How Getvisibility Can Help You Fight Insider Threats

Products

- Getvisibility Focus
- Getvisibility Synergy

Are Insider Threats a problem in your organization?

An insider threat is a threat to an organization that originates from malicious insiders such as employees, former employees, contractors, third-party vendors, or business partners, who have inside information about cybersecurity practices, sensitive data, and computer systems, and possible privileged access.

Interestingly, according to insider threat statistics from a Ponemon Institute study, the majority of insider threat incidents are caused by employee and contractor negligence. The same Ponemon study showed that accidental insider threat cost roughly $283,000 per incident, but due to their frequency, these incidents totalled up to $3.8 million per year.

(https://www.observeit.com/blog/six-insider-threat-statistics-that-prove-the-need-for-mandatory-insider-threat-training/)

Getvisibility can detect insider threats relating to documents and emails before any data leakage occurs. This is possible via the two components of the platform which are Getvisibility Focus and Getvisibility Synergy.

Overview

These components allow analysis and monitoring of documents and emails in the two crucial phases of their lifecycle. Firstly, end users can manually classify documents and emails on creation with the help of the Getvisibility AI agent that can provide suggestions and help. This classification can be checked and amended, or flagged, if needed by Getvisibility's machine learning engine.

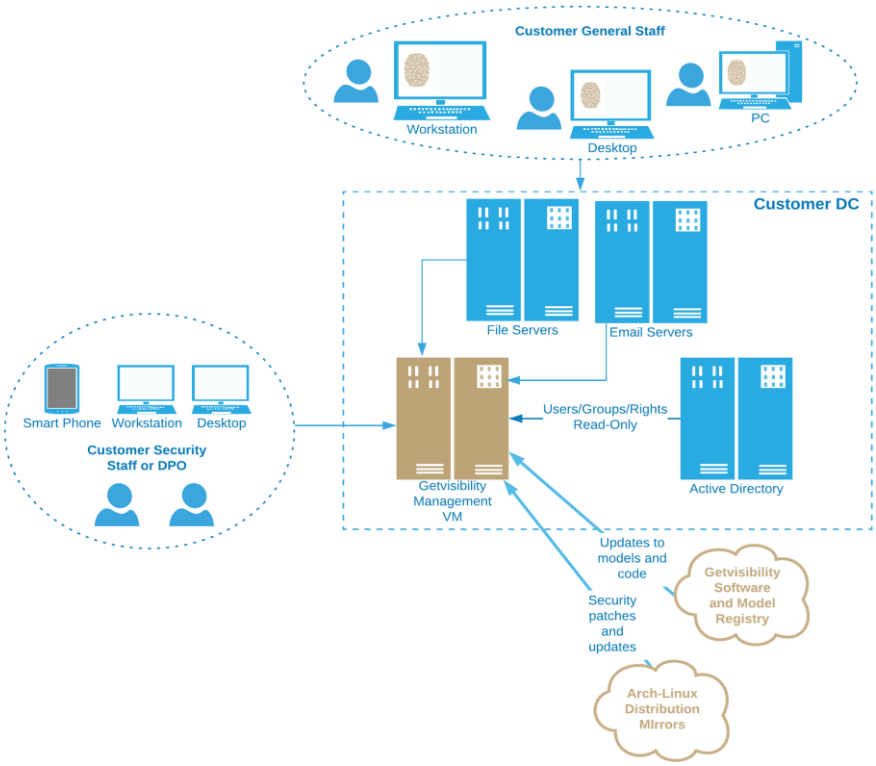
Secondly, the software can scan legacy documents in the organisation that may not have been opened in years. These documents are analysed and tagged depending on their sensitivity level and value, allowing staff and other automated tools to handle them correctly.

1. Agent Overview

As organizations are creating large amounts of documents and emails every day, and are now being audited more strictly than before, staff must practise good data safety. Getvisibility provides an agent for laptops and desktops that assists staff in avoiding dangerous activity, it will recommend sensitivity levels using AI, and block and log attempts to expose or put documents at risk. The Getvisibility agent also provides help and reinforces data security training for the staff. It supports the customers security levels and is aware of local regulations and can support multiple languages.

2. Automated Discovery and Classification

Over time, large amounts of documents accumulate on document stores and other storage areas in any organisation. These documents are of multiple file types and have varying levels of access permissions. Sensitive or important documents might be incorrectly exposed to many staff and this puts these documents at risk. Getvisibility also provides an automated discovery and classification scanner that uses AI that can automatically handle millions of documents and correctly analyse, tag and report on them. Documents at risk are highlighted and can be automatically tagged, marked for encryption, marked for deletion, or used in detail audits of file storage, never before possible.



