AVEPOINT COMPLIANCE GUARDIAN

Unified Risk Management. Mitigate risk from the moment data is created through its entire lifecycle, proactively monitoring and neutralizing violations of privacy, security, and compliance.

SUPPORTED PLATFORMS

SUPPORTED TECHNOLOGIES

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

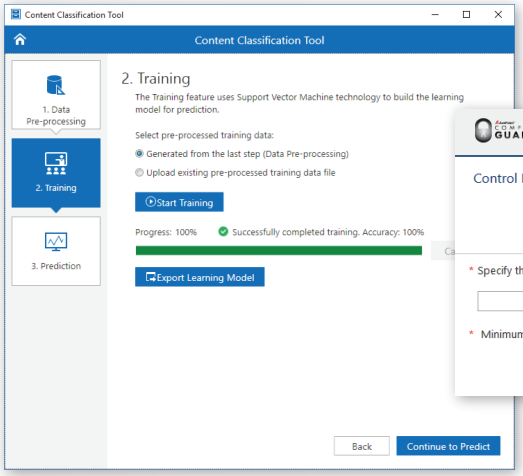
- SharePoint On-Premise
- Exchange On-Premise
- Office 365 – Exchange Online
- Office 365 – SharePoint Online
- Office 365 – OneDrive for Business
- Office 365 – Yammer
- Office 365 – DLP Feeds
- Skype for Business
- Box
- Dropbox
- Slack
- File Shares
- Databases
- HTTP/HTTPS-based websites and web applications

SUPPORTED FILE TYPES

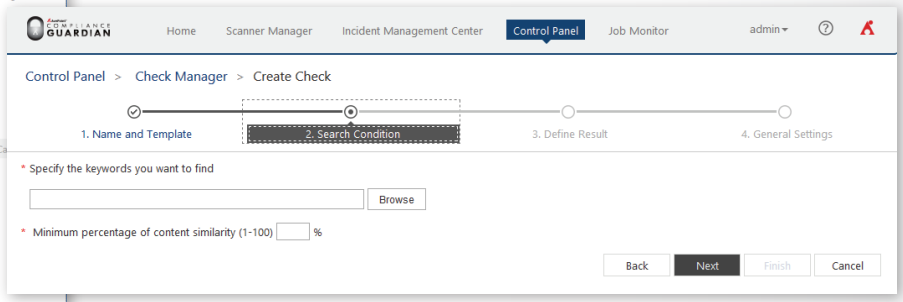
- **Support File Types** - Office files, PDFs, HTML/XML files, AutoCAD files, .zip files, and hundreds of file types for privacy and information security issues

DATA DISCOVERY

- **Comprehensive Scan for Multiple Information Gateways** - 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
- **Extensibility via the Compliance Guardian API** - Scan multiple content sources utilizing the Compliance Guardian API to integrate enterprise-wide content compliance efforts
- **Machine Learning-Based Analysis** - Apply complex machine learning algorithms to generate an accurate 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



Machine Learning Training



Machine Learning Check

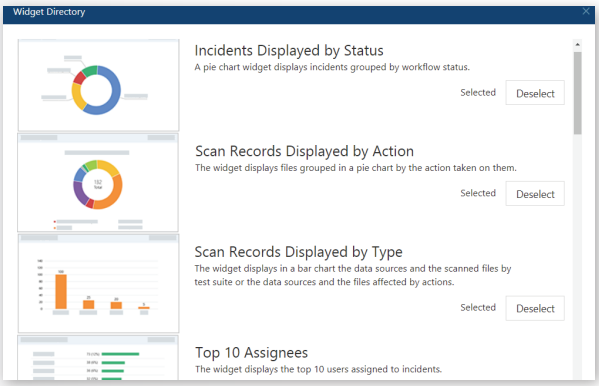
- **SIEM Integration** - Feed scan results and information around sensitive events into Security Information and Event Management (SIEM) solutions provided by HP ArcSight, IBM QRadar and Splunk via syslog in Common Event Format (CEF) to access detailed alerting and tracking
- **Built-in Power BI Report Template for File Analysis** - Quickly analyze file architecture and properties in your file shares and SharePoint to gain more powerful and dynamic insights about your data based on integrated Power BI reports – enabling you to identify and eliminate redundant, obsolete, and trival (ROT) data

DATA CLASSIFICATION

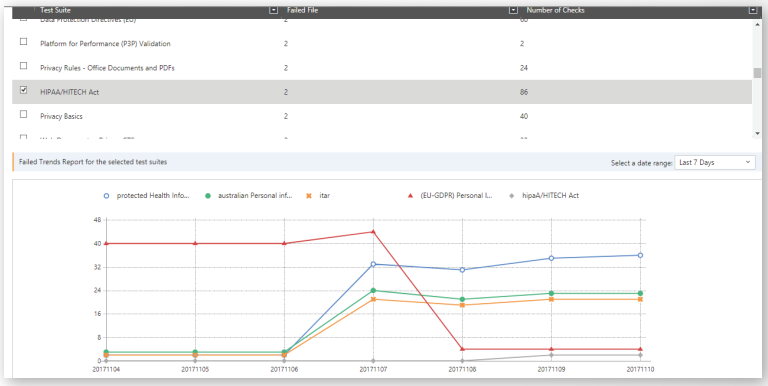
- **Content Classification** - Classify content with user-assisted or automated tagging via a Metadata Classification Engine
- **Metadata Consistency Checking** - Identify inconsistencies between document and system metadata, and synchronize the two to ensure metadata consistency across platforms

