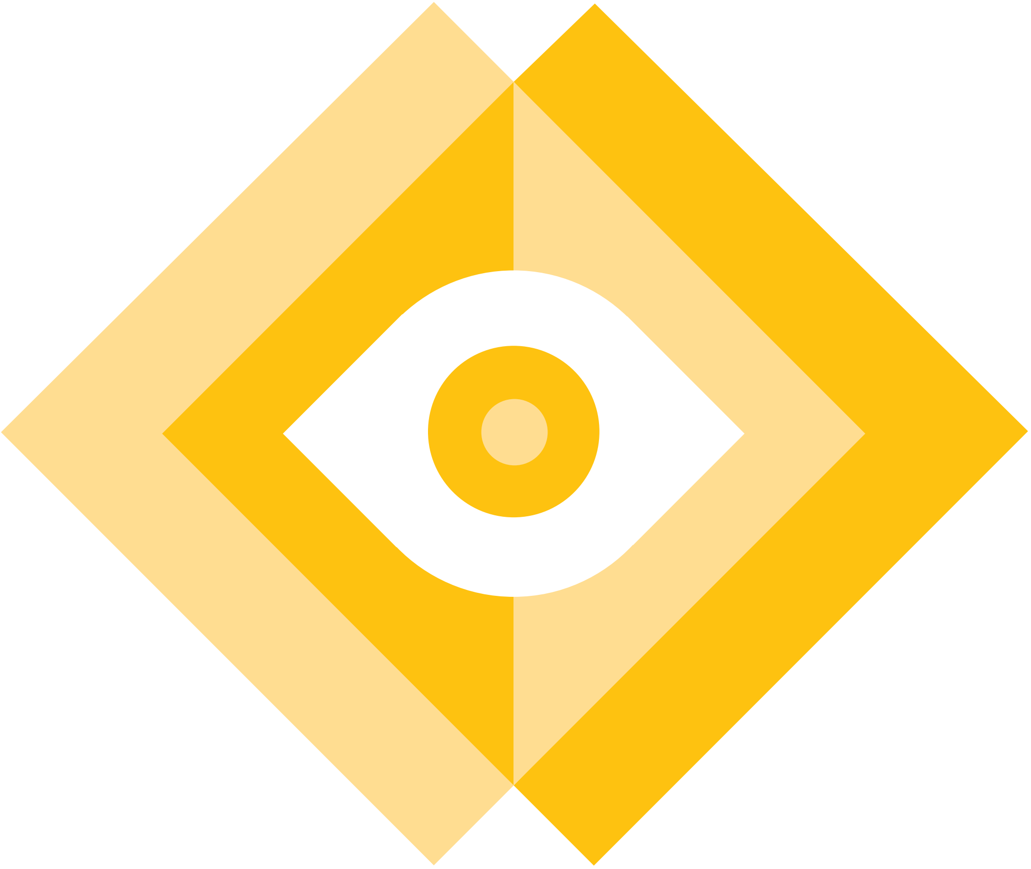


Symantec Content Analysis

Throwing Sand at the Cloud Pays Big Security Dividends

WHITE PAPER

Proxy and Multi-layered Threat Analysis + Enterprise-grade Sandboxing in the Cloud

As advanced threats ramp up, an integrated approach to security is critical. If you're considering moving to the cloud, this issue may become even more important as you sort out which security offerings will best protect your enterprise's information.

It's smart to consider your options carefully. We've all heard of the hard dollar impact of data breaches, but there's also an impact on your brand when a breach occurs. A Ponemon study found that data breaches cause a 5% drop in a company's average stock price the day a breach is announced, a 7% loss of customers, and 27% of consumers have discontinued a relationship with a **company that suffered a breach**.

Given those numbers, it's critically important to protect your data whether you're contemplating moving some or all of your infrastructure to the cloud. In this brief, we'll discuss exactly how you can best protect your information regardless of your pace to move to the cloud. We cover proxy versus next-generation firewalls (NGFWs), why retaining enterprise-grade threat protection is critical when you move to the cloud, and deployment options to consider.

Advanced Threat Protection: How Proxy Beats Next-Generation Firewalls

Next-generation firewalls have their place in your enterprise's security environment. For example, they're effective at preventing unwanted network communications over specified protocols, based on IP address or geolocation. They can also control and lock down multiple channels of communication from inside your organization to the Internet. If you are willing to take a large hit to performance, you can extend these capabilities to include simple stream-based malware scanning. However, when it comes to securing web traffic and protecting your organization from advanced attacks, zero-day threats, and sophisticated malware, nothing compares to proxy architecture.

