AvePoint
Compliance
Guardian

Technical Overview

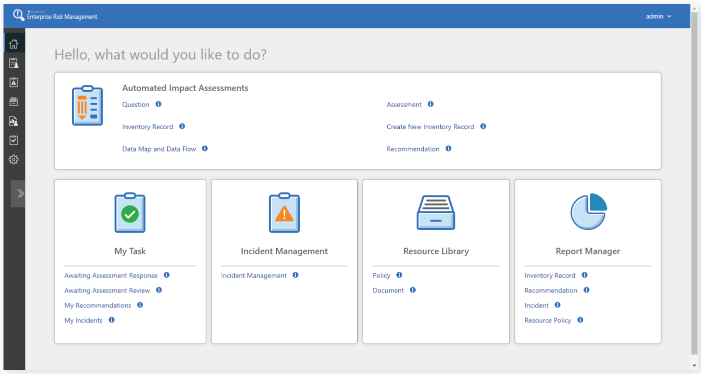
Enterprise Risk, Compliance, and Data Protection

Protect your unstructured and structured data—on-premises and in the cloud.

Supported Platforms

AvePoint Compliance Guardian protects the following enterprise information and collaboration gateways:

- SharePoint On-Premise
- Exchange On-Premise
- Office 365 – Exchange Online
- Office 365 – Exchange Public Folder
- Office 365 – SharePoint Online
- Office 365 – OneDrive for Business
- Office 365 – Yammer
- Office 365 – DLP Feeds
- Office 365 – Microsoft Teams
- Skype for Business
- Salesforce
- Dropbox
- Slack
- File Shares
- Databases
- ServiceNow
- Google Drive
- Gmail
- HTTP/HTTPS-based websites and web applications



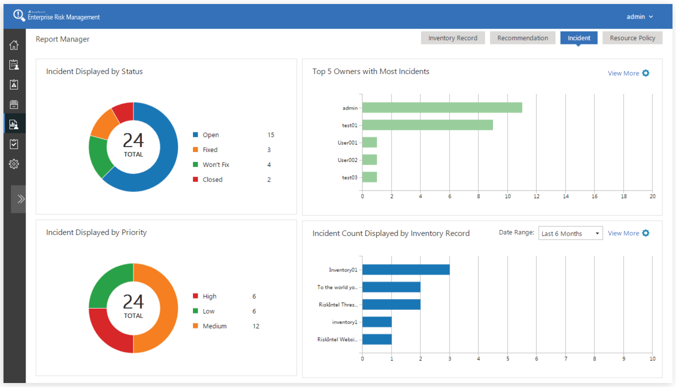
Carry out Repeatable Assessments via a Centralized Dashboard

Enterprise Risk Management (ERM)

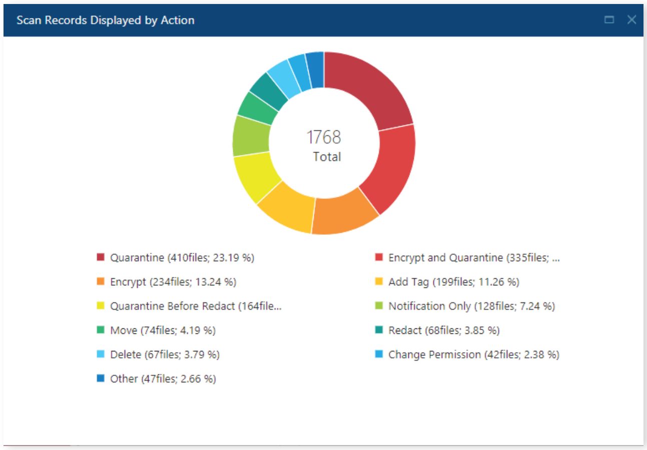
- **Inventory Manager** – Register a data inventory of your organization's information assets to understand what kind of sensitive data you hold and how the systems you use will collect and protect that data
- **Data Maps and Flows** – Visualize many-to-many associations between IT assets, data subjects, business processes, data handling characteristics, third parties, and jurisdictions via easily digestible data map and data flows.
- **Incident Management** – End-to-end incident management process to capture information, document an incident, prioritize it, determine what's been exposed, or which policies and regulatory requirements have been impacted
- **Privacy & Risk Assessment and Analysis** – Conduct automated Privacy, Risk, Security, and Data Protection Threshold and Impact Assessments, with configurable calculators for risk-based decisions and controls
- **Technical Controls** – Recommend and document appropriate Corrective and Preventive Action (CAPA) once any non-conformities or other undesirable situations are identified from assessments to ensure security and compliance
- **Resource Library** – A module designed to centrally manage policies and resource documents related to privacy and security policies – such as GDPR, HIPPA and FISMA – to build an accountable, repeatable process for governance, risk and compliance
- **ServiceNow Connection** – Organizations using ServiceNow can sync existing ServiceNow records into ERM as inventory records – or choose whether to sync all records or specific ones matching configured rules
- **Actionable Report** – Provide executive reports on Key Performance Indicators (KPIs), Key Control Indicators

