Symantec® DLP Cloud Service for Email

Secure Email Against Modern Threats

AT A GLANCE

Symantec DLP Cloud Service for Email empowers organizations to migrate email to the cloud securely and seamlessly.

KEY BENEFITS

- Comprehensive threat protection
- Consistent policy enforcement
- Real-time insights
- Accelerated incident response
- Rapid deployment

KEY FEATURES

- Advanced detection technologies
- Skeptic scanning technology
- Content-aware DLP in motion
- Seamless cloud and ESS integration
- Unified management console

The Cloud's Silver Lining Needs a Stronger Shield

Cloud-based email systems like Microsoft Office 365 and Google Workspace offer undeniable advantages, including enhanced agility, improved productivity, and reduced costs. These benefits provide organizations with a significant competitive edge. However, they also introduce heightened security risks. Built-in security measures in cloud email platforms often fail to address advanced threats such as ransomware, business email compromise (BEC), and phishing. Legacy email security solutions, constrained by limited analytics and siloed operations, are increasingly inadequate against today's sophisticated threat landscape, leaving businesses vulnerable.

Email remains a primary attack vector for cyber criminals, serving as the leading method for distributing ransomware and the second most common vector for breaches, according to the 2024 Verizon Data Breach Investigations Report. While cloud providers have improved the security and scalability of their data centers, the foundational security features in cloud email applications are insufficient to combat modern, complex cyber attacks. To fully leverage the benefits of cloud adoption, enterprises must implement advanced layers of protection to safeguard sensitive data and ensure resilience against evolving threats.

Introducing Symantec DLP Cloud Service for Email

Symantec® Email Security.cloud (ESS) offers a robust, comprehensive solution for protecting cloud-based email platforms. It enhances compliance and privacy efforts with built-in Data Loss Prevention (DLP) and policy-based encryption controls that identify and manage sensitive emails using over 100 predefined keyword dictionaries, regular expressions, and MIME-type lists. Integration with Symantec DLP further strengthens these capabilities, delivering enterprise-grade protection across email, endpoint, network, cloud, mobile, and storage systems.

Symantec DLP Cloud Service for Email empowers organizations to migrate email to the cloud securely and seamlessly. This holistic solution goes beyond basic compliance, safeguarding sensitive information from both accidental and malicious insiders while blocking email-borne threats. With industry-leading data loss prevention and email security integrated into a unified, easy-to-deploy platform, it provides enterprise-strength compliance and security controls for leading cloud email services such as Microsoft Exchange Online and Gmail for Business.

Enhance Data Loss Prevention for Email

Preventing data loss—whether accidental, negligent, or malicious—is crucial to the success of any information security program. Symantec DLP Cloud Service for Email ensures that you no longer have to worry about employees inadvertently exposing confidential emails and risking your company's reputation. This solution extends comprehensive, content-aware DLP capabilities to Office 365, Gmail, and Exchange, scanning outbound email traffic for sensitive content such as personally identifiable information (PII) and intellectual property.

The DLP Cloud Service for Email analyzes both message content and metadata context using the most advanced content detection capabilities available:

- **Exact Data Matching:** Detects data through fingerprinting or indexing structured data sources, such as databases and directory servers.
- **Indexed Document Matching:** Applies fingerprinting methods to identify data stored in unstructured documents, including Microsoft Office files, PDFs, and binary files like JPEG, CAD, and multimedia files.
- **Vector Machine Learning:** Protects intellectual property by detecting nuanced characteristics that are difficult to describe, such as those found in financial reports and source code.

As a result, the solution accurately identifies potential email data loss with minimal false positives, allowing you to focus on genuine incidents.

When sensitive content is detected, Symantec DLP Cloud Service for Email offers real-time protection. Automated response actions include notifying the user, blocking the message, or modifying it to enforce downstream encryption or quarantining.

Finally, the solution's Enforce Platform, a unified management console, enables you to create policies once and enforce them consistently across cloud, email, web, endpoint, and storage channels. From a single web-based console, you can author DLP policies, remediate incidents, and perform system administration, while quickly getting up and running with an intuitive policy builder and over 70 prebuilt templates. Additionally, the platform streamlines and automates incident response in high-traffic environments with robust workflow and remediation capabilities.

Protect Against Email-Based Attacks

The DLP Cloud Service for Email adds an essential security layer to cloud-based email services. Seamlessly integrating with Symantec ESS technology, it defends against targeted attacks, spear phishing, advanced malware, spam, and bulk mail. Advanced anti-malware and antispam capabilities block email-borne threats from reaching user mailboxes, while policy-based encryption safeguards sensitive communications with customers and partners.

A standout feature is Skeptic, Symantec's proprietary scanning technology. Skeptic examines multiple email attributes to detect anomalies, leveraging forward-thinking heuristics to predict and neutralize potential threats. This continuously learning system ensures proactive, immediate protection against evolving malicious content.

Secure Confidential Data in Motion

Symantec DLP Cloud Service for Email extends content-aware data loss prevention to Microsoft Exchange Online and Gmail for Business. With advanced detection technologies and built-in intelligence, it delivers accurate, real-time monitoring and analysis of data in motion, minimizing false positives and negatives, allowing organizations to focus on real incidents.

Automated response actions, such as message blocking, redirection, and encryption, prevent critical data loss in real time. Robust incident remediation options include customizable workflows, email notifications, and one-click responses to streamline incident management. An intuitive policy builder, prebuilt templates, and industry-specific solution packs simplify policy authoring, enabling organizations to write policies once and enforce them consistently across cloud and on-premise mailboxes.

Summary

Symantec DLP Cloud Service for Email provides a comprehensive solution to the security challenges of cloud-based email platforms like Microsoft Office 365 and Google Workspace. While these platforms offer significant business advantages, their built-in protections often fall short against advanced threats such as ransomware, phishing, and business email compromise. Symantec solutions bridge these gaps with robust data loss prevention, advanced threat detection, and seamless integration with Symantec ESS technology. Featuring tools like Skeptic scanning, real-time monitoring, intuitive policy authoring, and automated incident response, it ensures proactive protection against evolving cyber attacks while minimizing false positives. Backed by the world's largest civilian intelligence network and stringent SLA guarantees, Symantec solutions empower enterprises to embrace cloud email benefits without compromising security.

For more information, visit our website at: www.broadcom.com