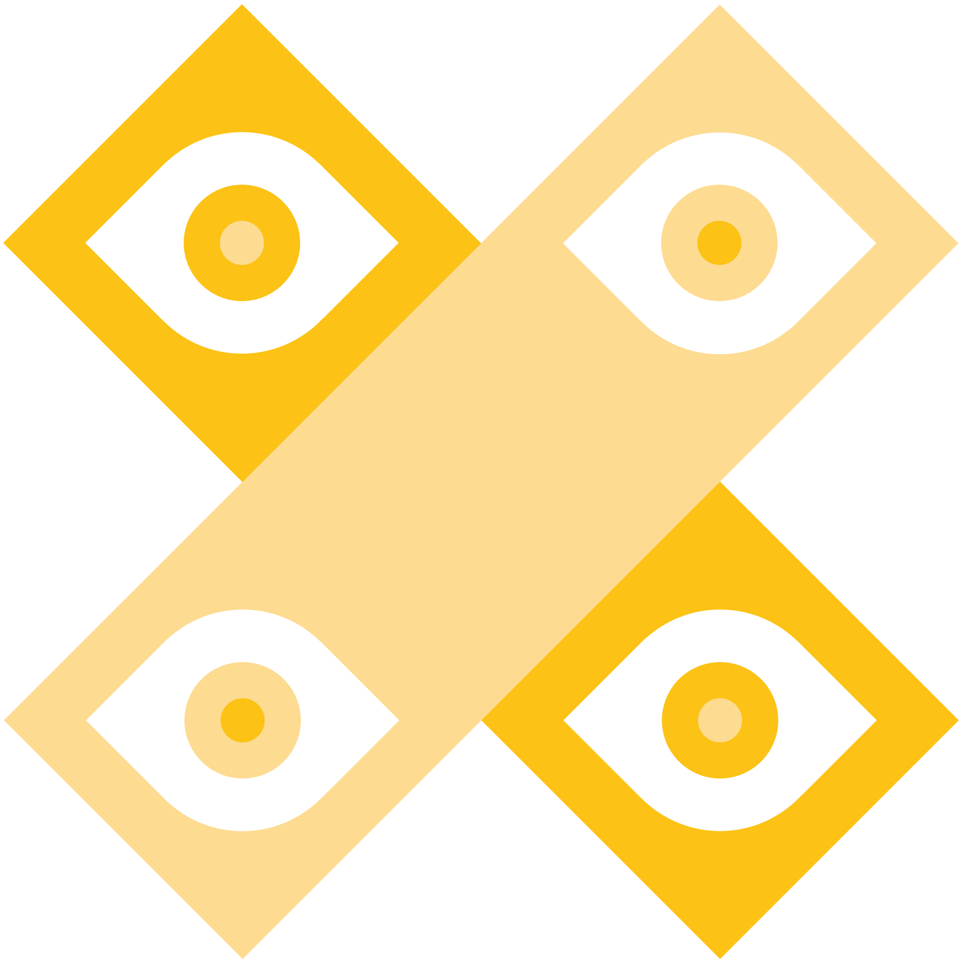


Network Security for the Cloud Generation—A Comprehensive Defense-in-Depth Approach

A Key Part of an Enterprise's Integrated Cyber Defense Platform

WHITE PAPER

Contents

The New Normal

Organizations once needed only a single on-premises security stack that protected endpoints in a single office. Those days are long gone. The new normal for the Cloud Generation is a threat landscape shaped by complex factors and demands:

- Data, devices, applications are no longer confined to the traditional perimeter. They exist on-premises, in the cloud, in a hybrid state, and outside corporate control. This is illustrated by the wide adoption of public and private clouds and an ever-increasing number of sanctioned and unsanctioned cloud applications and unmanaged devices. The new edge is wherever your data resides, and it demands maximum protection at all times.
- A rising number of sophisticated attacks target the network, endpoint, or cloud—sometimes all three. These multistage attacks come from more vectors and conceal themselves in encrypted traffic.
- Encryption presents new challenges. More and more traffic (cloud apps, web, email, and more) is converging on HTTP and the percentage of it that's encrypted is rising beyond 50 percent[1]. Organizations need to efficiently scan encrypted traffic for threats while ensuring employee and customer privacy and complying with regulations.
- Data compliance regulations are becoming more stringent and punitive. Data protection is now critical to your business as well as your clients—especially for cloud apps and cloud providers.
- A security solution must integrate with existing technologies as well as third-party solutions to make security operations more efficient and enable faster response.

What is Needed

Only a network security platform that integrates on-premises and cloud-delivered security—governing access, securing information, protecting against advanced threats, and providing security across the cloud, network, and endpoints—can protect organizations and users from today's sophisticated threats.

But in a sea of security technologies and opinions, how do you determine which way to go?

One tried-and-true method is to look at the strength of the platform's core components—all platforms have a foundation—and evaluate additional pieces from there. If your security foundation is not solid, your entire security posture is at risk.

For a true network security platform, we believe there are only two fundamental approaches to consider: A next-generation firewall (NGFW) or a secure web gateway (SWG). Both can play a role in your enterprise. But which one will you build your strategic security capabilities around? And beyond the platforms, which vendors provide the critical threat intelligence needed to identify and block sophisticated attacks?

A Next-Generation Firewall is Not the Answer

A number of firewall advances have taken the platform beyond the standard features you would expect. On the surface, the NGFW appears to check many boxes to help organizations complete a security strategy, while being easy on the budget.

The NGFW provides some protection for a broad spectrum of applications and protocols beyond the standard web-based protocols and beyond examining packet-based threats. If IT leaders in your organization decide you need those particular protections afforded by a NGFW are sufficient, it may be an excellent addition to your layered defenses.

Firewalls were well suited to the first internet generation, where there were lots of ports, protocols, and Layer 3 and 4 policies to configure. For example, virtual private networks and intrusion prevention systems grew up as added L3/L4 security layers. NGFWs consolidated these with a very high-scale, cost-effective architecture.

However, web, cloud, mobile, and email has collapsed onto HTTP. Now the key is deep application intelligence into HTTP and the ability to decrypt those communications. All while maintaining security and privacy, plus integrating threat protection and information security.

Where Next-Generation Firewall Vendors Fall Short

The Cloud Generation

NGFW vendors claim you get all-in-one protection by putting a box at the perimeter and scanning packets as they pass. The truth is the perimeter is eroding and, in some cases, doesn't exist at all. Mobile users work from home or travel the globe—the way we protect them must change. User mobility transcends the traditional network's physical boundaries. With applications migrating to the cloud, SaaS/IaaS/PaaS providers have replaced corporate IT.