(KCIs), or Key Risk Indicators (KRIs) to highlight areas in the organization that need to be addressed to reduce risk

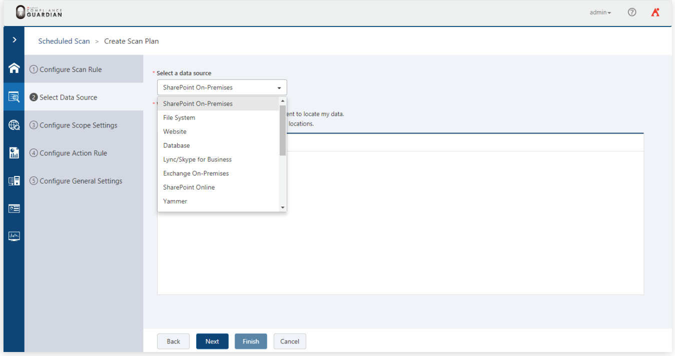
- **Risk Insights** – Run discovery as often as every 15 minutes to identify at-risk content based on common sensititve data definitions – including PII or classified data. Reports help quantify associated risk in heat maps and dashboards



Visualized Insights on Risk Level



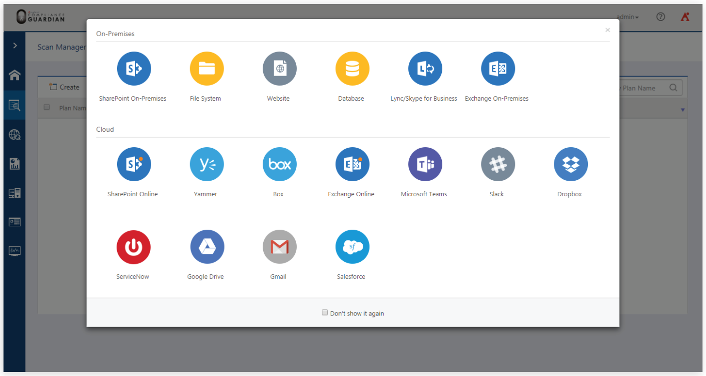
Scan Records Dashboard Displayed by Action



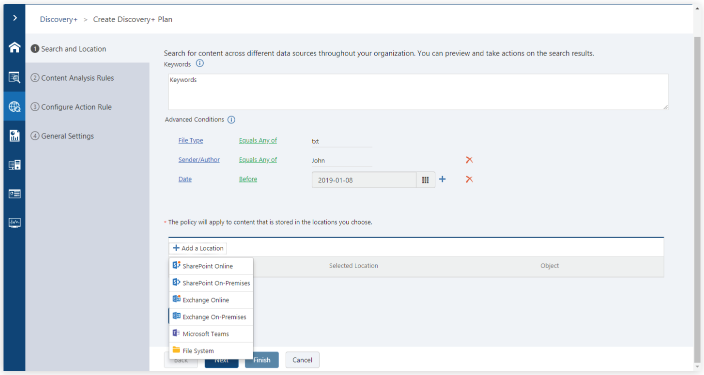
Risk Discovery on a Regular Basis

Data Validation and Classification (DVC)

- **Prerequisite Setup Wizard** – Quickly set up prerequisite configurations for applying licenses, the scan database, detection rules, data sources, connections and scan scopes.
- **Broad Enterprise Support** – Scan and crawl your enterprise information gateways, including file shares, SharePoint, Exchange, websites, cloud platforms, instant messaging tools, databases, and social networks, to ensure branding compliance as well as protection against privacy (PII/PHI), PCI, and security (SSI/ EU GDPR) violations.
- **Scheduled or Real-Time Scanning** – Scan content in real time or on a schedule against out-of-the-box or customized check files based on regulatory and statutory compliance—or your own policies that include plain text search terms, regular expressions, HTML elements, XML elements, and report criteria.
- **Discovery + Module** – Allow business users to search through content in emails, documents, and Teams conversations. Can be performed across multiple data sources at the same time and users can input keywords or define advanced conditions to search for content.



Comprehensive Scan for Multiple Information Gateways



Search for content across different data sources throughout your organization. You can preview and take actions on the search results.

File Type Equals Any of txt

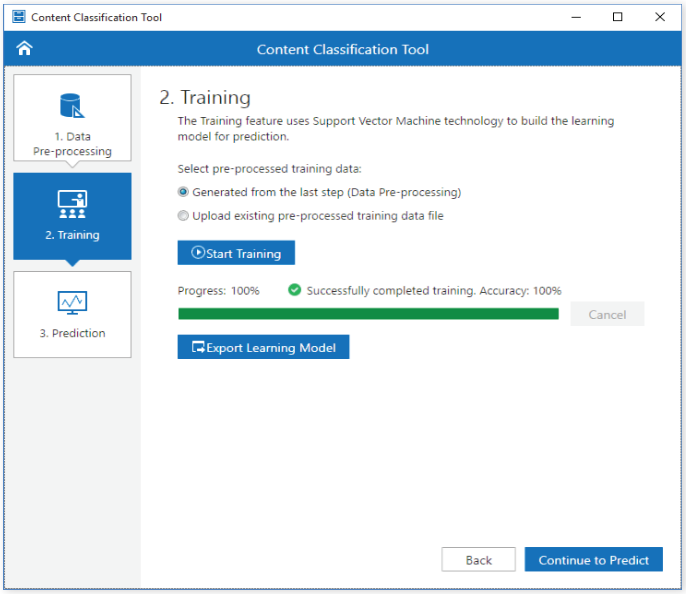
Sender/Author Equals Any of John

Date Before 2019-01-08

* The policy will apply to content that is stored in the locations you choose.

