White Paper

Information Protection in the Web and Cloud Era

Symantec

Today's Modern Enterprise Needs Security that Fits

Companies used to be able to lock their doors and shred their documents to keep their information from getting into the wrong hands. Then came the digital age - information was suddenly easily accessible and transferrable. To prevent it from being intercepted, stolen or accessed by unauthorized users, security technologies sprouted up to protect it as it flowed through the company's local area networks (LANs), between their remote sites, and in and out of their discrete data centers.

Over the past few years, however, we have seen the digital world evolve – it's been migrating to the cloud and going mobile - yet the security technologies designed to protect the data continue to operate as though there are defined digital boundaries to the business world. The reality is there is no containing data today – it's literally everywhere.

Users are storing and accessing corporate data from their smartphones, tablets, cloud apps, home offices and airport kiosks. They are going to their local coffee shop and connecting to public Wi-Fi to directly access their corporate apps and accounts in the cloud (e.g. Salesforce, Box, ServiceNow, etc.). All the while, traditional security controls, which exist in a company's data center, have no visibility into this activity – they are unable to monitor, control or protect the data the moment it's outside the company's direct control.

What's needed is a modern approach to this modern data protection problem. What's needed is a solution that can implement consistent controls and security, regardless of how data is accessed and where it is stored. This white paper explores the challenges associated with protecting data in today's enterprise and starts to detail how a modern data loss prevention (DLP) solution, delivered as part of a cloud-based web security gateway, can provide continuous monitoring and protection of sensitive data on mobile devices, on-premises and in the cloud.

Transport Encryption…the Good and the Bad

One way that organizations have attempted to protect data as it leaves their direct control is to encrypt it. Using the transport layer security (TLS) and/or the secure sockets layer (SSL) encryption, enterprises can protect the privacy and integrity of their data while it is in transit. It's why, as of January 2017, more than half the web's traffic was encrypted.

The problem is encryption can be both good and bad for security. It doesn't discriminate – it can be used to protect sensitive, confidential information, as well as hide a hacker's activities. In 2015, attackers using SSL/TLS encryption to conceal their activities affected at least 900 million users. Gartner has predicted that by 2017 50% of all network attacks will come through encrypted traffic, thanks to its ability to hide cybercriminals activities.

Unfortunately, most DLP solutions (and most other security devices) cannot see into encrypted traffic to ensure it is not hiding unauthorized document sharing or masking malicious activity. For those solutions that do have the ability to peer inside of encrypted traffic, decrypting is typically so process-intensive that it impacts the overall throughput of the solution, rendering the capability unusable. As a result, the blind spots created by encrypted traffic are big and only getting bigger.

Not only does transport-layer encryption create serious security holes, but also data compliance issues. Regional and industry regulations, such as the European Union's General Data

Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) in the Unites States, and the Payment Card Industry Data Security Standards (PCI DSS), impose strict guidelines around the handling and storage of personally identifiable information (PII) and other regulated data. Non-compliance can result in fines, lawsuits and even halted operations.

The increased web usage and cloud adoption only make the security and compliance challenges that much more difficult. Organizations need to be able to detect and prevent unauthorized attempts to access and share sensitive, regulated data, so they can comply with their corporate, security and regulatory requirements. Let's look at the implications for a DLP solution.

Top 5 Requirements for a Modern DLP Solution

To meet the data protection requirements of today's enterprises, organizations need a DLP solution that eliminates the blind spots that have been created by encryption, as well as mobile and cloud usage. They need a solution that can implement consistent, robust policy controls to help them achieve their security objectives and maintain compliance with relevant regulations. This requires the ability to:

