

# Symantec® Content Analysis

## Multi-Layer Threat Inspection, Detection, and Sandboxing Uncover the Unknowns



### TABLE OF CONTENTS

---

Protection and  
Empowerment in Today's  
Evolving Threat Landscape

The Industry's Attempt at  
Security

A Superior Advanced Threat  
Protection Architecture

Threat Isolation

Flexible Deployment and  
Integration Options

Conclusion

### Protection and Empowerment in Today's Evolving Threat Landscape

There is no question that security attacks on organizations will continue to grow and evolve. The question is, how can an organization respond to malware and other risks without unnecessarily constraining the workforce?

How can an organization get beyond the fear and anxiety that leads to excessive prohibition, prevention, blocking, and excluding so that security technology can both protect and empower people?

The answer is with a multilayered defense—one that uses advanced security technologies and sophisticated operational practices in combination to cover the full spectrum of threat vectors. This white paper explores the growing importance of multi-layered defense in today's fast-changing web environment and key considerations in implementing an effective multilayered defense strategy.

#### Overcoming the Obstacles of Securing the Web at All Entry Points

The web remains the primary source of malware distribution, but it is difficult for organizations to secure the web because of its ever-changing nature and massive scale. Highly motivated malware authors need just the tiniest security hole to exploit for financial and competitive gain or to achieve a political or ideological objective.

Attackers have a wide variety of methods that they can use in any combination to exploit vulnerabilities. The increased mobility of an organization's data, combined with bring your own device (BYOD) initiatives, are creating ample opportunities for cyber criminals.

The productivity advantages achieved by BYOD are tempered by the fact it introduces new platforms (for example, iOS and Android) that must be secured, but over which the organization has little control. Moreover, cloud and social media apps make it extremely difficult for organizations to keep up with all the potential vectors of attack.

According to the Symantec® Internet Security Threat Report, in 2018:

- 1 in 10 URLs analyzed was identified as being malicious
- 545,231 total ransomware detections; enterprise detections increased by 12%
- Web attacks on endpoints increased by 56%

## The Need for an Advanced Multi-Layered Defense

Since computers and networks can be infected from a variety of attack points, the days of single-point detection belong to the past. The rise of new, dynamic web threats and Advanced Persistent Threats demands a multi-layered security architecture that maximizes coverage to ensure best-in-class enterprise security.

Organizations must deploy combinations of security mechanisms to maximize their attack prevention coverage. That means not only using multiple security technologies in multiple layers of the environment but also deploying good operational practices, such as applying updates and patches on time and demanding that suppliers provide fast fixes to vulnerabilities.

From an antimalware/antivirus (AV) perspective, a multi-layer defense should include coverage at the desktop, server, and network levels. Industry standards such as PCI (Payment Card Industry) have strict requirements around what AV protection must be put in place in specific verticals. Quite often, end-customers want assurances all is being done to prevent a security breach. As a result, a multi-layered approach makes sense from a security perspective and a business perspective, helping mitigate risks to the organization and brand.

## The Industry's Attempt at Security

### Endpoint Protection: An Essential First Step

Endpoint Protection solutions address threats that originate from an infected desktop. They can help protect attacks that originate inside the network; for instance, when a user with an infected USB thumb drive plugs it in and uploads the malware to their computer. Some organizations may also use Endpoint Protection solutions from multiple vendors to maximize their attack coverage.

Endpoint protection is key; however, relying only on endpoint protection provides a false sense of security. Users can tamper and disable agent settings; they may not regularly update their software to protect against the latest threats. Also, with the advent of BYOD, many of the mobile devices being used to access an organization's resources are completely vulnerable—few AV solutions are available for iOS and Android devices, and even fewer users install these security apps on their devices. As a result, organizations must apply multiple layers of antimalware defense to optimize their coverage to include a wide variety of possible infection methods.

### Advanced Threat Protection at the Gateway: A Must

The Internet gateway is the entry point through which all Internet traffic passes from all types of end-points: PCs, laptops, tablets, smartphones, and IoT devices. By adding network-based threat protection, an organization can complement the security on the desktop and mitigate the risk of attacks, with a single point of control that users

cannot disable or tamper with. Catching malware as close to the security perimeter and as far away from the desktop as possible further reduces the risk of infected data reaching end users.

