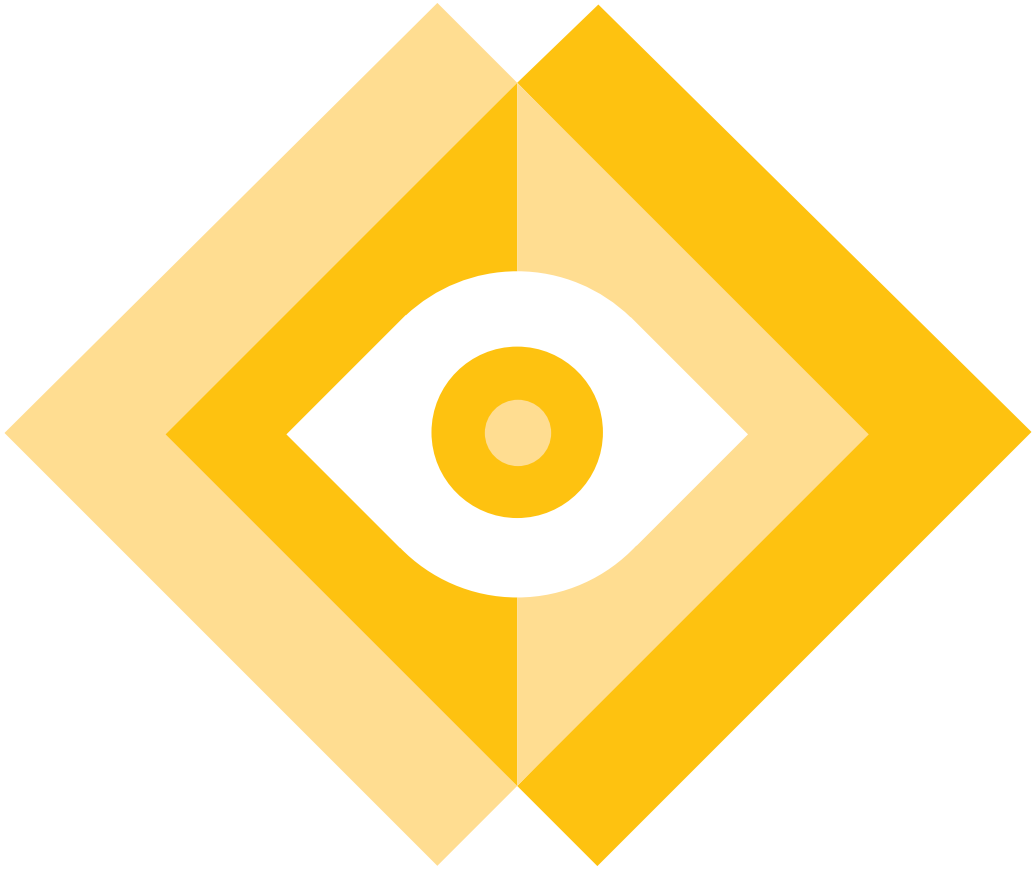


Symantec Content Analysis

Moving Beyond Detection to Prevention: Get automated, advanced threat protection at the gateway

WHITE PAPER

Symantec

The High Price of Too Many Alerts

As a new breed of attackers executes increasingly sophisticated and effective attacks on enterprises, it's challenging for security teams to keep up. According to the Ponemon Institute, organizations receive roughly 17,000 alerts a week. Sifting through all that information wastes an average of 395 hours weekly and costs, on average, a staggering $1.27 million annually.[1]

Alerts overwhelm security teams, and that can mean missed threats and attacks. The siloed approach many organizations use to fortify their defenses introduces challenges, including:

- **Many Attack Points**: Single-point detection tools aren't effective in protecting against dynamic web threats that use advanced and targeted methods.
- **Multiple Security Methods Needed**: Maximum protection requires multiple security technologies, but this requires more effort from a security team to maintain and patch every component in a timely and efficient manner.
- **Weak Threat Intelligence and Analysis**: Traditional blocking tools stop at simple signature matching and rely on threat intelligence that is often outdated or requires manual updates. Sophisticated attacks quickly bypass these weak, single layer defenses.