Discovery+

- **OCR Functionality** – Scan the content of pictures and embedded images with different contrasts, DPIs, font sizes, and word spacing to locate sensitive information.
- **Quick-Connect Framework** – Easily and speedily add new data sources.
- **Advanced Search Capability** – Quickly locate the specific datasets by integrating with our advanced search index while scanning data sources to meet customers' centralized policy-driven compliance and governance needs.
- **Any Type, Any Time** – Check Office files, PDFs, images, HTML/XML files, AutoCAD files, .zip files, Outlook PST files, Microsoft Access DB files and hundreds of file types for privacy and information security issues.
- **Machine Learning-Based Analysis** - Apply complex machine learning algorithms to generate an accurate risk check type to be used scanning against new content, improving and scaling complex analysis tasks across an organizational ecosystem without requiring the use of pre-defined rules.
- **File Analysis Report** – Interact with data at a lower level by filtering to gain insight from different angles.
- **Duplicate File Manager** – Take action against items on the report page to identify and remove duplicate files in SharePoint Online, SharePoint On-Premises and in File Systems.
- **SIEM Integration** – Feed scan results and information around sensitive events into Security Information and Event Management (SIEM) solutions provided by HP ArcSight, IBM QRadar and Splunk via syslog in Common Event Format (CEF) to access detailed alerting and tracking.
- **Sensitive Information Type Integration** – Leverage Microsoft 365 sensitive information types to create test suites that can be used to identify and classify sensitive items in SharePoint Online.
- **Built in Power BI Report Template for File Analysis** – Quickly analyze file architecture and properties in your file shares, SharePoint, and other data sources to gain more powerful, dynamic insights into your data, based on integrated Power BI reports—enabling you to identify and eliminate redundant, obsolete, and trival (ROT) data.
- **Content Classification** - Classify content with user-assisted or automated tagging via a Metadata Classification Engine.
- **Tag Your Way** - Tag or classify content using built-in properties, or assign custom tags that will help you sort, clean, or migrate data.
- **Metadata Consistency Checking** - Identify inconsistencies between document and system metadata, and synchronize the two to ensure metadata consistency across platforms.



2. Training

The Training feature uses Support Vector Machine technology to build the learning model for prediction.

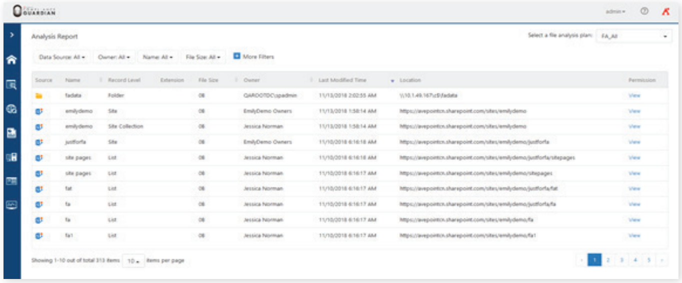
Select pre-processed training data:

● Generated from the last step (Data Pre-processing)

