SOLUTION BRIEF

Safe Adoption of Cloud Applications

Leveraging Integrated Cloud Security Gateways to Ensure Security and Performance for Enterprise Cloud Applications

Symantec

Introduction

Public SaaS application adoption is taking off even faster than many industry pundits predicted. SaaS apps, services like Salesforce.com, Office 365, and Box, are being adopted at a rapid clip. In fact, Gartner predicts that nearly 40% of enterprise IT application spend will be shifted to cloud versus on-premise by 2020.[1] Between the business productivity and cost benefits of the subscription cost model of cloud app services, corporate adoption of cloud-delivered SaaS apps appears to be only a matter of time.

However, while most IT departments evaluate and select cloud-based applications based on their many business productivity benefits, a number of critical and often overlooked security and performance issues need to be considered at the same time. Ultimately, as a customer of a cloud application service you are responsible for securing your users and content, not your vendor.

This guide details some of the major considerations when looking to secure cloud application use, the limitations of existing point-products, including traditional Secure Web Gateways (SWGs), and an overview of the integrated cloud security gateway approach that is needed to provide comprehensive, information-centric security as your data moves between your users and your cloud applications.

[1] Gartner report entitled ""Market Insight: Cloud Shift — The Transition of IT Spending from Traditional Systems to Cloud." July 2016
[2] Service Level Agreement for Microsoft Online Services. http://neonova.net/wp-content/uploads/2013/02/OnlineSvcsConsolidatedSLAWWEnglishJanuary2015CR.pdf
[3] Implementing Officce 365 – 2016 Gartner Survey Results and Analysis. Larry Cannell.

The Shared Responsibility Model for Cloud Application Security

The Service Level Agreement for cloud applications like those from Microsoft[2] emphasizes a shared responsibility model for security. They agree to provide infrastructure services to ensure hackers don't gain access and that their employees can be trusted not to exploit your data. However, cloud vendors typically do not take responsibility for controlling what, how, and with whom your employees and other users share data within your cloud application accounts. In addition, they will not take responsibility for what content users upload into the cloud. This is typical for other popular cloud services as well.

Your Responsibility: Cloud Application Usage and Performance

Gartner identifies both security and performance[3] as the key issues you must address when adopting cloud applications such as Office 365. Many organizations don't consider these issues because they inaccurately assume the cloud service provider will cover them, and are left scrambling to address them after the fact. Before taking the plunge, you must first consider how you will manage:

- **Large volumes of enterprise data stored and shared in the service provider's cloud** – this data is accessible by a wide array of users, and outside traditional enterprise IT control. This introduces data privacy, security, and compliance risks.

Accidental misuse, hacking, malware and data loss are typically due to accidental cloud app misuse by employees, which is likely why in 2016 Gartner predicted that, “95% of cloud security failures will be the customer’s fault.”

- **Data transmission cloud-to-cloud and between the cloud and endpoints** – data transmission between your primary cloud application service and other cloud services and accounts is invisible to traditional data security solutions. And endpoints, to and from which data is sent, are often located outside the network perimeter and are not managed by the enterprise. Both introduce many avenues to introduce malware or enable data exfiltration.
- **More concurrent open internet connections and larger volume of data moving through your perimeter** – organizations will need to accommodate and manage more network traffic to maintain cloud application performance service levels.

Ensuring Cloud Application Security and Performance

Given that you are ultimately responsible for your cloud application security, there are five key features that you must include in your cloud security platform and strategy to ensure your account, the data stored and shared in it, and its users are secure and compliant. These capabilities must integrate seamlessly into a complete solution which closes security gaps that exist in your current infrastructure that can lead to data loss, theft, or destruction.

[4] 2016 Shadow Data Report

1 Managing Cloud Application Access

Secure Web Gateway (SWG)

The Challenge: Managing Web & Cloud Application Access

Your employees are quickly adopting cloud apps and services, often without IT sanction or oversight – over 840 apps on average per organization.[4] Access to these apps needs to be managed. And even with trusted apps like ServiceNow or Office 365 you must have the ability to apply granular policy controls to ensure your sensitive cloud content stored and shared in it is secured and to protect your organization against the threats, hacks, and user errors.