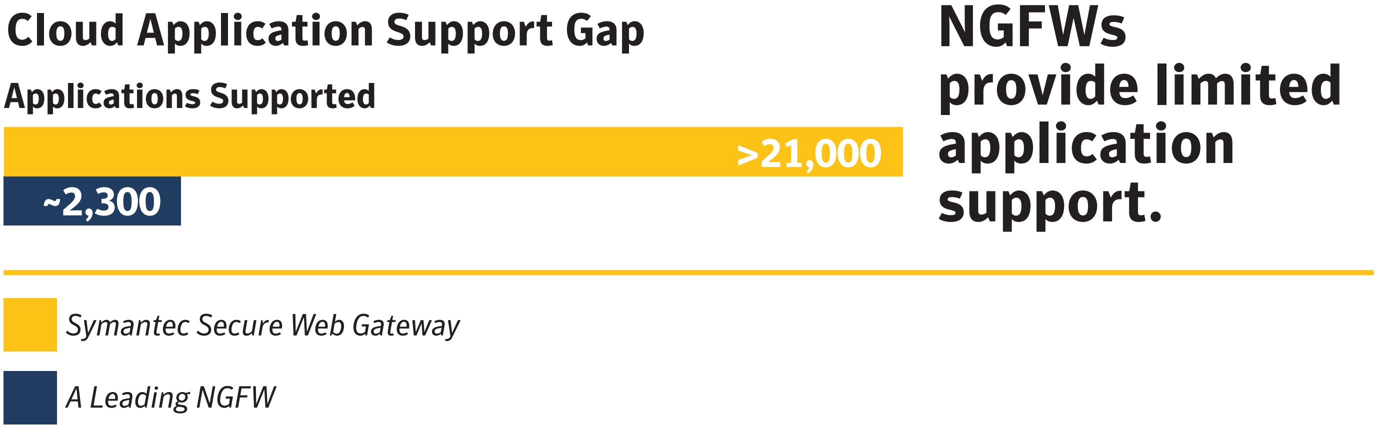
Mobile Growth

By 2020, there will be 105.4 million mobile workers[10]—**IDC**

For 2017, the number of mobile phone users is forecast to reach 4.77 billion[9]—**Statista**

As analyst firm Enterprise Strategy Group recently noted, "Next-generation firewalls (NGFWs) proved to be a stopgap at best .... It is 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."[2]

A recent Tolly Group report on security effectiveness concluded that a leading NGFW could support only an eighth as many cloud applications as the leading SWG[3] (*Figure 1*). Cloud and mobile support is essential as The Cloud Generation continues to grow.

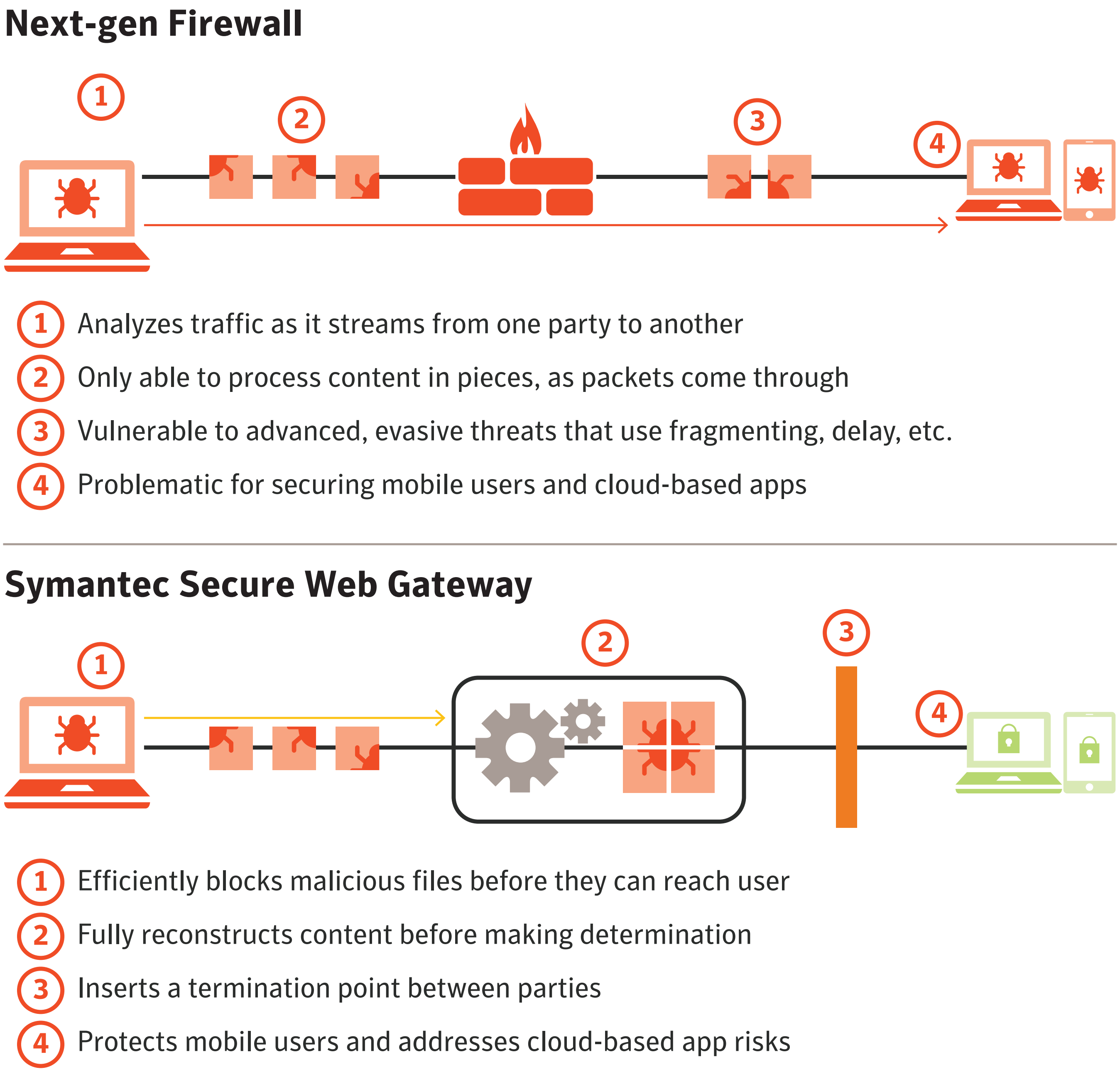


NGFWs provide limited application support.

Figure 1[3]

Inferior detection

NGFW solutions prioritize throughput over protection. This is because, as a stream-based solution, they simply scan and pass data—instead of looking at the entire session before deciding what to do next. This reveals a specific flaw: Malware and other threats can reach the internal network if the gateway or NGFW does not detect the threat in time, or doesn't send out a TCP reset packet in time to disrupt the flow of traffic.



