Information Security for the Modern Enterprise
How safe is too safe? - information lock-down vs sharing and collaboration

Sponsored by

OPENTEXT

aiim®
The Global Community of Information Professionals
About the White Paper

As the non-profit association dedicated to nurturing, growing and supporting the user and supplier communities of ECM (Enterprise Content Management) and Social Business Systems, AIIM is proud to provide this research at no charge. In this way the entire community can leverage the education, thought-leadership and direction provided by our work. Our objective is to present the “wisdom of the crowds” based on our 70,000-strong community.

We are happy to extend free use of the materials in this report to end-user companies and to independent consultants, but not to suppliers of ECM systems, products and services, other than OpenText and its subsidiaries and partners. Any use of this material must carry the attribution – “© AIIM 2012 www.aiim.eu / © OpenText 2012 www.OpenText.com”.

Rather than redistribute a copy of this report to your colleagues, we would prefer that you direct them to www.aiim.org/research for a free download of their own.

Our ability to deliver such high-quality research is made possible by the financial support of our underwriting sponsor, without whom we would have to return to a paid subscription model. For that, we hope you will join us in thanking our underwriter for this support:

OPENTEXT

OpenText
275 Frank Tompa Drive
Waterloo, Ontario
Canada, N2L 0A1
Phone: +1-519-888-7111
Web: www.opentext.com

Process used and Survey Demographics

While we appreciate the support of our sponsor, we also greatly value our objectivity and independence as a non-profit industry association. The results of the survey and the market commentary made in this report are independent of any bias from the vendor community.

The survey was taken using a web-based tool by 255 individual members of the AIIM community between October 26, and November 21, 2012. Invitations to take the survey were sent via e-mail to a selection of the 65,000 AIIM community members.

Survey demographics can be found in Appendix A. Graphs throughout the report exclude responses from organizations with less than 10 employees taking the number of respondents to 223.

About AIIM

AIIM has been an advocate and supporter of information professionals for nearly 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data. AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators and consultants. AIIM runs a series of training programs, including the Certified Information Professional (CIP) course. http://www.aiim.org/Training/Certification

About the author

David Jones is a Market Analyst with the AIIM Market Intelligence Division. He has over 15 years’ experience of working with users and vendors across a wide range of vertical markets. His experience has focused on taking complex technologies, such as business intelligence and document management, and developing them into commercial solutions largely in the retail, web and customer relationship management (CRM) areas. He has worked as a consultant providing document management, data mining and CRM strategy and implementation solutions to blue chip clients in the UK and Europe and produced a number of AIIM survey reports on issues and drivers for Capture Solutions, SharePoint, Cloud Computing and Social Business. David has a BSc in Computer Science, and is a qualified CIP, ECMP and SharePointP.
Table of Contents

About the White Paper:
About the White Paper .................................. 1
Process used .............................................. 1
About AIIM .............................................. 1
About the author ....................................... 1

Introduction:
Introduction ............................................. 3
Information Assets ...................................... 3

Data Location:
Data Location .......................................... 5

Security Risks:
Security Risks .......................................... 8

Corporate Issues:
Corporate Issues ...................................... 11

Conclusion and Recommendations:
Conclusion and Recommendations ............ 12
Recommendations ..................................... 13
References .............................................. 13

Appendix 1: Survey Demographics
Appendix 1: Survey Demographics ............. 14
Survey Background ................................... 14
Organizational Size ................................... 14
Geography ............................................. 14
Industry Sector ....................................... 15
Job Role .................................................. 15

Appendix 2: Open Questions
Appendix 2: Open Questions ....................... 16
Selected responses .................................... 16

Underwritten in part by:
OpenText ............................................... 17
AIIM ..................................................... 18
Introduction

Enterprise security is changing. The domain of the enterprise security professional is moving from that of internal access policies, VPN management and compliance techniques to a much wider context. Mobile, social and cloud technologies are extending the types and reach of the information that needs to be secured and managed.

The dilemma that organizations face is that whilst they may wish to protect their information from all possible risks, that does not marry well to the diverse and interactive nature of today’s business landscape. Information, much of which is now unstructured, is flowing in and out of organizations at an unprecedented rate and the challenge all organizations have is to balance the benefits of this information free-flow against the potential risks, and to deliver a security framework that maintains high levels of protection whilst not stifling business processes.

