Publication date:
Jan 2021
Author:
Maxine Holt
Andrew Kellett

Businesses Need a Smarter Approach to Data Protection

Data protection is the “one constant” that must be maintained across all environments

In partnership with:
helpsystems

Brought to you by Informa Tech

Contents

Summary

Data protection is the “one constant” that must be maintained across all environments

Organisations hold and are responsible for safeguarding vast amounts of data. This data must be appropriately protected, irrespective of its type or location.

To do this effectively and remain within the boundaries of regulatory compliance, organisations must have the ability to accurately identify, classify and protect data. An integrated combination of process and user-centric people-based capabilities are required, alongside technology, to deliver relevant data protection strategies for each business and its users.

The imperative to keep businesses and data safe while facilitating access and usability for all user groups has never been more challenging. The requirement to maintain essential and mandatory levels of data protection demands facilities that can operate seamlessly across all platforms and infrastructures.

Key messages

- Organisations remain responsible for protecting their data.
- Even before COVID-19, the need for remote working was well established.
- Data protection requires robust technology and human expertise.
- Flexibility hindered? Safety and efficiency must coexist.
- A growth mindset is required to accelerate digital opportunities.
- Data protection must adapt to reset normality.
- A combined technology and user-centric people-based approach is needed.

Data protection is essential, irrespective of circumstance

Organisations remain responsible for protecting their data

Organisations continue to generate vast quantities of data without always realising it is happening or, if they do know, often fail to fully understand the value of the data involved and the potential business risks it brings.

As technology advances continue to deliver business benefits, working environments and data storage systems simultaneously change and evolve. Businesses must balance the need for operational flexibility and openness, enabling their services to compete and remain profitable across global markets, with the regulatory requirements on them to protect data and keep the business safe.

As data volumes and originating sources grow, so the problems associated with data management, control and protection also multiply. Specifically, an ever-growing percentage of business data is now generated from external sources. These include remote and home-office locations, mobile workers generating information from multiple sites, customers and business partners.

In addition, well-managed cloud storage systems add mainstream flexibility and security benefits to enterprise operations, but their flexibility and ease of use can also expose corporate vulnerabilities. This is especially the case if separate and locally authorised facilities are set up and maintained away from central jurisdiction.

Irrespective of source, ownership of and responsibility for data remains with the business. The offices of the chief data officer and chief information security officer have shared responsibility for enterprisewide governance and utilisation of information as an asset and the security, protection and authorised use of those resources.

As data is generated and utilised it requires protection. Maintaining the confidentiality, integrity and availability (CIA) of data within an organisation is essential. To fulfill these obligations, strong usage and protection facilities are required to give appropriate and safe access to information, whenever and from wherever it is needed. Stakeholders should expect automated protection facilities to be in place that help define, measure and mark the status of data to ensure that it is maintained within secure and authorised repositories.

The data footprint grows across the complete data lifecycle as it is shared, updated and added to and as access is extended to external users. With this, stakeholder responsibilities increase alongside

the need for security controls that meet both the sensitivity of the information involved and its potential for theft and exposure.

This report assesses risk and data protection requirements in light of new business demands, changing working environments, and current and future operational constraints. It considers how new and updated levels of data protection are needed to fit in with specific business, security and regulatory demands.

Even before COVID-19, the need for remote working was well established

The need for remote working was well established before the COVID-19 pandemic. It was consistently being driven by the twofold efficiency and usage benefits that could be realised by businesses, their partners and users.

The immediate impact of COVID-19 was to change the remote-working dynamic. It abruptly moved from the comfort zone of active ongoing change, in line with identified business benefits, to a cliff edge of necessity. Those forward-thinking organisations that had already invested somewhat in remote working had a head start; nevertheless, few were able to position themselves as fully prepared for the business continuity demands of the pandemic.

