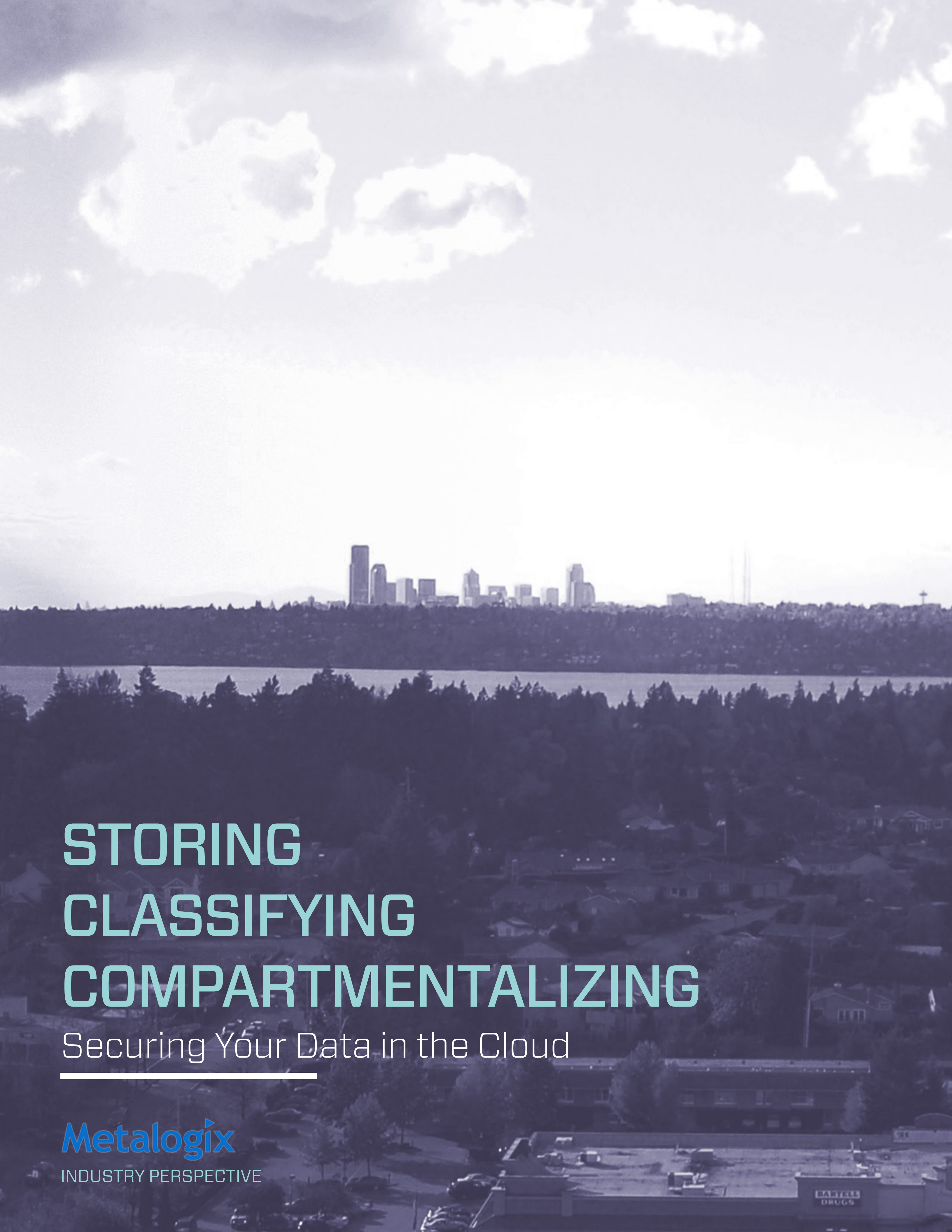

STORING CLASSIFYING COMPARTMENTALIZING

Securing Your Data in the Cloud

Metalogix

INDUSTRY PERSPECTIVE

EXECUTIVE SUMMARY

When we think of data breaches, we might picture a TV plotline on shows like "Quantico" or real-life examples like Edward Snowden – where someone intentionally exposes sensitive information. But the reality is that anyone in an agency, ranging from top-clearance levels down to an entry-level worker, can intentionally or accidentally misuse or leak critical data.