Here are examples of where a proxy is more effective at defeating malware than a next-generation firewall:

Full file reconstruction uncovers true identity – Next-generation firewalls are stream-based, which makes them vulnerable to evasive malware. In contrast, a proxy reconstructs the full session and its contents before delivering it to users. This approach reconstructs the communication and file to determine if it is harmful before sending it to the final destination.

Files are detained until verdicts are delivered – A proxy can detain files from delivery until all packets are gathered, assembled, and inspected using multiple methods of interrogation and analysis against all available threat intelligence. Only then—if it is determined to be safe—is it delivered to its intended destination.

Safe and scalable handling of encrypted traffic – For many organizations, encrypted data can account for 60-70% or more of network traffic. This data is also increasingly becoming the vehicle for attackers to hide malicious activity. For effective threat protection, traffic needs to be visible to security tools for analysis and inspection, yet at the same time, organizations must adhere to mandated privacy policies.

Additionally, **a recent academic paper** compared multiple encrypted traffic inspection tools, including next-generation firewalls and other streaming-based tools, in their effectiveness of intercepting encrypted traffic. The report found that nearly all tools degraded security, and many even introduced severe vulnerabilities. Only **Symantec ProxySG** received an "A", while all others received either "C's" or "F's".

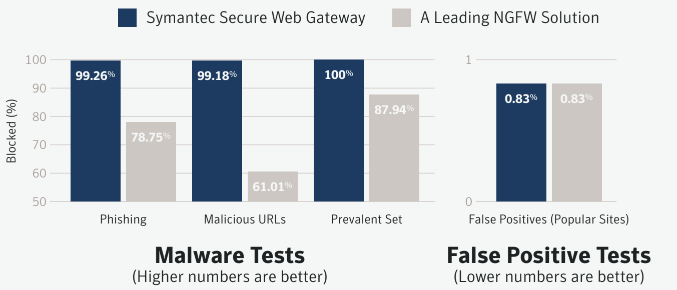
Proxy blocks more – When it comes to full session termination, decryption, and inspection – proxy wins. A **Tolly report**, which compares Symantec Secure Web Gateway to a leading NGFW solution, clearly shows how much more effective a proxy architecture is for web security. For malware tests comparing phishing, malicious URLs, and a prevalent set of known malware, Symantec Secure Web Gateway beat a leading NGFW hands-down based on effectiveness.

The Tolly report found that Symantec SecureWeb Gateway provides:

- Superior detection rates across the range of tested threats
- Superior malware database fed by the largest real-time intelligence feeds in the industry
- Exceptional detection of evasion techniques
- More options for anti-malware engines and sandboxing techniques

Symantec Secure Web Gateway vs. A Leading NGFW Solution

Web Security Effectiveness



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

Source: Tolly, March 2017

Figure 1: A Tolly report found that Symantec Secure Web Gateway has superior detection across the range of tested threats compared to a leading next-generation firewall solution.

Proxy Architecture = Better Protection

PROXY ARCHITECTURE WITH SYMANTEC	NEXT GENERATION FIREWALL
Superior malware scanning and protection • Termination of traffic • Multi-vendor open eco-system	No termination and inspection • Single vendor approach • Easy to bypass
Easily add inline data loss prevention	No ability to terminate and add inline data loss prevention (requires Proxy)
SSL decryption with leading cipher support	Limited cipher support with 60%+ performance degradation
Market leading Cloud Access Security Broker (CASB) controls	API protection only. No inline CASB capabilities
No hardware-needed cloud service to support roaming users or entire offices	Protection for roaming users requires VPN backhaul to customer hosted/owned firewall
Market leading endpoint integration • Indicator of Compromise (IoC) verification, blacklisting, and remediation	Limited remediation and no endpoint management

