AvePoint

Solution Brief

Compliance Solutions
for Operational Security

Internet based technology increases efficiency of communication, and produces countless advantages for the way individuals live and work. However, information placed on the Web or within internal systems, even with good-intent, can create operational and security gaps that could put assets at risk. Troop movement, dignitary visits, power plant schematics, bio hazards, diseases, border information, financial information, or an improper address or phone number may create security issues that could be taken advantage of by a third party. This type of information can create unintended consequences in perpetuating potential National Security threats and/or terrorist activities. The potential for inadvertent or unauthorized disclosure of sensitive information continues to grow. Using search engines and information compilation algorithms, a single user can aggregate, analyze, and construct new levels of understanding from unclassified sources.

AvePoint Compliance Solutions prevents the likelihood of security information leaks. Our Compliance Solutions provide the ability to scan content in real time or on a schedule based on out-of-the-box test definitions files that map to a wide range of US, International, and vertical specific requirements as well as legislation for Operational Security (OPSEC), Sensitive Security Information (SSI) and International Traffic in Arms (ITAR) requirements. Organizations can also tag sensitive data with either an embedded metatag within the document and/or with SharePoint metadata (if the content is managed within SharePoint) as well as indicate the sensitivity level of that content. Our Compliance Solutions provide unlimited extensibility for advanced metadata classification and schemas, including the ability to block, delete, quarantine, and move data to a protected location as well as protecting information in place through assignment of specific limited permissions based on the document classification.

Key Challenges

Detect

Automate a comprehensive assessment to identify content and framework OpSec issues

Track & Report

Reports, with accurate risk scores, can be distributed to compliance officers, administrators, and content owners for review and response

Respond & Resolve

Investigate, respond to and resolve compliance issues by prioritizing what to fix first, what to remove, and what issues may require no action at all

Prevent

Prevent compliance issues through real-time scanning, tagging and action

AvePoint Compliance Solutions for Operational Security & Secure Sensitive Information

Assess Existing Sites & Content

- Generate detailed, granular risk-level reports of content containing privacy and sensitive information with configurable scans for violations out of the box (e.g. OpSec, SSI, and ITAR) to locate offending content, informing organizations where the majority of non-compliant or content is stored
- Determine the nature of existing sensitive data by scanning against pre-configured or customizable test definitions files

Report on Compliance Violations

- Aggregate Security issues with additional "context" about the non-compliant content
  - What is the nature of the sensitive (or non-compliant) data
  - Where is it?
  - How old is it?
  - Who created it?
  - Who can access it and who has accessed it?
- Report on the age, update history, and user and content permissions as well as manage individual user or group profile security settings
- Track all user and group activity to determine origins of compliance infractions and users who have accessed this content

Respond & Resolve OpSec Violations

- Design an information architecture to address security requirements for all SharePoint and network content, including existing content and the content transferred in real time
- Determine appropriate actions to the at-risk sensitive information based on the security requirements of SharePoint or file-based information
- Tag and classify OpSec/SSI data to indicate the sensitivity level of that content
- Move, restrict permissions, or automatically notify appropriate team members to resolve compliance issues
- Strictly regulate user-generated content to prevent the creation or upload of sensitive, harmful content

Design a Comprehensive Information Security Risk Management Strategy

- Determine best practices and integrated full risk management life cycle approach for remediation of any identified security compliance issues
- Provide user generated or automated metadata (SharePoint or embedded metatags) to classify and protect sensitive content as it is added to a site
- Automatically process and protect sensitive information based on pre-defined rules to prevent exposure to users that should not have access. Delete, quarantine, encrypt, restrict access, and route the content to the appropriate location to comply with information governance policies
- Investigate usage patterns and monitor any information to assess the effectiveness of the privacy management strategy

This analysis identifies not only the existence of sensitive data, but also uncovers other key factors about the data, the SharePoint users, and the system itself, including the nature of the sensitive (or non-compliant data), where it's located, its age, who created it, and who's accessed it. With these findings, our team will then recommend a best practices approach to remediate any compliance issues, allowing the business to prioritize issues and implement a restructured compliance framework.

For organizations looking to move forward with an automated approach to manage risk in file shares, SharePoint sites, cloud platforms, websites, web applications, and social networks, AvePoint Compliance Solutions enable automated access and content controls to prevent, detect, respond to and subsequently resolve breaches. AvePoint helps to mitigate the likelihood of a catastrophic incident, and feeds back information that will lead to system hardening and improvements for the continuous life cycle that must make up a successful risk management program.

Next Steps

If you would like a solution demonstration or receive pricing information, please contact: ComplianceSolution@AvePoint.com or your AvePoint sales representative.

© AvePoint, Inc. All rights reserved. AvePoint and the AvePoint logo are trademarks of AvePoint, Inc. All other marks are trademarks of their respective owners.

Accessible content available upon request