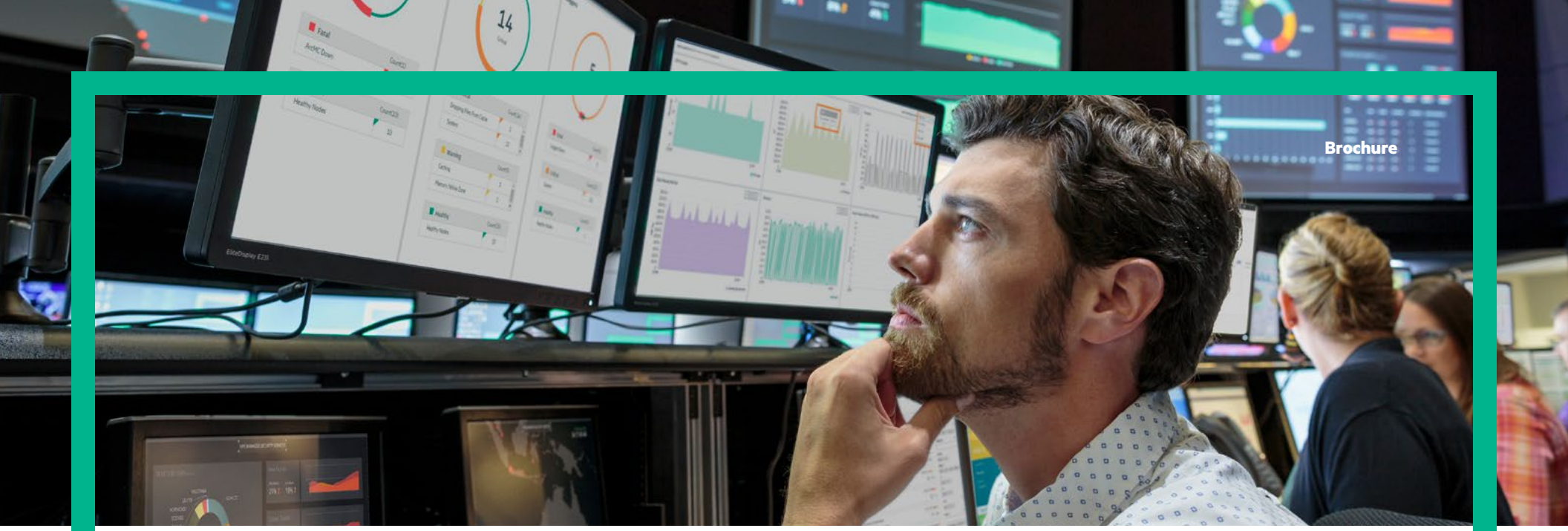


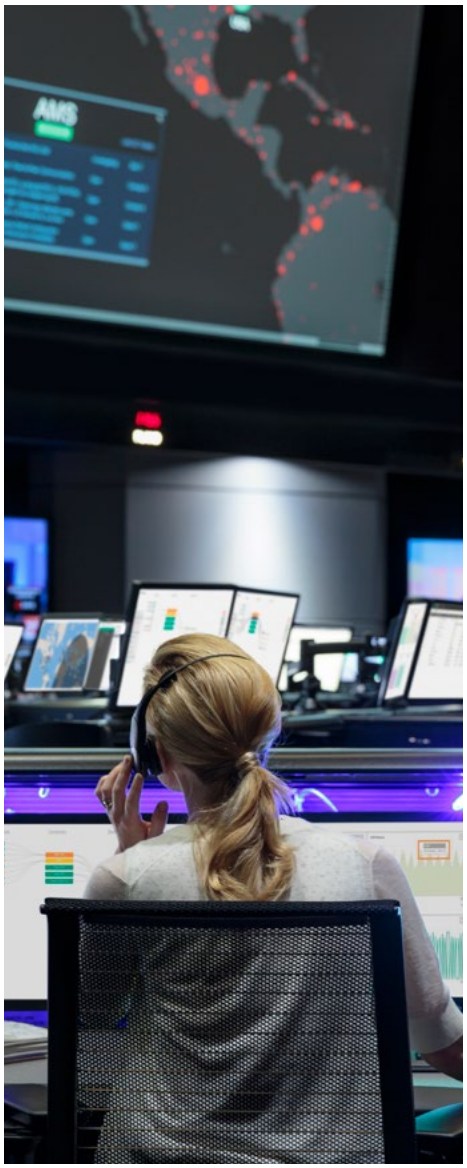
Protect your business with information insight