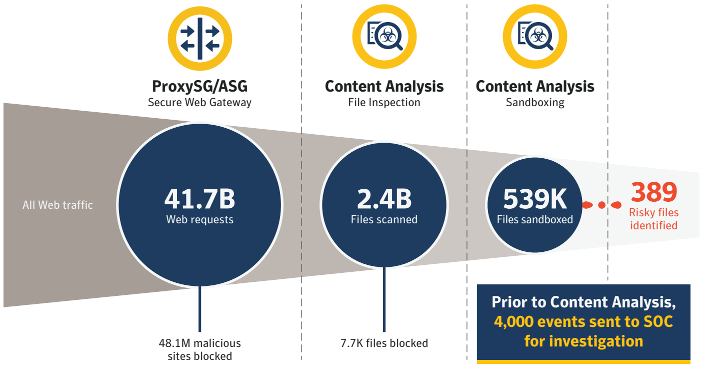
Get Better Protection with ProxySG, Content Analysis, and Sandboxing

Building on the strengths of the proxy architecture, Symantec enables Advanced Threat Protection through a multi-layered approach that sends extracted content from **ProxySG**, **Symantec Messaging Gateway** and **Symantec Endpoint Protection** to **Symantec Content Analysis** to efficiently uncover malicious activity in web or mail traffic. After utilizing file reputation services, dual anti-malware engines and advanced machine learning, only remaining "truly unknown" files are sent to a sandbox for complete detonation.

Figure 2 illustrates how a Symantec customer effectively benefited from this approach. In this example, the Fortune 20 customer received almost 42 billion web requests in 30 days. Symantec technologies analyzed all those requests using a multi-stage process and filtered them down to only 389 risky files that needed further investigation.

Powerful Results

Fortune 20 Company



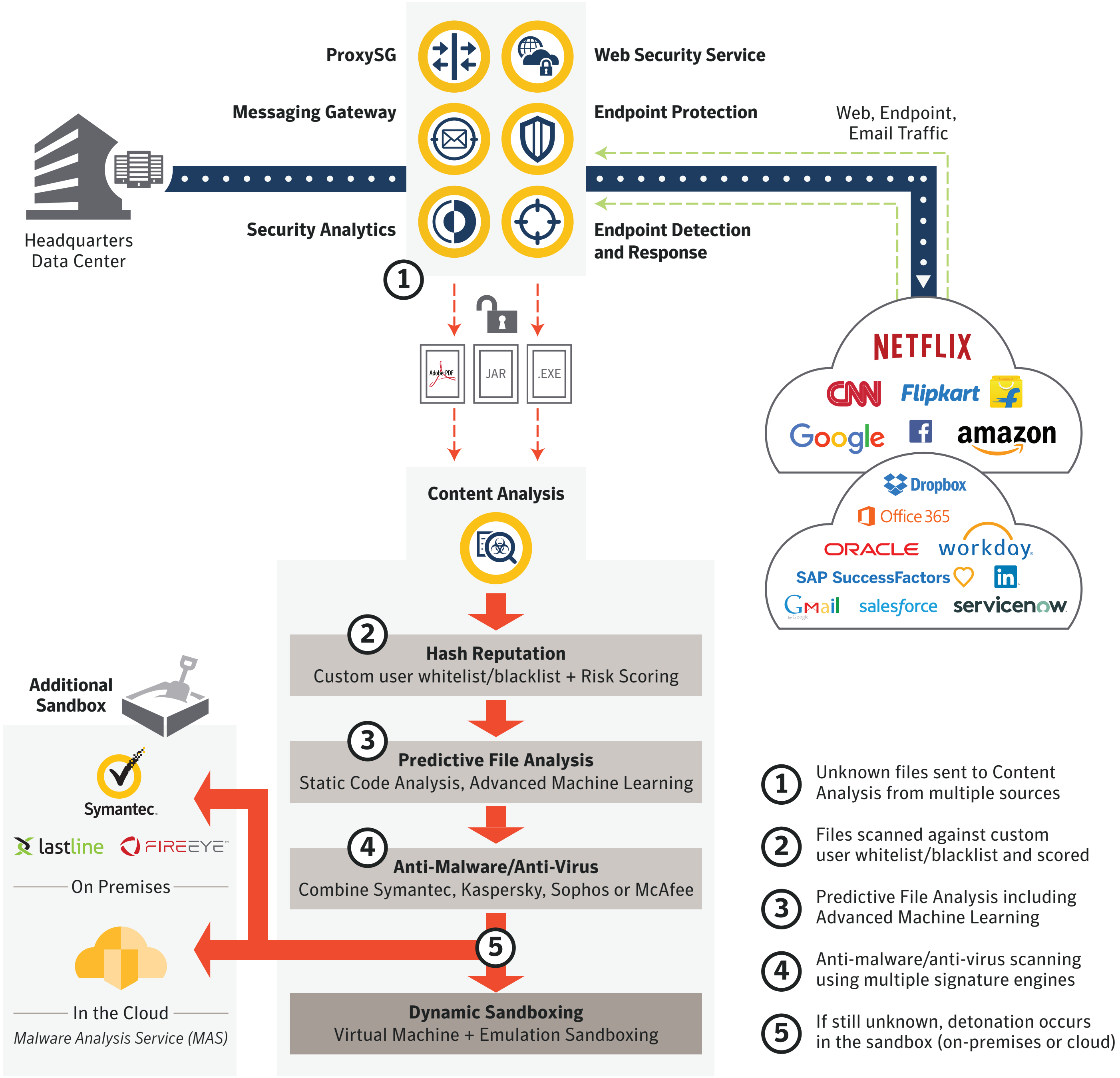
*30 Days of actual traffic at Fortune 20 Customer