Developing an SWG Foundation for Securing Cloud Applications

The first step to being able to get visibility and control over your apps, users, and groups, is to adopt a cloud-delivered Secure Web Gateway (SWG). A typical SWG, which sits in-line between your users and the internet, provides:

- **Application Controls** – this will enable you to block or allow access to cloud user accounts, with CASB integration with your SWG, you can also gain granular control over those apps. (see CASB section)
- **URL Filtering** – this will enable you to filter unwanted software and malware from user-initiated Web/Internet traffic.
- **Malware Protection** – a combination of real-time web ecosystem analysis and inline malware scanning can help you to identify malicious sites, malware prone file types, and “phone-home” or botnet traffic.

Be aware that many traditional cloud-delivered SWGs adequately perform a basic level of URL filtering, outbound DLP scanning, malware protection, and app control. However, they have proven mostly ineffective in the new world of cloud applications and services like Office 365, where the focus is on not just securing web traffic and data in motion by replicating the traditional security stack in the cloud, but rethinking the security stack to secure cloud apps and to uncover, categorize, and secure the data being stored and shared to, in, and between cloud services.

So when selecting a cloud SWG that addresses security for your cloud applications, look for an advanced solution that tightly integrates with an on-prem and cloud DLP solutions, Advanced Threat Protection (ATP), Bandwidth Control and Cloud Access Security Broker (CASB) capabilities to provide comprehensive data security no matter where that data resides or is transmitted.

Symantec SWG: Web Security Service

The Symantec cloud-based Secure Web Gateway solution – Symantec Web Security Service – filters unwanted software and malware from user-initiated web traffic and enforces corporate and regulatory policy compliance via a cloud-delivered proxy. Standard functions include:

URL Filtering & Categorization

- Leverages 12 security categories to block 90% of all threats
- Delivers unique URL Threat Risk Score to increase security without over-blocking
- Classifies URLs in one of 70 categories covering over 50 languages
- Provides dynamic, real time ratings for the latest information

User Authentication

- Identifies users with up to 9 authentication methods
- Integrates across multiple authorization systems used by your enterprise

Advanced Threat Protection

- Blocks malware using multi-layered dual anti-virus and heuristic analysis
- Utilizes customized White-List/Black-List capabilities and file reputation analysis

Web Security Service works with the Symantec Global Intelligence Network (GIN), the largest civilian threat intelligence network in the world, to ensure real-time protection against known and unknown web-borne threats. It collects, categorizes and analyzes over a billion previously unseen and uncategorized websites a day from our 15,000 enterprise customers and their millions of users accessing the Internet daily and feeds that information back to the Web Security Service. The GIN provides valuable data to the Web Security Service to keep you one step ahead of fast-changing security threats.

Symantec's Web Security Service operates with Symantec's DLP solutions, Advanced Threat Protection (ATP), Cloud Access Security Broker (CASB), and Bandwidth Control solutions to provide the extended functionality described in this paper.

Enterprises depend on Symantec's Web Security Service to support their web compliance and security requirements, whether it be for corporate access to cloud apps, remote or distributed offices or to protect their increasingly mobile workforce. It frequently makes sense to allow these users to go "Direct to Net", accessing web services and cloud applications directly via the internet instead of routing traffic back through corporate datacenters. Network Security teams can now support these users with the same robust security and compliance policies that are in place protecting their corporate office traffic.

2 Protecting Cloud Applications Against the Latest Malware

Advanced Threat Protection (ATP)

The Malware Challenge

When you adopt cloud applications, you open your organization up to attacks including malware looking for a method to infiltrate your organization, ransomware, bad actors bent on data destruction, and internal and external actors looking for a way to exfiltrate data from your organization. In addition, organizations have thousands of credentials in use by their employees that grant access to valuable data, a compromise of any one of these credentials can open the door to significant company-wide damage.

