Solution Brief

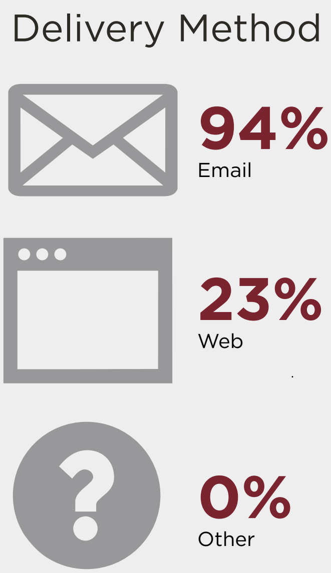
Symantec Network Security

Executive Summary

One malicious attachment, one unknown website, or one accidental click and you may be infected. You can mitigate some of this risk by running best-of-breed endpoint protection on all of your network-connected devices, but there will always be vulnerabilities. Whether it is that old fax machine in the corner of your office, that unpatched Windows 7 Server, that mobile phone or a well-meaning employee, you could become compromised. What happens next? It's little wonder that cyberattacks are the biggest Information Security concern for organizations.[1] Cyberattacks can feature targeted spear phishing, ransomware, denial of service attacks and impersonation, which may result in direct financial loss, information theft, lost productivity and reputational harm.

Web and Email are the primary attack vectors[2] for the ever-evolving cybercriminals who continue to use an array of different avenues to infiltrate your organization—either to attack and/or gain access to your data, including intellectual property, customer accounts and other valuable assets. Consequently, web and email security solutions are where IT professionals look for effective and efficient "defense-in-depth" protection against advanced threats that may get past a single endpoint. One of the best ways to protect every device—and by extension every user—in your organization and to prevent the spread of cyberattacks, is to prevent threats reaching devices in the first place.

Figure 1: Data Breach Report



Source: 2019 Data Breach Investigation Report, Verizon

What's more, effective web and email security goes beyond advanced threats because cyberattacks aren't the only risk. Data fraud & theft are also a top-of-mind information security concern. Sensitive data such as customer lists, intellectual property, confidential or personal data must also be protected. The culprit may be an employee with malicious intent, who doesn't follow company policy or one who accidentally sends an email to the wrong address. It could also be a user whose device or user credentials have been compromised. Regardless of the source, effective web and email security can also play a key role in preventing malware infiltration and data exfiltration as part of a multi-layered data protection solution.

Network Security: Web and Email Working Together

Shared Advanced Threat Defense

Web and Email threat vectors have their own unique security needs, which is why it remains important to have a powerful web security and an equally powerful email security solution that each have the latest security technologies and intelligence available.

While malware continues to be delivered as disguised attachments through email, it's increasingly common for emails to reference web links hosting malware or directing users to phishing sites. This combination of using both email and web for attacks will only continue as cyber criminals look for ways to get past both email and web defenses and exploit security gaps to ultimately gain access to sensitive network resources. This is why it's more important than ever for web and email defenses to share threat intelligence and have the ability to interact and relay threat information about specific threats targeting the organization.

[1] https://www.bsigroup.com/LocalFiles/en-GB/iso-22301/case-studies/BCI-Horizon-Scan-Report-2018-FINAL.pdf
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
[2] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Furthermore, leveraging common advanced network security capabilities ensures that both web and email vectors benefit from the same state-of-the-art protection, while also improving operational efficiency. Symantec offers some of the most advanced threat defense solutions, including the multi-layered defense of our Content Analysis System, and our latest technology – Threat Isolation. These technologies work with both web and email security, giving organizations the advantage of being able to share their security investments and reduce management requirements across multiple security infrastructure platforms.

Content Analysis and the Symantec Global Intelligence Network (GIN) benefit from the discovery of new threats coming in from any vector and from any customer throughout the Symantec community. All organizations within the community are automatically protected from new threats through the use of shared intelligence from Symantec GIN. This networked approach to security means every customer benefits from threats discovered by anyone in the Symantec community.

Consistent Data Loss Prevention

Symantec's industry leading Data Loss Prevention (DLP) features tight integration with both web and email security, offering a single pane of DLP management and configuration for creating and applying a single policy to protect an organization's sensitive data from leaving through these, and other, highly used network channels.

