White Paper

Office 365: Network Security and Performance—Simplified

Symantec® Network Protection for Microsoft Office 365

Migrating to Office 365

Cloud applications—services like Salesforce, Office 365, and Box—are being adopted at a rapid pace and are changing the way we work. Between the business productivity and cost benefits of the subscription cost model of cloud application services, ubiquitous corporate adoption of cloud-delivered applications appears to be only a matter of time.

Most organizations evaluate and select cloud-based applications primarily for their business productivity and cost benefits. To enable these benefits, IT and Security teams must address critical and yet often overlooked security and performance concerns. Ultimately, as organizations adopt cloud application services, these teams are responsible for securing users and content—not the cloud vendor. Office 365, in particular, is a popular cloud application and the teams supporting it are not immune to these challenges. For IT and Security teams planning an organization's migration to the cloud email platform, it is important to identify network solutions that deliver strong security and high performance to simultaneously protect users and to deliver the great web experience that employees expect. The ideal solution does this without adding operational complexity or overhead.

Performance, Latency, and Operational Complexity

There are many issues aside from security that cause enterprises to pause when contemplating an Office 365 migration. Office 365 is not a typical cloud application that gets used by a fraction of employees 10% of the time. It is a collection of applications that everyone uses most of the time. For example, a typical user of Microsoft Exchange Online maintains six or more concurrent Internet connections. An organization with 3500 people using Exchange Online likely requires an additional 200 MB of Internet bandwidth. Add new Office 365 applications, and concurrent connections can grow from six to forty, while bandwidth may reach 300 MB or more.

Moreover, the placement and configuration of Office 365 application servers can also cause unwanted latency and operational complexity. For example, when Microsoft scales out their infrastructure, the IP addresses and placement of their servers can change over time requiring operational complexity for organizations managing connections to them from their users.

Users notice any speed bump in the implementation of this particular cloud service. IT departments want to avoid swamping their help desks as an organization is adopting Office 365, which is why any security solution for the application needs to keep performance, scalability, and operational simplicity as key requirements.

Symantec® Network Protection Is Optimized for Office 365

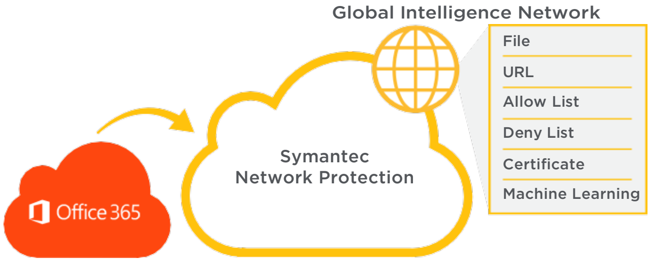
We have analyzed these challenges and built security solutions that address latency, complexity, and performance concerns as your organization makes a secure and compliant move to Office 365. Symantec® Network Protection offers a unique combination of API-based and in-line threat prevention and data compliance capabilities for an organization using Office 365. Before we provide an overview of the capabilities, let us first look at some of the innovations Symantec has built into its Network Protection infrastructure to optimize its interactions with Microsoft's cloud network.

Simplified Security Policy Governance

Keeping up with Microsoft's pace of change can be a challenge. One example? The myriad of IP addresses associated with the Office 365 apps frequently changes as a result of Microsoft's seemingly continuous cloud infrastructure scale-out.

Organizations trying to apply security policies on Office 365 applications, relying on IP address information to accurately identify the traffic, need to stay vigilant.

This situation is why Symantec partnered with Microsoft to automate the process of IP re-alignment for in-line Office 365 security policies enforcement. Microsoft provides Symantec the planned changes to IP addresses in advance. The new IP Address information automatically updates your policies through our App Definitions intelligence feeds, eliminating the need for your team to update your policies manually. This process ensures that your policies enforce correctly and consistently. In fact, the data shared between Microsoft and Symantec is so granular that we can enable policy control over individual Office 365 applications. For example, you can set policies to decrypt file downloads only from OneDrive, send them through dual-anti-virus scanning, and pending results, also send to cloud sandboxing for analysis .



Built-in acceleration technologies, such as content peering and optimized connection scaling, further improve key operational metrics and enable you to give your users the performance they demand. Symantec Network Protection for Office 365 is run on Google Cloud. Users enjoy the high performance connectivity that's used by YouTube, Gmail and the Google Ad Network. Content is peered with top cloud providers and offers TCP scaling and more.