Benefits of an Agent

With the launch of our agent technology we can deploy components of the software onto devices such as laptops, desktops and, coming soon, to mobile devices such as iPads and smartphones. These devices are where all the human interaction happens with documents and data. So, Getvisibility can now combine the automated scanning and classification of documents on file storage such as file servers with the interaction with live data and documents on all the endpoint devices in an organisation. This provides the first 360 degree view of documents and emails with AI technology monitoring and learning from the activities.

Getvisibility can now also **intervene in risky activities.** We're able to block or warn staff when they try risky activities such as emailing sensitive documents outside the organisation or classifying information at the incorrect, too low level.

Benefits of Documents and Email Tagging

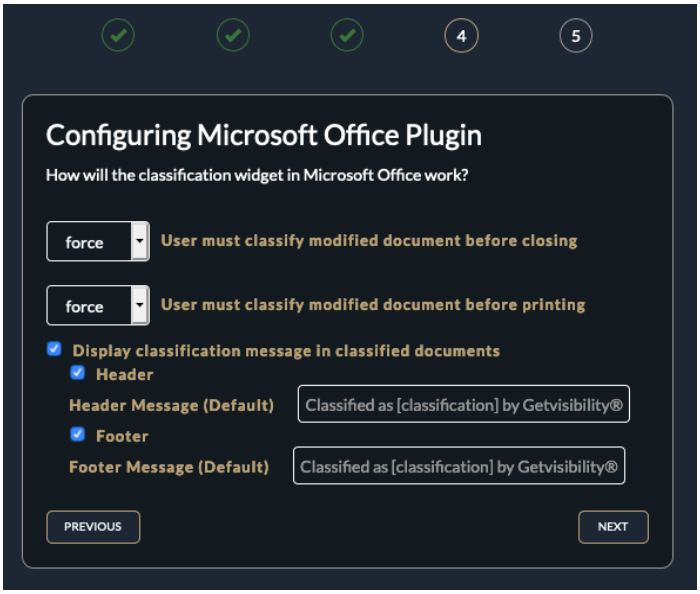
Many regulations and compliance standards such as ISO, HIPAA, PCI, GDPR, CMMC, DFARS, ITAR, EAR and others require, or benefit from, some form of visual document tagging that adds headers and footers such as:

This document does not contain Technical Data or Technology as defined in the ITAR Part 120.10 or EAR Part 772

This visual tagging can be manually inserted or added by software and depends on the content of the document. If manually added, the staff member editing the document must remember and insert the correct header based on the content of the document. This is easy to get wrong or to forget, especially when there are multiple regulations involved.

Our software is designed to use our existing AI and machine learning capability to examine the document text and recommend and write the correct header. This benefits the company because the documents are more consistently marked, the staff have less chance to make errors, and tracking of documents becomes possible.

The same is even more important for emails as these are designed to be sent between staff or out of the organisation. The value chain of organisations is now under more scrutiny than ever before due to data privacy or data security regulations. So, correctly marked emails become even more crucial than ever.



Our new agent software can be configured to enforce classification of document and visual tagging.

Notice that staff can be **Forced or Warned** to mark a document, or the event can be silently logged for later reporting and training.

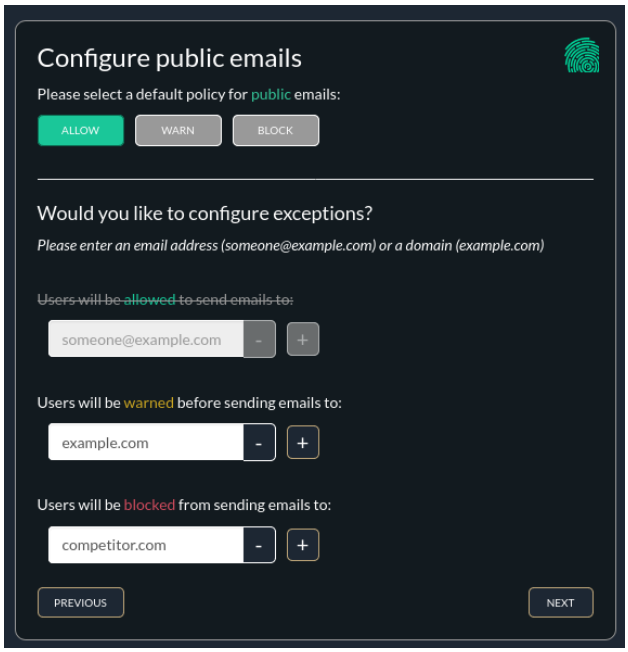
Benefits of Data Security Intervention

Emails sent outside the organisation or to the incorrect people are often the cause of data loss or security incidents. This is very difficult to catch in real time and some Data Loss Prevention (DLP) software vendors have built software that can intervene if an email has a sensitive attachment or if the email is flagged as confidential. This is potentially a good solution.

