WHITE PAPER:
WEB PROTECTION FOR YOUR BUSINESS,
CUSTOMERS AND DATA

Web Security.cloud

Web Protection for Your Business, Customers and Data

Who should read this paper

For security decision makers and administrators who are looking to understand more about how the Symantec Web Security.cloud offering enables customizable outbound data protection policies.

Symantec

Content

Introduction

Symantec Web Security.cloud - Web Data Protection

Robust web security that can thwart cyber attacks and stop malware from entering an organization's network has become universally established as a vital requirement in today's hostile threat landscape. But it's not enough to only put in place inbound controls that keep threats from getting inside the network. Whether it's via web mail, file sharing sites, or social networks, there can be no argument that there is an ever expanding outlet for organizations' valuable data to escape. Once out on the web, there's no bringing it back.

When it comes to your most prized information, insider threats – both unintentional and malicious – can be an even more serious concern than external threats. In fact, the 2013 Ponemon Cost of a Data Breach Study found that human errors and system glitches were responsible for nearly two-thirds of data breaches. That same report indicated that the total cost of a data breach for U.S. organizations averaged higher than $5.4 million.

While news reports often focus on stories regarding stolen credit card data, that's not the only type of data loss that organizations need to be concerned with leaving their network. Other personal customer data, health information, business quarterly results, merger and acquisition strategies, executive internal emails, employee data, source code, product designs, manufacturing plans, pricing, and any other type of valuable information that could harm your business needs to be protected from falling into the wrong hands.

For example, in a recent study conducted by the Ponemon Institute, 50 percent of survey respondents indicated they had taken intellectual property from a former employer and 40 percent of those indicated that they planned to use that information in their new jobs. That same study indicated that 41 percent download intellectual property to their personally owned tablets or smartphones and 37 percent use file sharing apps without permission from their employers.[1]

To help you keep your valuable data from leaving your organization via the myriad of different web outbound channels, Symantec has developed Web Data Protection capabilities as part of the Symantec Web Security.cloud offering. While Web Security.cloud has proven its ability to employ URL filtering and web policy enforcement to block threats before they reach your network, Web Data Protection complements that capability through web policy enforcement that lets organizations control outbound information flow via the web. Taking its vast experience, expertise and knowledge in data loss prevention, Symantec has now applied that to Symantec Web Data Protection.

By enhancing their level of control of outbound web communications, the Web Data Protection capabilities in Symantec Web Security.cloud enable organizations to:

- Protect their brand and reputation
- Preserve customer and employee loyalty
- Advance regulatory compliance efforts
- Enhance their data security best practices
- Reduce likelihood and costs of data breaches
- Maintain their competitive advantage by safeguarding intellectual property

[1]- "What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk.", Symantec/Ponemon Institute, 2013. http://www.symantec.com/about/news/release/article.jsp?prid=20130206_01

How Web Data Protection Works

Web Data Protection offered by Symantec enables organizations to identify and control any confidential, inappropriate, personal or proprietary content that their users might attempt to distribute across both HTTP and HTTPS communication. From within the unified management portal in Symantec Web Security.cloud, administrators can use pre-defined policy templates or create custom policies to easily control exactly what their users can send to web sites and via web based services.

For example, using Web Data Protection it is possible to:

- Analyze the contents of a file uploaded to Dropbox, or a similar file hosting service, to prevent confidential data from being extracted from the network to an unsanctioned cloud application
- Prevent password protected content from being uploaded to the web to evade controls
- Scan text entered into search engines for any inappropriate or unwanted searches
- Control the contents of both web mail and any attachments to prevent business information from being saved to personal mail accounts
- Block posts to social media sites such as Facebook that contain proprietary or confidential information.

The ability of Web Data Protection in Symantec Web Security.cloud to keep an organization's prized information from slipping out through web channels derives from the following two main aspects of the service:

- Policy controls and enforcement
- Enhanced reporting

Web Data Protection Policies

The flexible policy engine that powers Web Data Protection in Symantec Web Security.cloud enables organizations to create custom policies that meet their unique business requirements. For all outbound web activity, the service checks the web request against all active policies. When an event matches the rules and conditions of a policy, a designated action occurs, which might include blocking the event, logging the event, blocking and logging the event, or allowing the event.

Pre-defined Policy Templates

One of the greatest strengths of the Web Data Protection capabilities in Symantec Web Security.cloud is that it has been designed and built using Symantec's experience and expertise in the data loss prevention arena. These strengths particularly come through in the provided Web Data Protection policy templates, which utilize libraries, dictionaries and predefined rules based on insights and practices that Symantec has developed over several years through its extensive work with regulatory compliance, data loss prevention and security intelligence.

These pre-defined Web Data Protection templates contain rules, regular expressions and keyword lists that provide organizations a quick and easy way to create and customize robust and reliable policies that meet some of their most common web data protection needs. The templates can act as a solid starting point in helping organizations work towards addressing some of their regulatory compliance concerns. For example, Web Data Protection includes templates that focus on assisting with compliance with EU Data Protection Directives, HIPAA, PCI, Gramm-Leach-Bliley, International Traffic in Arms Regulations (ITAR) and other regulations.

In addition to the pre-defined templates, Web Data Protection also provides predefined keyword lists that organizations can leverage in any policy they want to create.

Rules and Conditions

A policy consists of one or more rules, and each rule comprises of one or more conditions. Exceptions can also be defined for a rule. Exceptions to a rule allow specific data or individuals to be excluded from detection. When an administrator creates a policy with multiple rules or conditions, the administrator also determines the "and/or" relationships between those multiple rules or multiple conditions.

