netgovern™

POLICY-BASED EMAIL SECURITY WITH DATA LOSS PREVENTION, ENCRYPTION, AND AS/AV

THE BUSINESS CASE FOR EMAIL SECURITY

Today's technologies and threat landscape are evolving at a pace that can leave skilled IT security experts breathless. Given the critical nature of email, which is increasingly hosted in the cloud, it is clear that a comprehensive information governance strategy is required to keep an organization's information protected, in transit and at rest. Since threats typically involve internal actors, either negligent or malicious, and external actors wielding malware or phishing attacks, IT teams need tools that offer visibility and control into outbound and inbound email traffic in order to avoid breaches and regulatory sanctions.

NetGovern DLP, paired with NetGovern Encrypt, protect from data leaks and losses by preventing sensitive content from being sent or by automatically encrypting it for a safe transit. NetGovern Audit and Remediation safeguards from sophisticated phishing attacks that could lead to compromised accounts and leaked information. NetGovern AS/AV prevents spam, viruses, and graymail from reducing productivity. This quartet effectively contributes to preserving a company's information, reputation, and profit margin across the live flow of email.

PROTECTING SENSITIVE CONTENT WITH INFORMATION GOVERNANCE

Cross-functional collaboration is paramount for any IG initiative to be effective. Similarly, cross-functional teamwork is essential to the success of any DLP tool. Data owners from every department need to work with IT and Legal to determine which information is sensitive and how much protection it needs. Data owners, with Legal's help, need to provide the right keywords for the content-filtering engine to detect, and to determine the appropriate response for each scenario, so adequate policies can be created. Policy-based data loss prevention and encryption alleviate the risk of sharing information. The addition of performant AS/AV reduces the cost of information by keeping useless spam out of an organization's systems. It also protects data at rest by stopping malware before any damages can be done. Combined, these tools empower organizations to stay protected, productive, and compliant regardless of the level of dutifulness and training of their staff.

POLICY-BASED EMAIL DATA LOSS PREVENTION

Industries have similar and different content to protect, and compliance requirements to fulfill. NetGovern DLP prevents critical information from leaving organizations through outbound email with a potent content-filtering engine, applying criteria from policies. Policies can be customized from templates or built from scratch, so any particular industry or specific need can be covered. The policies can be applied organization-wide or granularly.

Payment card information, personal identifiable information, protected health information, and any other critical content within email and attachments are consistently and automatically identified. Policy enforcement is powered by comprehensive lexicons that address any organization's gateway compliance needs, with multi-language support and proximity searching. Advanced Keyword Syntax is supported for deep content analysis, which provides a way to search for advanced combinations of characters. Policy transgressions are countered by diverse advanced email dispositions such as secure route, moderation, automated response, redirection, and BCC to.

ANTI-PHISHING

Industry analysts now estimate that up to 70% of security breaches leading to data leaks and financial losses are initiated through phishing or spear phishing attacks. Since the average data breach in the U.S. represents a $3.86M loss, taking all means necessary to prevent them dramatically lowers the potential cost of sharing information

through email. In order to detect and disarm the new breed of phishing attacks, NetGovern created a new layer of security to perform a real-time inspection of every URL that comes into a corporate network and ensure that it is a valid address. Blocking is based on a real-time worldwide database of all bad domain addresses. This approach is the only proven way to detect and disarm phishing attacks across all devices to mitigate risks of fraud. If a phishing email is suspected to have found its way into a mailbox, it can be retracted along with all other occurrences, analyzed, and either deleted or reinjected into the system.

EMAIL MODERATION

The presence of certain keywords in the subject line, body, or attachment of an email could automatically send it to the quarantine. A moderator with appropriate access rights could then review it before deciding if it should be released or blocked. For example, the word ‘‘proposal’’ could be a keyword for the sales team and an email containing it would have to be reviewed and approved by the sales manager before being sent out.

POLICY-BASED EMAIL ENCRYPTION

When information is sensitive but still has to be sent by email, NetGovern Encrypt offers protection during transit. If both the sender and the recipient of the encrypted message are NetGovern Encrypt users, the process is totally transparent. When the recipient is not listed as an encryption client, an email notification is sent. The recipient simply has to click on the provided private web link to log into the NetGovern Encrypt web-based portal. From there, the encrypted message can be read and an answer can be safely sent.

NetGovern Encrypt renders secure certificate exchange between known organizations and full support for S/Mime, ensuring the integrity, security, and privacy of email communications. Encryption policies, allowing organizations to comply with industry-specific rules and regulations such as HIPAA/FIPPA, FINRA, and SOX, can be granularly applied to a group of users or an entire company. The presence of confidential information in the subject line or body of an email, or a specific recipient, are some of the parameters that can be set to automatically trigger encryption.

MULTI-LAYERED VIRUS PROTECTION AND SPAM BLOCKING

With NetGovern AS/AV, inbound content can also be monitored. The antivirus engine provides protection against blended threats with automatic engine updates, zero-hour virus protection, IP reputation technology, and robust group policies that raise end-user awareness about proper email handling and online behavior. Spam represents 45% of today’s email traffic and is a common cause, or email server bloat. With our proprietary NSBL technology, NetGovern AS/AV performs a single lookup of a spam-friendly name server, automatically detects, and proactively blocks all email from that name server. While most security solutions can be configured to reject or flag messages from an IP address or range of IP addresses, NetGovern finds and blocks spam where it originates.

NETGOVERN AS/AV MAIN FEATURES:
ANTI-MASKING ▸ Figure out who email senders really are
LIMITS ▸ Block or slow connections based on content
PROTOCOL FILTER ▸ Block email containing defined keywords in the header
RBL/DBL ▸ Verify if the email is from a domain block list
BLACK/WHITELISTING ▸ Allow users to manage block and allowed senders
GREY LISTING ▸ Allow email from listed senders that have retried as spammers to only send email once
SPF/RDNS ▸ Verify email has been sent from a valid server
AI RECOGNITION ▸ Assess if an email has similitude to other spam, is usually wanted, is offensive, or has a format to speed up or trick AS
ANTI-PHISHING TECHNOLOGY ▸ Prevent phishing attacks
BEHAVIOR ANALYSIS ENGINE ▸ Analyze email patterns

Visit **netgovern.com** to learn how we help organizations deploy Information Governance software that provides clear answers.

180 Peel Street, Suite 333 Montreal, QC Canada H3C 2G7 • Toll-free: USA & Canada: 1-866-497-0101 • International: +1 514-392-9220 • Email: info@netgovern.com

www.netgovern.com