Before an organization can make any decisions it needs to analyze and understand the types of information that need to be protected and maintained, the relative importance of the various information assets, the processes that information is part of, the potential damage to the organization should that information not be secure, and the solutions available in the marketplace.

This paper will look at the various types of information that needs to be managed, how important this information is to organizations, the types of security being deployed and the potential risks should that security not be good enough. Finally the paper will provide a series of recommendations and steps towards securing these vital information assets.

Information Assets

Organizations store a multitude of information and content ranging from employees’ payroll details to product information and financial accounts. This information can be classified at various levels, according to widely accepted standards. The majority of our survey respondents (86%) store company confidential documents – although it would be interesting to know what the remaining 14% do with their important information.

Of interest are the surprisingly large number of organizations storing Secret (31%) and Top Secret (14%) information, especially in larger (>5000 employees) organizations where these rise to 40% and 17% respectively.

*Figure 1: Which of the following security-level documents is your organization storing? (select all that apply) (N=223)*
As discussed above, organizations store a wide array of information types, each of which will have a varying level of importance to each specific organization. This importance is of course subjectively based on the view of the individual respondent, and could be influenced by the department they reside in or the industry they work in (for example a research scientist may feel that intellectual property (IP) is more important than financial records), but given the wide range of job roles and organizational types of our respondents, the figures shown below can be deemed to be generally representative.

Understandably, customer information shows strongly with 27% indicating that this is their most important information asset. Without careful management of this information an organization would not be able to sell new products or services, invoice those customers or analyze their preferences to perform future marketing. Traditional customer information would purely have been data such as contact details, purchase histories and perhaps some additional lifestyle records – but customer information can now include social media history, geo-location data, and internet history records. The majority of this information is unstructured and the integration and management of this combination of structured and unstructured data is a key aspect to the success of any organization.

Respondents also recognized that other information types such as IP (20%), financial records (16%) and project documents (15%) hold significant value. Interestingly HR and employee information at 7% was not deemed as important – however, when it comes to securing information assets, this becomes one of the most important to manage.

Another important aspect when viewing the importance of data is the consideration of business value versus regulatory value. Certain types of information, such as IP and project documents, are important from the perspectives of running the organization. Other information types such as customer, staff and financial information hold business value but also have regulatory or data protection aspects - where rules and regulations firmly govern the security requirements and management of the data.

Figure 2: Which of the following would you say is your organization’s most important information asset? (N=221)

The relationship between information governance, compliance and IT is a complex balancing act and in order for an organization to successfully manage this balance a top-down approach is imperative. C-level executives need to appreciate the individual elements of this triumvirate in order to be able to determine which security controls are appropriate to manage their information, aligning these with the governance goals and compliance requirements of the organization to manage information risk as effectively as possible.

To that end, it is reassuring to see that over half (58%) claim to fully appreciate the value of their information and support active steps to secure it, but it is of concern that this figure is not 100%. A further 20% are keen to remain compliant but have no specific requirements. This could suggest that their primary focus is on protecting their organization should anything go wrong – but that they do not want to be specifically held responsible for regulatory compliance. Alternatively it could also indicate that they simply have not recognized the risk. A similar number (19%) has the same attitude; assuming that IT should deal with “that sort of thing”.

© AIIM 2013 www.aiim.org / © OpenText 2013 www.opentext.com
A small number of organizations have taken the very brave stance of embracing information sharing and exchange as a strategic decision. While this conceptually and philosophically may be the ultimate in liberating the workforce and freeing the organization’s information, we do all live in the real world, and some types of information simply cannot be freely shared. For example, an organization needs to store employee bank details in order to be able to process payroll. Executives and employees alike would not be comfortable with this type of information being freely available to share throughout the organization.

**Figure 3: Which of the following best describes how senior management in your organization view information security?? (N=221)**

Data Location

In this electronic, and increasingly cloud and mobile-based age it is interesting to see the amount of corporate information that is still held on paper: 14% across all information types and a massive 23% in HR. This highlights a leaning towards paper processes in HR and also raises the question as to whether HR is seen as an important business asset by the board.