1. **Protect data anywhere** - regardless of where the users are located (on the go, remote, etc.) or where the data is stored - on mobile devices, on-premises, or in the cloud.
2. **See inside encrypted traffic** – to uncover and mitigate any data sharing policy violations that may be hiding wrapped within TLS/SSL encrypted traffic.
3. **Identify sensitive data** – to ensure corporate IP and regulated data can be effectively protected, even when the content is embedded deep within a document – e.g. medical records, credit card information, employment data, bank accounts, documents that are in a similar format to other sensitive doc types, etc.
4. **Implement granular controls** - with an information protection framework that can meet the organization's varied requirements - e.g. "block any customer name and bank account number"; "block specific file types from being uploaded"; "block if there is 'xxx' pattern within a document," "stop spreadsheets from being sent out, only allow PDFs," etc.
5. **Support flexible deployment models** – to best address the way users are accessing and sharing content and maximize the utility and return of investment organizations receive on their DLP deployments. The DLP solution should be able to accommodate the cloud and web usage needs of the organization, whether that is to:
   - **Extend existing on-premises investments** – ensures the time and resources spent honing existing data loss policies can be leveraged and extended to the web and cloud. Organizations don't want to reproduce everything, they just need a web/cloud security service that can plug into their existing on-premises infrastructure and extend its capabilities.
   - **Utilize cloud-based DLP** – enables users to go directly to their applications, without having to route traffic back to the data center, while ensuring that web and access is complying with the same data loss policies enforced within the corporation. As a subscription cloud service, organizations get all the benefits of a cloud-delivered service (scalability, flexibility, and cost-effectiveness) to protect their remotes users and users on the go.
   - **Cover the cloud SaaS app blind spot** – keeps "out of band" access to cloud apps from introducing security risks and compliance violations. When users take alternative paths to access corporate data in cloud apps, such as using their mobile device on a cellular network to create sensitive information in Box, Dropbox, Google Apps, Salesforce, Office 365, etc., they have effectively side stepped your DLP controls. Modern DLP solutions need to address this by allowing organizations to regularly scan corporate accounts in the cloud, in an offline mode, and remediate any violations that are discovered.

The Solution: Cloud-Based Web Security Service, with DLP

The cloud-based secure web gateway from Symantec delivers a wide array of security capabilities, including the ability to discover, monitor and protect corporate data as organizations embrace cloud services and look to improve the productivity of remote and mobile users. With the Symantec Web Security Service (WSS) organizations can enforce data loss policies that maintain

the privacy and integrity of sensitive IP and regulated data on-premises, in the cloud and on mobile devices. As seen in Figure 1, the Symantec WSS sits between an organization's devices and their web and cloud apps to ensure all access can be effectively monitored, managed and secured.

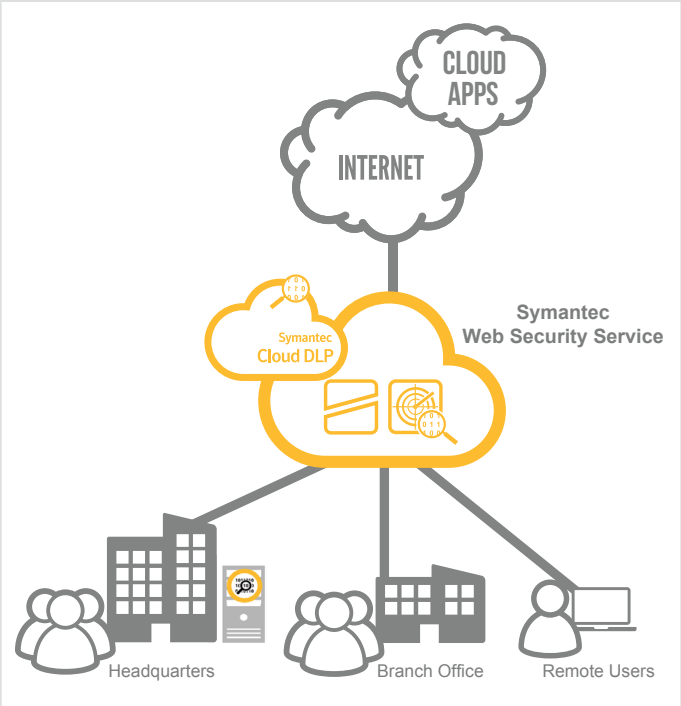

Figure 1 – Modern Enterprise Class Security

Using Symantec WSS with DLP, organizations can:

Protect Data Anywhere

Symantec WSS with DLP enables organizations to enforce information protection policies and prevent data loss, regardless of employee location or what devices they are using to connect. With Symantec WSS and DLP, organizations can consistently apply data loss policies to protect all their information; they can inspect all types of traffic, including:

- Traffic from on-premises, mobile and remote users
- Traffic from browsers, mobile apps, desktop apps, sync clients, etc.
- Content in and en-route to sanctioned cloud traffic/apps
- Content en-route to unsanctioned cloud traffic

See Inside Encrypted Traffic

The Symantec WSS aggregates all corporate, remote and mobile traffic, quickly and efficiently decrypts encrypted information, and hands it off to other inspection engines for analysis, making it the perfect complementary partner for DLP. As a result, organizations have the much-needed visibility and performance required to spot data protection policy violations that are hidden in encrypted traffic. Symantec offers granular controls over which traffic is decrypted and sent for inspection, so organizations can ensure they are adhering to corporate information privacy policies and external regulations.