### Network AV: A Key Component of Network Defense

Adding network-based AV protection to the organization can complement the security on the desktop and help mitigate the risk of attacks. While adding network AV can help, this step alone will not provide the protection required to identify today's threats. Relying solely on a single network AV engine means there is only a single detection method from one vendor. This design is limited to their view of a possible attack, their inspection methods, their update schedule, and their collection of threat intelligence, which may be from a small community of customers and may not contain the latest updates to identify the most current threats. While network-based AV is a critical component, it must be complemented with other detection methods to deliver more effective threat protection.

## A Superior Advanced Threat Protection Architecture

### Architecture Design

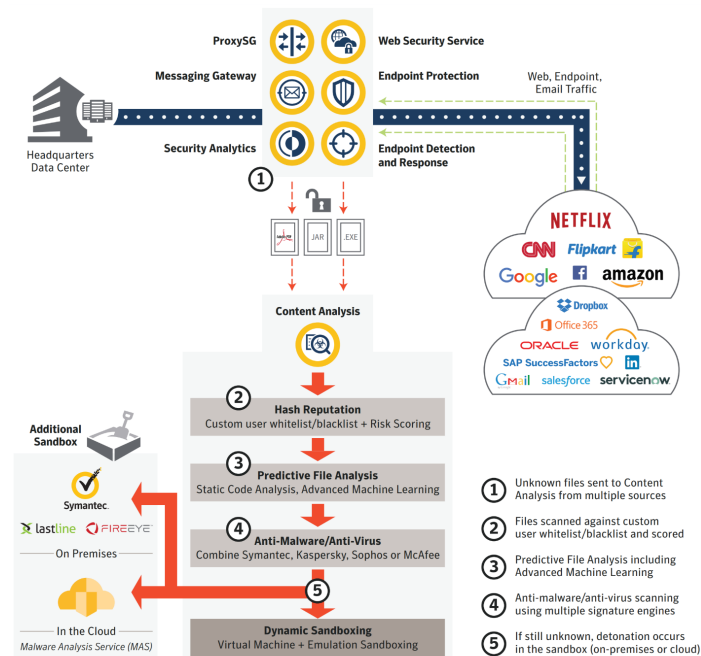
A single product or service cannot provide foolproof security. A superior security architecture requires many layers of protection that work together to give a sum greater than the parts. Symantec brings together the full range of products, services, and technologies to deliver advanced threat protection at the web gateway. It begins with the web proxy providing complete control over all web traffic and flows into the multiple layers of protection that Symantec provides. This termination point that leads into multiple layers of threat examination delivers superior advanced threat protection.

#### 1: Proxy: Necessary Termination Point

A web proxy, a form of termination point, provides a quarantine service for web traffic. It examines 100% of the traffic between users and HTTP/HTTPS sites and categorizes all URLs so that malicious sites or pages can be identified and blocked while good URLs remain accessible according to policies. Since the proxy provides the termination point, it can also use this advantage to pass the suspect files on to other security tools such as Content Analysis for further inspection.

Non-proxy network security deployments and other technologies such as next-generation firewalls (NGFWs, including TAP or SPAN port deployments), do not effectively terminate traffic. With TAP or SPAN port devices, the gateway sits off to the side of the network, observing traffic as it passes by, instead of intercepting and terminating it.

Figure 1: Content Analysis Provides a Multi-Layered Approach to Threat Detection

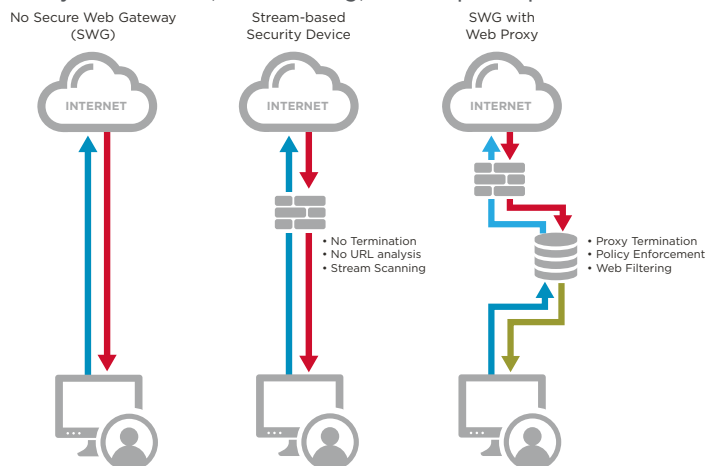


NGFWs use stream-based detection methodologies, examining the traffic as it streams by on the wire. These deployments have a specific flaw. Malware or other threats can get through to gateway or NGFW does not detect the threat in time or does not send out a TCP reset packet in time to disrupt the flow of traffic. Also, because of the nature of stream-based scanning, malware can be delivered using fragmented packets over a period of time and remain undetected. A proxy by its nature would wait for an entire object to be assembled and scanned before allowing it to be delivered.