Conditions are the tests that a policy rule will apply to a web request. For example, a condition might check whether a web request contains a social security number. Other conditions might check for file uploads that match a specific file type, such as video or audio type files.

The following represent a few of the conditions that can be used within policy rules:

- **Content Keyword List** – Includes keywords such as banking-related words, names of credit card issuers, product code-names, stock symbols, a company name targeted for acquisition, profanity, racial slurs, etc.
- **Content Regular Expression List** – It might include expressions for identifying bank account numbers, credit card numbers, social security numbers, and employee ID numbers.
- **Destination URL Category** – Compares the URL in a web request with one or more URL or URL categories, such as blogs, job search or social networking.
- **File Upload is Spoofed** - Checks for files that have had their file extension changed, which might indicate a possible attempt to bypass security scanning software.
- **User Group** – Determines if the user posting content to the web exists within one or more groups of users, including LDAP groups and custom groups.

Additionally, the Web Data Protection capabilities give administrators granular control in determining if the rules and conditions of a policy have been met. For example, the rules and conditions of a policy can specify that the policy will be triggered if the content of a web mail contains three words from a keyword list and if the email has a password protected attachment. In such a situation, the policy will be triggered only if all conditions are met.

Actions

As mentioned before, when an event occurs that matches the rules and conditions of a policy, the policy can be set to either block the event, log the event, block and log the event, or allow the event. The unique security and compliance needs of an organization will help it determine which action is best suited for different policies.

For example, an organization might want to keep certain innocuous or even inappropriate web activities from occurring, but it's not particularly concerned about investigating or knowing who attempted these web events. It just wants to block them from happening so therefore it would choose to block, but not log the event.

The log action might be used in policies that monitor web events that might result in a response from the HR department, these might not be critical events, but still unwanted at the workplace. These policies might watch for inappropriate web behavior by employees that could warrant disciplinary action. In these instances, the organization might not be as concerned about blocking the activity as they are about making sure they have a detailed paper trail to support any HR actions against the employee.

The block and log action would typically be used for more critical events that an organization not only wants to make sure don't occur, but they want to know how, by whom and when the attempts were made. These could include attempts by employees to post any confidential

information, such as product plans, customer personal data, source code, insider information, and more. It could likewise be used by both HR and security teams to create a paper trail of the unauthorized activity, while making sure that the activity is actually blocked.

The action to allow a certain web request is typically used to create an exception to a rule. For example, a corporation that plans to acquire another business might create a policy that blocks web mail or social media posts that contain the words “merger” or “acquisition” in combination with the name of the business to be acquired. However, the “allow” action would be used to create an exception that allows certain executives and members of the legal department to use those words as needed in web mail exchanges.

Notifications

When an organization uses Web Data Protection in Symantec Web Security.cloud to block a certain web request, it has the option to notify the user that the action has been blocked. Such notifications can take on a variety of forms. Web Data Protection provides its own default notification message, as well as allows organizations to create their own custom notifications.

Such notifications can contain a link to the organization's acceptable use policy that explains proper employee internet usage and conduct. A notification might simply indicate the reason why the user’s web activity was blocked. A notification might also contain an email address for the users to use to request further information.

Web Data Protection Reporting

To facilitate an organization’s ability to investigate or take action on incidents that violate policy, Web Data Protection in Symantec Web Security.cloud offers granular reporting about data protection events with three reporting options on logged policy events.

- Normal - Shows the content that triggered the data protection policy
- Redact Content – Shows the event but removes the data that triggered the data protection policy
- Show surrounding content – Shows the content that triggered the data protection policy and also the content that surrounded it

A normal report provides detailed information on the web request that triggered the policy. This includes showing in the report the specific content that matched the policy condition that caused the web event to be blocked or logged. For example, if a user attempted to upload a document containing confidential product plans to a file sharing site, the report might show the URL for the file sharing site and the keywords contained in the document that suggest it included the organization’s confidential product plans.

However, there are certain cases where an organization would not want the report to show the matched content that caused the policy to trigger. In these instances, an organization would use the redact content setting. Such instances would likely be for policies that block attempts to share customer personal data or similar confidential information would be one of these situations. Without the ability to redact the match content, the report would show the administrator the exact personal data or confidential information that someone else tried to share. Presenting this confidential information to the administrator in of itself could be considered a breach. This setting removes this data from the report and database logs. This allows administrators to be alerted that such an attempt occurred, but without exposing the confidential information to them.

To understand the true nature of web activity that triggered a policy, sometimes only knowing what triggered the policy is not enough. A report defined to show the surrounding content can provide the additional detail or context that a manager needs to determine whether inappropriate web activity actually occurred. For example, a web event that contains the word “heroin” might trigger a policy that monitors employees engaging in communications about drugs. However, a report that presents the surrounding text might show the security officer that “heroin” was actually a misspelling of the intended word “heroine”.

The reporting type is defined for each data protection policy. So, depending on the business reason for the policy, the most relevant reporting type can be selected.

Conclusion

Keeping Valuable Information Safe

The Web Data Protection capabilities in Symantec Web Security.cloud give organizations the granular data protection policies they need to monitor and control their users' web traffic activity in a way that is easy to manage, enforce and report. Whether it's company secrets, personal customer data or any other valuable information an organization wants to safeguard, it helps organizations make sure the things they want to keep confidential don't leak out via the web. It also helps control user web activity to minimize the risk associated with any unintentional or intentional behavior that could adversely affect the organization. Web Data Protection puts organizations in a better position to protect their brand, preserve customer and employee loyalty, address regulatory compliance, enhance web security practices, and reduce the likelihood and associated costs of web-based data breaches.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com