This potential is increasing as new technologies put more information and power in the users' hands. The complexity of governing, tracking and securing content and data has been magnified due to the growth of content-management systems like SharePoint, a business-critical tool that helps organizations place, store, organize and access information from almost any device in a secure manner.

Threats to data are expanding, and managing data in the cloud and on-premises is even more complicated. But there are steps you can take to keep your data secure. In an interview with GovLoop, Steven Murphy, Chief Executive Officer, and Jai Dargan, Product Manager, at Metalogix discussed how your agency can deploy cloud files safely and better store, classify and manage data across an organization.

Metalogix provides industry-recognized management solutions for mission-critical collaboration platforms. Its solutions are engineered to help you go beyond simply securing your agency's data, be it in the cloud or on-premises.

One such solution is ControlPoint with Sensitive Content Manager, which can help your agency automatically detect sensitive content, like Personal Identifiable Information (PII), so that during cloud migration, you can easily compartmentalize this type of data from other files.

In this industry perspective, we explain how Metalogix can help you secure your agency's sensitive content while still taking advantage of the flexibility of cloud systems like SharePoint Online.

> "Agencies now have to make sure that top-secret information is compartmentalized, where group X does not have access to group Y."
>
> **– Jai Dargon,** *Program Manager at Metalogix*

YOUR PLAN TO SECURING SHAREPOINT

Whether choosing a cloud or on-premises IT infrastructure, Murphy and Dargan recommend government agencies go with SharePoint systems for their content-management needs. SharePoint is a Microsoft Office tool that allows organizations to create websites and helps secure platforms to store, organize, share and access information from almost any device. SharePoint is particularly useful because it has a rules-based security model that controls everything within a SharePoint system, down to individual files. The system is also flexible and allows users to be assigned a mix of permission levels, granting them access to different SharePoint functions as well as content. This allows agencies to leverage users, content and permission levels in a variety of customizable ways.

The problem with SharePoint, however, is that it lacks a centralized way of defining or managing the application of permissions across an entire SharePoint farm (the connector of all installed SharePoint servers in your system).

"The main challenges that agencies face include admitting that the traditional cyberdefense paradigm isn't working; monitoring sensitive content at all levels; working with legacy systems that are 10 to 20 years old and an underestimation of the risk environment," Dargan said.

In order to help agencies tackle these challenges, Metalogix offers solutions that integrate directly with SharePoint to help manage various permissions and content so that agencies can better monitor their SharePoint systems.

"What we're doing at Metalogix is securing data in motion and at rest," Dargan said. "Castle walls simply aren't enough anymore, and the vast majority of IT security spending is still on password security. Recently, we've seen a more digital and global workforce with a massive collaboration market. That means there are a lot more data entry points while you still need access to content anywhere on any device without any hiccups."

It's especially important for agencies to have a concrete plan when securing data in SharePoint. Murphy and Dargan suggested a three-step approach to creating a secure environment:

1. **Define a security plan**
   Defining an overarching cybersecurity plan before, during and after you migrate to newer versions of SharePoint is critical to a successful cloud deployment and stronger content security. In addition, your agency should start to focus on defining a permissions model well in advance of implementation.

2. **Manage permissions**
   Permissions should always be applied using the "least privilege" principle. This means that users only have the minimum amount of permissions required to complete their job. This will help you better manage varying levels of user access to your content from the highest entity to the lowest.

3. **Monitor systems**
   Metalogix suggests using a general "monitor and revoke" policy. This means administrators should regularly review permissions and, when required, remove those that do not meet organizational policies. Monitoring your data systems and content should be a continual process.

Metalogix can help you complete those steps in securing and classifying SharePoint data using tools like ControlPoint and Sensitive Content Manager.

METALOGIX CONTROLPOINT & SENSITIVE CONTENT MANAGER

ControlPoint and Sensitive Content Manager are tools that help prevent SharePoint data loss.