Developing an Effective Cloud Defense Against Advanced Threats

With the risk of advanced threats growing quickly, an effective malware defense for cloud apps must include the ability to:

- **Identify malicious activity** – apply a layered security approach that can identify known malware, identify malicious activity, and tease threats into exposing themselves to reduce the risk to your organization.
- **Identify and control compromised accounts** – Implement a solution with strong user behavior analysis (UBA) capabilities to identify and mitigate damage caused by errant cloud usage by employees and compromised Office 365 accounts.
- **Automate anti-malware for your cloud** – Add anti-malware solutions that automatically scan and remediate malware infections in your user's cloud application accounts.
- **Provide advanced threat protection** – add a layer of advanced threat protection to analyze files moving in and out of your cloud accounts. The solution should take advantage of threat intelligence networks that monitor customer cloud usage to identify emerging threats in the wild before they can attack your cloud accounts, and sandboxing and code emulation to tease previously unidentified malware into exposing itself.
- **Combat attacks targeting cloud-based Email** – remember that email comes over SMTP, a different channel than most internet access, and needs threat prevention capabilities designed specifically for it. Your solution needs to protect you from advanced phishing attacks. And when emails contain file attachments or clickable URL's, make sure they are scanned with advanced malware detection engines and can be inspected with sandboxes.

Symantec Advanced Threat Protection Integrated with the Web Security Service

Combined with the Web Security Service, Symantec's malware analysis capabilities take a layered approach to detect and protect against known and unknown threats, advanced threats and targeted malware. These security layers include:

- **Deep inspection capabilities** that deliver highly available, inline detection with active blocking capabilities that prevent threats from entering the enterprise.
- **Mobile Device Security** that protects roaming and mobile users going direct-to-net to access business applications.

- **Advanced analysis** that uses static code, YARA rules and behavioral techniques along with inline, real-time file blocking to combat threats.
- **Sandboxing** to detonate suspicious samples using dual detonation techniques (virtual/emulation) and custom virtual machines to defeat sophisticated attacks.
- **Email Threat Prevention** to block targeted attacks, spear phishing, viruses and malware, and provides deep visibility into targeted attacks and accelerates remediation.

Web Security Service, integrated with Symantec's Malware Analysis and Email Security.cloud Services, delivers superior threat prevention performance and coverage, so you can protect your web traffic, including traffic to and from your cloud application accounts, against viruses, Trojans, worms, spyware, bots, and other forms of malicious content – complementing any anti-malware software that may be running on your endpoints.

With Symantec Advanced Threat Protection solution you can:

- Block known web threats
- Allow known good files
- Block known bad files
- Analyze unknown threats
- Update the Global Intelligence Network to protect against future attacks

3 Identification, Classification and Protection of Sensitive Data in Cloud Applications

Cloud Data Loss Prevention (DLP)

The Data Security Challenge

Of the data that a typical company stores and shares via cloud apps, 23% is broadly shared, meaning that it is being shared beyond the immediate team, with people outside the organization, or even with anyone and everyone who gets access to the link to the information, placing your company at increased risk of data leakage. To make matters worse 12% of broadly shared files contain confidential data such as PII, PCI, PHI and source code, putting your organization of increased risk of GRC violations.

Controlling cloud data loss requires the adoption of a SWG solution that has advanced DLP capabilities that can protect all of your web traffic, and CASB cloud DLP capabilities that will enable you to scan all cloud application accounts, including data at rest in various SharePoint servers, in/out mailboxes, and other locations.

Developing an Effective DLP Strategy

You must be able to identify and protect confidential data across your organization with a DLP solution that secures data in both your cloud accounts and on-prem systems including data at rest and in motion. You likely have confidential data in a broad number of applications. A high-quality DLP solution will provide consistent protection for all of this data and will minimize the human intervention required to prevent data loss. Adding to the challenge, you

need a DLP solution for cloud apps that will also secure outbound email against data loss.

If you already have a traditional DLP solution in place, you need to figure out how you are going to expand that same data protection to identify and classify all your data in the cloud. In many cases, you will need to rethink your DLP strategy to deal with the unique scenarios created by cloud application adoption.

Ideally, you will want the application of DLP policies to be centrally managed and applied so that the same content classification, workflows, and policies used on-prem can also be applied to content in your cloud application accounts.