Next-gen Firewall

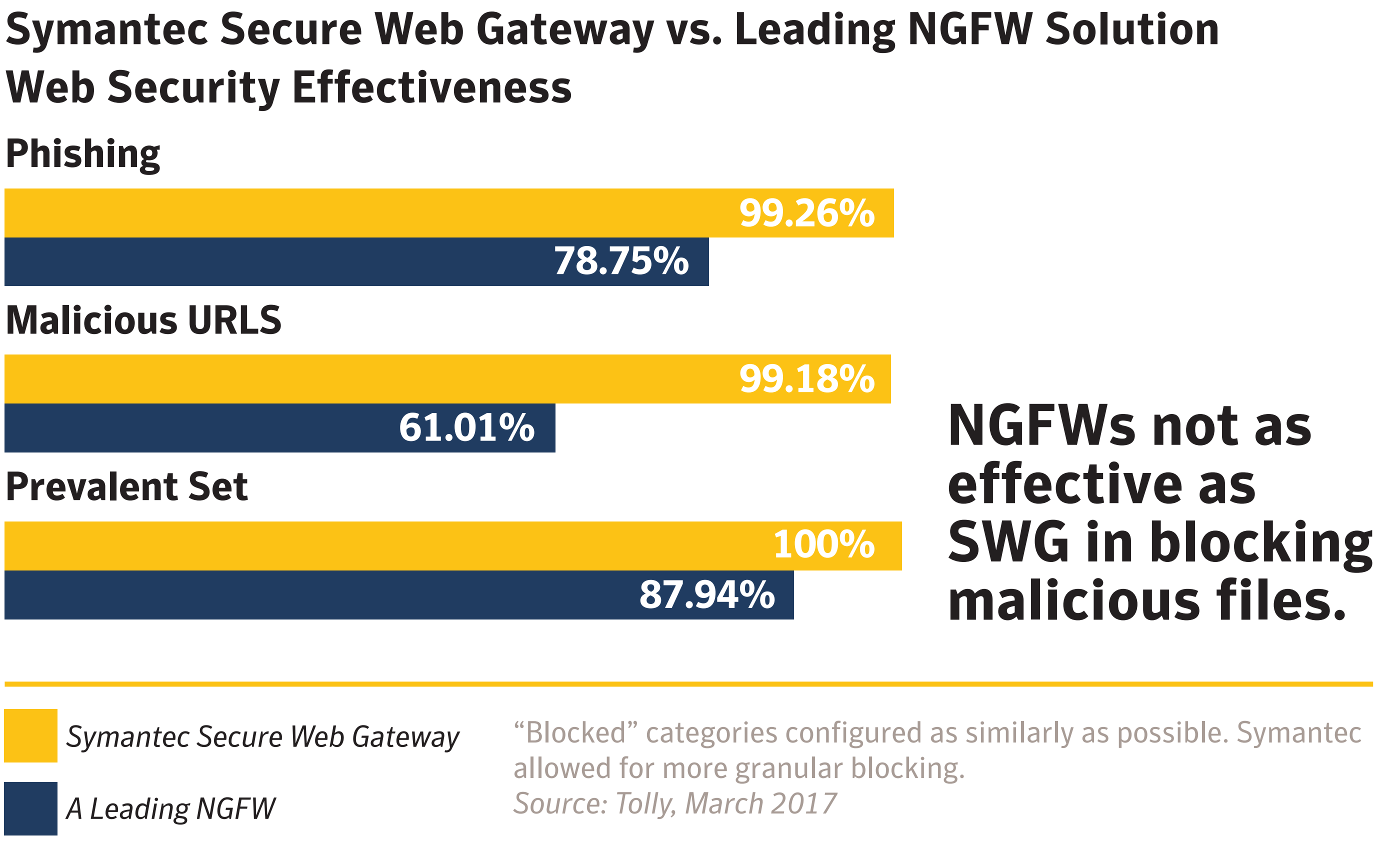
1. Analyzes traffic as it streams from one party to another
2. Only able to process content in pieces, as packets come through
3. Vulnerable to advanced, evasive threats that use fragmenting, delay, etc.
4. Problematic for securing mobile users and cloud-based apps

Symantec Secure Web Gateway

1. Efficiently blocks malicious files before they can reach user
2. Fully reconstructs content before making determination
3. Inserts a termination point between parties
4. Protects mobile users and addresses cloud-based app risks

Figure 2

Also, because of stream-based scanning's nature, simple obfuscation techniques can circumvent a NGFW. For example, packet fragmentation or base-64 encoding can easily bypass a NGFW scan mechanism (*Figure* 2). In contrast, a SWG by its nature waits for an entire object to be assembled and scanned before allowing it to be delivered. This enables the SWG to utilize extensive threat intelligence to detect and prevent more threats (*Figure* 3).



NGFWs not as effective as SWG in blocking malicious files.

"Blocked" categories configured as similarly as possible. Symantec allowed for more granular blocking.
Source: Tolly, March 2017

Figure 3[3]

Moreover, NGFWs are designed to allow traffic through the device before they properly categorize the application. Network World said this approach "… could easily result in unintended consequences and insecure configurations—a valid concern" during its Clear Choice test[4].

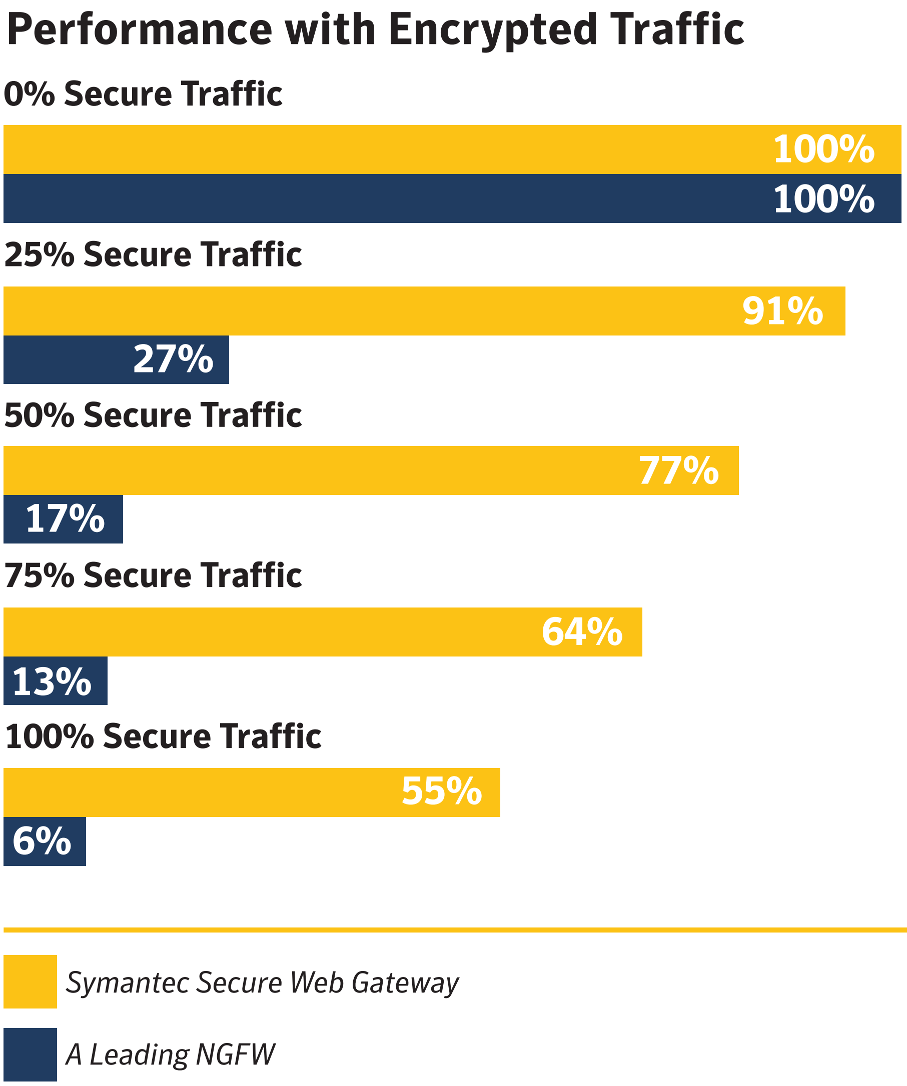
For more details on how proxies (SWGs) stand up better to malware than NGFWs, see MRG Effitas report: **Protection Comparison of Proxy and NGFW architecture against RAT and ransomware C&C**. MRG Effitas concludes: "The proxy architecture is more secure by default compared to the NGFW architecture because the architecture itself breaks multiple C&C channel classes, tunneling protocols and evasion techniques by default."[5]

Incomplete portfolio

NGFW vendors lack a complete portfolio, leaving large gaps in protection. Can your NGFW vendor cover endpoint detection and response (EDR), data loss prevention (DLP), cloud access security broker (CASB), email, web isolation, mobile security, and other aspects of effective security? Can they also deploy these capabilities not only on-premises but also through cloud services—avoiding costly network infrastructure bloat? Also, if your vendor's products don't fully integrate with third-party solutions, you limit visibility and will struggle with a patchwork security infrastructure.

Inability to effectively manage encrypted traffic

SSL traffic cripples the performance of NGFW solutions. NSS Labs found NGFWs that enabled SSL decryption lost an average 81 percent in performance[5] (*Figure 4*). As a result, most NGFW solutions let SSL traffic pass through uninspected. Given the prevalence of SSL, **with half the web encrypted[1]**, too much traffic is not being analyzed for attacks or policy violations. This is especially alarming when you consider that a **Ponemon study** found that nearly half of cyber attacks, over a 12-month period, used encryption to sneak into organizations undetected[6].