Accelerating Security Performance

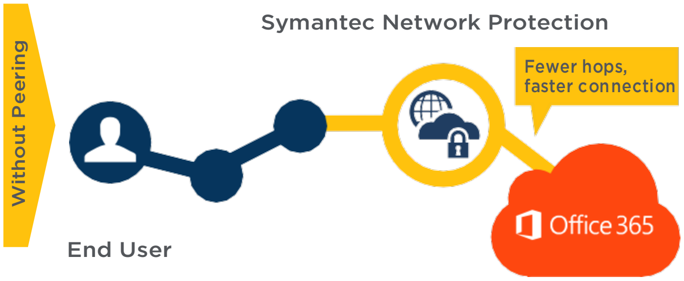
An advanced, cloud-delivered network security service provides simple, cost-effective, high-performance *direct-to-net* protection. Direct-to-net protection eliminates the resources needed for backhaul internet traffic to your corporate data centers.

Accelerated Traffic: Symantec and Microsoft Network Peering

Symantec has built peering interconnections between its global cloud data center network and Microsoft's major cloud data centers. The peering connections allow for a direct exchange of traffic between the two high-performance networks, so your Office 365 traffic benefits from extremely low latency connections between your applications and your Symantec cloud-delivered security and compliance services. Symantec's peering with Microsoft improves end-user experience and reduces the length of the path our customers' traffic needs to travel to get from source to destination. Performance improvements are dramatic, delivering latency drops on the order of 15-20% along with traffic yield improvements from 20-25%.

Peering Directly with Google

Qualifying enterprises may be able to get even more benefits from Symantec's peering infrastructure. If certain criteria are met, the enterprise itself can peer directly with Symantec within our peering exchanges. The result? Even faster performance, and likely substantial savings in bandwidth costs for enterprises when compared the alternative of building out their bandwidth and infrastructure as they re-architect their network for Office 365 traffic.



Accelerated Traffic: Internal Network Optimization

Maintaining performance is not only about what happens when the traffic leaves your environment, but it also about what is happening inside your network as well. Symantec has solutions that allow enterprises to make Quality of Service adjustments to improve internal network performance for specific applications. For example, you can specify a specific amount of your bandwidth on your internal network for Office 365 traffic, prioritizing it over other bandwidth intensive apps like YouTube, Netflix, and others.

Beyond Performance: Security and Compliance for Office 365

With performance requirements addressed through our cloud network innovations, and operational complexity eliminated thanks to our development partnership with Microsoft, Symantec offers the industry's most complete stack of security and compliance solutions for users of Office 365. Enterprises adopt our solutions to help address visibility, data protection, and threat prevention requirements associated with their adoption of Office 365.

Lack of Visibility

How do I authorize and log all interactions with O365 for audit/compliance and IR?

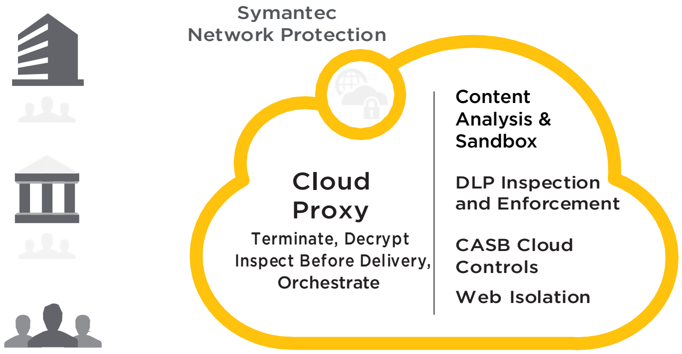
Data Protection and Compliance

How can I ensure we comply with internal and external data protection requirements?

Threat Prevention

How do I prevent malware from file downloads, phishing attacks, and so on?

This section of the paper summarizes some of the key components of our solution. We start with a discussion of our solution to secure Office 365 Email and then review our security controls for the remainder of the Office 365 Suite. Symantec has a deep security stack.



In-line Proxy-Based Security Controls: Symantec Web Security Service

Symantec Network Protection is a cloud-delivered security service, based on proxy technology that many organizations rely on to secure their use of Office 365. The service has a deep set of capabilities, from authenticating access and logging interactions to scanning for advanced zero-day malware attacks. It is a subscription-based service, and enterprise can license features and functions based on their specific requirements.

User Authentication

We can authenticate and log all of your Office 365 traffic, satisfying a key compliance and visibility requirement that many of our enterprise customers have. Symantec provides the flexibility to meet the needs of authentication through different means:

- Remote laptop user support with the Unified Agent program
- Mobile user support with Apple iOS an Android apps
- Active Directory connectivity and integration

Encrypted Traffic

Given the prevalence of SSL/TLS encrypted traffic within Office 365, an effective way to selectively decrypt files for inspection by malware and data loss prevention engines is a critical security and compliance requirement. Finding threats hidden within encrypted traffic is increasingly becoming an important topic in Office 365 migrations. Symantec Cloud Proxy can be configured to selectively decrypt your traffic, including Office 365 encrypted traffic, and inspected it for malware and data loss prevention (DLP) compliance. You can also configure policies on a per-application basis (for example, only decrypt files from OneDrive for inspection).