Leading Web Security

Symantec Web Security is based on an advanced proxy architecture, and provides superior defense against advanced threats, protects critical business information, and helps ensure secure and compliant use of the cloud and web. The traditional network perimeter is gone – today, the perimeter is wherever the data is. Users are everywhere and need quick access to data and cloud applications around the clock. In the cloud, on-premises or both, you need to stop inbound and outbound threats targeting your end users, information and key infrastructure. Symantec Secure Web Gateway is available via cloud, on-premises or as part of a hybrid proxy deployment to meet your specific needs and balance security, performance, complexity, and cost.

Leading Email Security

Email is currently the most common way cybercriminals launch and distribute threats; 65% of targeted attack groups employ spear phishing as their primary means of attack. As the volume of attacks has increased, so has the level of sophistication. To combat this, multiple layers of protection (including threat isolation) are needed against ransomware, spear phishing and business email compromise. Security teams require advanced analytics to identify, protect and respond to any manner of targeted attack, and to protect email against user error and data leakage.

Figure 2: 1 in 10 URLs are malicious

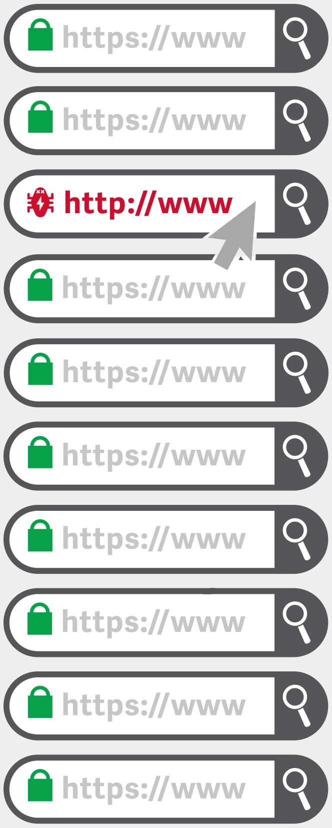
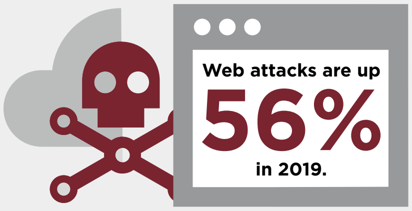


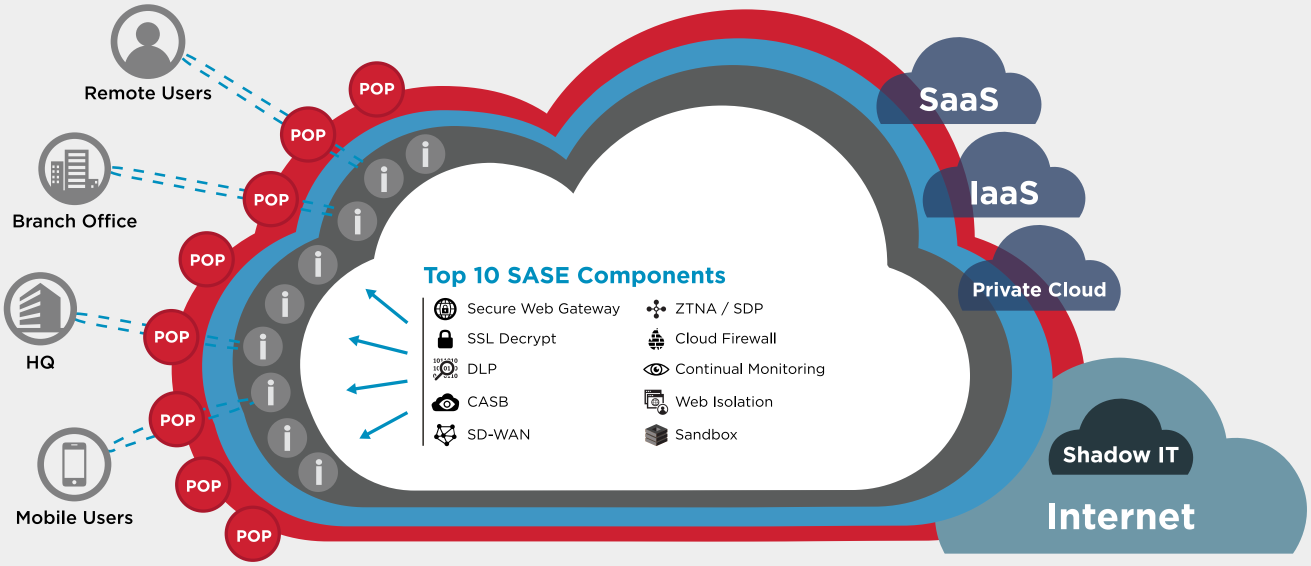
Figure 3: Web attacks are up 56% in 2019



SASE Framework

Existing network and security models no longer work as digital transformation, mobile devices, remote workers, and cloud adoption have radically changed network traffic. Customer demand for simple, scalable, fast, flexible, and secure access is driving key network security components closer to the end user, resulting in the adoption of a Secure Access Service Edge (SASE) framework.