Maintain performance even with threat prevention and/or SSL/TLS enabled

Figure 4[3]

The architecture of a typical NGFW is optimized for packet processing, either through specialized hardware or through allocation of resources to packet engines. SSL decryption requires stream processing; more specifically it requires the ability to manipulate and/or terminate TCP connections. SWGs are optimized for TCP connection processing, while a NGFW would most likely offload that capability to an exception handler. Furthermore, appliances have limited memory and processing resources, and the data structures required for TCP connection processing is vastly different from packet processing data structures. The NGWF would have to implement complex resource allocation algorithms in order to maintain performance levels with SSL decryption enabled.

Because proxies (such as SWGs) are built to decrypt and reassemble traffic efficiently, they can handle encrypted traffic to eliminate the SSL blind spot. But not all inspection products are the same: A US-CERT Advisory[7] warned that many HTTPS inspection products do not properly verify the certificate chain of the server before re-encrypting and forwarding client data. This means such products could be enabling a Man-in-the-Middle (MiTM) attack. To combat this potential vulnerability, the Advisory says 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 (for example, v1.2), and not allow weak ciphers.

Limited third-party integration

It's critical that your security solution plays well with others. Not only should it share data, but it should enable multiple third-party engines to scan content before determining a verdict. How can you center your security strategy around an NGFW if it doesn't integrate with the tools you're already invested in?

Top 5 Use Cases Your NGFW Vendor Does Not Solve

Web and email isolation

NGFW vendors do not provide web and email isolation, which enables you to access uncategorized or risky traffic and emails that would normally either be blocked or recklessly delivered. Isolation seamlessly executes web requests, delivering only a safe rendering of information to endpoint browsers, protecting against threats by ensuring website delivered zero-day malware are unable to reach and infect your devices. This technology also provides important advantages over NGFW when protecting against malicious files downloaded through the browser as well as phishing threats and credential theft.

Multivendor sandbox brokering

When you wish to further examine a suspicious sample you've identified on your network, you may want to submit it to multiple sandbox detonation systems, including in-house and third-party technologies. NGFWs cannot provide that range of flexibility.

Active inline network DLP

With NGFWs, you cannot place data loss systems inline on your network and actively block sensitive data from leaving your network. NGFWs typically can alert you only once the data has already left your network.

BYOD mobile device protection

NGFWs have no mobile clients to speak of, much less a complete mobile device protection solution. This would need to be provided by another vendor without integration.

Endpoint EDR integrations

NGFW vendors lack true EDR capabilities, thus preventing meaningful integration between the network and endpoints. One illustrative use case involves confirming indicators of compromise across all endpoints to understand what clients could be infected. Without this capability, incident response is much more challenging.

The Solution—Symantec Network Security Platform for the Cloud Generation

The Symantec™ Network Security Platform provides defense in-depth security as well as an orchestration layer with third-party systems.

The core of Symantec's Network Security Platform is its secure web gateway (SWG) technology, which is available in flexible cloud, on-premises, and hybrid configurations. We have the portfolio, we have the Integrations, and we have the global threat intelligence data from the world's largest civilian intelligence network—all brought together to secure your enterprise's data, employees, and applications.

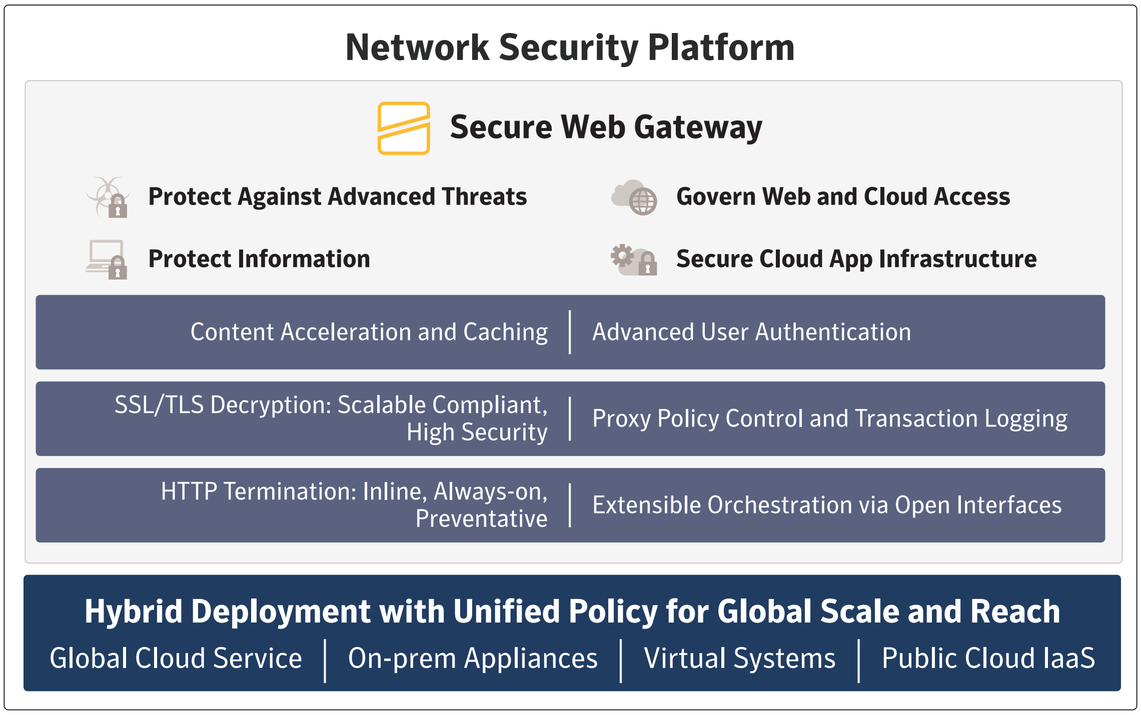

Network Security Platform
Secure Web Gateway
Protect Against Advanced Threats
Govern Web and Cloud Access
Protect Information
Secure Cloud App Infrastructure
Content Acceleration and Caching
Advanced User Authentication
SSL/TLS Decryption: Scalable Compliant, High Security
Proxy Policy Control and Transaction Logging
HTTP Termination: Inline, Always-on, Preventative
Extensible Orchestration via Open Interfaces
Hybrid Deployment with Unified Policy for Global Scale and Reach
Global Cloud Service
On-prem Appliances
Virtual Systems
Public Cloud IaaS

Figure 5

A complete security portfolio to protect your organization's interests

To form the foundation of a defensible architecture, the Network Security Platform starts with Symantec Secure Web Gateway and Symantec Content Analysis, and taps Symantec's Global Intelligence Network, to terminate traffic and intelligently orchestrate further security actions or analysis. For example, it will handle situations in which you ask:

- Should the endpoints be notified of a threat, and implement blacklisting?
- Should a file be forwarded to multiple in-house and third-party technologies for further analysis?
- Should incident response teams be notified of a threat requiring further investigation?

In addition to the core security components in the SWG-centered ICD, other important pieces in the portfolio with additional integrations provide stronger security, compliance, and data sharing.

Core Protection: Secure Web Gateway and Content Analysis—Symantec Secure Web Gateway provides a platform for a sophisticated ecosystem of technologies working together to protect your organization and offers advanced threat protection on-premises, in the cloud, and from the web to social media to mobile networks. In essence, Secure Web Gateway removes well-known threats and provides a "quarantine" service for web traffic. It terminates and examines 100 percent of traffic between users and the internet, and categorizes all URLs so that malicious sites and pages are identified and blocked, while good URLs can be accessed based on an organization's needs and policies. Symantec Secure Web Gateway provides complete control over all your web traffic that flows into the multiple layers of protection that Symantec Content Analysis provides, and also integrates with Symantec Data Loss Prevention to protect outbound data. Secure Web Gateway, acting as a termination point, leads into multiple layers of threat examination for superior advanced threat protection. Secure Web Gateway is instantiated in on-premises, cloud, and hybrid options utilizing ProxySG hardware or virtual appliances and Symantec Web Security Service.