Symantec DLP Integrated with the Web Security Service

Symantec DLP provides extensive web application controls, multi-layer file analysis and detailed reporting features, as well as the ability to:

- **Monitor and protect sensitive data** – including data traversing mobile devices, on-prem, and in the cloud using the most advanced DLP matching and recognition engines on the market
- **Extend your DLP coverage to the cloud** – get direct visibility and control of content in over 60 cloud apps. This functionality is achieved through Symantec DLP integration with Symantec CASB securlets (See CASB section below) to protect data at rest in cloud applications.
- **Create and enforce granular policies** that are instantly applied to all covered users, including fixed locations and roaming users.
- Apply the same data security policies on and off prem. DLP must be applied to on-prem and mobile users. Management for both should be done centrally from a single DLP management console.

DLP Cloud Service for Cloud-based Email

Symantec Data Loss Prevention Cloud Service for cloud-based e-mail, like Office 365 Email, is an optional service to the Web Security Service, providing real-time protection with automated response actions such as message blocking, redirection, and encryption capabilities. It enables you to focus on and prioritize real incidents with accurate monitoring and analysis and respond faster with one-click responses and automated workflow. Plus, sophisticated policy authoring allows you to enforce policies anywhere – across cloud and on-prem mailboxes. The email DLP cloud service enables you to:

- **Enforce data loss policies** across both cloud and on-prem mailboxes with sophisticated policy authoring
- **Prioritize real incidents** – not false positives or negatives – with accurate, real-time monitoring and analysis of data in motion
- **Respond to incidents faster** – with real-time protection and robust incident remediation workflow

4 Visibility and Control over Data in Sanctioned and Unsanctioned Cloud Apps

Cloud Access Security Broker (CASB)

The App Security Challenge: Controlling Shadow Data, Not Just Shadow IT

While some key enterprise cloud applications will likely be top of mind, the reality is that there are other cloud apps that are likely being used by your organization that you also need to be concerned about. As a result, you should implement a CASB that can not only uncover Shadow IT – that is, unsanctioned cloud applications on your network– but can manage Shadow Data – the unmanaged data resident in both sanctioned and unsanctioned cloud apps. Your CASB should be able to alert you when sensitive data is at risk in the cloud and offer automated prevention and remediation in the event that confidential information is exposed. In addition to shadow IT discovery and policy controls, your CASB should offer:

- **Cloud DLP based on dictionaries** – these dictionaries contain a set of algorithms that can detect specific kinds of data in your users' traffic such as credit card numbers, social security numbers and source code.
- **Data science-driven content analysis** – unsupervised machine learning to identify and classify sensitive information.
- **Custom content learning systems** – ideally the same ones used in your on-prem DLP, which will simplify management.

Developing a Cloud App Security Strategy

Your CASB should be tightly integrated with your SWG and your on prem/cloud DLP solution. If you don't already have a CASB, you need to get one, since your employees are likely already adopting cloud apps and services without your approval. And if you have decided to allow confidential data in the cloud, you should select a CASB that can also automatically encrypt sensitive data in the cloud – adding additional protection for PII, PCI and PHI against data breaches.

Don't be deceived by some SWG vendor's claims to provide CASB-like functionality to manage and control cloud applications. A closer look shows they offer only simplistic controls to allow/block access to a limited number of cloud apps. In some cases you will see that all they offer is an application feed from a 3rd party CASB vendor that provides some limited app visibility and does not even allow you to define cloud access control or data protection policies.

A best-in-class solution is one in which your SWG is tightly integrated with a CASB, enabling much more granular visibility and controls over cloud apps, users and their data, and the application of cloud specific data policies from your SWG dashboard.

Symantec CASB Integrated with the Web Security Service

Web Security service is tightly integrated with the Symantec CASB solution, enabling:

- **Shadow IT analysis and control capabilities** – Symantec's Web Security Service customers get granular cloud app discovery information so they can see the risks associated with the adoption of cloud apps in their

By 2020, 85% of large enterprises will use a Cloud Access Security Broker product for their cloud services which is up from fewer than 5% today.[5]

[5] Gartner's Market Guide for Cloud Access Security Brokers (CASBs)

environment and set controls to manage these risks.

  - **Information on more than 15,000 applications,** with over 60 attributes per app that can be used to implement appropriate policy controls by the Symantec Web Security Service.
  - **The ability to create simple, targeted policies** on the Web Security Service to block specific apps or implement controls over multiple apps directly from the Web Security Service management console.