More likely is the fact that, as alluded to above, the type of information stored by HR is of a more sensitive nature (bank information, addresses, salary details, etc.) and requires a higher level of security than other areas such as marketing or product management. This should not be seen as a valid reason to avoid moving to electronic storage; quite the opposite, it should be used a driver to improve overall, organization-wide security mechanisms to secure this and other types of information.

Also of interest is the apparent reluctance of organizations to use the cloud as their primary information space with only 2% claiming they are using the public cloud as their primary space to store client (or CRM) information. With cloud-based services such as Salesforce.com claiming huge user numbers² this very low figure seems strange, however, it may highlight a misunderstanding about how data on such SaaS (Software-as-a-Service) applications is stored – do users believe that their data is stored in a private cloud, not in a private instance on a very public cloud?
The potential misunderstanding of where data physically sits continues when looking at future storage options: only 10% claim they would consider storing CRM information in a public cloud. Project documents (14%) and product information (12%) are the information types with the highest potential public cloud storage levels – but neither are particularly large, or reflect the adoption levels found in other AIIM research.

It appears that the jury is still out regarding cloud in general, with private clouds being considered by around half (51%) but with the low positive responses for public clouds, a similar number do not expect to store information in any cloud offering – indeed 53% would not consider storing any of their IP in a cloud service.

**Figure 5: Would your organization consider storing the following information assets in the cloud?** (N=217)
Data sovereignty is defined as the consideration of laws and regulations that come into play when data that is generated in one country is then stored in a different country. For example, if content is created in the UK and stored on a cloud server in the US, whose laws govern that data?

This concept is not always understood with 24% not aware of any regulations applying to them, and even where it is understood steps are not always taken to manage it -10% are aware of regulations but are not managing them.

Over a third are aware of these issues, however, and are managing them accordingly. This number may also have influenced the adoption of the cloud in this area\(^4\), given that a number of cloud services do not publicise or indeed guarantee the physical locality of data stored on their servers.

*Figure 6: Is any of your data subject to any particular data sovereignty regulations (i.e. data has to remain within particular geographical regions)? (N=212)*

The issue of data sovereignty becomes relevant when you consider that a combined 48% store content in a country other than where it was created, either in public cloud, private cloud or on-premise.

No problems exist if these organizations are fully aware of any data sovereignty issues and are managing them – but for those that either aren’t dealing with these issues or are not aware of them, serious challenges may be encountered in the future. This becomes particularly prevalent in regard to localized legislation, such as the US Patriot Act or UK Data Protection Act, which give investigatory powers to authorities in the relevant geographies that may not be expected, or indeed welcome. For example, a European organization storing customer data on a US-based server may not be aware that the US Government, as part of its anti-terrorism initiatives, can delve into that data and perform extensive analysis on, potentially in contradiction to the laws and regulations in the country from where the data originates.

*Figure 7: Do you store data in any of the following? (Select all that apply) (N=208)*
Security Risks

Having assessed the information assets within organizations, their relative importance and where they are stored, it is time to dive deeper into how these assets are secured.

It would appear that the so-called “traditional” security risks of external hacking and malware/viruses have been secured, at least to the satisfaction of most respondents. Unauthorized access to content from staff is also well secured in the eyes of the majority. However, how well founded is this confidence – is an organization fully secured because a firewall or antivirus system has been installed? We explore this further in the next section.

Data leakage via social media has a fairly even split between those who feel fully secured and those who have some security but not enough – this raises the interesting question of “what is fully secured” in relation to social media? Is it that all posts need to be approved, that automated tools constantly search for references to posts relating to the organization, simply that the organization has a social media acceptable use policy – or that social media usage is banned in the organization? None of these in singularity will fully protect against data leakage in this manner and a software and staffing combination of all of them is required to carefully manage social media content in general.

An interesting result relates to unauthorized access by ex-staff where many (71%) believe that they are not sufficiently covered. Why do they think that ex-staff have more potential access to information than current ones? What happens differently when they leave the organization? Perhaps the concern is more of a perceived issue than a real one, driven largely by the fact that the organization is no longer in control of that person’s primary point of information access, i.e. their desktop.

Figure 8: What level of security does your organization have in place to protect from the following risks? (N=219)

The confidence in managing external security risks shown above follows through to where respondents see the most likely security breaches coming from – a relatively low number see external hacking (20%) and malware/viruses (14%) as the most likely source of a security breach.