○ Upload existing pre-processed training data file

Progress: 100% ✓ Successfully completed training. Accuracy: 100%

Machine Learning-Based Analysis



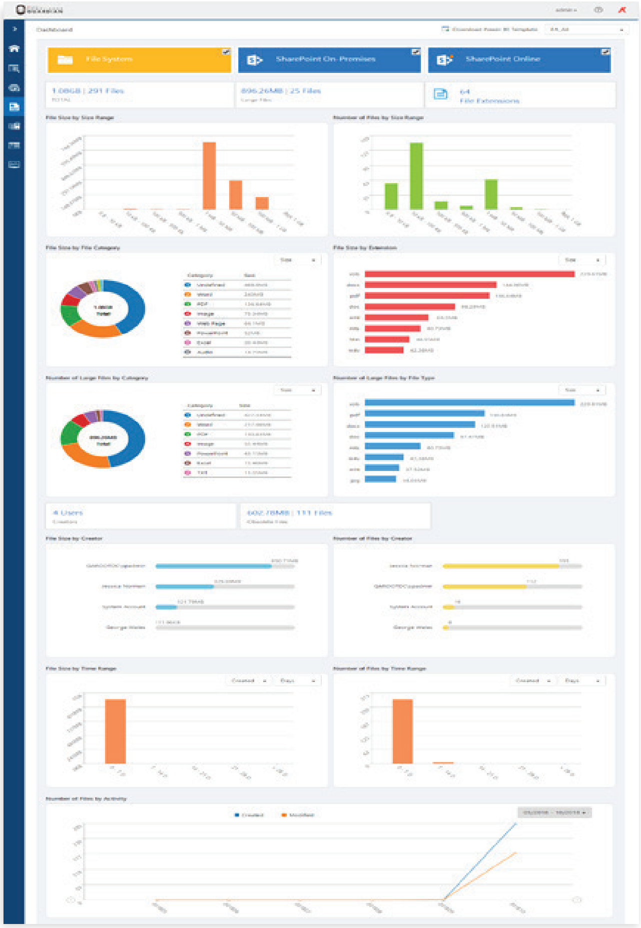
Analysis Report

Select a file analysis plan: FA_All

Source	Name	Record Level	Extension	File Size	Owner	Last Modified Time	Location	Permission
	fadata	Folder		0B	QAROOTDC\spadmin	11/13/2018 2:02:55 AM	\\10.1.49.167\c$\fadata	View
	emilydemo	Site		0B	EmilyDemo Owners	11/13/2018 1:58:14 AM	https://avepointcn.sharepoint.com/sites/emilydemo	View
	emilydemo	Site Collection		0B	Jessica Norman	11/13/2018 1:58:14 AM	https://avepointcn.sharepoint.com/sites/emilydemo	View
	justforfa	Site		0B	EmilyDemo Owners	11/10/2018 6:16:18 AM	https://avepointcn.sharepoint.com/sites/emilydemo/justforfa	View
	site pages	List		0B	Jessica Norman	11/10/2018 6:16:18 AM	https://avepointcn.sharepoint.com/sites/emilydemo/justforfa/sitepages	View
	site pages	List		0B	Jessica Norman	11/10/2018 6:16:17 AM	https://avepointcn.sharepoint.com/sites/emilydemo/sitepages	View
	fat	List		0B	Jessica Norman	11/10/2018 6:16:17 AM	https://avepointcn.sharepoint.com/sites/emilydemo/justforfa/fat	View
	fa	List		0B	Jessica Norman	11/10/2018 6:16:17 AM	https://avepointcn.sharepoint.com/sites/emilydemo/justforfa/fa	View
	fa	List		0B	Jessica Norman	11/10/2018 6:16:17 AM	https://avepointcn.sharepoint.com/sites/emilydemo/fa	View
	fa1	List		0B	Jessica Norman	11/10/2018 6:16:17 AM	https://avepointcn.sharepoint.com/sites/emilydemo/fa1	View

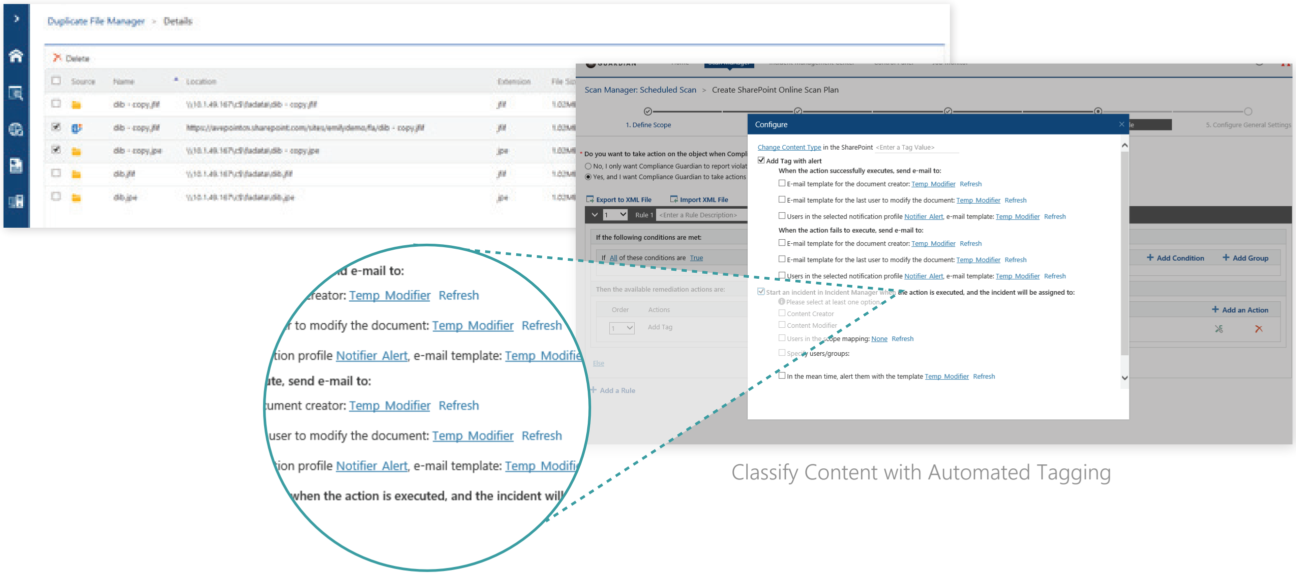
Showing 1-10 out of total 313 items 10 items per page

