AVRIO
SOFTWARE

Digital File Compliance

Introduction

Digital content creation is exploding. According to some estimates[1], we are creating as much as 2.5 quintillion (10^{18}) bytes of data per day, with 90 percent of the data in the world generated in the last two years alone. This staggering quantity of data includes data in dramatically different formats:

- Data can be structured (like databases), semi-structured (like XML or JSON documents), or unstructured (like this whitepaper).
- Data can be searchable (like Office documents), or unsearchable (like photos and videos, or a scanned PDF).
- Data can contain explicit words and phrases, or fall into predictable data patterns (like social security numbers, or an IP address).

It's also important to note that every company's set of data is different. There is no magic wand, or "one size fits all" when it comes to sifting through the vast historical and exponentially growing archive of content that most companies maintain. Moreover, companies are slowly coming to grips with the reality that they don't even know what content they have – especially in the realm of corporate files. This lack of insight causes a measurable and material increase to risk: it is impossible to purposefully and intentionally protect unknown information. This situation requires additional exploration, as well as a toolset designed to mitigate these risks.

Threats and Risks

There are a number of overlapping factors that together increase the risk landscape related to corporate file management:

- **File Storage Services.** There has been a recent explosion of new file storage services, including authorized content storage and collaboration services such as Google Drive, or Slack, or Microsoft SharePoint/OneDrive/OneNote, as well as "Shadow IT" storage services such as DropBox or iCloud.
- **Cloud Migration.** Cloud restructuring puts files in motion and changes security posture, sometimes in very unexpected and undesirable ways.
- **Complexity.** The increase in complicated new technologies such as cloud services, blockchain, machine learning, and IOT has created risks to the enterprise that are only slowly beginning to be understood and addressed.
- **Ransomware.** The leaking of an NSA SMB rootkit in 2017 that included a number of zero-day SMB hacks has seen a dramatic increase in the prevalence of devastating ransomware attacks.
- **Privacy Regulations.** Increasing regulations both public and private across multiple industries has raised the bar on privacy compliance, as well as the risks and costs associated with non-compliance.

[1] Marr, Bernard. "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read." https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read. 05/21/2018, retrieved 06/15/2020.

Costs

The potential costs associated with a failure to safeguard company data can be devastating, and are not limited to regulatory fines for accidental data exposure.

- **Data Exposure.** Confidential data such as company financial information or intellectual property can be exposed either accidentally or through willful exfiltration, creating a serious market disadvantage.
- **Reputational Damage.** Companies can suffer loss of public trust, which in some cases can destroy a company's business model.
- **Rework.** According to Microsoft, an average of just 0.45% of files are opened by someone who is not the original author. The cost of rework and loss of value is hard to quantify, but likely enormous.
- **System Availability.** Ransomware attacks can completely shut down a business, sometimes for days or weeks.
- **Regulatory Action.** Last but not least, fines and potentially even jail time may await companies and executives who fail to comply with regulatory standards.

The Consequences Of Getting It Wrong

- Target estimates the cost of its 2003 data breach at $202 million.
- Maersk estimates the cost of its 207 cyberattack at $300 million.
- Yahoo's compromise of three billion user accounts in 2013-2014 shaved $350 million off its sale price.
- Equifax reports their 2017 data breach cost $1.4 billion, plus legal fees.

Legal Backdrop

A number of legal standards have evolved that specifically address the twin and overlapping. requirements of data confidentiality and customer privacy. The fines and penalties associated with these standards are becoming increasingly worrisome as caselaw and precedence evolves. Here are a few examples of the penalties associated with some of these standards:

> **GDPR.** The European General Data Privacy Regulation protects personally identifiable information (PII) of European citizens. Violators may be fined up to €20 million, or up to 4% of the annual worldwide revenue of the preceding financial year, *whichever is greater*.
>
> **HIPAA.** The Health Insurance Portability and Accountability Act protects patient health records. The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year. Violations may also carry criminal charges that can result in jail time.
>
> **CCPA.** The California Consumer Privacy Act applies to any business that collects data from California resident, regardless of where the business is headquartered. Fines for CCPA violations range from $2,500 to $7,500 per record, depending on intent.
>
> **SOX.** The Sarbanes-Oxley Act applies to all publicly traded companies in the United States, and requires the establishment of internal controls and procedures to track (among other things) information access. SOX violations carry penalties of $1-5 million, depending on intent, and can result in company officer jail time.

AVRIO
SOFTWARE

Introducing SIFT™

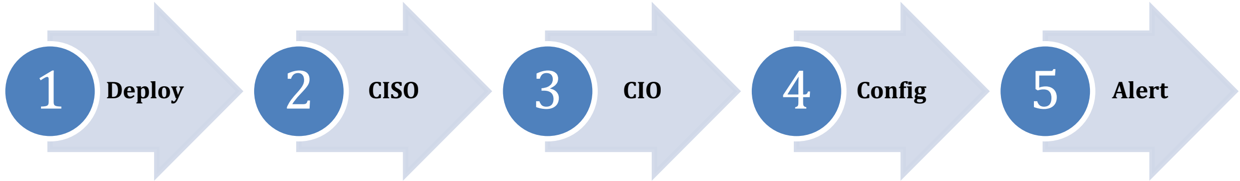
SIFT™ is a next-generation, regulatory compliance and monitoring toolset that discovers, tags, and protects sensitive files across the network:

- **Discover.** SIFT™ uses patented techniques to scan and analyze files across your network, both on premises and in the cloud. SIFT™ offers out-of-the-box support for a wide range of file types, including most Microsoft Office and Adobe documents, as well as picture, video, and scanned PDF documents.
- **Tag.** SIFT™ stamps files with useful metadata, including full support for both static and pattern-based keywords, like SSNs or credit card numbers, as well as image identification based on machine learning models.
- **Protect.** SIFT™ continuous monitoring supports fast identification of data spills, and can provide automated file quarantine for enclave content violations.

Path To Compliance

SIFT™ provides a clear and straightforward path to full regulatory and privacy compliance:

1. **Deploy.** Deploy SIFT™ onto the company network, either on premises or in the cloud.
2. **CISO.** Work with company CISO's staff to determine any regulatory compliance requirements.
3. **CIO.** Work to company CIO's staff to understand the company's data, and identify file repositories on premises or in the cloud.
4. **Configure.** Configure SIFT™ with rulesets and scanning jobs, and to quarantine and/or restructure files in accordance with compliance requirements.
5. **Alert.** Configure company SIEM, or visualization tools, to track and alert on compliance issues.



1 Deploy
2 CISO
3 CIO
4 Config
5 Alert

Value

Deploying SIFT™ in your company's environment brings clear benefits to your information compliance program, especially in advance of a cloud migration effort, including:

- Avoid costly fines and embarrassment by safeguarding your valuable data
- Protect sensitive company information, and retain your market position
- Provide automated response and reduce exposure time for spills and breaches
- Extract full value from your file collateral, by making all documents searchable
- Avoid cloud vendor-lock with an easy button for cloud restructuring
- Inoculate against ransomware by moving files off file shares and into cloud-native storage

Contact Us

Visit our website at www.avriosoft.io to learn more about SIFT™ or email info@avriosoft.io to schedule a product demo.

SIFT