“With Sensitive Content Manager, we’ve combined ControlPoint’s permissions and reporting capabilities with a content awareness tool that can detect, classify and act on sensitive content,” Dargan said.

Through these capabilities, ControlPoint and Sensitive Content Manager detect threats, help IT teams better classify permissions and users and take action on any potential breaches.

“ControlPoint is like our traffic cop,” Dargan said. “It’s our administrative tool that sits on top of SharePoint and allows administrators to seamlessly govern their users and content. It especially helps with permissions management, auditing capabilities and reporting capabilities.”

Combined, these tools help agencies better combat Data Loss Prevention (DLP) for sensitive content such as PII in SharePoint, both on-premise and in the cloud. Powered by advanced machine learning technologies, Metalogix ControlPoint and Sensitive Content Manager provide more accuracy for the filtering and classification of permissions and content. While other DLP solutions employ rules and techniques that make it too simple to find PII, Sensitive Content Manager provides more in-depth analysis of the true nature of your content.

“When we talk about breaches, we usually talk about exposure of PII,” Dargan said. “This means that anytime your office is migrating to new systems like SharePoint, you’re moving all types of content, which includes content that should not be there, like PII. Tools like Sensitive Content Manager act as a filter that can catch important data and automate red flags should it detect PII left behind by somebody in the organization.”

Metalogix’s ControlPoint and Sensitive Content Manager can help your agency:

- **Detect the presence of PII**
  Sensitive Content Manager allows clients to identify, track and secure documents using advanced powered machine learning, which enables a higher level of contextual content awareness in complex enterprise environments.

- **Take action**
  Upon detection of PII that could pose serious security threats, ControlPoint can alert, isolate or remove files that violate policy. ControlPoint can also customize workflows so that they easily enforce governance strategies while reducing the workloads on SharePoint administrators, content owners and compliance officers.

- **Manage your content**
  With the addition of Sensitive Content Manager, your SharePoint administrators can manage your agency’s content in real time. Administrators can use on-demand scanning, flag specific libraries, sites or site collections for content discovery or enable a real-time content shield to perform analysis of files as they are created, modified, moved or destroyed.

METALOGIX IN ACTION

ControlPoint has helped agencies get secure in the cloud at both the federal and local levels. In the following case studies, the Department of Defense (DoD) and the city of Bellevue, Wash., demonstrate how agencies can tackle the challenge of securing their data in the cloud using Metalogix solutions.

CASE STUDY ▶▶▶▶

CONTROLPOINT FORTIFIES DEPARTMENT OF DEFENSE SHAREPOINT COLLABORATION STRATEGY

Using ControlPoint, DoD was able to better manage its complex and mission-critical collaboration platform.

An IT team at DoD, with only one SharePoint administrator on staff, needed a way to get an entire team of eight IT administrators familiar with SharePoint systems they had never used before. To add to the pressure, the team was on a tight timeline and budget. They reached out to Metalogix and had ControlPoint for SharePoint Administration installed.

Within the first four months, the team received rapid return on investment. For auditing and governance, the team was asked to provide a list of all documents for which a particular person had access within the last 90 days. Before, the team would have rejected such a request, but with ControlPoint, it was able to respond to the inquiry using a simple report with almost instant results.

In addition to the rapid ROI, DoD now has powerful permissions management. For example, the IT team was able to build in permission levels for people who don't need permission to the data, but need to know who has access to what. Additionally, the auditing capabilities of ControlPoint for SharePoint Administration helped the IT team remove personnel from SharePoint that have moved over to other installations.

Finally, ControlPoint can lessen the impact of SharePoint concerns unrelated to governance and administration, such as disaster recovery. After DoD encountered a problem with content in its database, it was determined that it would be best to revert to a previous configuration. Going back meant users would potentially lose data or administrators would have to spend several hours trying to restore the entire system.