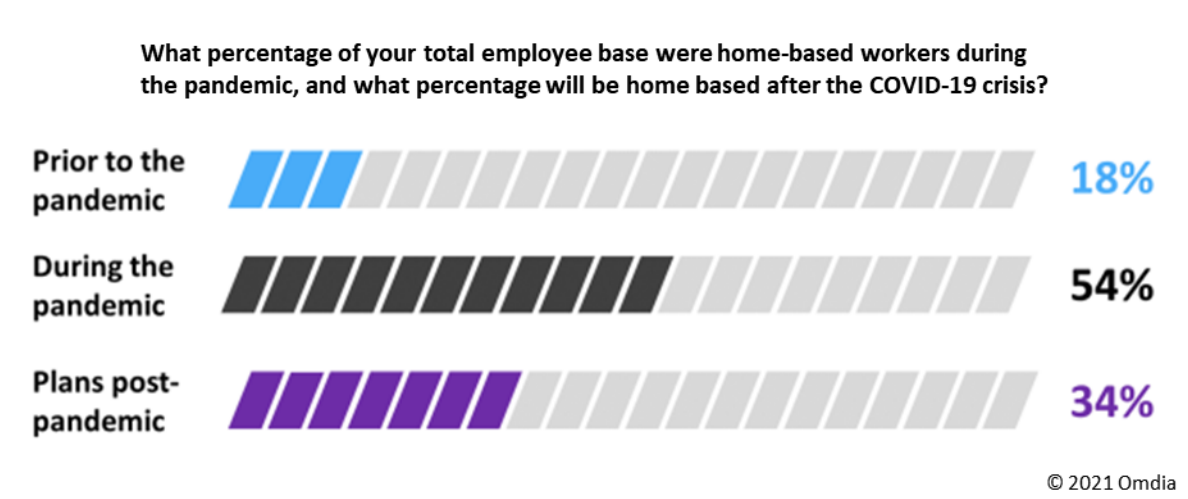
Typically, organisations found that existing technology was unable to cope with the so-called “new ways of working.” Accessibility, bandwidth and usage demands spiraled. Organisations were forced to prioritise essential users and services that would keep the lights on and the business running. As a result, the initial priority of achieving continuity and maintaining levels of service that would save the business from being unable to operate often came at a cost to security and regulatory considerations.

Immediate and ongoing priorities have included working to ensure safe access and functionality for users. Specific usability and continuity requirements include

- Provision of access for previously unimagined numbers of users working away from the office
- Maintaining safe access from a mix of business and privately owned devices and from a difficult-to-control range of locations
- The need to offer high volumes of all-day, every-day access and support for customers looking to buy goods and services online or access information about those goods and services
- The ongoing and future issues of managing mixed remote and office working environments
- More challenging longer-term opportunities to remind users and keep people updated on data protection responsibilities as a greater proportion of remote working becomes the norm
- Keeping security and regulatory requirements at the forefront of the business mindset to affect how people are thinking

After experiencing an extended period of COVID-19 restrictions, both employees and employers expect that levels of office working are unlikely to return to prepandemic levels. The working environment in the reset normality must be reviewed to recognise data protection lessons that still need to be learned and identify additional benefits that can be achieved going forward. Omdia research clearly shows that expectations are that postpandemic remote working will almost double from prepandemic levels (see **Figure 1**).