However, it relies on having accurate knowledge of the sensitivity of the attachment or the email itself. This is usually found by requesting the staff member themselves to select a sensitivity level. The possible problem with this approach should be apparent. Any staff member who is untrained in proper document classification, or cannot remember the training, or is in a hurry, or has a misconception of the different levels available, or is not aware of new regulations, or changes to new regulations, or is intent on stealing data, will not be a reliable source of classification.

Our Getvisibility agent can now use our machine learning model to create a *second opinion* in a few seconds for every new document or email opened. This opinion can be presented to the staff member as a guideline or reference. It can also be used to check on the classifications being done manually. This has not been possible up until now and is a major product differentiator.

We can also now intervene when a highly sensitive set of text appears in an email or document or attached document and this is misclassified or tagged at too low a level, or is correctly tagged but about to be sent outside the organisation.

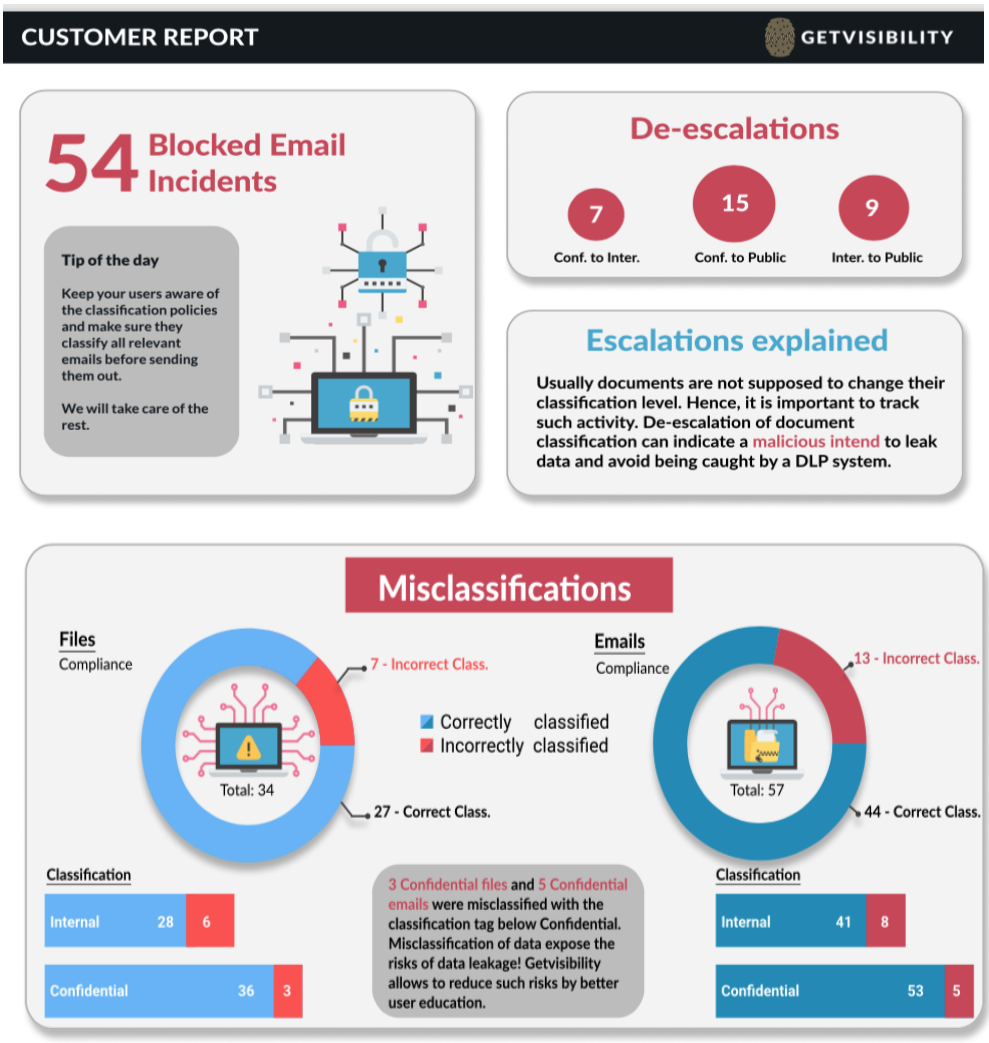


See how Microsoft Outlook can be configured to force classification before sending or printing, and how emails that should remain internal can be restricted. We also allow different levels of intervention based on the customer's unique classification and sensitivity levels. Default rules and exceptions can be configured.

