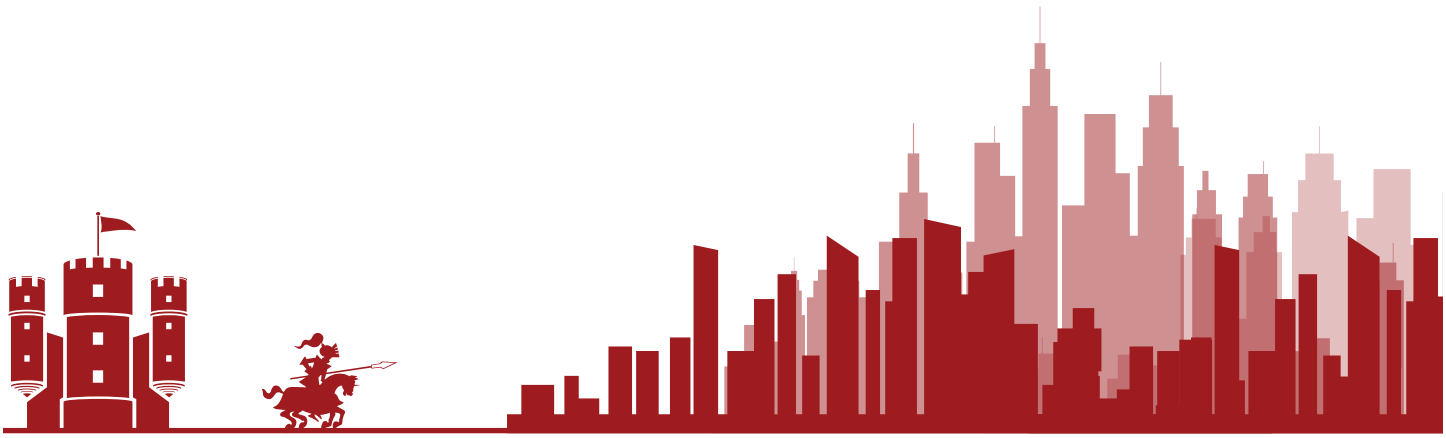


The Enterprise **Rights Management Renaissance**

Aberdeen's research findings show a renaissance in the deployment of enterprise rights management technologies, both currently and planned in the near term. This reflects not only the benefits of persistent controls, to simultaneously protect data while also sharing it more freely in support of collaboration – but also the transformation of enterprise rights management solutions in recent years, to improve ease of deployment and ease of use.

ABERDEEN GROUP | SECLORE

1 Overview

Enterprise data needs to flow freely to the users and business processes that need it, when and where they need it. Accordingly, data today is flowing more freely outside traditional enterprise boundaries.

Aberdeen's research confirms that the traditional tensions between enabling the business on the one hand, and managing risk and compliance on the other hand, are at play in what drives organizations to invest in protecting their sensitive data.

The fact that enterprise IT and security teams are focusing on both, as opposed to just one or the other, underscores the slow but steady shift in the perception of information security from that of being an obstacle, to one of being an enabler.

Aberdeen research provides further insights into the dynamics of data use in the extended enterprise and the ensuing need for it to be protected.

Enterprise end-users do their work from 1.6 devices on average. Further, 2% of traditional PCs and laptops are lost, stolen or unaccounted for before the replacement/refresh cycle; the average for smartphones is even higher at 5%. In addition to lost or stolen devices, security-related incidents are a concern for companies; 75% of Aberdeen respondents experienced one or more incidents in the last 12 months.

The free flow of users, devices and data is growing staggeringly large:

4 billion*
internet users

21 billion*
networked devices

116 billion+
business emails per day

1 billion+**
business email accounts

500+
file sharing applications available at no or low cost in the iTunes App Store

(*) Cisco Visual Networking Index (VNI)
(**)Radicati Group Email Statistics Report, 2013 -2017

2 Rewarded vs. Unrewarded Risk

The types of risks that respondents identified, including the above examples, are grouped into two categories as the top drivers for their current investments in endpoint security and mobile security, as shown in Figure 1:

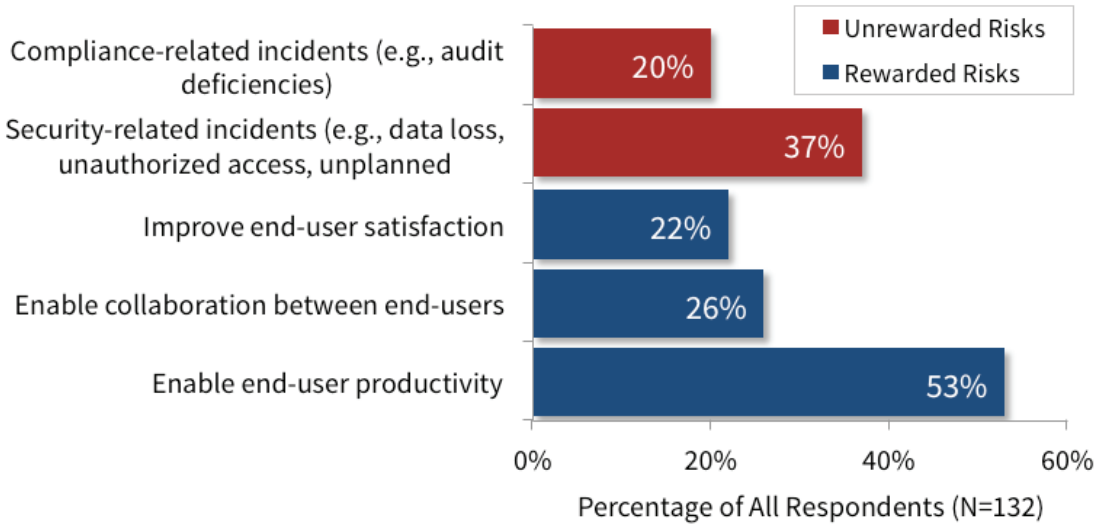
"Rewarded" types of risk:

these enable the organization's pursuit of *productivity, collaboration* and *user satisfaction*

"Unrewarded" types of risk:

these are about protecting the organization from *data loss or exposure, unauthorized access, unplanned downtime,* and *compliance deficiencies* with auditors or regulators

Figure 1: Top Drivers for Current Investments in Data Security



Source: Aberdeen Group, March 2015

3 Strategies for Safeguarding Shared Data

To address the challenging task of simultaneously sharing and protecting their sensitive data, organizations have implemented a wide range of technical security controls – but a closer look reveals that even the most complex mix of technologies actually reflects just 6 basic strategies.

6 Strategies for Safeguarding Sensitive Information

1. **Do nothing:**
   Not all data needs protecting; making identifying and classifying enterprise data an important step in any enterprise security plan

2. **Protect and manage access to a centralized data store:**
   To restrict access to authenticated and authorized users only

3. **Monitor data as it is being accessed and distributed:**
   Utilize technologies like data loss prevention and email/web security to gain visibility into the data that is being accessed and utilized across the organization

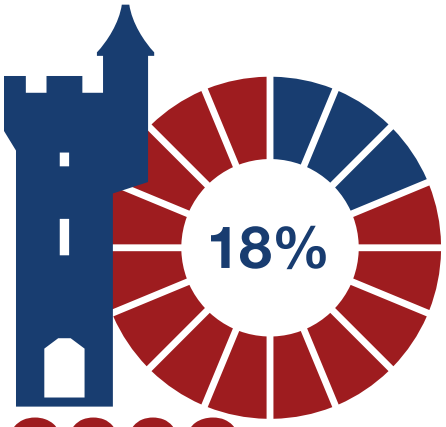
4. **Encrypt the data:**
   At rest in the back-end systems, in motion on the network and in use at a wide variety of endpoints

5. **Substitute non-data for data:**
   Employ technologies such as tokenization, format-preserving, encryption or data masking to take data out of the business process

6. **Apply persistent controls to the data:**
   To allow capabilities for confidentiality, integrity and access controls over enterprise data; this is a key differentiator of enterprise rights management solutions

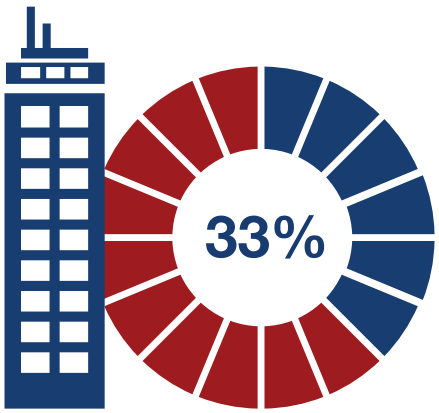
4 Use of Enterprise Rights Management Increasing

Compared to previous years, Aberdeen research shows a significant jump in current implementations of enterprise rights management, as well has strong indications for near-term growth in deployments.