Identify Sensitive Data

Symantec Web Security Service's cloud DLP enables organizations to locate where their sensitive information resides across their cloud, mobile, network, endpoint and storage systems and understand the context of how it is being used, including what data is being handled, by whom, so they can take appropriate measures to maintain its security and privacy. Symantec offers the most advanced detection technologies available to accurately identify intellectual property:

- **Described Content Matching** looks for matches on regular expressions or patterns, e.g., "block whenever a credit card pattern is found."

- **Exact Data Matching** identifies sensitive data directly in the organization's database, e.g., "block exfiltration of any customer name and their associated bank account number."

- **Indexed Document Matching** applies a "full file fingerprint" to identify confidential information in unstructured data, including Microsoft Office documents and PDF files, as well as binary files, such as JPEGs, CAD designs, and multimedia files.

- **Vector Machine Learning** automatically learns and identifies the layout of sensitive document types, such as financial documents, source code, etc.

- **File Type Detection** recognizes more than 330 different file types, including emails, graphics and encapsulated formats, as well as virtually any custom file type.

Implement Granular Controls

Symantec Web security Service's DLP allow organizations to apply consistent, fine-tuned policies that protect their information when its on-premises, in the cloud, or on the go. Because of Symantec's highly accurate, robust data identification capabilities, organizations can dictate exactly how sensitive or regulated data should be managed to meet their security and compliance requirements. If a mix of cloud and on-premises secure web gateways are being used, data protection policies can be defined once and then distributed to cloud and on-premises gateways for enforcement. Symantec offers centralized visibility and reporting, so organizations can quickly spot issues and make adjustments to keep effective data loss controls and policies in place. Symantec also supports out-of-the-box compliance templates for regulatory categories, such as PHI, PCI, etc. and provides incident management with closed-loop workflows that allow organizations to investigate, alert, and manage threats to minimize the impact of any breach or data loss.

Support Flexible Deployment Models

Symantec WSS supports various DLP deployment scenarios. It can be used:

- **To extend existing on-premises DLP investments** – enabling organizations to maximize their return on their current on-premises DLP solution, from Symantec or another provider, and extend the policies that are already in place to protect their cloud applications and web use. This avoids policy rework and minimizes compliance issues and costs associated with "new" policy mistakes. It utilizes the Symantec "Cloud to Premises" connection technology, which establishes a highly secure and resilient connection between the Symantec cloud and the organization's data center, without requiring any firewall modifications (see Figure 2).