As mentioned above, tracking activity happening on the endpoint devices as staff interact with the documents is valuable as we can derive information from the logs. Some examples are presented:

Type of Event	Intelligence Derived
Document classified	Staff member's view of the document's sensitivity, allows us to report on which types of documents reside where and who is accessing and creating these documents
Difference in classification	Either that the staff member needs training, or that a new type of document is discovered or created in the organisation, or that the model has not seen this type of file and can take the new classification for training purposes
Blocked sensitive email	Determine actual frequency of potential data leaks, identify bad data practices in certain departments or staff, determine the types of data that would be potentially exposed

The diagram below is an excerpt from the agent reports and shows some statistics relating to the above events.



Benefits of reminders

Reminders appear when **warnings and blocking occur**. These reminders provide the same useful task as the help text, in that they can be customised and provide useful information about what just happened.

A warning with very specific information about why an email was blocked due to export restrictions.

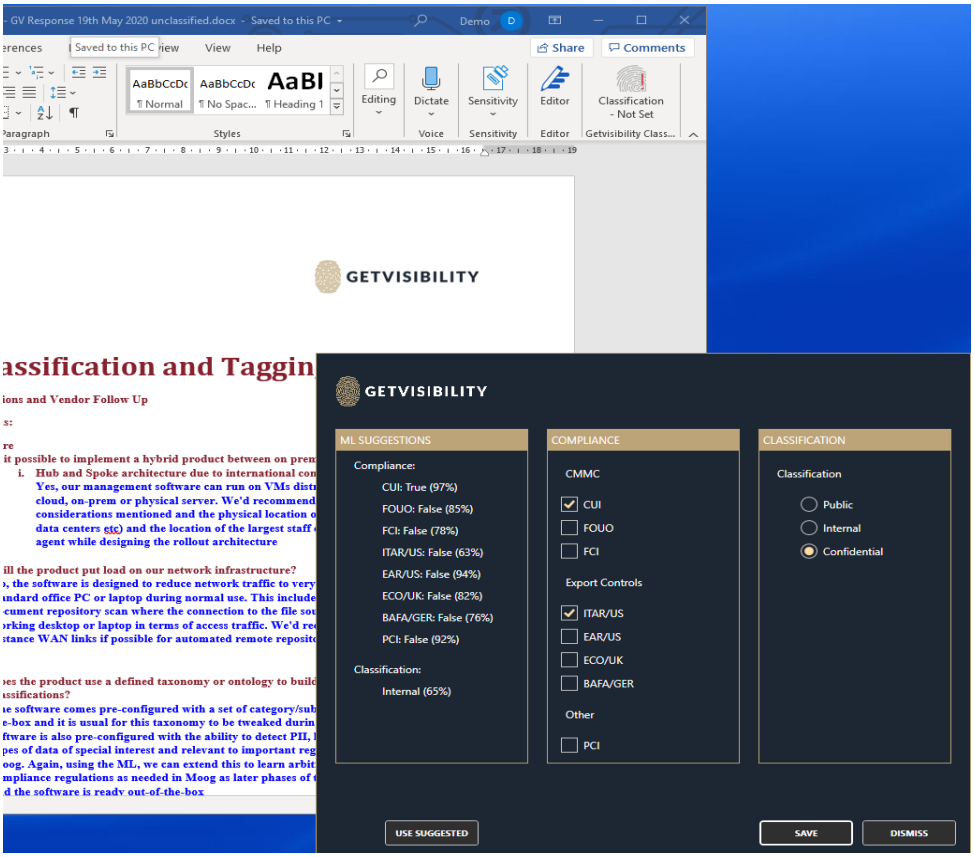
This provides very detailed information on the problem and relates to the email content and possibly any attachments. This is a very valuable assist for the user as they work.

Benefits of recommendation

One of the most challenging factors in document classification and tagging is the manual interpretation by staff that might not be fully trained or aware of the sensitivity. They might also be interested in *misclassifying* the documents. Also, as new regulations and compliance standards appear, they might start struggling to distinguish the differences or tagging the document correctly.

To assist with this issue, we have built in the recommendation feature that provides a *suggestion* to the staff member about tags to use for the document or email they are editing. This is based on the text, and allows them to see the second opinion of the machine learning model and, optionally, use it on the document. This saves time and can also work as a crutch to allow them to learn about new regulations or tags. This is a differentiator.

Staff can choose to use different tags from the suggestion, and this can have positive benefits to the platform to learn the correction, or to highlight that the staff member needs training. Consider the screenshot below that shows a large set of advanced compliance tags that the staff member needs to understand to make a correct selection. This is a real-world example of the compliance standards at work in a Department of Defence contractor in the United States.



For more information please visit

www.getvisibility.com

or contact us on

Email: contact@getvisibility.com