Despite feeling that they have protection in place against it, almost half (49%) believe that unauthorized access by staff is the area of largest concern. This is significant as it shows that the internal risk is perceived to be much greater than the external risk, and also potentially highlights that this sort of threat is not so straightforward to protect against. Perimeter security such as firewalls and the like do not provide any protection against an in-house threat.

An interesting distinction is also made by respondents – accidental or inadvertent breach by staff was only selected by 5%, indicating that the internal risk from staff is not likely to be accidental but quite deliberate, although there will no doubt still be occasional instances of laptops being lost, and the data on them therefore exposed to risk.
In an attempt to secure their internal data, organizations are deploying a multitude of techniques, the most prevalent of which are permissions and access control (94%), anti-virus/malware tools (91%), strong passwords (84%) and perimeter security (76%). Again the majority of these are focused on protecting from external threats, with only permissions and access control only partially addressing the internal threat from abuse by staff. While it could be argued that abuse by staff cannot be addressed by the toolset listed, rights management solutions do exist – they simply are not being used by many (15%). This could be for any number of reasons – complexity, lack of understanding, or prohibitive cost are possibilities – possibly leaving an opportunity for a new breed of intelligent, automated exception detection and tracking tools. Given the complexity and cost of such a new breed of tools it is unlikely that organizations will be able to deploy these short-term, so it is important that organizations do as much as they possibly can to minimize the internal threat with the tools they already have. Ensuring the correct allocation, and de-allocation, of access rights to content and information is an excellent place to start, ideally by means of a role-based authentication and permission system. Logging of content interactions is also a pre-requisite, as is the analysis of such logs for exceptions and misuse.

An alternative, but even simpler approach, is the password protection of individual files which is performed by 46% of respondent organizations. This approach maintains high levels of protection but is prone to error. Apparently it is not uncommon to find an unprotected version of a password-protected file. An automated agent that trawls the corporate network identifying such files, or even finding unprotected files that contain keywords such as salary, medical conditions, personal, etc. would be a simple but effective first line tool for organizations.

Figure 10: How do you secure your internal information assets? (Select all that apply) (N=211)
Despite the fact that the majority of information that needs to be secured is inside the firewall, no organization is completely insular, and at some stage will see its information go “beyond the firewall”, or move from information at rest to information in motion. This information in motion is not confined to purely sending documents to external contacts but can include email access on tablets, information saved on USB memory sticks, documents saved to cloud-based file-share services and more. As a result securing this type of information requires a different mindset and approach – new security models where security stays with the data, as opposed to housed in the applications, are being deployed, particularly to combat mobile device security issues.

Despite the availability of tools and techniques to secure information in motion, small and medium organizations (<5000 employees) tend to share their information in a relatively free manner (43%), probably due to a number of reasons, such as the need to be responsive and respond quickly to competitive threats, but also in reality because they don’t have the ability to stop, or the means to police staff passing information beyond the firewall.

An argument could be made that smaller organizations do not have the IT budget to deploy techniques such as encryption to manage this data, however, the opposite is true with 27% of small organizations (<500 employees) making use of encryption versus 29% of large organizations (5000+) and 21% of medium organizations (501-5000).

Around 18% of organizations do not allow staff to pass information beyond the firewall. How well this is regulated and whether it actually happens may well be a different matter. On the flip side, this means that 82% are conscious of the fact that they have data outside of their immediate control and are at least taking some measures to manage it.

Figure 11: Which of the following best describes your approach to managing internal data that has passed beyond the firewall? (N=205)

![Diagram showing approach to managing internal data]

Just because an organization has an approach to managing information beyond the firewall, does not necessarily mean that approach is working. As if to reinforce that concept, 28% of respondents claim that they have no way to tell if their approach is working or not, with a further 5% claiming that their organization is not managing their external information at all.

On initial inspection the 45% who claim not to have had any problems delivering their strategy would appear positive. However, a word of caution – if those organizations do not have the right tools in place they may be looking purely at the tip of the iceberg and not aware of the numerous issues that might be occurring under the waterline.