A better way to manage and govern information

Get started >

Hewlett Packard
Enterprise

Table of contents



This is not the digital dividend you were counting on

You expected more information to mean more opportunities. But with data gushing in today from so many angles—e.g., social media, instant messaging, IoT, emails, texts, streaming video—and at such velocity, more information also means more management challenges. And not just because of the time and investment required to store your data. As data mounts, so does your vulnerability to risk and financial ramifications—if you can't control and protect it.

Based on the results of a recent industry report, 51% of businesses surveyed acknowledged a data-related incident in the previous 12 months, and 50% said a lack of information governance would make it difficult to defend themselves in court over deleted data.[1] Privacy, compliance standards, and business continuity are all under threat, and the related costs can add up fast—from the expense of additional storage hardware to rising regulatory sanctions and legal fees, to the consequences of an overworked staff.

In fact, the solution for defending yourself against the data deluge is present within the data itself. By applying analytics to the information as it arrives, then automatically classifying and sorting what's critical from the inconsequential, you can begin to proactively back up, protect, and manage your data, and make it an asset rather than a source of anxiety.

[1] Association for Information and Image Management, AIIM Industry Watch Survey 2016.

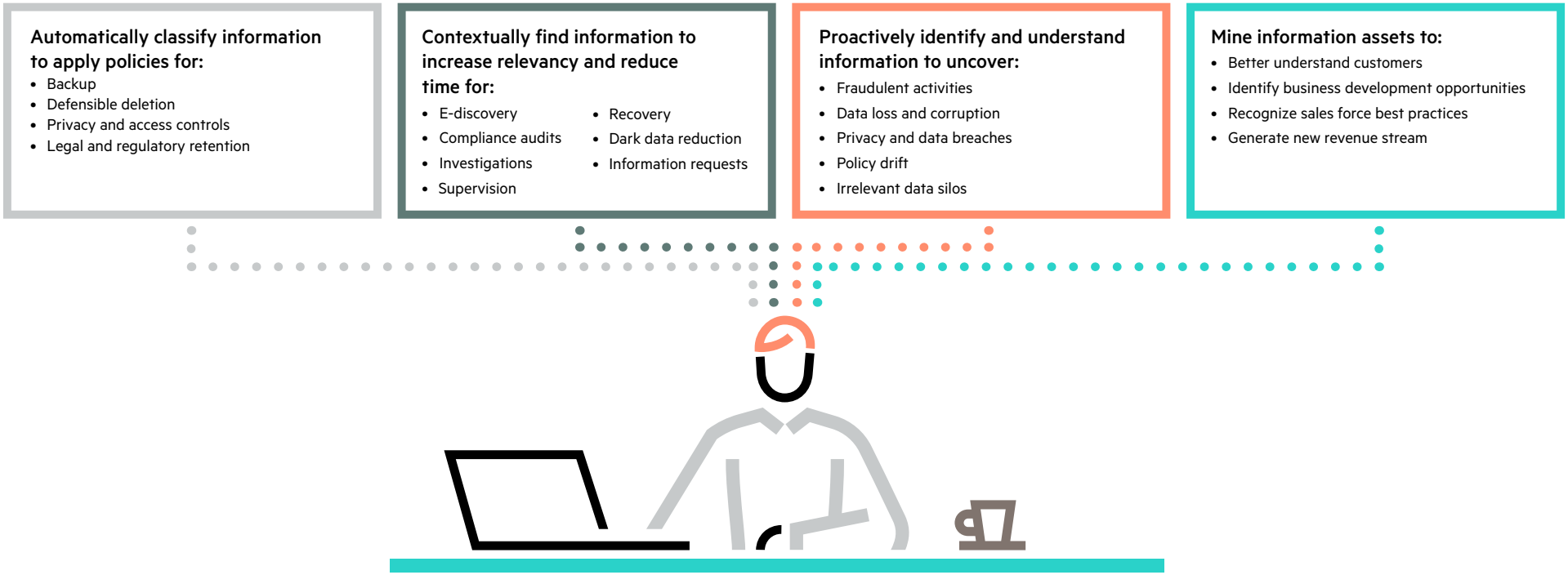


Figure 1. Address the spectrum of risk with analytics

Making a difference with your data

Rethinking information management and governance

With enterprise data piling up at a rate of 52% each year,[2] we're finding that much of what ends up in storage is useless. In fact, the condition has given rise to an industry acronym—ROT, for "redundant, outdated, and trivial." On average, half of the information that organizations retain carries no business value.[3]

[2] IDC, 2016 Data Center Survey, 2016.

[3] Association for Information and Image Management, AIIM Industry Watch Survey 2016.

That's largely due to passive retention practices that allow data to be shunted into siloes, without recognition of what's important to the business. And when the time comes to pick out the data that's needed, you may find yourself banking on ill-equipped staff using inadequate point solutions to search laboriously through the collected mass of material.

Reducing ROT in your data requires clear insight and understanding of information across disparate data types, siloed repositories, and modular data protection solutions—so you can intelligently automate information management, contextually govern data, and uncover areas of risk for the business.

By managing your data with analytics at the core you gain the capacity to respond to numerous vital use cases. Let's take a closer look at some of these:

Average amount reduced from cyber crime cost with the use of advanced backup and recovery

Cost of Cyber Crime 2016: Reducing the Risk of Business Innovation, Ponemon Institute LLC, October 2016.