In the fast-moving web environment, where hackers frequently change their tactics, a defense-in-depth strategy of deploying the Symantec ProxySG in conjunction with an NGFW is essential for providing optimal protection. The ProxySG is engineered to withstand evasion techniques, making it a perfect complement to a NGFW. Its leading web-proxy technology identifies and blocks malicious web content, and its open architecture allows integration with best-of-breed products for an enhanced security posture.

Symantec ProxySG, the industry-leading proxy solution, has been named a leader by Gartner for the past 12 years and is a key piece in an organization's network security architecture. ProxySG will protect web traffic, providing URL reputation, SSL Decryption, categorization and policy control, and real-time blocking. After stage 1, anything that is not immediately blocked via the Proxy is passed on to Content Analysis for inspection and interrogation.

Figure 2: A Proxy Solution Provides a Termination Point to Enable Policy Enforcement, Web Filtering, and Deeper Inspection



## 2: CA: Hash Reputation and File Reputation Services

After ProxySG analyzes and categorizes all web-based traffic, hashes of unknown files are sent from the proxy and then analyzed to determine known reputation.

They are compared against a database totaling over five billion records that is updated daily. Using custom approve and deny lists and file reputation from many vendors, including our own Global Intelligence Network, Content Analysis will perform real-time application and file identification. These files will receive trust scores from 1 to 10.

Content Analysis will pass known 'acceptable' files to users and block those that are identified as 'known bad.' This filtering will further decrease the number of files passed on to the downstream stages of antimalware inspection and sandboxing.

To prevent unnecessary scanning and analysis on files with an identified reputation, you can add a list of SHA1 hashes to Content Analysis. During file processing, Content Analysis will check these lists before reaching out to the cloud-based File Reputation service. The manual approve/deny list configuration results in a quick 'allow' or 'deny,' with no further analysis required. If the hash exists in either list, the file will either be permitted or denied without further processing.

## 3: Predictive File Analysis/Machine Learning

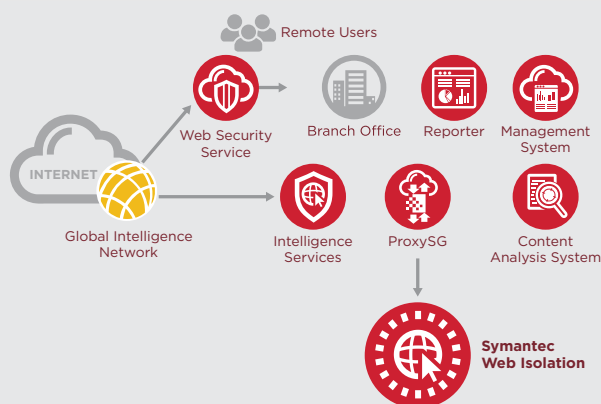
During the Predictive File Analysis stage, Content Analysis runs static code analysis and Advanced Machine Learning to determine if anything within the file code is flagged as malicious. It will parse and extract the file code for comparison to over 5 million data points of known bad data or known bad code.

By combining in-depth knowledge of threats and files with state-of-the-art machine learning, Symantec Advanced Machine Learning (AML) can understand the characteristics of files and create a probability score to determine whether a file is safe or malicious. This probability score determines what Content Analysis should do next with the file:

## Threat Isolation

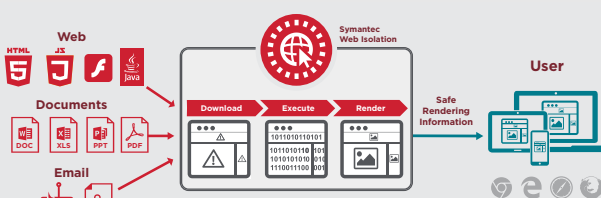
Another innovative piece in advanced threat protection is threat isolation. This layer does not depend on a cycle of detect and prevent. Instead, it isolates malicious web and email content without impacting users. It assumes everything can allow the forwarding of all requests to websites categorized as 'Unknown' or any request coming from critical employees to Threat Isolation. This allows access to the sites while insulating them from any threats.