DATA LOSS PREVENTION (DLP)

- **Actions on Risk-defined Files** - Based on content classification, delete, quarantine, encrypt, redact, anonymize, pseudonymze, or route the content to the appropriate location to comply with information governance policies
- **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



Available Dashboards

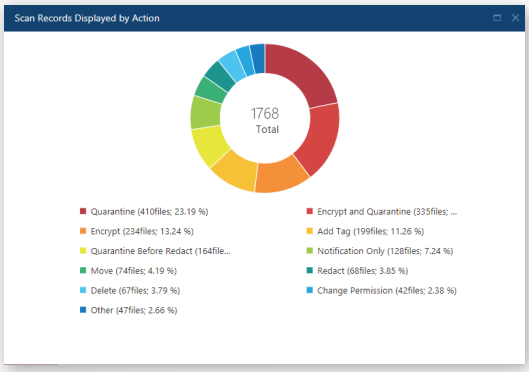


Compliance Violation Trend Reports

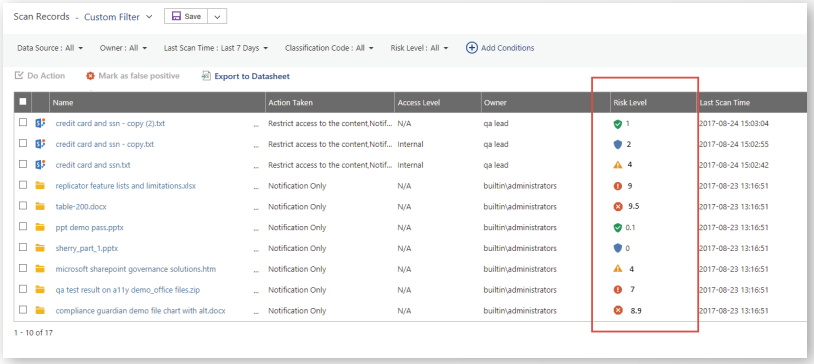
- **Trend Reports** - Track historical risk analyses on your corporate data with trend reports to accurately measure compliance improvements
- **Integration with DocAve SharePoint Auditing Reports** - Analyze audit results to calculate a refined risk list by aggregating audit and security data from AvePoint's DocAve Software Platform, reporting on 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

INCIDENT MANAGEMENT

- **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, 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
- **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



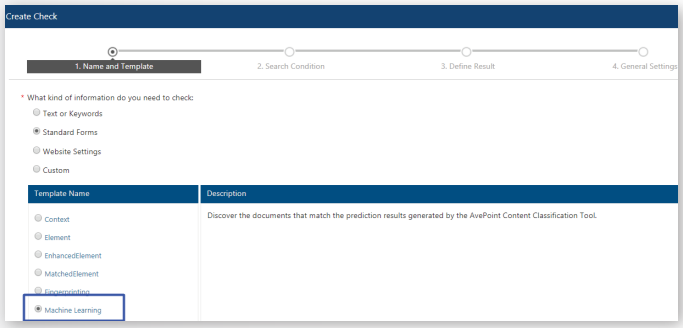
Scan Records Dashboard Displayed by Action



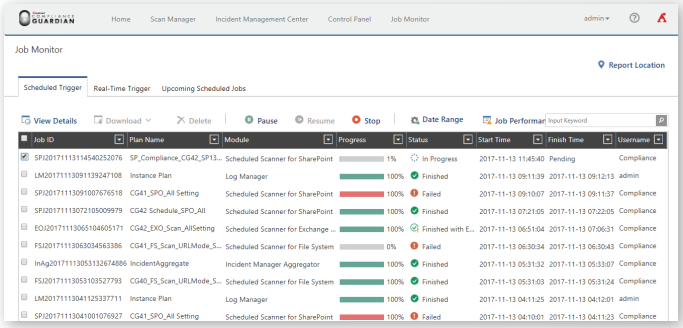
Risk Score and Risk Level in Scan Record

- **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 files' check 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 action



Human Review



Job Monitor

ADDITIONAL FEATURES

- **Deeper Insight into Compliance Guardian Environment** - Detect software and hardware configurations, such as free disk space and Compliance Guardian Agent permissions, with a self-checker to automatically troubleshoot system errors that impact platform performance

How to Buy AvePoint Compliance Guardian

Call: 201.793.1111
E-mail: Sales@AvePoint.com

AvePoint Global Headquarters
525 Washington Blvd. Suite 1400
Jersey City, NJ 07310

Join the conversation at **www.avepoint.com/community**

Accessible content available upon request.