"Understanding your data is the key to an effective backup strategy and regulatory compliance."

—Data, the lifeblood of the modern digital economy, infographic, IDC, October 2016.

Manage and protect data based on its value

Efficient management and governance through data insights

As we've discussed, traditional approaches to storing and managing data are based on defensive instincts—blindly dumping data into storage without visibility to what's actually there. One common outcome is that organizations generate and keep as many as 10 copies of the same sets of unstructured data. That means more data to store and more storage capacity required to keep it. Consequently, the backup and recovery process slows down, and the cost and complexity of management rises. Another outcome is a mounting trove of "dark data," submerged deep in storage and beyond the reach of our search capabilities.

The solution starts with a modern backup and recovery approach that not only protects your data but provides the analytical tools to classify information even before you choose to back it up. Here's a closer look at how modern backup and recovery can help you establish a position of strength, from which you can apply the policies that sustain efficient management and governance:

- Employing analytics in the backup process, you're automatically gaining insight into the data as it comes in, making ensuing data protection processes more efficient, cost-effective, and reliable.
- Utilizing backup and recovery capabilities within your information management and governance framework, you can optimize your backup environment. As a result, you can automatically dispense with redundant or obsolete data, accelerate the backup and recovery process, and gain visibility into the information that is actually getting used across your enterprise.
- Leveraging these modern capabilities, you gain added benefits such as efficient deduplication for reducing data volumes, policies to support defensible deletion, and access control to meet privacy objectives.

€20m

or 4% of annual revenue

Maximum fine for failure to comply with GDPR

EU GDPR Article 83.

"Implement technologies and processes such as file analysis and archiving to make sure it is possible to comply with requests from natural persons protected under the GDPR and EU supervisory bodies."

—New GDPR Mandates Require Changes to Storage Management Strategies for All Global Enterprises, Gartner, August 26, 2016

Address privacy now

Keeping up with GDPR regulatory demands

Already a tangled web for IT departments around the globe, regulatory compliance has become even more complex with the emergence of the European Union's General Data Protection Regulation (GDPR). The EU policy sets high standards for multi-national organizations—and with the impact of e-commerce, that's a wide net—to keep their customers' information secure with the threat of substantial fines and sanctions.

With a rules-based, unified information management and governance framework, you can classify and take action on sensitive information as required by the GDPR. Using analytics, you can automatically access, understand, and apply governance policies to your data—meeting GDPR guidelines for ensuring that data is backed up at the right time and in the right way.