- **Automatic upload of activity log files from the Web Security Service to the CASB** to get detailed information on employee usage of cloud apps like Office 365.

Securing Shadow Data with the Cloud Application CASB Securlets

Accidental misuse by employees, hacking, and malware typically come in through the front door of your cloud application accounts, which is likely why in 2016 Gartner predicted that, "95% of cloud security failures will be the customer's fault."

Symantec provides Cloud Securlets for a large number of enterprise cloud applications to complement the Web Security Service's DLP, ATP and web access control functionality. Securlets deliver API-based security to address risky user activities by providing advanced security functionality, including visibility and control over how your employees share and access sensitive data in cloud applications.

Symantec Cloud Securlets provide the ability to:

- **Automate** classification and governance of compliance related data, such as PII, PCI and PHI and determine which files that are exposed publicly, externally or internally. ContentIQ, which uses advanced semantic analysis to free you from manually having to define keywords or regular expressions, automatically highlights possible compliance risks.
- **Detect and Prevent** threats based on patent-pending data science algorithms and UBA. This includes identifying users with the most compliance risks and exposures. You can also identify potential malware attacks through automated monitoring of account behavior, then create policies that generate alerts and/or block suspicious account activity in real-time.
- **Define and Enforce** content-aware and context-aware policies to automatically remediate risks and exposures as they occur, prevent data leakage and thwart malicious activity.
- **Streamline Reporting and Incident Response** tapping granular log data with powerful analysis tools. Symantec's Cloud Securlets enable you to go back in time and zoom into a specific user, document or activity and correlate events.

5 Optimizing Cloud Application Performance

Bandwidth Control

The Performance Challenge

Adoption of some cloud applications, like Office 365, may create performance issues that can complicate adoption. For example, a typical user of MS Exchange Online will maintain six or more concurrent internet connections and an organization with 3500 people using Exchange Online likely will require an additional 200MB of internet

Conclusion

If you are planning to adopt cloud applications, security, compliance and performance should be your top concerns. Otherwise, the business benefits of the service will be overshadowed by risks to your sensitive data and poor network performance.

The market is full of point products designed to address certain aspects of Office 365 security, but only Symantec has a complete, integrated solution designed to secure your cloud application data and accounts.

Symantec's Web Security Service provides best-in-class core capabilities for securing your move to the cloud, and its integrations with other key products in Symantec's broad portfolio combine to deliver the industry's most advanced solution to ensure your cloud application accounts remain efficient, effective, secure and compliant.

bandwidth. Add additional Office 365 apps and concurrent connections can grow to 40+ and bandwidth increases to 300MB or more. To maintain performance, you have two options – increase network bandwidth, which is expensive, or throttle bandwidth use of less-business critical apps to maximize bandwidth dedicated to apps like Office 365.

Developing Critical Bandwidth Control Capabilities

A cloud adoption security solution, then, should have bandwidth control capabilities which can:

- **Reserve bandwidth** for critical and real-time applications like Office 365
- **Limit disruptive and recreational** traffic such as YouTube while reclaiming bandwidth from non-business usage
- **Support cloud adoption** and embrace new trends such as BYOD, video and social media
- **Eliminate unnecessary bandwidth increases** and save on operating cost

Symantec PacketShaper Integrated with the Web Security Service

With Symantec PacketShaper you can:

- **Prioritize traffic** – ensure you are prioritizing business-relevant applications over recreational content, which not only increases performance but also saves against unnecessary and costly upgrades.
- **Differentiate Office 365 traffic from social media** – throttle down internet servers flooding the network with traffic and "negotiate" throughput with the cloud/SaaS server to ensure smooth and optimized performance.
- **Enable BYOD without increasing bandwidth** – control the impact of BYOD and recreational traffic by establishing a partition with a lower bandwidth limit (20 percent, for example) and make it burstable at low priority when unused bandwidth becomes available. This can reclaim 20-40 percent of bandwidth costs while fixing performance issues.

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

SYMC_SB_Safe_Adoption_Cloud_Apps_EN_v1a