Figure 1: Approaches to remote working



Source: Omdia

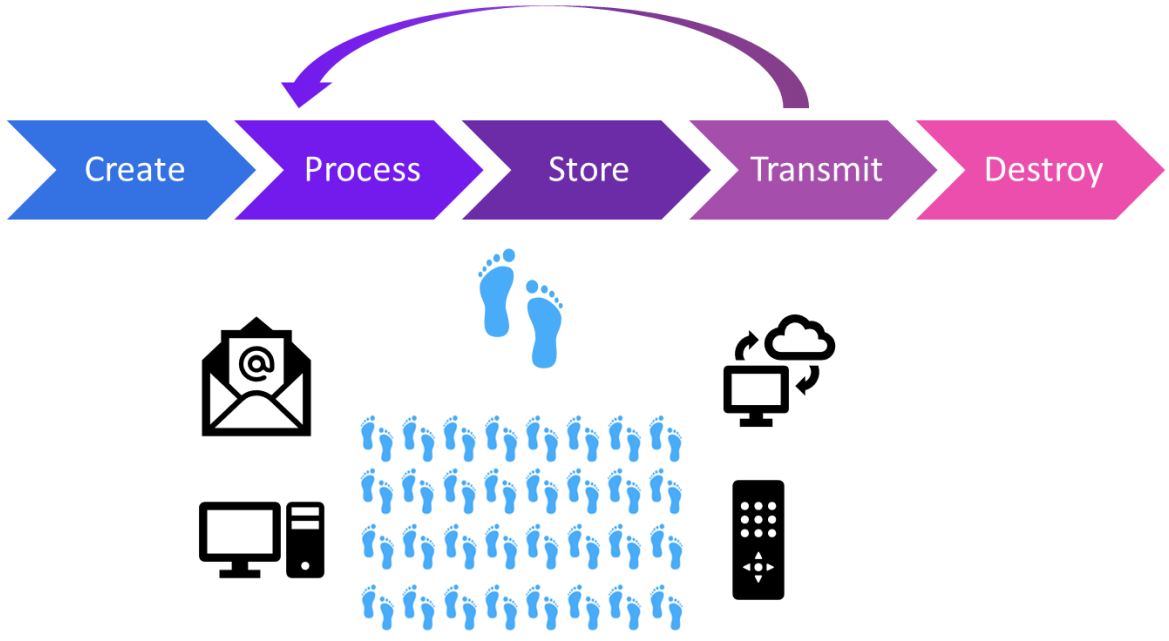
Short-term security compromises that were necessary to keep business operations viable during the initial stages of the pandemic are now being reviewed by data protection professionals to maintain and, where necessary, improve remote working services. Remedial actions against any vulnerabilities or weaknesses found will be needed before organisations can move onto the next stages.

People, process and technology all play a role in data protection

Data protection requires robust technology and human expertise

The information lifecycle gives rise to a significant footprint (see **Figure 2**).

Figure 2: The information lifecycle creates a significant footprint



Source: Omdia

Technology is required to address this footprint of information. However, automation and technology are less effective when used in isolation. Better results are achieved from a combined people, process and technology approach.

Robust, efficient and business-ready data protection technology is available to organisations today. Combining good data protection technology with human expertise and processes provides benefits that include

- The ability to integrate technology-based automation alongside the knowledge, usage and efficiency requirements of data creators/owners with responsibility for the data and how it is used on an everyday basis
- Using technology-based automation to assimilate knowledge about data and apply rule-based controls that fit the current and expected future needs of the organisation without imposing additional operational overheads
- The delivery of security that meets the data protection requirements of all data classification types and levels

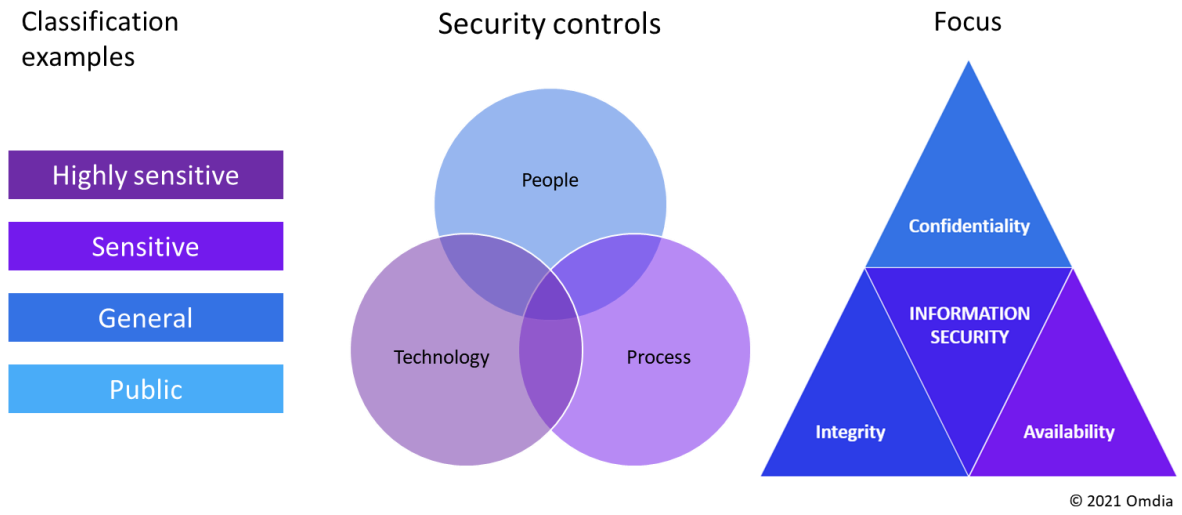
Combining people, process and technology covers key data protection and control requirements: understanding and managing data, the breadth of coverage that needs to be supported on a local and remote basis, and suitability for working alongside stakeholders and user groups.