Content Analysis offers a platform for multilayered/multivendor threat detection and protection (*Figure 6*). Incorporating Secure Web Gateway and Content Analysis, a Symantec solution:

- Blocks known malicious URLs at the gateway
- Conducts extensive whitelist and blacklist scanning
- Analyzes unknown files through advanced static code file analysis and machine learning

- Scans content with dual antimalware engines for greater detection accuracy
- Detonates unknown files via on-box sandboxing, or dedicated sandboxes
- Integrates with many Symantec and third-party security tools including Symantec Endpoint Protection to provide endpoint visibility, protection, and response

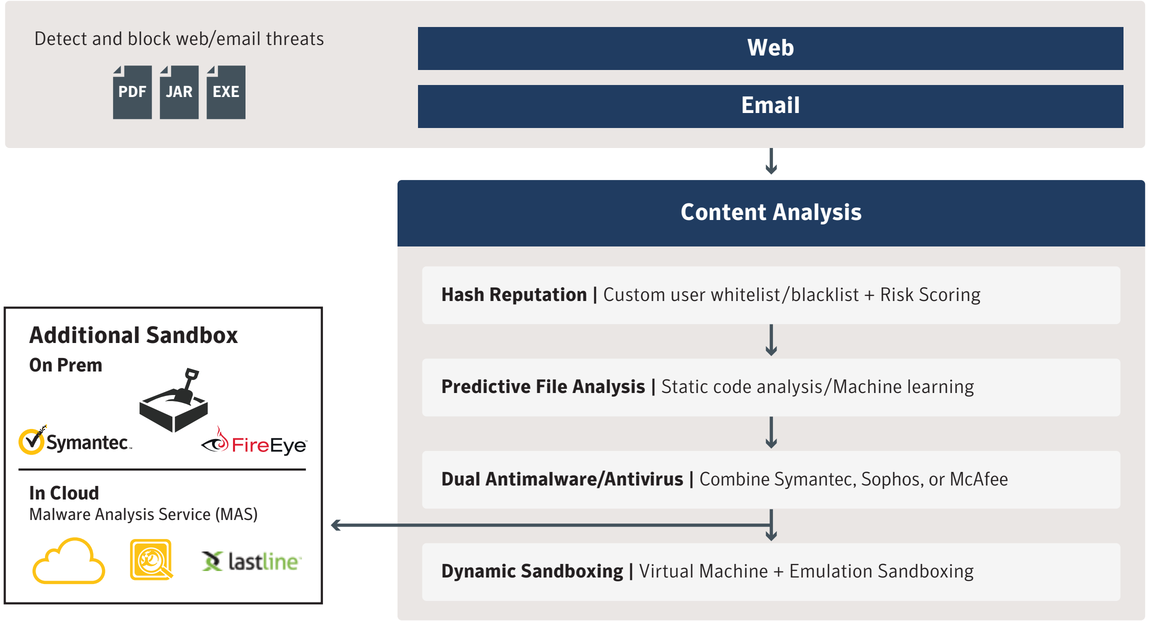

Detect and block web/email threats
PDF
JAR
EXE
Web
Email
Content Analysis
Hash Reputation | Custom user whitelist/blacklist + Risk Scoring
Predictive File Analysis | Static code analysis/Machine learning
Dual Antimalware/Antivirus | Combine Symantec, Sophos, or McAfee
Dynamic Sandboxing | Virtual Machine + Emulation Sandboxing
Additional Sandbox
On Prem
Symantec.
FireEye
In Cloud
Malware Analysis Service (MAS)
lastline

Figure 6

Secure Web Gateway and Content Analysis (with malware scanning and whitelisting) inspect sources and signatures to block all known threats and can centrally analyze unknown content. The threat intelligence is shared locally between Secure Web Gateway and Content Analysis, and worldwide via the Symantec Global Intelligence Network. This community-watch effect constantly fortifies your security. Uncategorized zero-day threats are escalated automatically and brokered to dynamic sandboxing technology. This technology offers a unique hybrid analysis protocol, including the customizable IntelliVM virtualized sandbox to replicate production environments, and a bare-metal sandbox emulator for accurately analyzing and detecting VM-evasive malware. Content Analysis file filtering mitigates false positive identification of malware and it significantly improves sandbox efficiency by reducing the number of files unnecessarily sent for analysis.

Web and email isolation—Symantec acquired Fireglass to bring market-leading isolation technology to our entire customer base. Web isolation seamlessly executes web requests remotely and transforms all web content into a safe visual stream, protecting against threats by ensuring website-delivered zero-day malware are unable to reach and infect your devices (*Figure 7*).

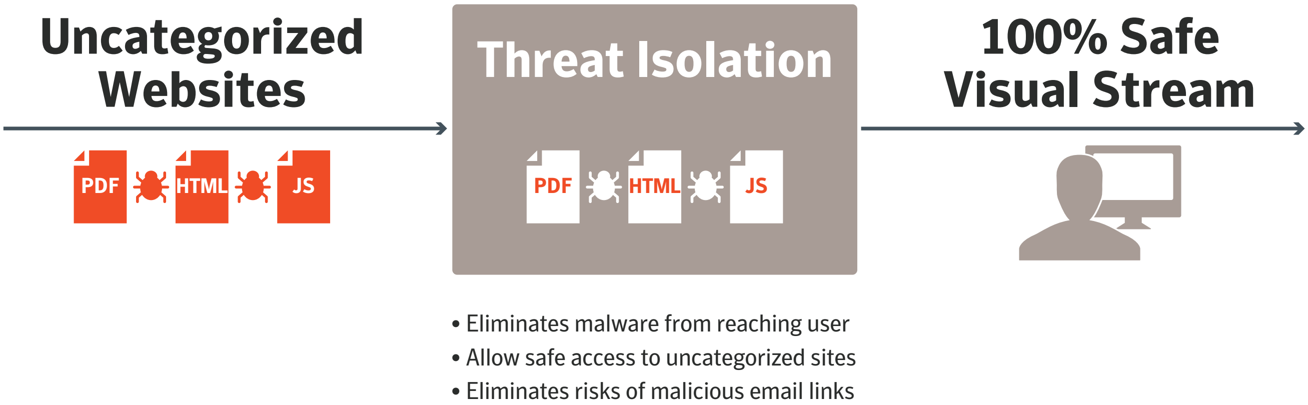
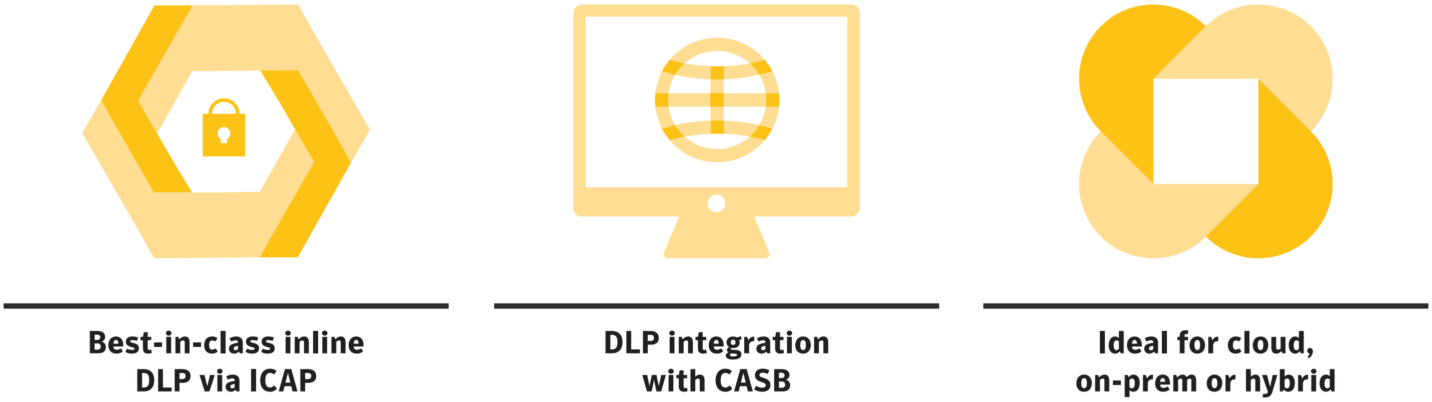