Figure 3: Symantec Web Isolation Integrated with ProxySG and Web Security Service Provides a Safe Browsing Experience



Symantec Web Isolation can be easily integrated into advanced threat protection by allowing it to isolate all unknown/risky websites as well as enabling it to isolate links and attachments in email.

Figure 4: Unclassified Sites, Links, and Content are Safely Rendered to the End User and Isolated in a Disposable Container that Protects the User from Unknown Malware



- Files with a high probability of being malicious will be blocked outright (convicted).
- Files that are not convicted are forwarded to the remaining security stack for further analysis.

AML includes additional controls to define the threshold and aggressiveness at which AML file blocking occurs. With a high detection sensitivity, AML will be aggressive in its determination of whether a file may be a threat, at the risk of blocking files that may not actually be malicious. With a lower sensitivity, AML will block fewer files, but with a risk of some threats not being detected.

Rather than using signatures to match patterns, machine learning uses proven, well-tested, statistical methods. This allows AML to learn about files in a way that signatures cannot. Using this approach, new, previously unknown threats can be stopped. Even when the attack changes, through replication mechanisms, distribution mechanisms, or the payload itself, AML works to stop threats effectively.

## 4: CA: Antimalware/Antivirus

Content Analysis can deploy a combination of two engines from either Symantec, Kaspersky, Sophos, or McAfee. Signatures are evaluated to identify known bad files and the bad files are blocked. Internal Symantec testing has identified a 12% increase in detection capability when two engines are used, instead of just one. Signature databases are updated every 5 minutes, and support file sizes up to 5 GB.

Utilizing multiple AV engines does more than just block more malware and viruses, it also has other benefits. With multiple engines, there is an advantage of not being tied to a single update schedule or limited to a single scanning technology. The selection of AV engines can best match the ideal defense strategy. If utilizing an antimalware/antivirus engine to scan endpoints, using a different vendor at the network level can be incrementally effective.

## 5: Sandboxing

Symantec sophisticated sandboxing capability is also available with Content Analysis. Organizations can license this sandboxing capability on the same Content Analysis appliance or as a hosted sandboxing service from Symantec. Content Analysis sandboxing has many advanced features that makes it a more-compelling sandboxing option compared to the competition. These features help to quickly analyze and prioritize advanced malware and zero-day threats for remediation and enable continuous security improvement:

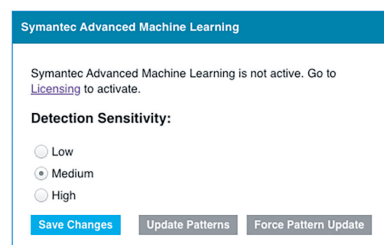
- Unique Dual-Sandbox Architecture:** Emulated and virtualized hybrid support for best evasion detection
- Standard Image Profile Replication:** Customizable analysis environments closely match production systems
- Malware Evasion Detection Methods:** Content Analysis employs a set of aggressive countermeasures to detect and thwart evasive malware



- **Ghost User Plugin:** Simulates user behavior, including keystrokes and acceptance of installation steps to trick malware into executing and therefore trigger detection
- **Detection Pattern Library:** Patterns can detect targeted and single-use malware, and do not rely on signature-based detection methodologies
- **Sandbox Avoidance Detection:** Detects and bypasses both long and short sleeps designed to wait out sandbox analysis and also Identifies attempts to detect if the malware is being inspected in an artificial analysis (virtual machine) environment
- **Static Code and YARA Rule Analysis:** Performs file fingerprinting, detects packers, analyzes strings, and uses textual and binary patterns to identify and classify malware samples
- **Detailed Reports:** Custom reports showing overall risk score, key risk indicators, detailed malware activity report, screenshots of malware execution behavior, and the ability to download malware artifacts all ease malware identification and remediation
- **File Detention:** With the Symantec ProxySG as the termination point, Content Analysis can detain a file while it is being inspected and only deliver it to the user after it has been fully analyzed and deemed safe to send on. This is a unique capability compared to our competitors who simply send on unknown files while sandboxing is still happening.

For organizations that have more demanding performance requirements, that sandboxing functionality can be deployed as another Content Analysis appliance configured just for sandboxing by Symantec, or FireEye or Lastline can be used. There is also the option to forward unknown files for inspection to Symantec cloud sandbox through Malware Analysis Services.

