Data Classification - Why Organizations Need a Specialist Security Provider

Executive Summary

Today organizations are working with multiple security vendors and as this landscape grows in complexity, it is tempting to consolidate down to a few. Particularly appealing on the surface are the bigger vendors who are offering a one-size-fits-all approach to security that promises to deliver everything. However, organizations need to evaluate which vendors are truly offering the best security solutions.

In this whitepaper we look at how the security landscape has changed in the last couple of years. We examine what organizations need to think about in order to future-proof their environment and why data classification, a crucial part of any data security strategy, requires a specialist provider. We explore why it is important for any classification labeling policy to meet the needs of the business rather than the tool, and the importance of sophisticated and flexible metadata. The paper explains why you need to be picky when it comes to a single vendor approach and finally, why it is so important to make sure the organization gets the product support it needs from its provider.

Overview

Securing the hybrid environment

When the Covid-19 pandemic accelerated digital transformation, it also accelerated the trend for not only employees, but also digital assets, increasingly being located outside of the traditional enterprise infrastructure. This meant that cybersecurity teams were being asked to secure countless forms of applications and other new technologies. To effectively do this requires security options that are flexible, agile, and scalable, especially to enable the organization to move into the future, in a secure way. In fact, according to the 2021 Gartner CIO Survey, 64% of employees are now able to work from home, and two-fifths actually are working from home. What was once a privilege only available to executives, senior staff, and a handful of others, is now mainstream.

According to the Gartner 2021 CIO Survey 64% of employees are now able to work from home. This means that more and more digital assets are also located outside the traditional enterprise perimeter.

While the movement to a hybrid work environment is expected to continue into the future, from a security perspective, this will require a total review of policies and tools to better mitigate risks. Additionally, with the expanded threat surface that comes with a more distributed workforce, cyber threats are escalating and likewise unfortunately breaches are also becoming mainstream.

An increasingly consolidated market

As a result, demand for security solutions is rising. However, having too many security vendors in the mix can result in complex security operations and increased security headcount. Most organizations see vendor consolidation as an avenue for more efficient security. Large security vendors are responding with better-integrated products. But the downside is that we are seeing more vendors than ever before offering solutions which claim to cover all of an organization’s security needs. And while, from a consolidation perspective, multiple to fewer vendors is certainly the direction that most enterprises are moving in, they need to ensure that this strategy will deliver against the organization’s security needs.

According to Gartner most organizations have anywhere between 80-90 cybersecurity tools, therefore, adding another 10 or 20 tools doesn’t necessarily mean the firm’s defenses will be any better. That said, there are times when working with a specialist provider and having that deeper knowledge around a solution/problem is the only way organizations can protect sensitive data.

Add to this the increasing regulations and compliance landscape in 2022. In Gartner’s Top Eight Security and Risk Trends for 2021, cybersecurity and regulatory compliance were the two biggest concerns of corporate boards, with some organizations adding cybersecurity experts specifically to scrutinise security and risk issues.

Putting the foundations in place for robust data security

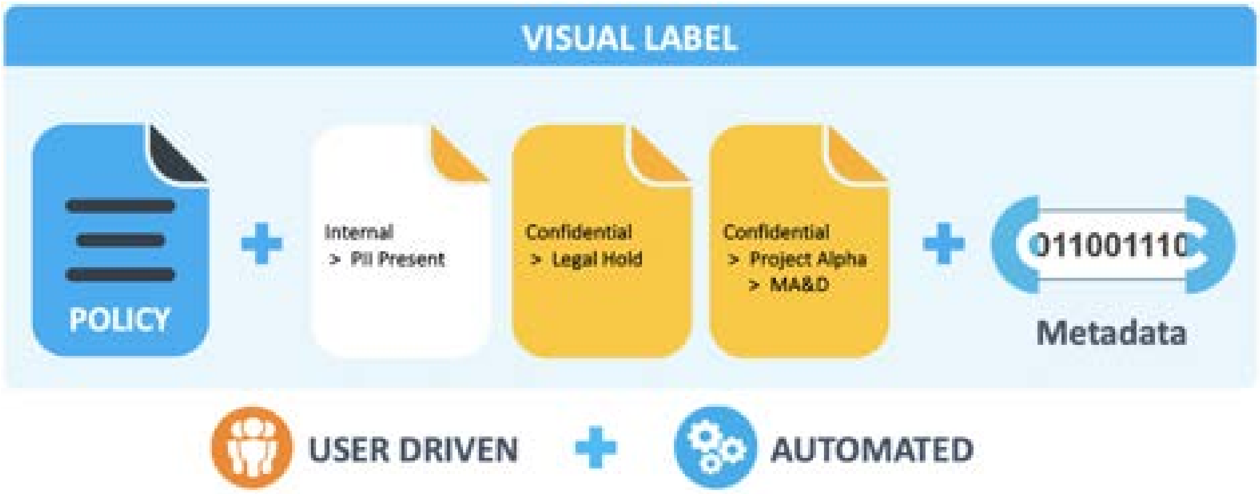
All too often, data lacks context, security professionals are bombarded with too many false positive alerts, and accidental breaches occur. At the same time, regulations are making organizations more responsible for the protection of their data.