Uncategorized Websites
PDF
HTML
JS
Threat Isolation
PDF
HTML
JS
100% Safe Visual Stream
• Eliminates malware from reaching user
• Allow safe access to uncategorized sites
• Eliminates risks of malicious email links

Figure 7[3]

When combined with Symantec Secure Web Gateway, policies can help isolate traffic from uncategorized sites or URLs with suspicious or potentially unsafe risk profiles often used to deliver malware and phishing threats. Also, leveraging its tight integration with Symantec DLP, Web Isolation can enforce DLP policies even when traffic is isolated on Symantec cloud.

Web Isolation also effectively combats phishing threats and credential theft. In addition to executing web sessions remotely, which eliminates the possibility of infection, Web Isolation can render sites in read-only mode. This functionality disables web input fields and prevents users from disclosing credentials and other sensitive information through risky sites.

Data loss prevention—Organizations need a solution that will safeguard their data wherever it travels. The solution needs to take into account the expanding data threat landscape and the evolving behavior of trusted users who have access to sensitive information, which may lead to data leakage across outbound communication channels. Your DLP solution needs to integrate with your web protection to provide real-time defense against data leakage outside your network. Secure Web Gateway integrates with both Symantec Data Loss Prevention and third-party DLP products so you can monitor and prevent sensitive data from being leaked through shadow applications. Secure Web Gateway enables your DLP to enforce policy compliance by directing outbound files to DLP via Internet Content Adaptation Protocol, as well as direct integration with CloudSOC.



Best-in-class inline DLP via ICAP

DLP integration with CASB

Ideal for cloud, on-prem or hybrid

Figure 8

Email—Email may be the lifeblood of your organization, but it's also a huge point of entry for targeted attacks. Office 365, Gmail, and other cloud-based productivity tools offer convenience but increase your vulnerability. Protect yourself from the most advanced attacks with Symantec's messaging security platform for cloud-based and on-premises email.

Symantec Messaging Gateway also integrates with Content Analysis to deliver unknown content for further inspection and provide actionable intelligence.

User authentication/Single sign-on (SSO)—Symantec Validation and ID Protection Service (VIP) is a leading user-friendly, cloud-based user authentication service that provides secure access to sensitive data and applications anytime, anywhere, from any device.

Bring your own device (BYOD)—Symantec's recent acquisition of Skycure delivers comprehensive Mobile Threat Defense capabilities against all mobile threat vectors while complying with the OS vendor's policies and using only approved public APIs. Users gain a fully capable app that is publicly available, via the App Store and Google Play, greatly simplifying installation, supporting seamless updates, and future-proofing full functionality against the removal of deprecated private APIs.

Encrypted traffic—A recent independent study by leading academics, Google, Mozilla, and others looked at SWG, NGFW, and application delivery controller (ADC) solutions to determine who was following industry best practices for securely intercepting encrypted web traffic[8]. What they found: Only Symantec Secure Web Gateway appropriately manages decryption and maintains high security standards. Symantec's SWG solution (ProxySG) received an 'A' rating; all other products tested received either a 'C' or an 'F.'

Symantec also provides an integrated solution where the TLS intercept duties are offloaded to a Symantec SSL Visibility appliance (SSLV), which then feeds decrypted content to one or more SWGs while simultaneously feeding third-party security tools (which could even include a NGFW). The SSLV is dedicated to TLS intercept on all ports and protocols, and provides both performance benefits and security benefits to attached tools.

Proper certificate validation, the latest ciphers, and advanced TLS support are just some of the reasons why Symantec came out on top—and why you can count on us to help you securely manage encrypted threats.

Network forensics—Symantec Security Analytics will transform manual forensics into automated incident response. With a fully enriched 'system of record,' your incident response teams will reduce time-to-resolution and answer the what, when, and how of any security incident through full packet capture, root-cause exploration, deep packet inspection, integrated reputation services and data enrichment, and advanced context-based reporting on malicious activity. Security Analytics—it is like a security camera and DVR for your network.

Management and reporting—Management Center provides a unified management environment for the Symantec portfolio of products. Management Center brings Symantec's network, security, and cloud technologies to you under a single umbrella, making it easier to deploy, manage, and monitor your security environment—all at a lower cost of ownership. Key capabilities include:

- Centralized configuration, deployment, device monitoring, and backup
- Consolidated reporting
- Policy provisioning
- Role-based access control
- Integrated analysis and reporting with policy creation
- Single console for network, security, and cloud
- Streamlined management and reporting

Deployment flexibility

In addition to providing complete protection for any port and protocol, Symantec also provides deployment flexibility—from an all-cloud or on-premises solution to hybrid options. Optimize your deployment type to best fit your organization's requirements and administer a universal policy across all environments. Within deployment types there are additional options to suit different cloud and on-premises strategies:

- Cloud—public cloud or full private cloud service
- On-premises—virtual or hardware deployments
- Hybrid—cloud-assisted devices, which reduce your on-premises deployment needs

Symantec's flexible portfolio provides a path forward for all organizations, even those that don't currently embrace the cloud fully.

Orchestration layer for integration

The orchestration layer enables automated orchestration with all your Symantec and third-party security tools. Open orchestration, secure APIs, ICAP, forwarding, text streaming, and logs feed decrypted data to third-party services, integrating infrastructure and simplifying network operations. This integration provides an unprecedented level of timely information sharing between products and our Global Intelligence Network, bringing protection to the highest levels.

Use this increased integration between Symantec products and third parties to create customizable playbooks. These playbooks enable you to match different products and feature sets to build an integrated cyber defense platform, tailored exactly to your needs, utilizing cloud, on-premises, and hybrid approaches.