The same IT team needed to restore to a point before the data corruption, which is very disruptive to users. By using ControlPoint, however, the team was able to quickly attain a list of everything that was changed in the system and by whom. All the team had to do then was back up and restore those individual items separately. In five hours, users had a seamless experience. No data was lost and the team rolled back to where it needed.

CASE STUDY ▶▶▶▶

THE CITY OF BELLEVUE & SECURING SENSITIVE CONTENT

Bellevue is the fifth-largest city in Washington, with a population of more than 130,000. Technology is considered a core enabler of many of the city's programs, including enhancing community participation in government, bringing city services to customers' doorsteps and making information easily and broadly available. For this, the city government relies on SharePoint.

Bellevue's journey began when it undertook a migration from SharePoint 2007 to 2010. The migration was a slow and painful process. The content cleanup before migration involved manual, time-consuming processes. Additionally, the city had to deal with incorrect permission levels and lack of visibility into which employers were getting certain privileges.

The solution? After choosing Metalogix ControlPoint to manage its SharePoint 2010 environment, Bellevue set out on a "SharePoint Clean-Up Project." With the help of ControlPoint, the city was able to achieve:

Greater transparency & control of permission:

With ControlPoint, Bellevue can now confidently manage permission policy compliance and ensure permissions are set up carefully, the right way. This helped the city better control who accesses sites and document libraries, making sure there's less rogue document creation and deletion.

A cleaner SharePoint environment:

Cleanup is streamlined while offering greater attention to detail. Employees were able to run inventory reports for each individual site collection, without the painstaking manual processes of going through files, identifying users and distinguishing user permissions.

Document retention compliance & protection against fines:

Retention policies are now easily applied, reducing the risk of litigation and financial penalties. Bellevue's IT team can set retention of documents to last for any amount of time, ensuring they comply with legal use.

User adoption monitoring:

ControlPoint helps gauge the value and return on investment in taxpayer dollars that SharePoint provides. By monitoring user activity, Bellevue can determine best practices, set permission policies and improve user adoption in other departments.

Both the city of Bellevue and DoD were able to save time, money and resources by deploying Metalogix's ControlPoint to manage their SharePoint systems. It has enabled both entities to be more proactive and secure, while keeping within tight budgets.

CONCLUSION

We live in an age where it is increasingly important to be sure who's using your data and to keep out those who shouldn't be.

"Agencies now have to make sure that top-secret information is compartmentalized, where group X does not have access to group Y," Dargan said.

Imagine someone in your agency trying to access a piece of data that he's not supposed to, or trying to download more files than he usually does. Now, imagine that your SharePoint systems could identify any unusual activity outside of an employee's normal behavior – and actually stop this type of data misuse in its tracks.

That hypothetical is now a reality. We live in an era where an agency's data system, like SharePoint, can actually monitor individual behavior and halt any activity that falls outside an individual's norm or clearance level. That is the future with Metalogix.

As government agencies continue to move their content to the cloud and administration systems like SharePoint, Metalogix will be there to help agencies navigate the process. Securing data and content has become more of a challenge in an age of increased collaboration, flexibility and innovation in the cloud. While threats may increase in complexity, government can rest assured that it has the available tools to tackle current and future security challenges.

ABOUT METALOGIX

Metalogix is the premier provider of management software to move, manage and secure content for Office 365, SharePoint, OneDrive for Business, Exchange and other leading enterprise collaboration content management platforms in the cloud, on-premises and in hybrid environments. Over 20,000 clients rely on Metalogix and the industry's highest rated LIVE 24x7 support to enhance the use, performance and security of content collaboration in the cloud, on-premises and in hybrid environments. Metalogix is a Microsoft Gold Partner, an EMC Select Partner, and a GSA provider and a multi-year honoree on the Inc. 500|5000 fastest growing company list as well as the prestigious NorthFace ScoreBoard Award for World Class Excellence in Customer Service.

Visit us at www.metalogix.com or call us +1.202.966.9100

Engage with us on Twitter @Metalogix and LinkedIn.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 200,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report,
please reach out to: info@govloop.com.

www.govloop.com

@GovLoop

Metalogix

govloop

govloop

1152 15th St NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com

@GovLoop