File Analysis Report



File Analysis Dashboard

Duplicate File Manager-Detailed page



Duplicate File Manager > Details

Delete

	Source	Name	Location	Extension	File Size
☐		dib - copy.jfif	\\10.1.49.167\c$\fadata\dib - copy.jfif	.jfif	1.02MB
☑		dib - copy.jfif	https://avepointos.sharepoint.com/sites/emilydemo/fa/dib - copy.jfif	.jfif	1.02MB
☑		dib - copy.jpe	\\10.1.49.167\c$\fadata\dib - copy.jpe	.jpe	1.02MB
☐		dib.jfif	\\10.1.49.167\c$\fadata\dib.jfif	.jfif	1.02MB
☐		dib.jpe	\\10.1.49.167\c$\fadata\dib.jpe	.jpe	1.02MB

Scan Manager: Scheduled Scan > Create SharePoint Online Scan Plan

1. Define Scope
5. Configure General Settings

* Do you want to take action on the object when Compli
○ No, I only want Compliance Guardian to report violat
● Yes, and I want Compliance Guardian to take actions

Export to XML File Import XML File

1 Rule 1 <Enter a Rule Description>

If the following conditions are met:

If All of these conditions are True

Then the available remediation actions are:

Order	Actions
1	Add Tag

Else

+ Add a Rule

+ Add Condition + Add Group

+ Add an Action

Configure

Change Content Type in the SharePoint <Enter a Tag Value>

☑ Add Tag with alert

When the action successfully executes, send e-mail to:

☐ E-mail template for the document creator: Temp Modifier Refresh

☐ E-mail template for the last user to modify the document: Temp Modifier Refresh

☐ Users in the selected notification profile Notifier Alert, e-mail template: Temp Modifier Refresh

When the action fails to execute, send e-mail to:

☐ E-mail template for the document creator: Temp Modifier Refresh

☐ E-mail template for the last user to modify the document: Temp Modifier Refresh

☐ Users in the selected notification profile Notifier Alert, e-mail template: Temp Modifier Refresh

☑ Start an incident in Incident Manager when the action is executed, and the incident will be assigned to:

Please select at least one option.

☐ Content Creator

☐ Content Modifier

☐ Users in the scope mapping: None Refresh

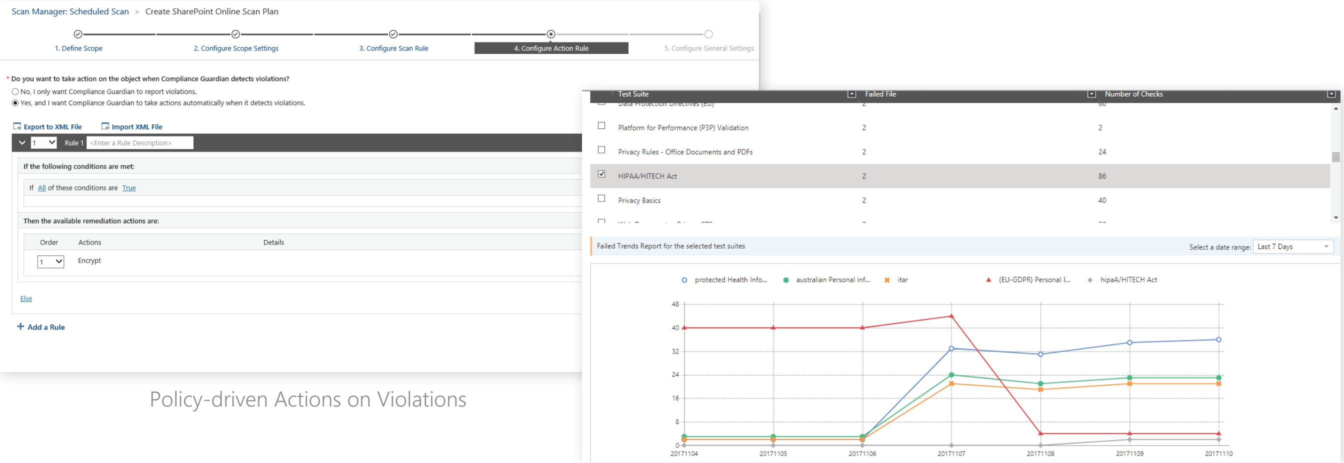
☐ Specify users/groups:

☐ In the mean time, alert them with the template Temp Modifier Refresh

Classify Content with Automated Tagging

Data Validation, Classification and Protection

- **Actions on Risk-Defined Files** - Based on content classification, or risk level and score, act to delete, quarantine, encrypt, redact, anonymize, export, change permissions or route the content to the appropriate location to comply with information governance policies such as "Right of Access" declaration in EU GDPR
- **Cryptovirus/Ransomware Detection** - Detect cryptoviruses and ransomware attacks in data sources, and review insights via a dashboard that displays potential threats, to ensure data security.
- **Records Management for Instant Message Conversations** - Archive Skype for Business conversations, initiators, and participant information with retention policies to local storage, including the ability to export specified conversations to Concordance, Electronic Discovery Reference Model (EDRM), or HTML files for further legal review
- **Trend Reports** - Track historical risk analyses on your corporate data with trend reports to accurately measure compliance improvements
- **Auditing Reports** - Analyze audit results to calculate a refined risk list by integrating with Box, Dropbox API, or aggregating audit and security data directly from AvePoint's DocAve Software Platform to report on SharePoint and Office 365 content age, number of times accessed and by which users, and security settings
- **Secure Externally Shared Files** – Prevent the sharing of content to external users across multiple Cloud gateways including Box, Dropbox, Slack, SharePoint Online, and OneDrive for Business by performing scheduled or real-time scans to check existing data and monitor newly created or modified files, triggering aggregated risk score once an exposed file is identified



Scan Manager: Scheduled Scan > Create SharePoint Online Scan Plan

1. Define Scope
2. Configure Scope Settings
3. Configure Scan Rule
4. Configure Action Rule
5. Configure General Settings

* Do you want to take action on the object when Compliance Guardian detects violations?

○ No, I only want Compliance Guardian to report violations.

● Yes, and I want Compliance Guardian to take actions automatically when it detects violations.

Export to XML File Import XML File

1 Rule 1 <Enter a Rule Description>

If the following conditions are met:

If All of these conditions are True

Then the available remediation actions are:

Order	Actions	Details
1	Encrypt	

Else

+ Add a Rule

Policy-driven Actions on Violations

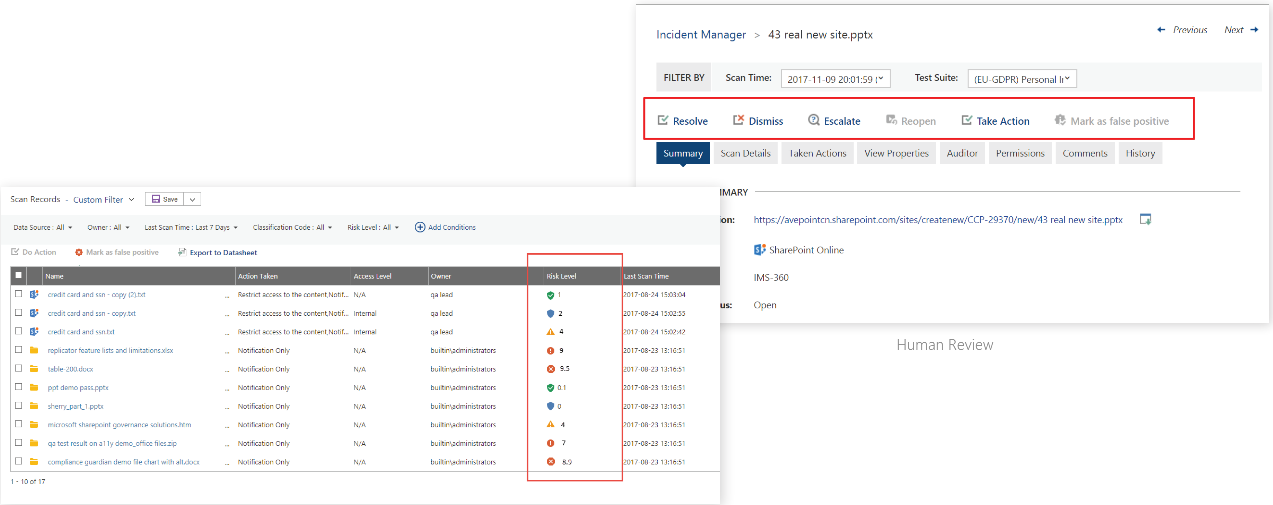
	Test Suite	Failed File	Number of Checks
☐	Platform for Performance (P3P) Validation	2	2
☐	Privacy Rules - Office Documents and PDFs	2	24
☑	HIPAA/HITECH Act	2	86
☐	Privacy Basics	2	40