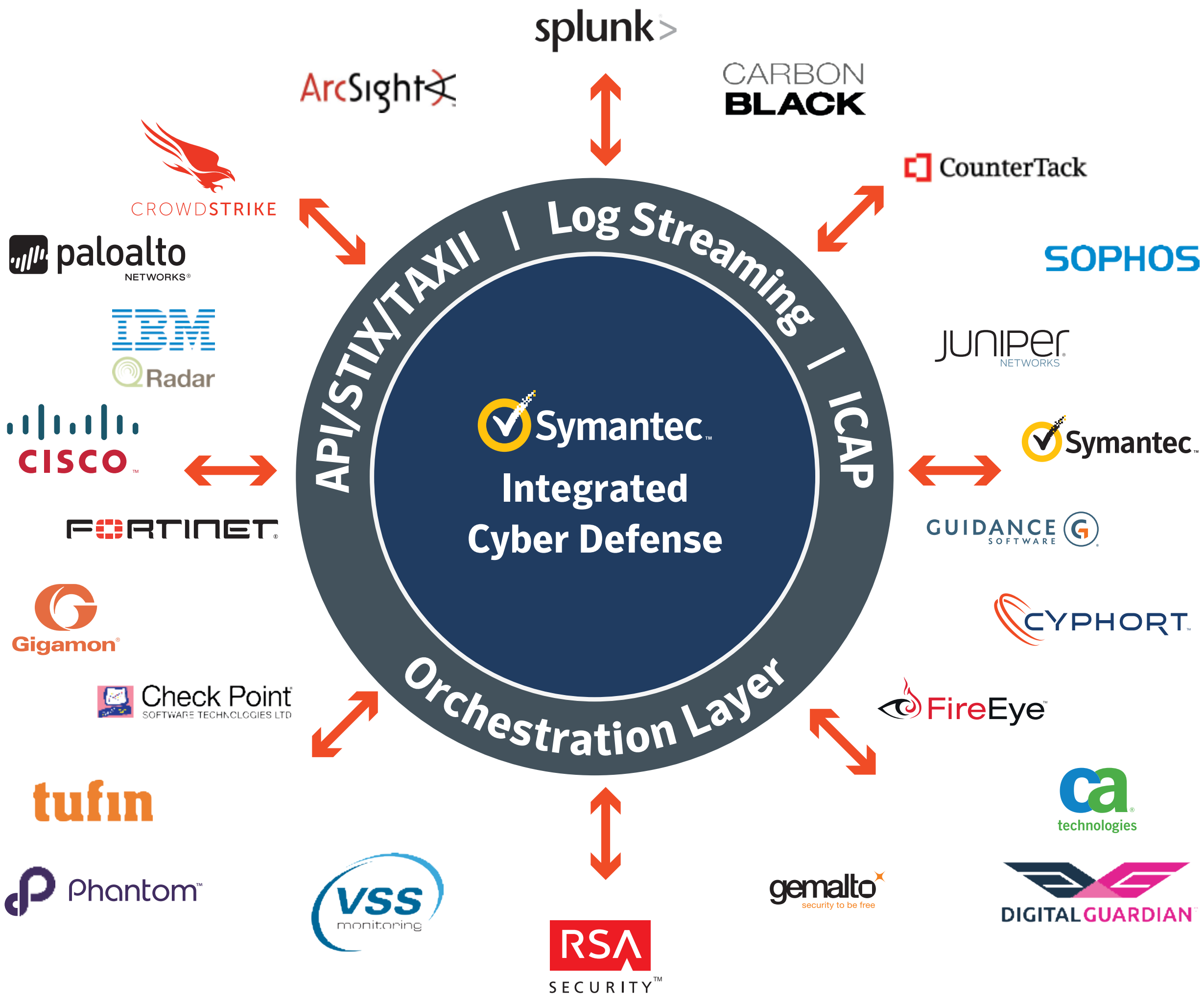


Figure 9

Largest cyber security data network

Symantec now protects 163 million email users, 80 million web proxy users, 175 million consumer and enterprise endpoints, and processes nearly eight billion security requests across these products every day. This level of visibility across endpoint, email, and web traffic enables Symantec to discover and block targeted attacks that would otherwise be undetectable from any single control point. What's more, our combined portfolio provides the foundation for Symantec's Integrated Cyber Defense Platform, which enables Symantec products to share threat intelligence and improve security outcomes for customers across all control points. Symantec's Global Threat Intelligence Network—the world's largest civilian intelligence network—has always lived natively in the cloud, complementing both on-premises and cloud SWG deployments.

Symantec is the only vendor to connect endpoint, email, and web protection across a single integrated intelligence platform, which was made possible through the acquisition of Blue Coat Systems. The combination of Symantec + Blue Coat has enabled Symantec to block 3.2 million additional attacks every single day for our customers. It turns out that 1 + 1 is a lot bigger than 3[9].

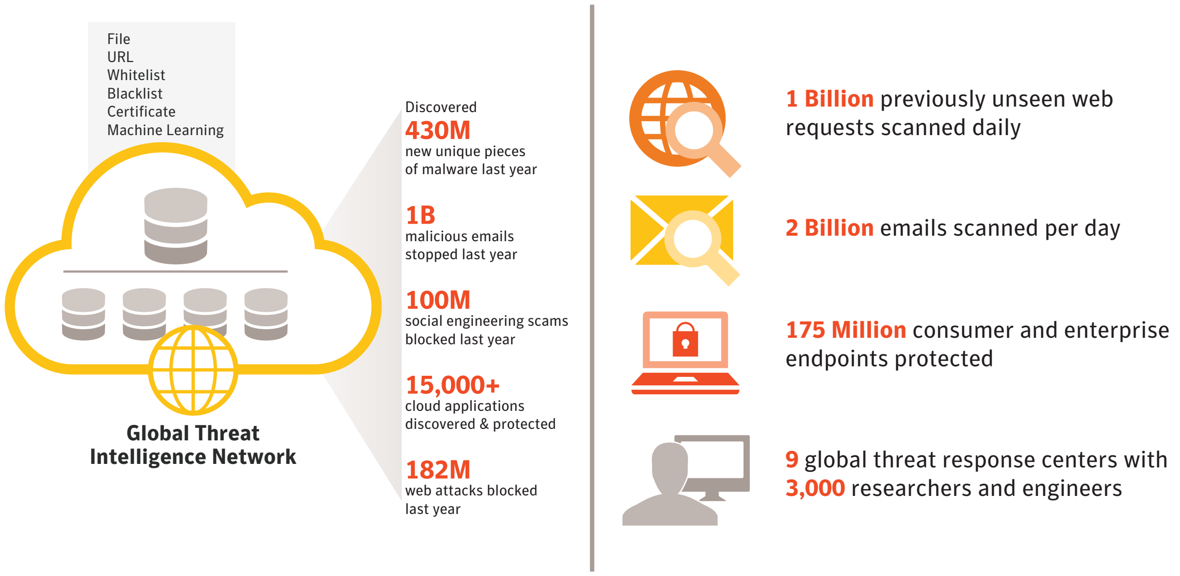

File
URL
Whitelist
Blacklist
Certificate
Machine Learning
Global Threat Intelligence Network
Discovered
430M
new unique pieces of malware last year
1B
malicious emails stopped last year
100M
social engineering scams blocked last year
15,000+
cloud applications discovered & protected
182M
web attacks blocked last year
1 Billion previously unseen web requests scanned daily
2 Billion emails scanned per day
175 Million consumer and enterprise endpoints protected
9 global threat response centers with 3,000 researchers and engineers

Figure 10

Symantec Network Security—Part of The Symantec Integrated Cyber Defense Platform

Symantec's network security portfolio is part of Symantec's Integrated Cyber Defense Platform, the only unified platform to integrate on-premises and cloud-delivered security to govern access, protect information, protect against advanced threats and secure the public cloud, across endpoint, network, and cloud.