- With the critical capability of recognizing information in its proper context, you can ensure the proper approach to disposition, and align your governance practices with the GDPR's "right to be forgotten" policy surrounding personal information.
- On balance, by addressing the GDPR standards, you're in a better position to detect and defend against security breaches, optimize backup and recovery, and protect your data wherever it resides—in use, in transit, or in storage.
- Whatever the compliance mandates that you face, using analytics and e-discovery capabilities can provide you with an assertive posture to help you recover information quickly and accurately for legal reviews, compliance audits, and investigations.

2.4m

Average fine for information-related non-compliance

The Cost of Information Governance Non-Compliance, Compliance Week, 2016.

"Information loss or theft is now the most expensive consequence of a cyber crime."

—Cost of Cyber Crime 2016: Reducing the Risk of Business Innovation, Ponemon Institute LLC, October 2016.

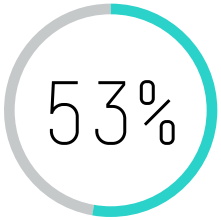
Prediction equals prevention

Using analytics to stay a step ahead of fraudulent behavior

Organizations are under more pressure than ever to avoid fines and sanctions stemming from non-compliant and fraudulent behavior. To guard against legal and financial risk, it's critical to have contextual insight into the information and communications across your organization. But with investigative analytics, you can also make your data work on your behalf—to help you intervene in the type of behavior that can compromise your compliance, endanger your reputation, and lead to significant legal and financial repercussions.

Look for a solution with the means to identify non-compliant behavior within your enterprise, flag it, and take action before the business is exposed to harmful and lasting damage. An investigative analytics platform will provide you with three key capabilities to proactively take on compliance risk:

- **Data lake.** A scalable, elastic data lake comprises indexed data from disparate sources, such as email, IM, and voice archive, as well as structured data from trading, risk, market, and surveillance systems. From the gathered data you can build models and conduct social analysis of employee communication to better understand relationships between individuals and groups.
- **Event-based analytics.** By leveraging analytic functions such as natural language processing, machine learning, network analytics, and linear regression, you can establish an event-based risk framework. With this risk framework you can address scenarios that require unique attention, such as mergers and acquisitions. Such advanced forensics allow you to model and explore behavior to detect non-compliant actions such as insider trading, collusion, and client misrepresentation.
- **Secure access to data.** Investigative analytics help provide secure access to all your critical business information. With audited and secure APIs that are open and extensible, you can maintain access to all the elements of the data lake in order to work with, analyze, and report on that content.



Percentage of IM professionals who agree that using content analytics for auto-classification is the only way to get content chaos under control

Information Management in 2016 and Beyond, AIIM, 2016.

"New content sources are growing at an exponential rate, yet they are the least likely to have retention policies applied."

—A New Set of Challenges Keeps Information Governance Professionals Up At Night, Forrester Research, 2016.

Achieve compliance through automation

Balance collaboration and productivity with information security

In the interest of productivity, you want to embrace collaborative practices and tools that make information accessible to employees and customers. But in the interest of data security, privacy, and regulatory compliance, you are duty-bound to be guarded with much of that same information.

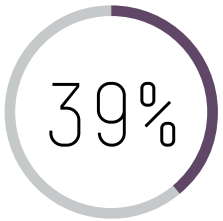
How do you strike a functional—and affordable—balance between productivity and security? With automated content management capabilities that allow you to better analyze and identify sensitive content as it's being ingested, you can reduce the cost and complexity of keeping your information secure while still facilitating collaboration and authorized sharing of business data.

- Most organizations today store content in business systems and database applications without clearly understanding its sensitivity and risk that it might pose. Automated analysis identifies sensitive and high-risk data, categorizes the information, and applies appropriate polices for governing access and retention. By combining powerful search capabilities with policy-based management, the task of finding permissible data comes far easier.
- You can manage your unstructured content—such as emails, spreadsheets, or draft documents—in-place, or move it to a secure repository; and with structured data extracted from database applications, you can apply security and access controls before intelligent archiving. Consequently, real-time access and reporting are supported without the legacy application.
- Automation addresses an often-overlooked facet of content management. The risk of exposing sensitive data increases when apps are retired or databases are duplicated for development and training environments. Automation helps you identify, extract, mask, and secure sensitive data from applications prior to retirement, and makes that data easily accessible for reporting.