Failed Trends Report for the selected test suites

Select a date range: Last 7 Days

Compliance Violation Trend Reports

- **Compliance Report Dashboard** - Present scan and risk assessments in graphical dashboard displays, or automatically input all compliance risk data and reports into Power-BI report templates, HTML or Microsoft Excel files for download and reference
- **Compliance Report Formats** - Provide a variety of easily consumable compliance reports – including incident status, incident priority, scan results, top 10 assignees, top 10 incident creators, violation, risk trend, scan history, top active users-exposure, shared files trend by time range, classification code and violations by exposures – to satisfy diverse business demands
- **Error Highlight Report** - Highlight the areas that violate the specified compliance standards or guidelines in files, instant message conversations, or web pages to help organizations quickly address non-compliant information
- **Risk Score and Risk Levels**- Sophisticated logic presents risk scores and risk levels within content and scan results using out-of-the-box risk calculation formulas
- **Incident Prioritization** – Assign priority to incidents automatically or manually to ensure the most critical violations are addressed as soon as possible
- **Bulk Incidents** – Review the whole result as an incident to reduce work redundancy
- **Centralized Dashboard with Decentralized Workflow** - Security, Privacy, and Compliance Officers can maintain an organization-wide view into compliance risk, but optionally use Compliance Guardian's delegated and security-trimmed workflow capabilities to assign appropriate business or content owners to address potential violations. The system maintains a full audit trail for issue resolutions or escalations, allowing the security operations center to focus on high risk issues and business owners to resolve low risk issues
- **Incorporate Human Review** - Involve human review to take resolutions, including resolve, dismiss, escalate and reopen, enabling flexible remediation and reducing false positives
- **Human Review Tracking** - Track human auditing history, including which filecheck status is changed and by whom, and export to Microsoft Excel files for distribution
- **System Overriding** - Instruct the system to not test or review the file again after its check status has changed by human review unless the test suite, rules, or file itself has changed, allowing you to override the system
- **Incident Tracking and Management** – Easily access relevant information on discovered incidents to ensure they are reviewed, tracked, and acted on in accordance with your organization's information governance policies
- **Email Notification** - Generate actionable email notifications upon identification of sensitive or non-compliant content for end users or compliance teams to take decisive actiones
- **AvePoint Perimeter Integration** – Perimeter's 'Live Preview' integration lets business users directly and securely open files in an IMS report using the URL link provided



Scan Time: 2017-11-09 20:01:59 (

Test Suite: (EU-GDPR) Personal In

ion: https://avepointcn.sharepoint.com/sites/createnew/CCP-29370/new/43 real new site.pptx

SharePoint Online

IMS-360

us: Open

Human Review

Data Source : All   Owner : All   Last Scan Time : Last 7 Days   Classification Code : All   Risk Level : All

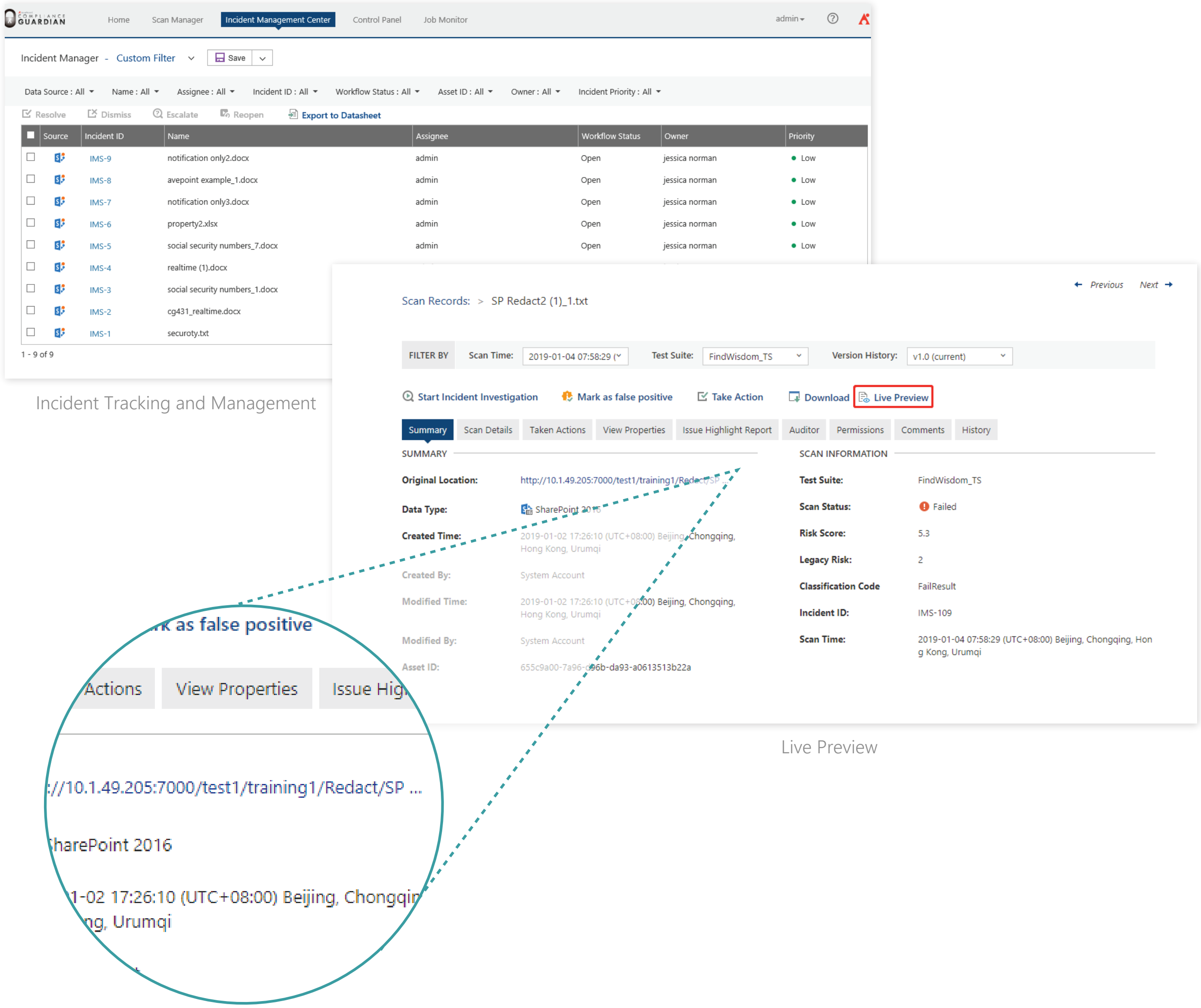
☐	Name	Action Taken	Access Level	Owner	Risk Level	Last Scan Time
☐	credit card and ssn - copy (2).txt ...	Restrict access to the content,Notif...	N/A	qa lead	1	2017-08-24 15:03:04
☐	credit card and ssn - copy.txt ...	Restrict access to the content,Notif...	Internal	qa lead	2	2017-08-24 15:02:55
☐	credit card and ssn.txt ...	Restrict access to the content,Notif...	Internal	qa lead	4	2017-08-24 15:02:42
☐	replicator feature lists and limitations.xlsx ...	Notification Only	N/A	builtin\administrators	9	2017-08-23 13:16:51
☐	table-200.docx ...	Notification Only	N/A	builtin\administrators	9.5	2017-08-23 13:16:51
☐	ppt demo pass.pptx ...	Notification Only	N/A	builtin\administrators	0.1	2017-08-23 13:16:51
☐	sherry_part_1.pptx ...	Notification Only	N/A	builtin\administrators	0	2017-08-23 13:16:51
☐	microsoft sharepoint governance solutions.htm ...	Notification Only	N/A	builtin\administrators	4	2017-08-23 13:16:51
☐	qa test result on a11y demo_office files.zip ...	Notification Only	N/A	builtin\administrators	7	2017-08-23 13:16:51
☐	compliance guardian demo file chart with alt.docx ...	Notification Only	N/A	builtin\administrators	8.9	2017-08-23 13:16:51