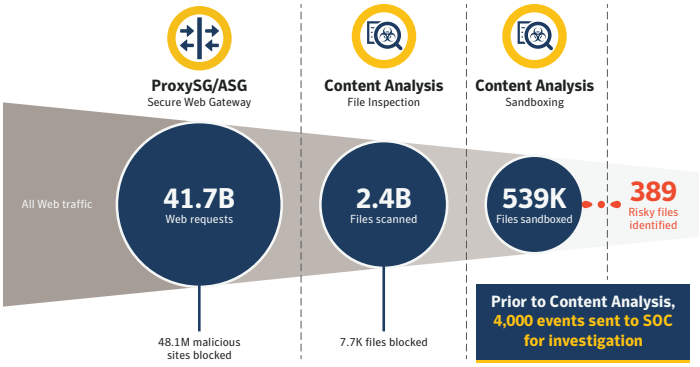
Symantec Content Analysis Uncovers, Analyzes, and Blocks Any Threat

The best approach is to use multi-layered security for the most effective defense against known and unknown threats. Symantec Content Analysis works in conjunction with Symantec's ProxySG, the secure web gateway used by 70% of the Fortune Global 500, to block all known malicious URLs using Symantec's massive Global Intelligence Network. It then orchestrates unknown content for centralized analysis, inspection, and blocking. Symantec Content Analysis filters these unknowns through a multi-stage analysis process to investigate if the unknown truly is harmful, and if your security team needs to conduct further investigation and remediation.

Symantec Content Analysis is often attached to ProxySG to perform deep analysis of content from all web sites interrogated by ProxySG. It is also of interest to Symantec Endpoint Protection and Secure Messaging Gateway customers since these products are integrated to provide even stronger protection for network, endpoint, and email traffic. Read on to learn more about the newer features in Content Analysis including "on-box" support for sandboxing, threat intelligence from a vastly larger Global Intelligence Network, integration with Symantec Endpoint Protection Manager, and an open API to support numerous third-party solutions.

Powerful Results

Fortune 20 Company



*30 Days of actual traffic at Fortune 20 Customer

Figure 1: In this example, Symantec ProxySG and Content Analysis analyzed billions of web requests using a multi-stage process and filtered them down to only a handful of valid alerts that required further investigation by a security team.

Flexible Deployment

Symantec Content Analysis offers many deployment options to meet your organization's needs. It's available as a physical or virtual appliance. Our new virtual appliance options offer increased performance – up to 1.6Gbps on VMware ESX. Sandboxing is offered both in on-box as well as a cloud option. For organizations deploying Symantec's Web Security Service (WSS), the same content inspection engine in Content Analysis is available within WSS as well.

Improve Sandboxing Efficiency with "On-Box" Malware Analysis

Symantec Content Analysis acts as a pre-filter to sandboxing by using multi-layered analysis to block malicious content. Pre-filtering improves performance by eliminating the number of files sent for sandboxing by up to 37%.[2] Additionally, the dynamic sandbox can be configured and customized to mimic different client software configurations that closely match your OS environment. Sandbox analysis is more efficient as you are only inspecting files that might pose a threat to your specific configurations, significantly reducing the number of false positives. With sandboxing and Content Analysis now together on a single appliance, you reduce your sandbox footprint and create a centralized architecture with lower capital acquisition costs. For enterprises that need more throughput, Symantec Content Analysis and sandboxing can also be deployed on two separate appliances.

Content Analysis also protects your users from potentially dangerous files, such as zero-day threats, with dynamic sandboxing and validation. Other sandboxing solutions send these risky files on to users – even when they're still undergoing detonation and analysis testing. With Content Analysis, a sandboxed file is "trickled" to users and won't be delivered in full until all testing is complete, and the file is deemed safe.