Of further concern are the 17% who see staff bypassing the security restrictions placed on them, presumably a number of whom are sharing information via cloud-based file-sharing tools, such as Skydrive or GoogleDocs. Surely a better approach for organizations in this situation would be to provide this type of sharing facility and create corporate, enterprise-grade accounts with security-oriented cloud file-share vendors and ensure that relevant levels of security are used – which normally are non-existent on freemium versions of the tools.
Information Security for the Modern Enterprise: How safe is too safe? - information lock-down vs sharing and collaboration

Corporate Issues

It is always important to look at the attitudes and culture of organizations in addition to the purely technical aspects of security. From our respondents it is clear that the majority see adherence to compliance regulations (65%) and ensuring the privacy of their customer data (67%) are absolutely essential. These far outweigh the need to be able to collaborate, either internally or externally, which are deemed important but by no means essential.

This highlights the conflict that exists in organizations worldwide: the constant need to balance the creativity and productivity that collaboration can deliver with the overriding need to ensure that the organization remains compliant with required industry or geographical regulations. Obviously the need to remain compliant trumps anything else; an organization that is closed down due to non-compliance is useless.

Therefore, the key aspect of deploying any security strategy within an organization is to find the best balance between remaining compliant and encouraging innovation, collaboration and creativity. No longer can content and information be locked away for safekeeping. Business recognizes the benefits and productivity gains to be gained from effective collaboration, uninhibited content creation and mobile access. Organizations now need to utilize their investment in information infrastructure and selectively expose and mobilize the content that matters: set your data free – but put a GPS tag on it for good measure.

Figure 13: Rate the following in terms of their importance to your organization (N=211)

- Adherence to compliance/governance regulations
- Ensuring privacy/security of customer data
- Ability to collaborate internally effectively
- Ability to collaborate externally effectively
- Ability to quickly create new content
- Allowing mobile access to information

© AIIM 2013 www.aiim.org / © OpenText 2013 www.opentext.com
As a final salutary note we take a closer look at some of the ramifications of getting information security management wrong. The results are quite sobering as almost half of respondents (46%) have seen some form of staff disciplinary action within their organization in relation to information security and over a third (34%) have seen job losses as a result.

To further highlight the importance of getting information security right, 1% of respondents have seen a jail term as a result of a security breach or misdemeanor.

Company punishments have also been seen but in lesser numbers than punishments to employees – a word of caution indeed to all working with information.

**Figure 14: Has your organization ever been involved in any of the following regarding information security? (Select all that apply) (N=199)**

<table>
<thead>
<tr>
<th>Punishment</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff disciplinary action</td>
<td>40%</td>
</tr>
<tr>
<td>Job loss</td>
<td>30%</td>
</tr>
<tr>
<td>Company disciplinary action</td>
<td>20%</td>
</tr>
<tr>
<td>Company financial penalty</td>
<td>10%</td>
</tr>
<tr>
<td>Loss of license</td>
<td>5%</td>
</tr>
<tr>
<td>Court case</td>
<td>5%</td>
</tr>
<tr>
<td>Jail term</td>
<td>Less than 1%</td>
</tr>
<tr>
<td>None of these</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Conclusions**

Enterprise information security is more than just protecting against viruses and hacker attacks. The diverse and collaborative nature of modern business means that information is being created, accessed and shared both internally and externally at a faster rate than ever before – and the consequences of this information falling into the wrong hands have never been higher, or more visible to the world.

A “batten down the hatches” approach is also being taken with regards to the management of external threats, with perimeter security such as firewalls, VPNs and SSL being regularly deployed and the concept that cloud storage of information should be limited to private clouds.

Organizations think that they are secured against the well known threats of viruses, malware and external attacks, often simply because they have deployed perimeter security and internal antivirus software to manage these risks. Where they are less confident is with respect to unauthorized access by staff, suggesting that this internal threat is both harder to identify and to manage.

We have seen that organizations are highly conscious of the need to maintain compliance and ensure the privacy aspects of sensitive data, but in complete contradiction some operate on an information “free-sharing” basis. The need to collaborate effectively is being actioned on a day-to-day basis despite the knowledge that regulations needs to be adhered to.