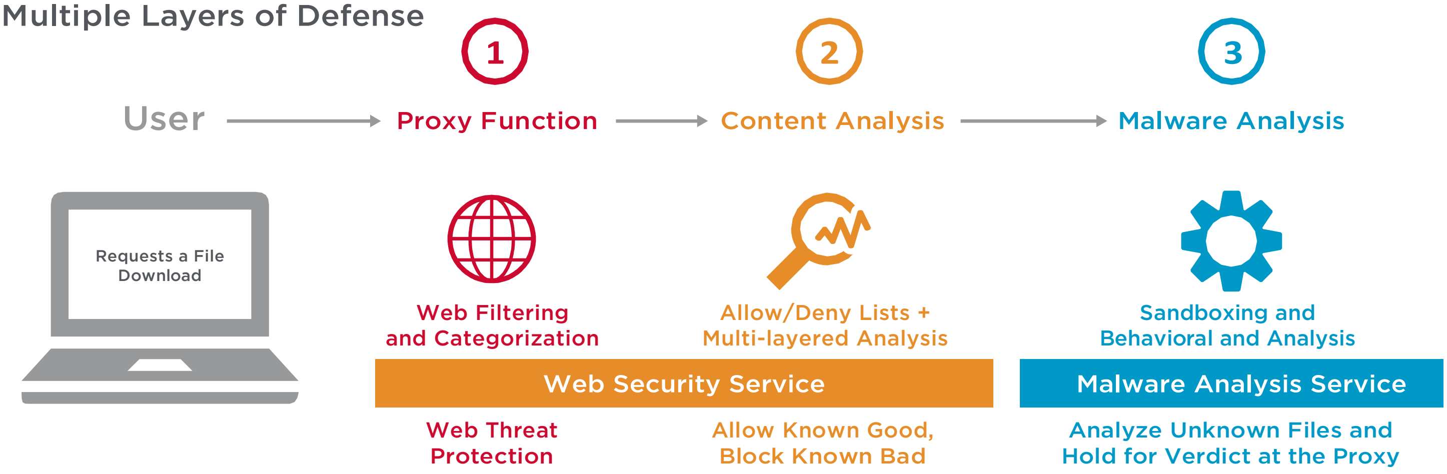
The industry has been urging enterprises to make sure they understand how different solutions perform the function of SSL inspection. This industry focus underscores the importance of Symantec Network Protection work with advanced protocols such as TLS 1.3 and HTTP2 to enable inspection, while not degrading the strong protections that hey give Office 365 users.

Malware and Threat Defense

Symantec Network Protection has multiple layers of cloud malware and ATP defense. The service includes Deep Threat Inspection capabilities along with core proxy functions which integrate together to provide a robust solution to root out malware efficiently. Here is a breakdown of the multilayered defense:

- Proxy function – Web filtering and categorization, Web Threat protection, policy control by GIN, SSL inspection, and Web application controls
- Content analysis – Allow/Deny lists and multilayered analysis, allow known-good, and block known bad files
- Malware analysis – Sandboxing and behavioral analysis, analyze unknown files and hold for the verdict

Multiple Layers of Defense



User → Proxy Function → Content Analysis → Malware Analysis

Requests a File Download

1 Proxy Function: Web Filtering and Categorization

2 Content Analysis: Allow/Deny Lists + Multi-layered Analysis

Web Security Service

Web Threat Protection

Allow Known Good, Block Known Bad

3 Malware Analysis: Sandboxing and Behavioral and Analysis

Malware Analysis Service

Analyze Unknown Files and Hold for Verdict at the Proxy

Data Loss Prevention

Many of our customers want to take advantage of in-line document DLP scanning, leveraging the SSL inspection capabilities of the Web Security Service, to enforce their data compliance policies when using Office 365. They want to make sure that documents being stored and shared in applications like OneDrive do not contain sensitive data or information subject to compliance and privacy requirements. Symantec Network Protection provides two options for this need:

- Symantec DLP Cloud – Symantec Network Protection integrates with our market-leading Cloud DLP service. The solution allows you to selectively decrypt traffic to specific applications in the Office 365 suite and route them to DLP scanning engines in the cloud. This process identifies policy violations and takes the appropriate remediation action.
- Cloud to On-Premises DLP – If you already have a DLP solution that you want to leverage to enforce consistent policies for your data going to Office 365, you can configure Symantec Network Protection to route specific traffic to an on-premises DLP solution for scanning and remediation.