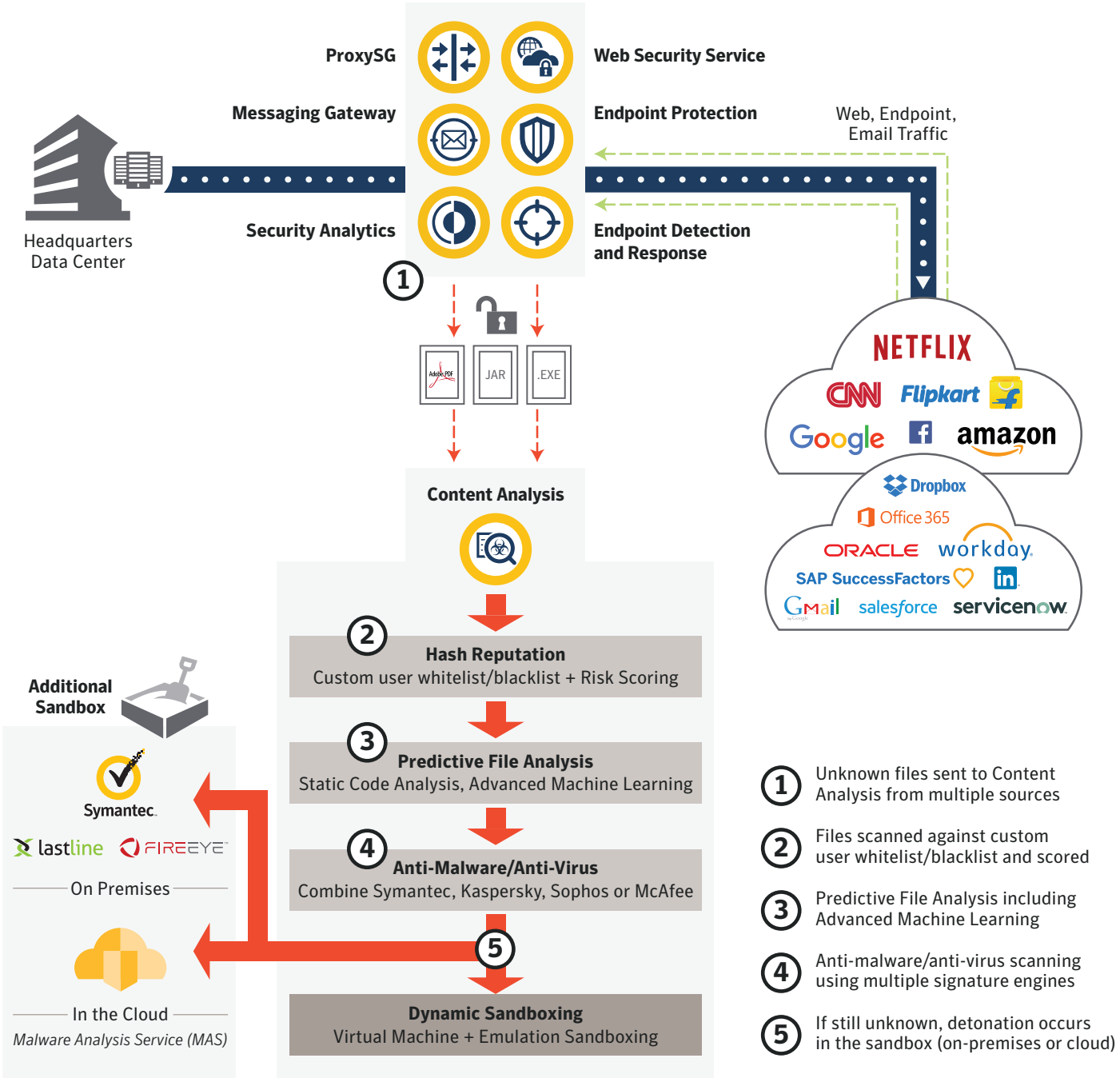


Figure 2: After ProxySG scrutinizes web traffic, Content Analysis analyzes any files within that traffic based on hash reputation, advanced machine learning, and then scans for malware and viruses using dual-antivirus/antimalware engines. Any remaining "unknown" files are sent on to dynamic sandboxing.

Block More Threats with a Massive Global Intelligence Network

The stronger the intelligence behind threat analysis, the more effectively risks can be blocked. Symantec's powerful Global Intelligence Network has been combined with the Blue Coat intelligence network, which increases the number of records that are analyzed from 1 billion to over 4 billion. Symantec Content Analysis uses this full file reputation service to identify threats and assign risk scores to each file. "Known good" files are passed to users, "known bad" files are blocked, and unknowns proceed through the process for further analysis and ultimately, are sent for customized and efficient sandboxing.

Protect Your Endpoints with Symantec Endpoint Protection Manager Integration

Threat protection requires a coordinated effort between your network and endpoints. Symantec Content Analysis integrates with Symantec Endpoint Protection (SEP) Manager, which means your endpoints are protected when malicious content is detected. The process starts with Symantec Content Analysis identifying potential threats using information from the Global Intelligence Network and its multi-stage analysis. Once an unknown is deemed malicious, that information is then sent to SEP Manager to verify the threat at the endpoint where security professionals can take action to prevent the lateral spread of infection and perform automated remediation. SEP Manager can also be configured to send files from SEP clients to Content Analysis to deeply analyze any file downloaded at the endpoint.

Integrate with Third-Party Security Solutions (including FireEye)

The open REST API and support for Symantec Integrated Cyber Defense Exchange (ICDx) enable third-party security tools to leverage the powerful threat analysis capabilities of Symantec Content Analysis. This enables integration with many other tools including, other sandboxes, and can dramatically reduce costs and increase sandboxing efficiency. Content Analysis functions as a "pre-filter" for FireEye by blocking known threats and sending only truly unknown threats on to FireEye. This approach lowers costs because far fewer sandboxes are required – the overcapacity that's typical in sandbox installations is no longer needed.

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 or Symantec Messaging Gateway, 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.

References

[1] *The Cost of Malware Containment*, Ponemon Institute.
[2] Based on internal Symantec tests.

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**.

Symantec™

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

20B265887_WP_ContentAnalysis_EN