$26/GB

Average cost for enterprises to manage unstructured data

The Cost of Managing Unstructured Data, Enterprise Strategy Group, 2016.



Percentage of organizations that now need to restore critical workloads in minutes, not hours

Reinventing Data Protection Fit for Digital Transformation, IDC, 2016.

Analyze to optimize

Improve backup resource utilization and planning

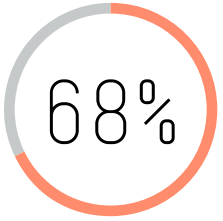
Establishing a backup infrastructure that will support your existing data protection needs is a challenge. But making sure your infrastructure is capable of supporting continued data growth, evolving compliance responsibilities, and the SLAs necessary to keep your business healthy, represents an even higher hurdle if you lack operational control over your backup environment.

Conventional backup operations already capture massive troves of data for your business. Among common issues today: the painful and time-consuming process to get reports that you need, a lack of visibility into what is happening in your environment, and the inability to predict what storage resources are needed—all leading to a lack of confidence that the SLAs can be reliably met.

- With a modern approach that utilizes operational analytics in your backup environment, you can optimize your backup processes and bring these challenges under control. Interactive web-based monitoring and reporting provide you with centralized management and tools for visibility such as dashboards, graphs, and charts on backup performance and capacity utilization.
- With expanded insights, you can simplify the task of managing multi-cell deployments, identifying operational inefficiencies, and forecasting resource conflicts before they lead to problems such as outages or data loss.
- Greater control over the backup process includes the ability to run what-if scenarios to determine how your environment would respond to changing SLAs, identify impacts to the backup infrastructure, and reveal the best ways to balance the demands of new data within the existing infrastructure.

Framework and solutions

A unified information management and governance framework bridges data silos and provides analytic tools and applications to help convert normally passive information into valuable big data assets.



Share of organizations that believe the risk of information-related compliance fines can be reduced by investing in information governance software or technology