Figure 5: Set the Detection Sensitivity for Symantec Advanced Machine Learning in Content Analysis

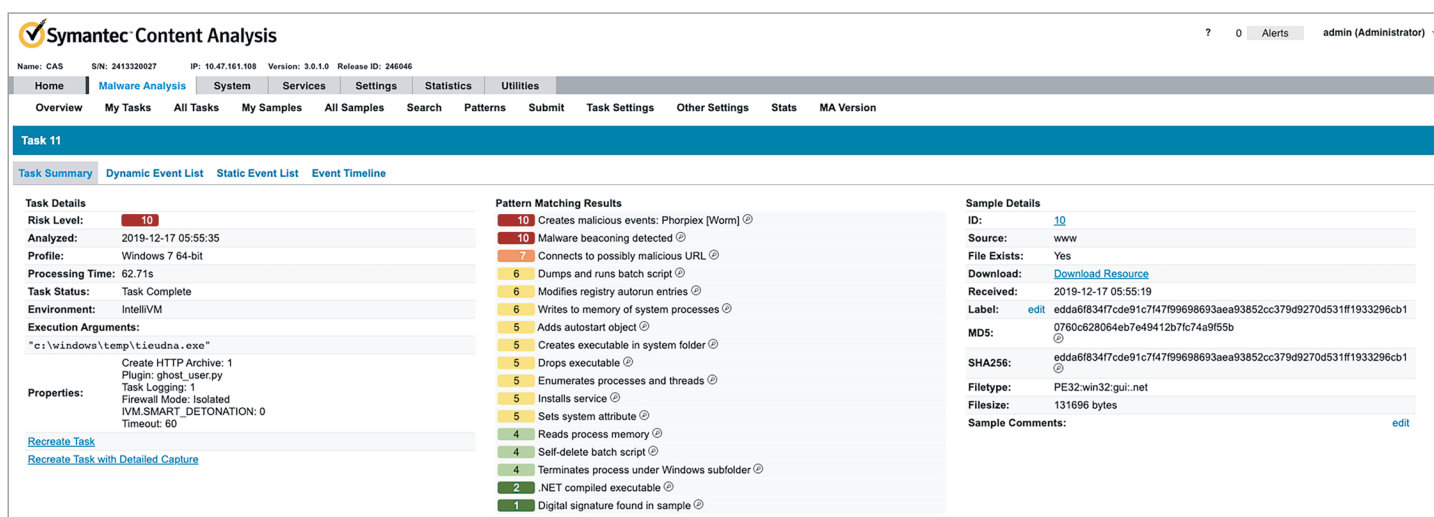


## Flexible Deployment and Integration Options

Symantec Content Analysis offers many deployment options to meet organizational needs. It is available as a physical or virtual appliance. Virtual appliance options offer increased performance: up to 1.6 Gb/s on VMware® ESX. Sandboxing is offered in on-box as well as a cloud option. For organizations deploying Symantec Web Security Service (WSS), the same content inspection engine in Content Analysis is available within WSS as well.

Integrating Content Analysis with other security tools also provides great value. Utilizing ICAP, Content Analysis can also receive unknown files from other sources, not just from the proxy. This enables deep inspection for unknown content originating from the firewall, mail gateway, Endpoint Detection and Response (EDR) solutions, or other sources in the environment. Content Analysis has integration with Symantec Endpoint Security to provide the network to endpoint visibility, analysis, blocking, and remediation required to protect the organization from today's advanced threats. If malware is identified by Content Analysis, it can send Indicators of Compromise (IOC) to Symantec Endpoint Security Manager—or other EDR solutions such as CounterTack—to validate if the network-borne threat made it to the endpoint. It can then inoculate all other endpoints and enable swift response and remediation.

Figure 6: Detailed Sandboxing Reports Indicate Specific Malware Activity



## Conclusion

Unlike the competition, Symantec implements a multi-layered approach that creates a funnel effect, utilizing swift scanning technologies upfront before sending truly unknown files for more in-depth inspection by more sophisticated, compute-intensive processes. This can result in fewer false positives, more efficient scanning, and focused response only on actual threats that matter to the organization.

Implementing a multi-layered cyber security platform will help take the burden off security teams as well as reduce the anxiety of wondering if a point solution will be good enough. With security attacks continuing to grow and evolve, a comprehensive multi-layered security approach is required to protect the organization.

Figure 7: Symantec Multi-layered Funnel Effect

