netgovern™

DATA AUDIT & REMEDIATION

THE BUSINESS CASE FOR DATA AUDIT & REMEDIATION

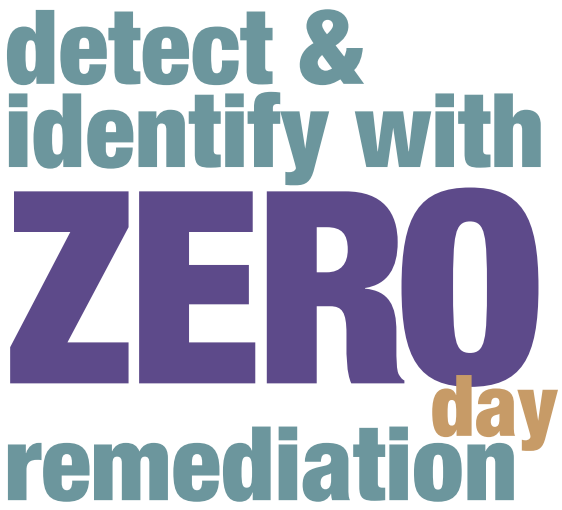
With the increasing popularity of cloud technologies, the use of more business applications than ever before, combined with on-premise storage and legacy file servers, the number of data locations in organizations are multiplying. When thinking about security and compliance, this poses a variety of challenges. Amongst these challenges, jumping from one location to another to audit an exponentially-growing amount of data is time-consuming which does not help with shrinking IT resources.

However, auditing unstructured data in all locations is necessary to locate and remediate sensitive information that tends to find its way everywhere. Noncompliance with regulations related to PII, PHI, and PCI can cost an organization a reputation and a lot of business. Securing intellectual property is also one of the business stakes making data auditing critical.

As laws and regulations adapt to the big data era and hackers get smarter, it is crucial for organizations to take a new approach to information governance to find and secure sensitive data. NetGovern Audit & Remediation allows data auditing in any repository through a single pane of glass, minimizing the resources needed to reduce risks.

REGULAR AUDITS FOR A STRONG INFORMATION GOVERANCE PROGRAM

Keeping track of what information is stored and its location is a crucial part of any information governance initiative. Regular audits drastically minimize the risks associated with sensitive information. Sensitive content can be identified, managed, and protected proportionally to its importance. The cost of storing information is reduced because redundant, outdated or obsolete data is identified and regularly disposed of. Dark data, which represent about 52% of information kept by organizations, can be leveraged and secured when it would have otherwise stayed in the dark potentially posing unknown security risks. This touches some of the most important facets of information governance including records and information management, InfoSec and protection, compliance, data governance, risk management, data storage and archiving, and privacy. Proactively undertaking these kinds of initiatives undoubtedly gives organizations a competitive advantage.



DATA PRIVACY AUDITS

Some data types, like personal identifiable information, are sensitive and require higher standards of protection. Although a good starting point to secure sensitive content is training and the creation of policies, it is not enough. When personal information finds its way to unsecured locations, there are always risks of unauthorized access. NetGovern Audit & Remediation sanitizes unsecure data repositories by providing the tools to remediate sensitive content. It can either be moved to appropriate locations or disposed of when outdated.

ALERTS FOR TIMELY REMEDIATION

Set and get alerts when sensitive data is stored in an inappropriate location, so the right action can be taken promptly. If an email containing a client's health record is saved in a PST file, the appropriate authority can be instantly alerted. This email could then be moved to safe storage or to quarantine for later review through the NetGovern web-based interface. The user who breached policy could then receive training, a warning, or a penalty, depending on the organization's policies regarding protected health information.

ADVANCED FILTERING AND SEARCH OPTIONS

NetGovern Audit & Remediation has an advanced set of filtering options that make it simple for reviewers to locate the precise type of information they are looking for. Reviewers can activate multiple search tabs to conduct different filtered searches within a single audit case. Searches can be performed by filter, keyword, message or user. Intricate results can be generated with number or pattern searches, as well as Natural Language Processing. Saving an audit scenario makes results immediately accessible in the portal. No need to re-run searches and wait. NetGovern provides continuous and up-to-date visibility into your unstructured data at all times.

FULL REVIEW WORKFLOWS

Fast and reliable audits are facilitated by teamwork. With NetGovern, audit managers, assigned by IT, create audits and define the scope of the search. Audit managers review the broad criteria of the search, tag all necessary documents and assign reviewers to the case. Reviewers identify, classify, and remediate sensitive data.

LIMITING VISIBILITY FOR PRIVACY

As members of organizations have different roles and responsibilities, it makes sense that not everyone would have access to the same data. With NetGovern, data locations have to be assigned to audit managers and reviewers according to need. Multiple cases with different scopes can be created at the same time and content with various levels of privacy can only be searched by people with the appropriate access rights.

SEARCH ALL CONTENT

NetGovern Audit & Remediation allows compliance, audit, and information security teams direct visibility into a document's contents and metadata wherever it resides, through the same interface. On-premise locations, hybrid clouds, or public clouds can be searched individually or at the same time. Indexing jobs can be performed regularly to ensure visibility into live data at all times. NetGovern Audit & Remediation is fully-integrated with NetGovern Archive for swift searches through archived emails and effortless remediation of potential threats. NetGovern's growing list of available connectors ensures searches are possible in a variety of repository types, and on live and archived email and files.

sanitize your data

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