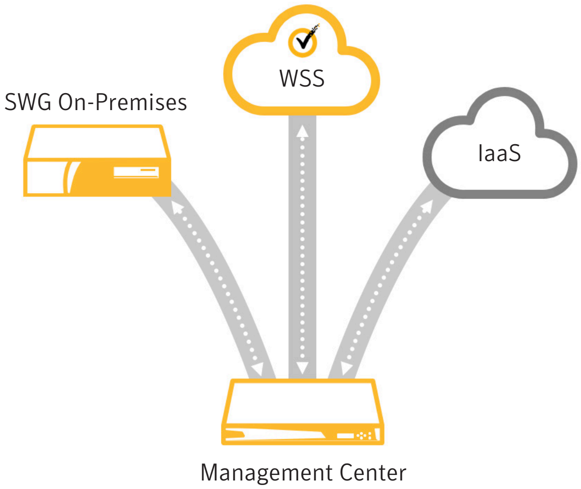
- **Deliver Unmatched Performance and Reliability** – Symantec bases performance numbers on how the solution handles traffic when all capabilities are turned on, not just a subset. This allows you to right-size your deployments and ensure an optimal user experience. You don't have to worry when you turn on logging, decryption, content analysis, etc. – the solution will perform as advertised.

  The Secure Web Gateway has been purpose-built to meet the many demands of the enterprise, with a custom operating system designed for security that enables it to efficiently inspect and protect web transactions. In addition, the Secure Web Gateway delivers capabilities that improve the overall performance and availability of your business apps and media, with bandwidth management, content caching, traffic optimization, and streaming media splitting and caching features.

- **Minimize management** – Symantec simplifies web security across on-premises and cloud environments. A single policy can be written or revised and applied to all on-premises and cloud services for consistent enforcement. Everything remains in sync from deployment and enforcement to reporting, making it easy to keep your security and compliance in force.

  Symantec works to ensure these integrations are seamless to you and imperceptible to your users. The communication between systems often runs in the background, as it does between Symantec Secure Web Gateway and Symantec CloudSOC, which delivers a combined view of all your on-premises and mobile users. The combination of SWG and CloudSOC can track, measure, monitor and appropriately control all your web activity from a single location for tight alignment with your security and compliance objectives. When a user initiates a connection to a web app, Symantec Secure Web Gateway confirms the app is sanctioned and the user authenticated and then sends it to Symantec CloudSOC. The Secure Web Gateway includes the user's authentication information, so there are no extra steps for the end user - they don't have to interact with CloudSOC or log in again.

Universal Policy Enforcement



Summary

Secure Web Gateways provide the necessary control point you need to protect your business from web threats. The Symantec Secure Web Gateway gives you visibility into your web traffic, even encrypted traffic, to uncover attacks and apply effective, granular controls that keep your business operating as it should. The Symantec Secure Web Gateway improves the efficiency and effectiveness of your entire security infrastructure, ensuring all traffic is appropriately inspected for consistent security and policy enforcement. As a result, you can confidently embrace the cloud to support the varied needs of your users, without sacrificing security or jeopardizing compliance.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, 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 suite of products for protection at home and across all of 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 or connect with us on Facebook, Twitter, and LinkedIn.

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