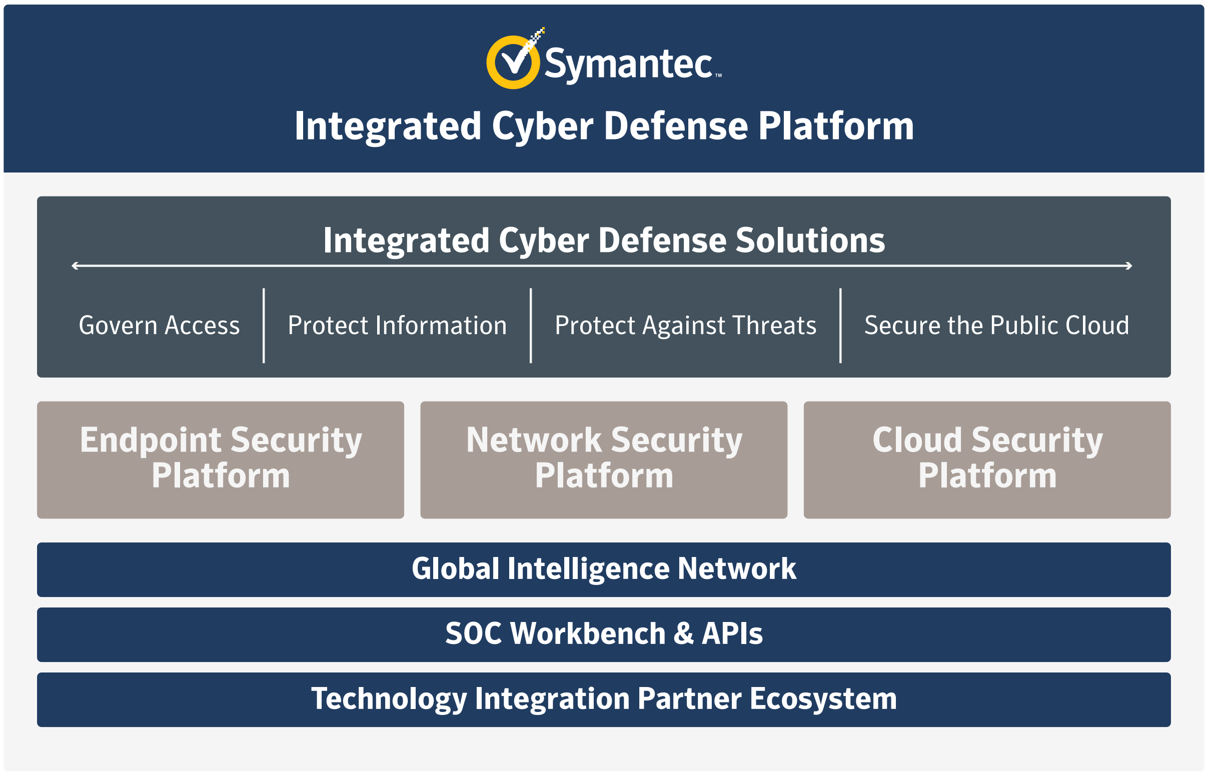

Symantec
Integrated Cyber Defense Platform
Integrated Cyber Defense Solutions
Govern Access
Protect Information
Protect Against Threats
Secure the Public Cloud
Endpoint Security Platform
Network Security Platform
Cloud Security Platform
Global Intelligence Network
SOC Workbench & APIs
Technology Integration Partner Ecosystem

Figure 11

Integrating Network Security with the Symantec Endpoint Security Platform

Symantec provides the full cycle of endpoint security from threat prevention to detection and response, optimizing existing investments without adding new agents. It protects, detects, investigates, and remediates threats across all endpoints through a single agent by:

- Blocking threats across the attack chain with few false positives
- Detecting anomalies and investigating suspicious events
- Remediating complex attacks in minutes, with one click

When you discover a threat via the Network Security Platform, Symantec can share this threat data with Symantec's Endpoint products to confirm endpoint IOCs, use blacklisting to stop attacks from spreading, and remediate the endpoints.

Integrating Network Security with Symantec Cloud Security Platform

In addition to being able to deliver its network security capabilities as a cloud-delivered service, Symantec offers a Cloud Security Platform that provides a complete application and workload protection, threat prevention and monitoring across public clouds, private clouds, and across on-premises data centers.

A key component of this platform is Symantec's Cloud Access Security Broker (CASB) service, called CloudSOC. The service enables companies to confidently leverage cloud applications and services while staying safe, secure, and compliant. It provides visibility into unsanctioned cloud application usage (Shadow IT), governance over data in cloud apps, and protection against threats targeting cloud accounts. With intelligence on over 21,000 cloud applications, CloudSOC enables you to identify and block the riskiest known applications immediately.

Symantec CloudSOC and Secure Web Gateway within the Network Security Platform integrate with each other in two key ways. First, Secure Web Gateway enables the CloudSOC Gateway to inspect, in real time, data moving to the cloud by directing cloud-bound traffic through the CloudSOC Gateway. This traffic control enables the CloudSOC to actively enforce sanctioned cloud application and DLP policies to monitor and control your organization's critical data.

Also, the products complement each other to monitor and control unsanctioned cloud applications or Shadow IT. CloudSOC audit uses data from Secure Web Gateway to audit all the cloud applications in use in your environment. CloudSOC takes the data it finds to identify cloud applications in use; this data can be fed back into Secure Web Gateway, so it can block cloud applications by name, category, and even vulnerability.

Conclusion

You need a cyber defense platform you can rely on to protect your data and users across your networks, clouds, and endpoints in the corporate office, on the VPN, or directly on the internet. With the traditional perimeter disappearing and the threat landscape increasing, such a platform is essential.

There may be a place in your network for a NGFW, but with its many issues in performance, security, and integration, an NGFW would be a poor choice as the foundation of the network component of your overall cyber defense.

Conversely, by providing a termination point to safely examine all traffic and intelligently orchestrate other Symantec and third-party solutions, the Symantec Secure Web Gateway is the optimal foundation for your network security platform. Symantec's Network Security Platform offers a complete suite of products, Global Intelligence Network, and third-party integrations. Moreover, by integrating with Symantec's full portfolio of products and services that protect your endpoints and cloud applications, it uniquely provides an Integrated Cyber Defense platform to protect your business from the threats it faces in the Cloud Generation.

Contact your Symantec Product Specialist or partner representative for more information and to request a demo or trial.

Learn more about the Cloud Generation and Symantec's Integrated Cyber Defense Platform: **https://www.symantec.com/solutions/cloud-generation**.

References

[1] **Finley, Klint.** Half the Web Is Now Encrypted. That Makes Everyone Safer. wired.com. [Online] https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/.

[2] **Oltsik, Jon.** Analyst Report: Full-service Hybrid Proxy Architecture. Symantec.com. [Online] https://resource.elq.symantec.com/LP=4441?cid=70138000001QMGRAA4&inid=symc_performance-center_regular_to_leadgen_form_LP-4441_esg-network-security-demands-full-service-hybrid-proxy.

[3] **Tolly.** Symantec Secure Web Gateway Web Security Effectiveness & Features Versus A Leading NGFW Solution. s.l. : Tolly, 2017.

[4] **Snyder, Joel.** Next-gen firewalls: Off to a good start. Network World. [Online] https://www.networkworld.com/article/2187980/network-security/next-gen-firewalls--off-to-a-good-start.html.

[5] **Pirc, John W.** NSS Labs Research Finds SSL Traffic Causes Significant Performance Problems for Next Generation Firewalls. NSS Labs. [Online] https://www.nsslabs.com/company/news/press-releases/nss-labs-research-finds-ssl-traffic-causes-significant-performance-problems-for-next-generation-firewalls/.

[6] **Ashford, Warwick.** Encryption hiding malware in half of cyber attacks. computerweekly.com. [Online] http://www.computerweekly.com/news/450303346/Encryption-hiding-malware-in-half-of-cyber-attacks.

[7] **US CERT.** Alert (TA17-075A): HTTPS Interception Weakens TLS Security. us-cert.gov. [Online] 3 16, 2017. https://www.us-cert.gov/ncas/alerts/TA17-075A.

[8] **Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan,** The Security Impact of HTTPS Interception. jhalderm.com. [Online] https://jhalderm.com/pub/papers/interception-ndss17.pdf.

[9] **Statistica.** Number of mobile phone users worldwide from 2013 to 2019 (in billions). statistica.com. [Online] 2017. https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/.

[10] **IDC Forecasts U.S.** Mobile Worker Population to Surpass 105 Million by 2020. businesswire.com. [Online] http://www.businesswire.com/news/home/20150623005073/en/IDC-Forecasts-U.S.-Mobile-Worker-Population-Surpass.

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** 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