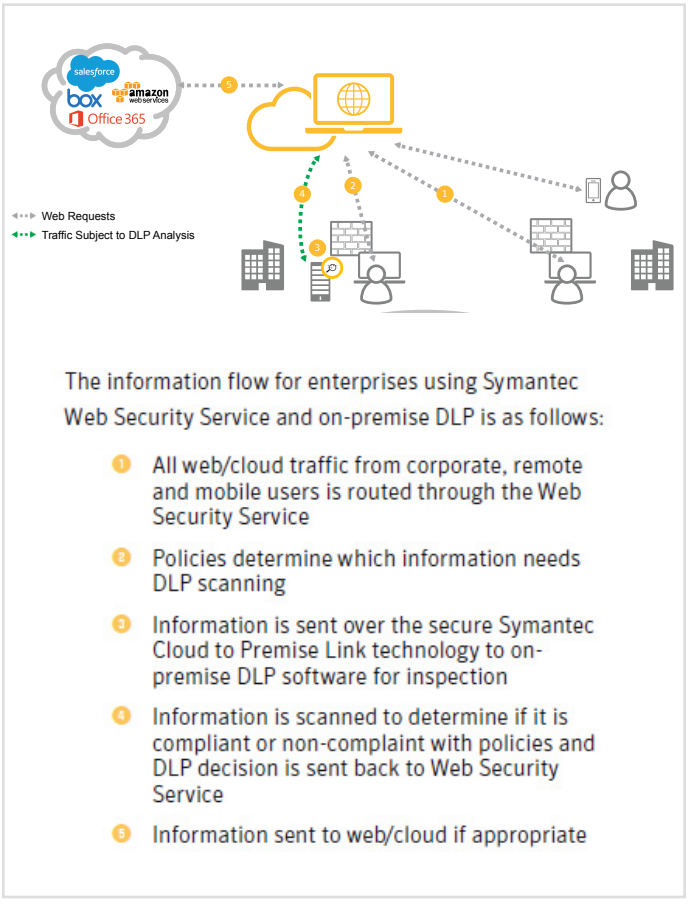

Figure 2

- **In concert with the Symantec Cloud DLP** – providing the scalability, flexibility and cost-effective benefits of a cloud delivered service. Organizations are free to focus on their business, while the Symantec Cloud DLP handles the deployment, management and ongoing maintenance of the infrastructure required to support their DLP needs. Organizations have the peace of mind that their corporate data loss policies are consistently being enforced as their users traverse the web and use cloud apps (see Figure 3).

The information flow for enterprises using Symantec Web Security Service with Cloud DLP is as follows:

1. All web/cloud traffic is routed through the Web Security Service
2. Policies determine which information needs DLP scanning
3. Information sent to Symantec DLP Cloud for inspection
4. Information is scanned to determine if it is compliant or non-complaint with policies and DLP decision is sent back to Web Security Service
5. Information sent to web/cloud if appropriate

Figure 3

- **To cover the cloud SaaS app blind spot** - discussed earlier in the paper. It can be configured to perform offline cloud SaaS app DLP scanning via our Symantec CloudSOC technology to ensure the content in cloud apps adheres to compliance and security policies. Symantec supports more than 60 cloud apps, such as Office 365, Box, Dropbox, Google Apps and Salesforce, to ensure "out of band" activity does not violate security or compliance requirements. Organizations can leverage Symantec Cloud DLP policies and workflows for cloud apps, as well as endpoints, networks and data centers to maximize their DLP investment. An added benefit is the increased performance enjoyed by organizations, as they leverage an integrated, pure cloud solution to optimize bandwidth and minimize latency (see Figure 4).

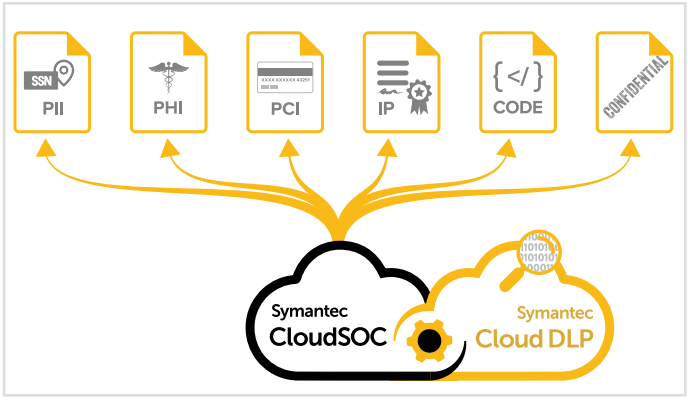

Figure 4

Benefits of Symantec WSS and DLP

The modern enterprise requires a modern approach to data protection that can keep up with the changing nature of information and how it is being shared on the web and in the cloud. Symantec WSS and DLP provides a solution that can match the fluidity of today's information. Symantec gives organizations the ability to discover where sensitive and regulated data is located, monitor it to understand the context of its use, and apply consistent controls and data loss policies to prevent it from being leaked or stolen. It doesn't matter, whether the data is located - on-premises, in the cloud or on a mobile device - if it is encrypted or not, or how users want to access it, Symantec can provide consistent protection that meets the organization's security and compliance requirements, while enabling users to get the information they need (and are authorized to use) to get their work done. With Symantec, organizations can be confident that data compliance policies ae being enforced, while their employees enjoy the efficiency and productivity gains of increased web and cloud application adoption.

About Symantec

Symantec Corporation World Headquarters
350 Ellis Street, Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934

www.symantec.com

02/17