Figure 4: SASE Framework



Key Capabilities

Cloud and Hybrid Options

While on-premises solutions remain the primary defense mechanisms for many organizations' data centers, the disappearance of the traditional network security perimeter, the need for cost reduction, and support for mobile and remote users has driven the need to move to security in the cloud. By offering email and web solutions in the cloud, Symantec offers options for any deployment, on-premises, cloud, or a hybrid solution of both.

Content Analysis

Symantec Content Analysis delivers multi-layer file inspection to better protect your organization against known and unknown threats. Known threats are efficiently identified and blocked by ProxySG, Symantec Messaging Gateway or other tools, while unknown or suspicious content is identified and delivered to Content Analysis for deep inspection, interrogation, analysis and ultimately blocking, if deemed malicious. Recent enhancements to Content Analysis include the ability to use on-box or cloud sandboxing, integration with endpoint protection and response and the addition of Symantec Antimalware and Advanced Machine Learning to Content Analysis for increased threat detection capability. The result is an extremely effective and efficient defense-in-depth model that detects even the most advanced attacks without requiring excessive or redundant infrastructure.

Threat Isolation

Symantec Web Isolation and Email Threat Isolation executes web sessions away from endpoints, sending only a safe rendering of information to users' browsers, thereby enabling users to visit potentially dangerous websites without the risk of infection by preventing any website-delivered zero-day malware from reaching their devices. When combined with Symantec Secure Web Gateways, rich policies can evolve from the standard (and inefficient) allow/deny model by isolating traffic from uncategorized sites or URLs with suspicious or potentially unsafe risk profiles. By integrating with Symantec messaging solutions, Threat Isolation isolates links and attachments in email to prevent phishing threats and credential attacks.