This is one of the reasons why organizations should take a layered approach to security defences, starting with data classification which is one of the key solutions within a solid data security stack. That's because data classification provides the key to better control of sensitive data, and in turn delivers better cybersecurity within the business. This means that organizations should be consulting with expert solution providers to make sure they get this layer of data security right first time.

We see data security as an ecosystem where classification is one of the core tenets of any good data security plan.

Data classification is a data management process whereby organizations categorise various information assets based on the sensitivity of the document's contents..

How data classification helps



Modern data classification solutions combine visual labeling with labels applied to the file's metadata to protect and control use. These labels enhance the performance of third-party technology solutions to determine how a piece of data should be treated, handled, stored, and finally disposed of.

Data classification streamlines the load when it comes to handling data, as well as enhancing data security and compliance – making an organizations' investment in security applications work harder. Once data has been classified, organizations can confidently continue their data security journey.

Here at HelpSystems, we recognise the importance of protecting data and can provide a suite of data security solutions that help organizations regain control by identifying and classifying all the different data types, from personal identifiable information (PII), to personal health information (PHI), to payment card industry and financial data. We see data security as an ecosystem where classification is one of the core tenets of any good data security plan.

Therefore, why build up your security ecosystem using a solution that simply isn't going to be able to truly fulfil the organizations needs into the future?

So, what should an organization look for when choosing a specialist provider?

There are four key aspects that are critical to successfully classifying data.

1. Data classification with a labeling policy that reflects the way the business uses data

Organizations should select a data classification tool that is able to provide a labeling policy that reflects the way data is used within the organization, as opposed to having to sacrifice business requirements for classification to fit into a generic, non-flexible, classification schema set by the solution. Users must have the ability to set unambiguous labels in order to understand how to handle data within the business.

The policy needs to be able to support both sophisticated visual and metadata labels. Sophisticated visual labels give greater context to the data, which in turn allow for more accurate and secure handling of data. Using a blanket label of "Confidential" may work in some instances but using a more granular label of "Confidential – Board – PII" allows for quicker identification of sensitive information, as well as indicating what should be done with it.
The greater the granularity provided by data classification, the more a policy can be enforced, as well as providing far more accurate downstream support for other data security tools such as DLP, DRM, and encryption.

2. Sophisticated and flexible metadata

When the organization is looking for more accurate support, and value add to downstream security solutions, the business needs to be using sophisticated metadata.

More often than not, non-specialist security solutions will offer basic metadata functionality, and there are some solutions that don't use metadata at all but organizations can added metadata which can be further utilized by control tools. By using sophisticated, flexible, and customisable metadata, the organization can set metadata to trigger functions such as email encryption applied to data leaving the business based upon classification levels specified within the metadata. Another example is to use information set within flexible metadata to block certain types of data being uploaded to the cloud via CASB solutions, ensuring sensitive data isn't leaving the organization when it shouldn't be.

Another frequent downfall with non-flexible metadata are the issues that arise when working with the supply chain, who may be using different classification methods, meaning the classification may be lost during exchanges of data or information. By using flexible metadata, the organization can ensure consistent labeling when data is being shared back and forth between parties.