2008

18% of all respondents indicated current deployments of enterprise rights management



2015

33% of all respondents indicated current deployments of enterprise rights management; an additional 17% indicated plans to deploy in the next 12 months

Aberdeen research shows

a significant jump in current implementations of enterprise rights management, as well as strong indications for near-term growth in deployments

5 The ERM Transformation

Why this change in the uptake of enterprise rights management deployment? In addition to the ample motivations provided by disruptive changes in IT and a rapidly changing business context, the capabilities of leading enterprise rights management solutions have also been transforming to become significantly easier for companies to deploy and manage.

Examples of How Enterprise Rights Management Solutions have Evolved to be Easier to Deploy and Manage

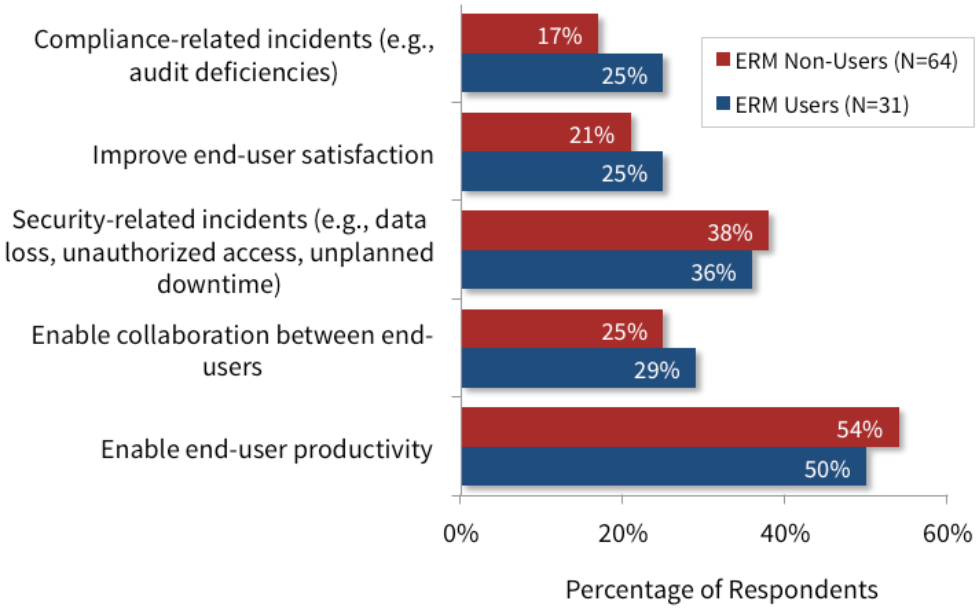
ERM Solution Attributes	Then	Now
File Types	Limited file types, primarily Microsoft Office documents	Multiple file types, including Microsoft Office, PDF, AutoCAD, Visio, and dozens of other file formats
Endpoint Types	Agent-based software; requires direct enterprise management and control	Agentless; easier for the enterprise to control file usage on a wide range of endpoints including traditional desktops and laptops, tablets and smartphones
Scope of Use	Point solution, often devoted to a particular platform or file type	Common infrastructure, with pre-built connectors for DLP, ECM, file shares, and ERP systems
Support for Collaboration	Well suited for internal use, but not as good for external collaboration	Viewers, flexible authentication options, and greater ease of use support external collaboration
Integration with Existing IT Infrastructure	Rigid identity management; e.g., requires user enrollment in enterprise-managed Active Directory	Flexible identity management; e.g., support for authentication using social identities

While enterprise rights management initiatives are not new, disruptive changes in IT have transformed the business context; these changes combined with the ongoing evolution, and transformation, of enterprise rights management solutions make these initiatives even more relevant and adoptable.

6 ERM Creates Value for Organizations

Aberdeen's analysis of 31 organizations currently using enterprise rights management, compared with 64 organizations that are not, shows that all are after pretty much the same things out of their investments for the security of their enterprise data – support for productivity, collaboration and user satisfaction, while simultaneously sustaining privacy, integrity and regulatory compliance.

Figure 2: ERM Users and ERM Non-Users Have Similar Motivations for Investments in Security for Enterprise Data – But ERM Users Experienced More than 50% Fewer Incidents



Source: Aberdeen Group, March 2015

The use of enterprise rights management is correlated with significantly better outcomes.

But here's the upshot: the enterprise rights management users in Aberdeen's study experienced 56% fewer security incidents than non-users over the last 12 months. Motivations and objectives are one thing, but the achievement of results is another – and the research shows that the use of enterprise rights management is correlated with significantly better outcomes.