Across the majority of organisations, data creators and users (the human element) bring in-depth knowledge of data and information and play an important part in how it should be categorised for future access and use. These data protection contributions provide the ground rules under which automated protection and access control rules are applied.

In addition to initial insights into the data they generate, in order to provide a fully rounded contribution toward the protection requirements of their data, stakeholders must understand the data protection policies of their organisation. This is needed to ensure that correct levels of shielding are applied at source and can then be extended to the ongoing protection needed as data is used and its risk of exposure increases.

No two organisations and their data usage requirements are the same. Thus, when considering levels of data responsibility required across the workforce, all types of data and levels of protection must be considered. Consistency of use and secure data sharing need to be supported across the business so that data can be protected appropriately (see **Figure 3**).

Figure 3: Applying appropriate protection to the CIA of data and information



Source: Omdia

Data protection that fits each organisation and its everyday needs is required. Higher levels of protection are a must for top-secret and business-sensitive data and for data categorised as personally identifiable information (PII), considering the impact it has on the business and its ability to maintain regulatory compliance. The combination of local knowledge and technology-based automation is required to assess threats and determine risk.

Organisations now need to be looking at the extended impact of high-volume remote working, what that could mean to existing security and regulatory controls, and how physical and digital protection will need to be treated across the enterprise.

There are important steps that C-level security leaders will by now have considered, such as ensuring that they have made changes to business operations while remaining compliant with the data protection rules that apply within their sector. This involves working through all appropriate regulations (e.g., GDPR, SOX, PCI DSS, HIPAA and more) to prove that the processing of data is compliant. One way of demonstrating the right levels of accountability when processing sensitive data is through a data protection impact assessment (DPIA) on all new areas of risk and new operational approaches.

For each new activity a DPIA should cover the data protection risks involved, the necessity and benefits of the approach, mitigating actions that can counter the risks, and confirmation that protective actions are effective.

Each assessment needs to be designed to be flexible and appropriate to the changes involved. It should be reviewed on a regular basis and be updated in line with business and regulatory requirements and future changes.

Flexibility hindered? Safety and efficiency must coexist

Few organisations remain unaffected by the COVID-19 pandemic. Many are having to make significant efficiency savings, with budget and recruitment activities likely to be constrained for the foreseeable future. This being the case, organisations will, by necessity, be more selective than ever about their technological investments.

Areas where organisations ought to consider making further changes and where they should invest in technology as part of the security controls to keep their operations safe and efficient include

- Further efficiency changes to meet new productivity targets and to extend remote-working strategies to meet the distributed operational needs of the future
- The delivery of efficiency benefits that do not leave the business short on regulatory protection
- Continued focus on business context and the ability to understand data and risk
- Smart data protection facilities to make the right decisions on access and availability
- Technology-based efficiency and automation (where appropriate) to adequately support ever-increasing volumes of data

There is an ongoing need to identify and maintain control over organisational data. Enterprise-level data protection must extend to an in-depth knowledge of what data is held and where, and what changes to security controls are needed to keep the data safe.

Beyond the high-level requirement to protect confidential and sensitive data, businesses must also apply data protection rules that are applicable to PII, which is gathered, used and stored by almost all businesses. Organisations must make better use of data protection tools to identify PII and where it resides. It should be classified for sensitivity and level of threat, acceptable usage policies should be established and appropriate levels of protection added, and these should be backed up with regular user training and education.

Establishing PII culture takes clear thought and action and cannot be achieved without a defined line of responsibility that starts from the top of the business and brings together the responsibilities and skills of stakeholders and users at all levels.

From a data protection perspective, businesses are required to manage all forms of data appropriately, including ensuring that it is not lost or accessed by unauthorised parties. Failure to comply can involve a heavy fine and, potentially, severe damage to corporate reputation.

The need for data protection that takes into consideration human factors and the requirements of all users, particularly those who are identified as being vulnerable or susceptible to threats, is paramount. It is also interesting to look at how corporate culture has a role to play. We can define how well security culture is treated within offices, how policies around data protection are enacted,

and so on. However, it will not be much of a surprise to find that those entities that do not do well within the corporate firewall also struggle to extend security coverage to remote working.