The Cost of Information Governance Non-Compliance, Compliance Week, 2016

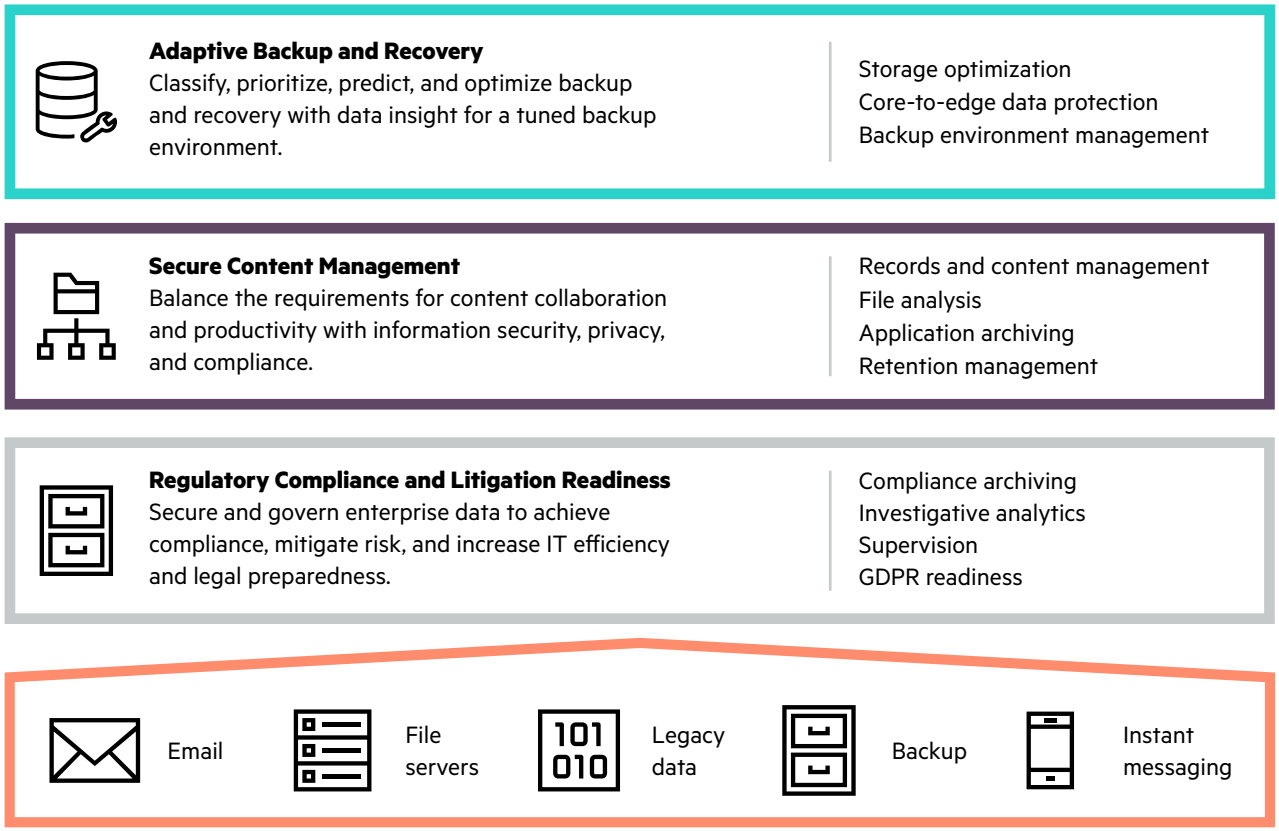


Figure 2. Information management and governance solutions

A framework for the future

As the volume and velocity of enterprise data run rampant, and regulations become more stringent, conventional methods of information management and governance have become outdated. It's no longer viable to store, safeguard, and search your information effectively from a passive posture. By applying analytics to enterprise data, HPE has built a unified framework for advanced information management and governance. By taking a modern, proactive approach, you can automate information management, contextually govern data, and actively protect your business from risks.

Adaptive Backup and Recovery

Actionable insight and operational analytics power our Adaptive Backup and Recovery (ABR) suite designed to efficiently manage and fine tune backup environments. The ABR suite is comprised of three companion software products: Storage Optimizer manages data based on its value; Data Protector provides comprehensive, high-performance backup and recovery across complex, heterogeneous environments, and Backup Navigator helps analyze and efficiently manage backup environments. Together, they leverage operational analytics and data insight to lower risk and cost, enabling a tuned backup environment for today's dynamic data-driven enterprise. With the ABR suite, customers gain a 360-degree view of their backup environments and constant tuning of processes.

Learn more

Secure Content Management

Our Secure Content Management suite helps you balance collaboration and productivity need s with information security, privacy, and compliance across enterprise systems with reduced risk, complexity, and cost. Content analysis identifies sensitive and high-risk data, categorizes that data, and then applies policies to govern access and retention to the data. Powerful search coupled with policy-based management makes it easier to find the permissible data you are after. Unstructured content can be managed in-place or moved to a secure repository while structured data extracted from database applications has security and access controls applied prior to intelligent archiving. Real-time access and reporting are supported without the legacy application.

Learn more

Regulatory Compliance

Our Regulatory Compliance solutions include hosted archiving, supervision, e-discovery, and investigative analytics in a private cloud, and is a core component of our information governance portfolio. Compliant archiving manages and controls data across multiple channels and information repositories to enable compliance, mitigate risk, increase IT efficiency, and support legal preparedness. This suite enables intelligent and insightful data visibility to support access, retention, and disposition of information, while incorporating policy management, e-discovery, legal hold, advanced search, end-user access, and supervision.

Learn more

With HPE, you can gain proven information management and governance—visibility and control that are enabled by analytics, allowing you to identify, understand, and protect the data that matters, and be prepared to keep your business out of harm's way.

Learn more at
hpe.com/software/img

Sign up for updates

Hewlett Packard Enterprise

a00001980ENW, March 2017