By using flexible metadata, the organization can ensure consistent labeling, especially when sharing with external parties.

Regulatory requirements are increasingly asking for the archival of sensitive data after a set time period, for example, the archiving of financial data once it has been held for 6+ years within the business. Flexible metadata allows the business to set retention and archiving values within the data so that the organization remains compliant with these requirements.

3. Understand why it is helpful to reduce security agent complexity

With vendor consolidation top of mind, it is easy for the CIO or CISO to think that it's much easier to select one provider and get all the security tools they need under one roof. And that might seem like utopia initially, but typically that only gets the business so far. Here though it is important to consider that vendor consolidation doesn't necessarily mean that the organization should utilize all of the security capabilities from one vendor but utilize the ones that can give the business the best results. For example, combining data classification and DLP from one vendor will deliver bigger benefits. Overall, it is helpful to reduce security agent complexity, as this provides more seamless integration and helps in overall workflow automation. That said,the organization will most likely have a variety of security solutions already integrated and well established within the business. Here using a best-of-breed solution provider approach means the business can choose the best security solutions for the organization's needs that will provide the best protection to the business, its users, and processes. When it comes to the organization's security, no business can afford to compromise.

One group of people who would be very happy to see the organization choose a single vendor for all their security are hackers. If a hacker knows just some of the compromises that a single vendor has, this is precisely the key they need to access a whole world of data within the organization, and the consequences could be disastrous.

Our advice really is to avoid adopting lower end data security solutions. While they may seem tempting, the security offerings usually come as part of a wider platform and are not built with the flexibility and functionality that a best-of-breed provider can offer. The organization is also at risk of "vendor lock in", where it is at the mercy of one provider controlling every element of its data security, even down to non-negotiable annual price increases for software.

4. Getting the product support the business needs

And finally, will a single vendor approach support all the products the business is using? Will the organization get the product support it needs?

While most data classification solutions will generally support the likes of Word, Excel, and PowerPoint within the MS Office product set, it's likely that a lot of the organization's IP may be located in other programs such as Visio and Project, on Mac or Google Workspace, or within CAD solutions - to name a few, which solutions such as Microsoft AIP do not extend to.

Classification within an organization needs to go beyond the borders of the basics of MS Office, and be able to classify all file types, while also understanding the classification values within alternative file stores in the business.

Likewise, businesses want to work with a vendor that will listen, can be extremely flexible and agile in its approach, so that as the organization's requirements change over time, the vendor can respond and adapt accordingly.

Conclusion

The data security landscape today requires organizations to be compliant with far more regulations than ever before, and this is only increasing. Likewise, data is prolific and good data governance is an ever-growing requirement, as is securing sensitive data against accidental and inadvertent loss, which could lead to a data breach. From the moment data is created, it becomes a liability. Data costs firms money to store and poses a risk if it inadvertently falls into the wrong hands.

Data classification provides the key to better control of sensitive data, and in turn, better cybersecurity within the business. Therefore, organizations need to be consulting with expert solution providers to ensure that their data protection and classification requirements are properly met.

Why HelpSystems data classification solutions

HelpSystems provides best-of-breed data classification solutions tailored to specifically fit individual customer requirements or circumstance. Because a "one-size-fits-all" approach doesn't work with classification, we work with customers to advise on current legislation, such as CUI, CCPA, or GDPR, and what that means for their business. We help organizations plan out and implement a solution relevant to users and the business, putting customers fully and securely in control of their data – from business critical to public.

HelpSystems data classification solutions are built from the ground up, to comply with current and future needs. Our specialist tools have the capacity and flexibility to provide a comprehensive and user-friendly solution that works in line with our customers' controls and business processes, and which will classify and protect data in line with industry standards.

Our detailed, business centric labeling offers clarity as to how data can be used. Clarity for users and clarity for downstream security tools. Once organizations know what their data is and where it is stored, they can then protect it according to its business value. Data classification from HelpSystems gives organisations both a foundation for their wider security posture AND competitive advantage.

helpsystems

www.helpsystems.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.