Global Intelligence Network

The Symantec Global Intelligence Network underpins our threat prevention solution. It collects data from multiple vectors and uses it to help all enterprises using our products. This network—the largest civilian intelligence network of its kind— lives natively in the cloud, complementing both on-premises and cloud deployments. 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

Symantec Global Intelligence Network

Discovered **430M**
new unique pieces of malware last year

1B
Malicious emails stopped last year

100M
Social engineering scams blocked last year

23,000
Cloud applications discovered and protected

182M
Web attacks blocked last year

6B
Previously unseen web requests scanned daily

2B
Emails scanned per day

175 Million
Consumer and enterprise endpoints protected

9 Global threat response centers with
1,000 threat researchers and engineers

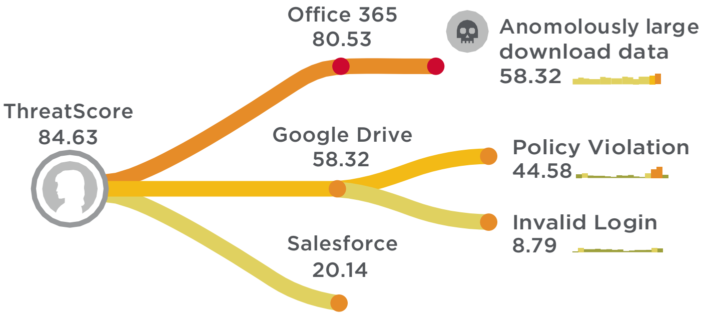
day. This level of visibility across endpoint, email, and web traffic enables Symantec to discover and block targeted attacks that would otherwise be undetectable from any single control point. Our solution provides real-world benefits for you and your Office 365 deployment.

Cloud Access Security Broker Security

Cloud Access Security Brokers (CASB) have become an essential element of any cloud security strategy, helping organizations govern the use of cloud and protect sensitive data in the cloud.

Symantec CASB is an established leader in the market. The service enables companies to confidently use 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 such as compromised credentials. For Office 365 there are four areas that we should highlight:

- Intelligent threat protection – CASB implements User and Entity Behavior Analytics (UEBA) to set baselines on *normal* activity levels for different types of users in Office 365. You can track behavior against those baselines to create threat indicators that can flag risky behavior to security personnel for further investigation, automated account freezes, and more. This approach is a very effective way to quickly identify malicious behavior that may associate with account take-overs (for example, compromised credentials) or insider threats.



- Information Centric Encryption (ICE) – You can set rules to dynamically encrypt content based on the classification of the content. Individual access rights can be enforced and revoked at any time at the document level. For example, when an employee leaves the organization, access to documents on their devices can be revoked.

Office 365
CASB
ICE

- DLP – DLP options integrated with CASB can be used to enforce your strict data compliance and security policies with Office 365. A key feature of the solution is its ability to scan your Office 365 accounts on a scheduled basis to check for policy violations. For instance, imagine a situation where an employee uses their phone to access the corporate OneDrive account over a cell network and places a document there that contains some restricted information, like employee social security numbers and salaries. Even the best in-line DLP scanning approach in the world cannot catch this sort of *direct-to-net* case with a personal device. Symantec can catch this *Shadow Data*; the service can be configured to scan your corporate accounts offline to check for information security policy violations and take steps to remediate violations.
- Incident analysis and response – Security professionals know that time is of the essence when responding to a security event. The first step in any investigation is to get the relevant data, and this step can be a process-intensive task when dealing with a SaaS provider like Microsoft. Symantec CASB integrates with Microsoft's APIs to present all relevant end user and data interaction information to you in a rich information dashboard that offers powerful visualization and search tools. Incident Response teams, armed with these tools, can quickly get to the job of assessing incident impact, identifying causes, and identifying remediation steps.

Email Security

Symantec Email Security.cloud safeguards cloud and On-premises email such as Office 365 and Microsoft Exchange. It blocks email threats such as ransomware, spear phishing, and Business Email Compromise with the highest effectiveness and accuracy using multi-layered defense and insights from the world's largest civilian threat intelligence network. Email security solutions include the strongest protection against spear phishing attacks with defense including protection, isolation, visibility, and user awareness techniques plus advanced email security analytics that provide the deepest visibility into targeted attack campaigns.

Conclusion

Symantec Network Protection uniquely addresses the performance and operational complexity issues that are frequent concerns when securing Office 365. As a result, enterprises can take advantage of our security solutions to authenticate and log Office 365 use, securely inspect Office 365 SSL traffic, prevent threats and malware from Office 365, and enforce DLP/information security policies. Also, you can use deploy Symantec CASB solution to control threats such as compromised credentials and Email Security.cloud to manage the unique security issues associated with email.

Contact your Broadcom Account Team or partner representative for more information and to request a demo or trial. Learn more about the Symantec Network Protection and Symantec DLP Cloud: Broadcom.com/SASE

Symantec™
A Division of Broadcom

For more product information: broadcom.com