1 - 10 of 17

Risk Score and Risk Level in Scan Record

Perimeter

- **AvePoint Perimeter Integration** – Perimeter's 'Live Preview' integration lets business users directly and securely open files in an IMS report using the URL link provided
- **Secure Sharing** – Securely share content with external parties directly from on-premises or cloud libraries
- **Very Insightful** – Offers insights and monitoring on all externally shared content—for both internal users who share content and external users who access it—via dashboard reports
- **MyDrive & Thrive** – Upload files directly to Perimeter's "MyDrive" to share with external parties for a secure, on-prem alternative to cloud-based file sharing like an on-prem Dropbox



Source	Incident ID	Name	Assignee	Workflow Status	Owner	Priority
	IMS-9	notification only2.docx	admin	Open	jessica norman	● Low
	IMS-8	avepoint example_1.docx	admin	Open	jessica norman	● Low
	IMS-7	notification only3.docx	admin	Open	jessica norman	● Low
	IMS-6	property2.xlsx	admin	Open	jessica norman	● Low
	IMS-5	social security numbers_7.docx	admin	Open	jessica norman	● Low
	IMS-4	realtime (1).docx				
	IMS-3	social security numbers_1.docx				
	IMS-2	cg431_realtime.docx				
	IMS-1	securoty.txt				

1 - 9 of 9

Incident Tracking and Management

Scan Records: > SP Redact2 (1)_1.txt

FILTER BY Scan Time: 2019-01-04 07:58:29 (Test Suite: FindWisdom_TS Version History: v1.0 (current)

SUMMARY

Original Location: http://10.1.49.205:7000/test1/training1/Redact/SP ...

Data Type: SharePoint 2016

Created Time: 2019-01-02 17:26:10 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Created By: System Account

Modified Time: 2019-01-02 17:26:10 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Modified By: System Account

Asset ID: 655c9a00-7a96-d96b-da93-a0613513b22a

SCAN INFORMATION

Test Suite: FindWisdom_TS

Scan Status: Failed

Risk Score: 5.3

Legacy Risk: 2

Classification Code FailResult

Incident ID: IMS-109

Scan Time: 2019-01-04 07:58:29 (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

rk as false positive
Actions
View Properties
Issue Hig
://10.1.49.205:7000/test1/training1/Redact/SP ...
harePoint 2016
1-02 17:26:10 (UTC+08:00) Beijing, Chongqin
ng, Urumqi

Live Preview

For a comprehensive list of new features in this release, please review the release notes on your AvePoint Account Portal.

How to Buy AvePoint Products

Contact: 201.793.1111 | Sales@AvePoint.com
AvePoint Global Headquarters | 525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310

Start your free trial today:
www.avepoint.com/download

Accessible content available upon request