A growth mindset is required to accelerate digital opportunities

Like all sectors of the community, businesses initially struggled to make their data operations COVID-19 safe during the early days of the pandemic. Nevertheless, those with forward-thinking technology development strategies are now embracing the opportunity to "reinvent" data protection and flexible user access as the impact of the pandemic continues.

Those organisations that maintained a prepandemic fixed and inflexible mindset on the protection of data and user access are already finding it more difficult to recover and harder to provide their users with the tools needed to do their jobs, and they will continue to be slower to respond to customer requirements.

Many organisations started out with concerns that the infrastructure systems they had in place would not be sufficiently robust to deal with the new working practices needed to keep their operations running. Other concerns included maintaining channels of communication with business clients and customers, and that data protection and regulatory-requirement timescales could not be met, with responses to information requests taking longer than would normally be acceptable.

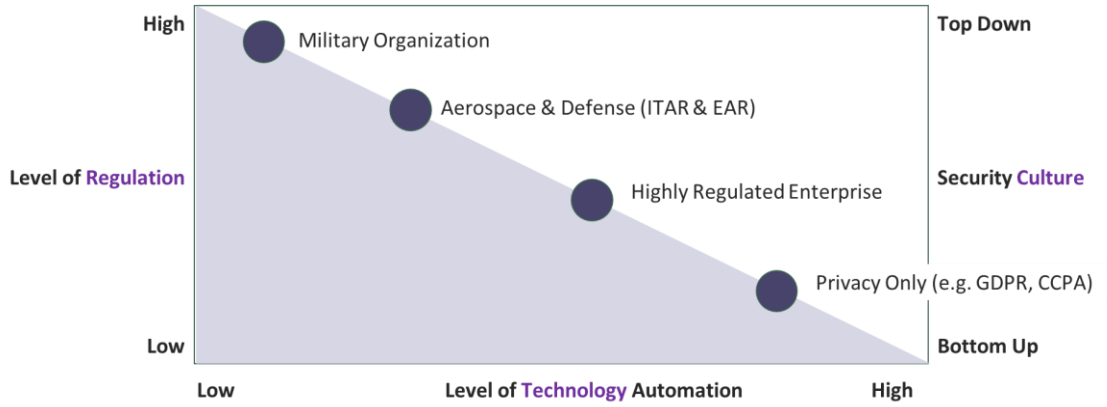
Regulatory bodies were unable to formally extend statutory response timescales. However, there is evidence to suggest they made communications channels available to inform people that understandable delays might be experienced during the pandemic because businesses were working under extreme levels of pressure.

With significantly more staff working remotely during the pandemic, businesses that were able to deal with the extra demands quickly identified that there were clear business benefits to be gained. They also began to understand that data protection was not, in itself, a barrier to increased levels of remote working.

Data protection laws do not prevent increased levels of remote working, but in many cases improvements to security and associated data protection facilities are necessary. Organisations must ensure that remote workers, their devices, and their communications facilities are as well protected as in the office.

Many of these businesses will look very different in the postpandemic era. By necessity, the survivors are going to be smaller and leaner. They will need to improve operational efficiencies through the use of automation, including investment in data-driven digital access technologies and cloud. However, automation is not a one-size-fits-all approach, and different types of organisations will face various levels of regulation that will affect how much automation can be applied (see **Figure 4**).

Figure 4: Automation is not a one-size-fits-all approach



Source: HelpSystems

The intended outcomes of these investments must be to deliver agile, automated operations with the variable cost structures needed to build back strength and profitability while maintaining safe and secure customer services.

All organisations will need to focus on the results-driven benefits new and extended working practices can provide and use these as opportunities to improve competitiveness and growth. Safe user and data access must be at the center of these strategies.

Approaching data protection in a postpandemic environment

Data protection must adapt to reset normality

Wherever organisations and their staff choose to work from, one fact is indisputable: they will collectively generate more data than ever before. Some of that data will be top secret or business sensitive. By far the greater part will be regular business data, but it will still need to be analysed and protected because of the PII material it contains. The sheer volumes involved make it ever-more difficult to protect sensitive information and drive an urgent need for more inclusive and more automated forms of data protection.