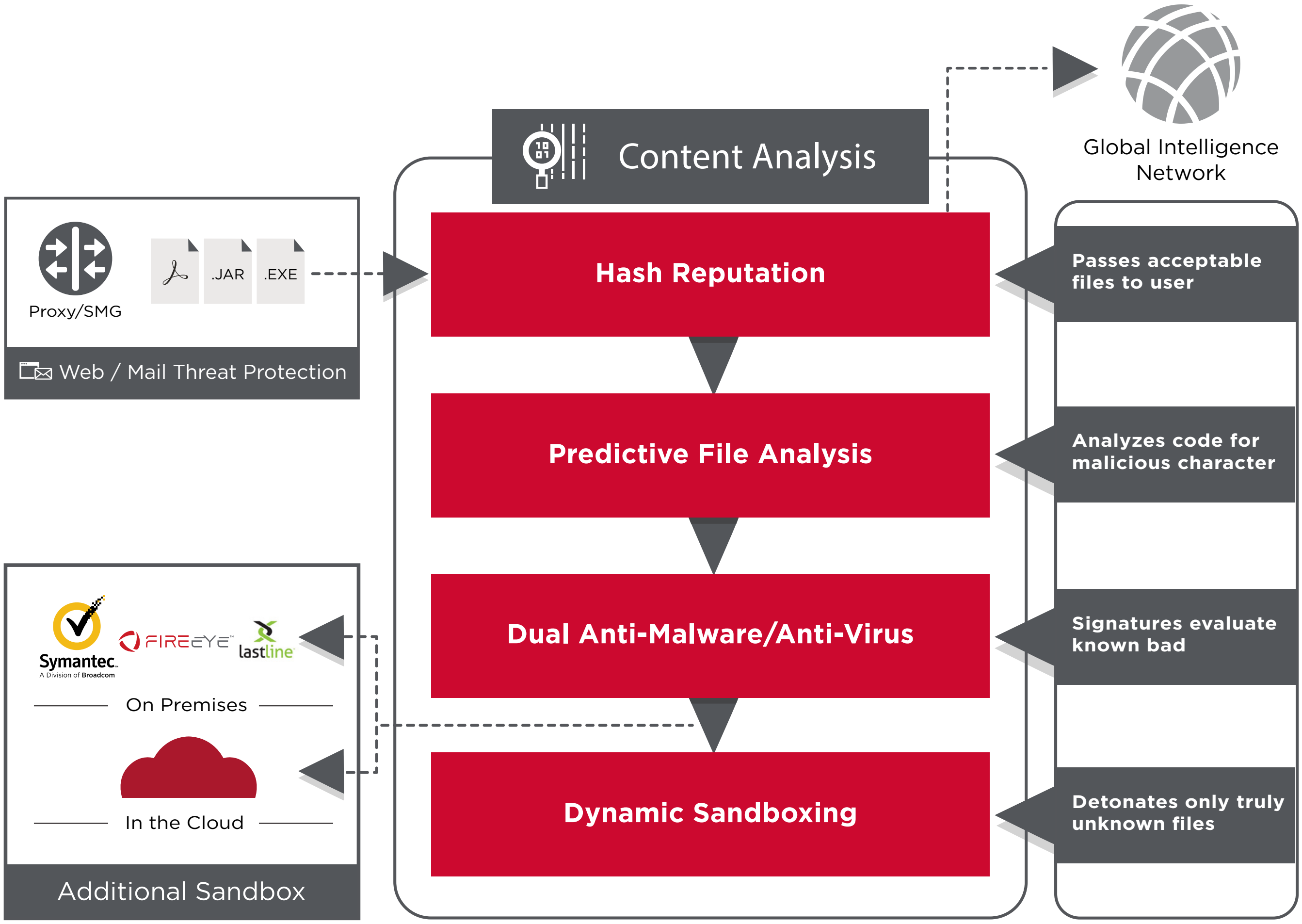
Security Analytics

Effective security organizations understand the need to be prepared for the unknown and are effectively equipped for swift incident response. Symantec Security Analytics provides a clear view of what is happening in your environment. It delivers enriched, full-packet capture for complete network and cloud workload visibility, advanced forensics, anomaly detection, and real-time traffic analysis of everything crossing your network or to and from the cloud. Armed with this detailed record, incident response teams can conduct detailed forensic investigations, respond quickly to incidents, and resolve breaches in a fraction of the time they would spend with conventional processes.

Strong Encryption

Strong encryption is essential for secure communication, privacy protection and data integrity. Unfortunately, cybercriminals know this too. Most cyber threats hide in SSL / TLS encryption, which is often the majority of all network traffic. Symantec Proxies and SSL Visibility Appliance decrypt traffic, feed a wide variety of security tools, all while adhering to data privacy policies, laws and regulations. Just as important, these solutions manage encrypted traffic while preserving the original strong encryption strength.[3]

Figure 5: Content Analysis


Global Intelligence Network
Content Analysis
Proxy/SMG
.JAR
.EXE
Web / Mail Threat Protection
Hash Reputation
Passes acceptable files to user
Predictive File Analysis
Analyzes code for malicious character
Dual Anti-Malware/Anti-Virus
Signatures evaluate known bad
Dynamic Sandboxing
Detonates only truly unknown files
Symantec
A Division of Broadcom
FIREEYE
lastline
On Premises
In the Cloud
Additional Sandbox

Multi-layer threat inspection, detection and sandboxing uncover the unknowns.