Figure 2: A Symantec customer receives billions of web requests in 30 days - but which ones warranted further investigation? The combination of ProxySG, Content Analysis, and sandboxing filtered the requests down to just 389 files that required the security team to investigate.

Why a Stepped Approach to the Cloud is Best

You might have multiple concerns about moving to the cloud, including being forced to take an all-or-nothing approach or lowering your expectations for security. You might also worry about maintaining productivity and performance because you don't want your IT administrators and security analysts to throw away their hard-earned investments in existing skills, processes, policies, or integrations.

Organizations see the value of moving to the cloud, but when it comes to security, many are not ready to go "all-in." Policy, performance, regulations, and other requirements may require that you take a more measured approach in moving to the cloud. That's why we believe it's important to make a move on your terms when you're ready, and a stepped approach is best. Analysts have stated there are significant advantages to security professionals who take a hybrid approach of deploying cloud-based security along with on-premises.



1. Unknown files sent to Content Analysis from multiple sources
2. Files scanned against custom user whitelist/blacklist and scored
3. Predictive File Analysis including Advanced Machine Learning
4. Anti-malware/anti-virus scanning using multiple signature engines
5. If still unknown, detonation occurs in the sandbox (on-premises or cloud)

Figure 3: After ProxySG scrutinizes web traffic, Content Analysis analyzes any files within that traffic based on hash reputation, advanced machine learning, and then scans for malware and viruses using dual-antivirus/antimalware engines. Any remaining "unknown" files are sent on to dynamic sandboxing.

Are You Tapping into the Cloud + On-Premises Security Advantage?

Symantec offers excellent solutions for securely protecting your enterprise, whether you adopt an on-premise, hybrid, or all-cloud approach. You expect enterprise-grade advanced threat protection on-premises, and there's no reason to lower your security expectations when moving to the cloud. Fortunately, Symantec delivers by offering:

- Flexible policy enforcement – acceptable use and risk mitigation
- Universal policy shared between on-premise appliances and the cloud
- Market-leading URL classification/categorization
- High-performance/throughput
- Authentication
- SSL Decryption
- Shadow IT visibility and control
- Web isolation for safe browsing of unknown sites
- Largest civilian threat intelligence network in the industry
- Multiple malware scanning engines
- Dual-detection (VM & emulation) sandboxing
- Comprehensive reporting and visibility

Why Trust Symantec to Carry You to the Cloud?

Symantec is the world's trusted security vendor and the clear leader in numerous security areas, including secure web gateway, data loss prevention, cloud access security brokers (CASB), email, endpoint security, and encrypted traffic management.