Something has to give – and this can be seen by the large number of disciplinary hearings and job losses as a result of information security mishaps. However, the frightening knowledge exposed here is that it is not the organization that would typically face the consequences for these mishaps – it is the employee.
The modern enterprise has to adapt. It is no longer a valid strategy to keep important information locked behind closed doors. Information is in motion, internally, externally, on mobile devices, in the cloud – constantly. Understanding this is the first step in being able to develop a security strategy that protects key information in new and innovative ways, enabling the corporation to collaborate, be creative and evolve, while still firmly remaining secure and compliant.

**Recommendations**

1. Identify a “Security Champion” at as high a corporate level as possible. This champion can be used to create the top-down awareness that is required for information security to be treated properly throughout any organization.

2. Perform an audit of the information assets that your organization uses or has access to.
   a. Detail these from the perspective of where they live, who uses them, what value they have to the organization and what the consequences of misuse are

3. Be aware how beyond-the-firewall information sharing can benefit your organization – and include this in your information security strategy.

4. Identify the 3rd party services that employees are using to bypass in-house restrictions – evaluate the benefit in purchasing enterprise licences for these types of tools.

5. Deploy a roles- or group-based permission system for employees and ensure that roles are kept up-to-date, especially when staff leave the organization.

6. Understand that protecting information both inside and outside the firewall requires a rethink in terms of linking information governance and compliance requirements with the information security controls that address information protection. Identify vendors and solutions that can work with you to both develop your information security strategy and then deploy it.

7. Use external consultants to test your security mechanisms

8. Develop acceptable use policies that detail how information can and should be shared. Communicate these with staff and explain the penalties for non-conformance

9. Continually review the all aspects of enterprise security to ensure their continued effectiveness.

**References**

   [http://en.wikipedia.org/wiki/Classified_information#Classification_levels](http://en.wikipedia.org/wiki/Classified_information#Classification_levels)


3. Content in the Cloud - AIIM Industry Watch

4. Data sovereignty vs Cloud adoption
Appendix 1: Survey Demographics

Survey Background
255 individual members of the AIIM community took the survey between October 26, and November 21, 2012, using a Web-based tool. Invitations to take the survey were sent via email to a selection of the 65,000 AIIM community members.

Organizational Size
Survey respondents represent organizations of all sizes. Larger organizations over 5,000 employees represent 28%, with mid-sized organizations of 500 to 5,000 employees at 33%. Small-to-mid sized organizations with 10 to 500 employees constitute 40%. Respondents (32) from organizations with less than 10 employees have been eliminated from the results.

Geography
69% of the participants are based in North America, with most of the remainder (20%) from Europe.
Industry Sector

Local and National Government together make up 23%. Finance, Banking and Insurance represent 14%. IT accounts 15%. Education shows at 5%, with Utilities also at a lower than normal 5%. The remaining sectors are fairly evenly split. Normally, to avoid bias, suppliers of ECM products and services are eliminated from the results, however, given that this report is focused on general information and its security, the views of IT companies are equally relevant and therefore included.

Job Role

The two main groups of respondents for this survey come from the records/document management or compliance/info management fields (39%) and from IT (40%).
Appendix 2: Open Questions

What is your biggest concern regarding information security in your organization?

Selected responses

- A lot of companies still bury their heads in the sand, unless something happens, at which time it’s too late.
- Extremely difficult topic...everyone understands the importance of it, but not always considered a top priority until a problem occurs.
- I think IT organizations are cavalier about data security because they have false sense of control and because their business-critical data is often not personal sensitive data.
- IT folks need to ensure that Records and Information requirements are met -- duration of E-records requires longer retention criteria -- Migration cost is expensive
Underwritten in part by

**OpenText**

**About OpenText**

OpenText provides Enterprise Information Management software that enables companies of all sizes and industries to manage, secure and leverage their unstructured business information, either in their data center or in the cloud. Over 50,000 companies already use OpenText solutions to unleash the power of their information. To learn more about OpenText (NASDAQ: OTEX; TSX: OTC), please visit: [www.opentext.com](http://www.opentext.com).

Organizations are embracing EIM to tap the potential of information to uncover new opportunities, reduce and control costs, gain insight into operations, and impact the top and bottom line. At the heart of EIM, though, is an uncompromising principal that security is critical.

Trust OpenText and EIM to help strike the balance for your organization – fast, easy, and flexible use of information assets and the peace of mind of impermeable information security policies. On-premise or in the cloud, EIM protects vital information assets from unauthorized access and distribution.