Through necessity or indeed choice, many organisations will operate with fewer office-based staff. If project and productivity targets can be met remotely, workers may not be required to attend an office every day, and a hybrid approach enabling rotational office working and hot-desking will come into play.

Potential security and business protection issues that need to be addressed include ensuring that remote working is not considered by enterprises as a “get-out” clause when regulatory failures occur. During 2020 organisations had to adapt very quickly to new remote-working practices, which in turn may have led to normal policies and procedures not being strictly adhered to. Potential security breaches caused by human failures become more likely, for example, accidentally sending private data to incorrect recipients when using personal devices without data loss prevention (DLP) technology and/or not following company policy. Specific data creation and linked protection facilities need to be considered for all remote workers.

Security and data protection awareness and education for all staff must be extended but must exist at a level that is workable and does not interfere with productivity. Data protection systems are required that offer consistent levels of protection and include DLP-type controls to ensure data transfer is limited to authorised recipients and to reduce accidental failings.

To protect data, organisations must be fully aware of its existence and the risks around it and retain the capability to scan and analyse data at creation, in transit, when it is shared between users, and when it is stored and at rest. Facilities are needed to maintain appropriate identification attributes, apply and detect metadata and prove regulatory compliance.

Data classification facilities should be in place to support an effective information governance strategy. All data needs to be classified so it can be managed and handled appropriately. By

identifying the true value and protection requirements of data, organisations are able to make intelligent decisions on how to safely handle it.

Increasing automation of these products helps improve processing efficiency and reduce the burden on frontline security and data management staff, enabling them to spend time more productively on core business objectives.

A combined technology and user-centric, people-based approach is needed

Good quality and inclusive data protection is a necessity for all organisations: the detection and protection of personal data goes beyond well-formed data types such as bank account and credit card numbers. Personal data is often highly contextual and includes personal, national and highly sensitive information including health, security and, more recently, social media links.

Approaches and levels of protection are dictated by factors such as sector of operation, type of business and sensitivity of data held. Context and stakeholders are also key considerations. The ability to understand and consider all relevant data issues is important; these include data origin, usage requirements, sharing issues and timelines. The ability to work with stakeholders and users to understand data protection requirements and policies is a key part of the overall data protection picture.

Developing and building out the combined technology and user-centric, people-based approach to data protection is not straightforward. There is no natural synergy between the rules-based automation that technology offers and the way that stakeholders respond when adding new information or data types.

Culture and the integrated use of technology is a subconscious thing; it must be embedded and automated wherever possible. Delivering the best combination requires the right policies to be in place. To drive integration and automation as quickly as possible, the balance between “it just needs to happen” and “at the right time” should aim to become seamless. For example, data classification tools not only help organisations protect their data by applying appropriate security labels but also help educate users to understand how to treat different types of data with different levels of classification and sensitivity.

Employees play a vital role in ensuring the enterprise maintains a strong data privacy posture. To achieve this, organisations must provide regular security awareness training with the objective of changing behavior in the protection of sensitive information. The security culture of the firm must be inclusive for employees, ensuring continuous training and education so their approach to security becomes part of everyday working practice, and security is embedded into all actions and the ethos of the business.

The successful balance is less about full automation than about the unified interaction with valuable user input at the right time. Just-in-time intervention delivered through knowledge-based awareness and process can deliver the right combination and can help to educate those involved and provide a strong and valued learning experience.

Appendix

Author

Maxine Holt
Senior Director, Cybersecurity
maxine.holt@omdia.com

Andrew Kellett
Associate Analyst, Cybersecurity
andrew.kellett@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About HelpSystems

HelpSystems is a software company focused on helping exceptional organizations Build a Better IT™. Our cybersecurity and automation software simplifies critical IT processes to give our customers peace of mind. We know IT transformation is a journey, not a destination. Let's move forward. Learn more at www.helpsystems.com.

In June 2020 HelpSystems acquired Boldon James and Titus. Through this acquisition HelpSystems added best-of-breed specialists in data classification and secure messaging to its data security solutions portfolio and now delivers globally recognized innovation, service excellence, and technology solutions to a worldwide customer base.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, and agents disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.