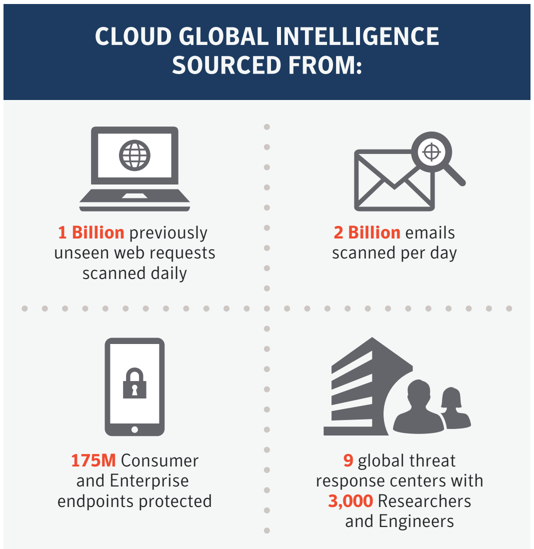

CLOUD GLOBAL INTELLIGENCE SOURCED FROM:
1 Billion previously unseen web requests scanned daily
2 Billion emails scanned per day
175M Consumer and Enterprise endpoints protected
9 global threat response centers with 3,000 Researchers and Engineers

Figure 4: The Symantec Global Intelligence Network offers an unparalleled level of visibility across endpoint, email, and web traffic to discover and block advanced targeted attacks that would otherwise go undetected.

Unfortunately, most security providers simply provide isolated security solutions, but the cloud mandates a new model of integrated security. The Symantec Cloud Security Platform provides a unique way to securely enable cloud adoption while unifying both cloud and traditional on-premise environments for seamless security.

Symantec's superior threat intelligence, which is powered by the massive **Global Intelligence Network**, offers integrated cyber defense for unparalleled visibility and protection. By using the vast amounts of computing power available in the cloud, we analyze over 3.7 billion lines of telemetry, which is the broadest and deepest set of threat intelligence in the industry.

It's Your Choice: On-Premises, Cloud, or In-Between

Dip your toe in and test the water or dive in headfirst – it's your choice. Either way, Symantec ensures the water is safe. Regardless of the approach you choose to take, these industry-leading Symantec services are cloud-based and can support your enterprise security requirements:

- Proxy/Web Security Services
- Information Protection
- CASB
- Web Isolation
- Cloud Workload Protection (IaaS)
- Sandboxing
- Endpoint Protection
- Email
- Identity

Here are the combinations of solutions we recommend based on your environment's requirements:

- If you choose on-premises for your entire organization, consider ProxySG + Content Analysis and a dedicated Content Analysis Appliance configured for sandboxing
- If you choose a hybrid approach for your primary locations/users, consider ProxySG + Content Analysis + cloud-assisted sandboxing. For remote locations/users, consider **Web Security Services** + **Malware Analysis Service** for sandboxing
- If you want to move your entire organization to the cloud, choose Web Security Service + Malware Analysis Service for sandboxing

Concerned about the impact on your IT team's productivity when it comes to administering these solutions? With Symantec Universal Policy, you can configure and manage your policy in one place, so it spans your data centers, remote and branch offices, and mobile users. Universal Policy includes policy control for malware scanning, URL and risk scoring, SSL decryption, authentication, and more with the ease of central management. With this capability, moving to the cloud is seamless, smooth, and as secure as ever.

Moving to the cloud can pay huge security dividends for your organization, but you'll want to make a move in a responsible way that maps to your overall IT cloud strategy and your business imperatives. Rest assured, Symantec is there for you every step of the way.

Conclusion

Unlike traditional blocking tools, Content Analysis delivers an enterprise-level, single-box platform with a multi-layer scanning and analysis approach to more effectively detect and block known and unknown threats. This optimizes the workflow of Security Operations and Incident Response teams, so they address real threats that only affect their environment. All content passes through these steps to scan, identify, and block uncovered attacks to the organization using a sophisticated filtering approach to threat detection and protection.

About Symantec Content Analysis

Together with the ProxySG, Symantec Messaging Gateway, or Symantec Endpoint Protection, Content Analysis blocks known threats, sources and signatures, and centrally analyzes unknown content. Zero-day threats are automatically escalated and brokered to Symantec's dynamic sandbox for validation before sending content to users. Content Analysis is a sophisticated, multi-layer inspection platform that combines reputation services, white and blacklisting, static code file analysis, machine learning, dual anti-malware signature inspection engines, and on-box or cloud sandboxing to protect against known and unknown threats. Integration with **Symantec Security Analytics**, Endpoint Protection Manager, and many other third-party security technologies enables threat validation, inoculation, and swift remediation across the network, cloud, and endpoint.

For More Information

Visit us online for additional resources at **http://go.symantec.com/content-analysis**.

To get started now or for help designing your Content Analysis solution, contact your Symantec channel partner or Symantec Representative.

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**, subscribe to our **blogs**, 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**