[3] https://jhalderm.com/pub/papers/interception-ndss17.pdf

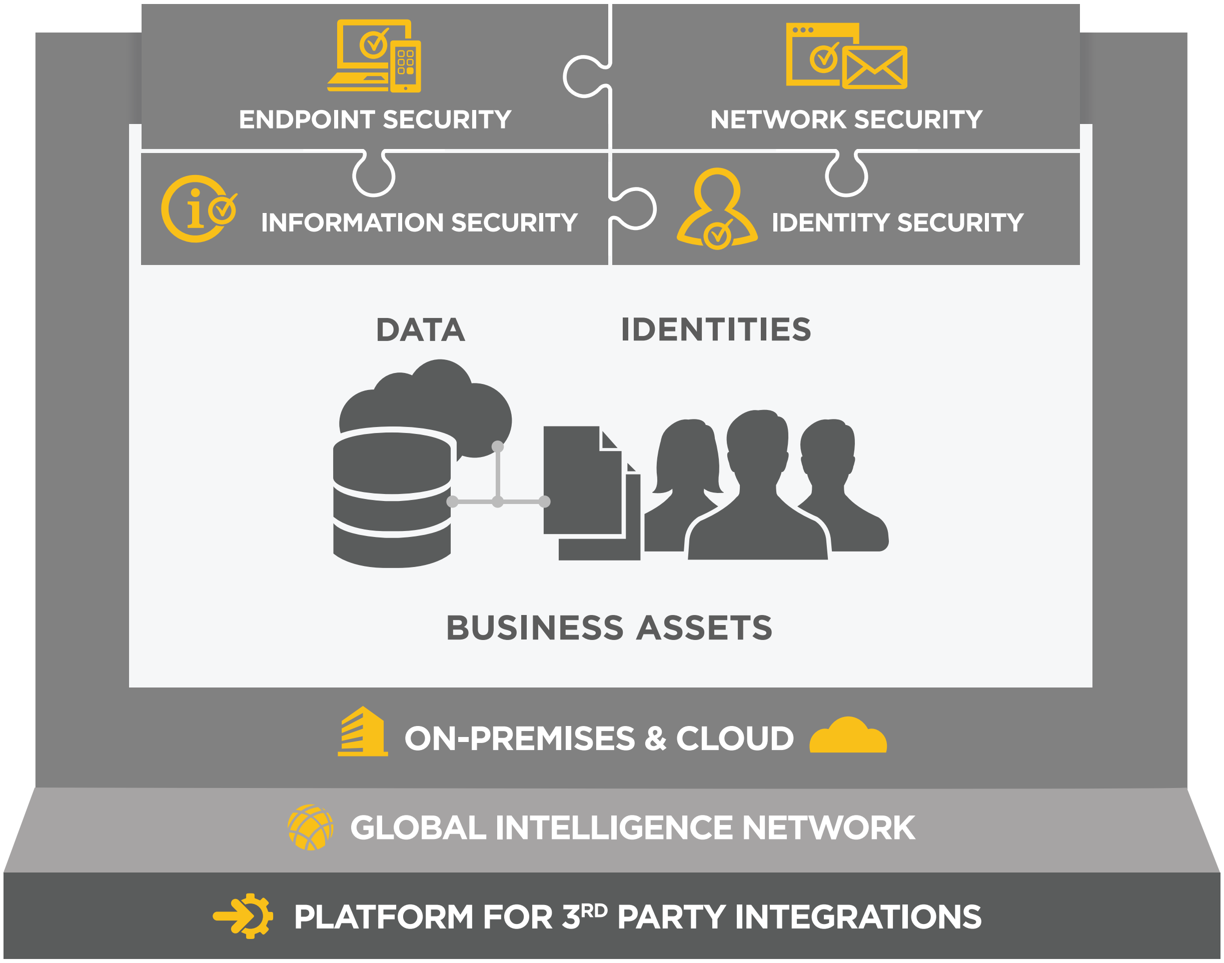
Symantec Email Security includes isolation technology so inbound, encrypted email attachments can be opened in a secure web container allowing users to access attachments whilst keeping them safe from any malicious content. For outbound email, sensitive data can be encrypted allowing secure communications between customers and business partners. Encryption can be set automatically via integration with Symantec DLP.

A Critical Component of the Symantec ICD Framework

Network Security is one of the four core components of the Symantec Integrated Cyber Defense (ICD) framework. With Endpoint Security, Information Security, Identity Security and Web and Email Security solutions, Symantec safeguards your business assets, while taking advantage of a platform that shares threat intelligence to all Symantec customers. Any discovered threat intelligence is shared between solutions in the Integrated Cyber Defense Exchange (ICDx) and with 3rd parties for collaborative integrations across security products. Additionally, organizations can deliver integrated, multi-vector security workflows that substantially reduce risk or improve efficiency.

The Symantec ICD Platform unifies products, services and partners to drive down the cost and complexity of cyber security, while protecting enterprises against sophisticated threats. ICD combines information protection, threat protection, identity management, compliance and other advanced services, powered by shared intelligence and automation across endpoints, networks, applications, and clouds.

Figure 6: ICD Framework



Symantec™
A Division of Broadcom

For more product information: broadcom.com

SED-WES-SB100 April 22, 2020