RANSOMWARE RECOVERY MANAGER

THE CHALLENGE

It is no longer a matter of if but when ransomware will strike an organization. CISOs today are bracing for long-term impact and Board Management is requiring many to have full disaster recovery plans in place. With majority of these plans focused on perimeter solutions, employee training, and internal monitoring and threat analysis to detect in-progress events, organizations are still vulnerable to attack even with appropriate measures in place.

Ransomware remains one of the costliest IT security problems of the modern-day business and even with hefty budgets for mitigation tools, protection for the endpoint can be left exposed. The consequences of an attack can be severe, and there's no guarantee that organizational data will ever be recovered, even if the ransom is paid.

THE SOLUTION

Organizations must plan for the post-event and expecting the eventual failure of controls is the best defence. Data443 Ransomware Recovery Manager is the only industry solution that actively recovers the device, operating system, and data with a simple reboot. Using patented, proven technology, the product produces 100% effectiveness for the whole device and datasets.

Coupled with Data443's Data Identification Manager and Secure Content Manager Solutions, this offering is designed to identify all types of data on a device and encrypt it at rest, ensuring that even with potential exposure of the data set(s), Ransomware Recovery Manager's dual-private key infrastructure safeguards your files, rendering them useless in the hands of attackers without matching keys, consequently greatly mitigating the extortion risk of any ransomware scenario.

Leverage Ransomware Recovery Manager and save your organization from:

- Lateral spread
- Breach exposure and associated ransom risk
- Public data exposure
- User productivity loss
- Manual IT cleanup, including reimagining machines
- Governmental Fine, Civil penalties and lawsuits
- Personal, Employee and Customer data Extortion Risks
- Lateral movement is denied by machines not carrying infection, stopping spread of attacks
- No IT assistance is required to restore operations

ONBOARDING

- Deploy from Data443's Cloud for instant delivery & management
- Deploy from your favorite software distribution software or use Data443's
- Design a simple Data Loss Prevention (DLP) policy with our design team or manage your own
- Design a simple Data Classification policy set, or use our workshops to design with industry best practices
- Configure your encryption and protection policies

KEY FEATURES

- Alert & Infection Recovery Notifications
- Centralized management of all endpoints from a single console
- Manage all functions of PC capability, including DLP, reboots, updates, remote control, and power savings
- Restore workstation to last known safe state, even after a complete infection of virus or ransomware attack
- Full encryption of all sensitive data sets – even if egressed
- Data Classification, tagging and labelling built in

HOW IT WORKS

Using patented and patent-pending technologies, Ransomware Recovery Manager utilizes portions of the devices' local disk to snapshot continuously and repeatedly (by policy) to ensure a completely recoverable device. Upon any reboot action –from infection, from user, or from IT Admin actions- the device is analyzed against policy and previously known stable configurations and is restored against deltas. Primary boot partitions and other aspects of the boot device are not able to be bypassed, ensuring a complete recovery in every scenario.

With Ransomware Recovery Manager, data that is stored within the recoverable data portion is salvaged, and any sensitive data that is encrypted is also restored if egressed encryption policies still apply.

BENEFITS

- The only industry guaranteed virus and ransomware device and software recovery platform option
- Options for cyber & risk insurance reductions
- Business Loss and labor utilization protection
- Customer/patient and other data set protection built in
- SLA and other performance metric protection
- Little to no risk of extortion risks
- Sensitive data identified, double key encrypted, then placed in secure locations on a disk, so ransom demands have little to no impact
- Ingesting of additional file repositories ensures audit compliance for long term retention requirements – including roll offs of any data set as required
- Rapid data consolidation, ROT analysis and management
- Specific IT security and data policy enforcement – across the entire data estate
- Select user roles and permissions based on your customizations
- Search and extraction are based on the entire data estate that in attached to the platform

ABOUT DATA443

Data443 Risk Mitigation is a leader in data security and privacy management – a critical element of IT security protecting access to All Things Data Security™ across the enterprise and in the cloud. Data443 provides the necessary visibility and control needed to protect at-scale, obtain compliance objectives, and enhance operational efficiencies.

101 J Morris Commons Lane, Suite 105,
Morrisville, NC 27560

data443.com
info@data443.com

Toll Free
+1 855-DATA-443 (855-328-2443)

US
+1 919 526 1070

UK
+44 203 7693 700

DATA IDENTIFICATION MANAGER

THE CHALLENGE

Despite efforts by organizations to increase security parameters, the threat landscape is still ever evolving, and business face heighted challenges around cyber-resilience. This expanded attack surface has generated numerous privacy, data protection, security and compliance questions, which are driving organization's to ensure their digital transformation programs are not only secure, but forward looking.

In regulated environments, privacy requirements force examinations of all aspects of data infrastructure: where data is, who has access to it, how sensitive it is, and how quickly it can be accessed. A strong security posture must now take these aspects into consideration while being able to control, manage and report on them.

As organization accelerate their adoption rates, many Security, Operation & Compliance teams lack the cross-platform visibility and controls needed to efficiently manage their data and follow best practices around data governance and management. This challenge is heightened by lack of automation, in which customers are leveraging entire teams to manually search and find data, resulting in human-errors, failed audits, loss of insurance coverages, and heavy fines.

Particularly in large enterprise environments, investments in vendor technologies have proven ineffective, and having an inconsistent approach to managing data can quickly become a fatal security risk and obstacle to operational efficiency.

THE SOLUTION

Data443 Data Identification Manager is a solution that reduces risk by shining a light on dark data across cloud, on-premise and hybrid environments. From a centralized dashboard, Data Identification Manager provides the ability to automatically inventory all data repositories, classify & tag all data, and enable global search and discovery – all through an agentless deployment.

Data Identification Manager leverages 900+ sensitive out-of-the-box data types in 14 languages and applies artificial intelligence (AI) to move data from exposed locations automatically based on sensitive data rules. This allows organizations to continuously access their data, assess excessive permissions and identify potential high-risk assets without disrupting business operations.

ONBOARDING

- Immediate, automatic
- Less than 2 hours to full deployment and solution value
- Self Service for Target Additions
- Immediate reporting as data comes in
- Live Online & Scheduled Expert Classification Design & Workflow Engineers
- Dynamic Compute Scaling automatically

KEY FEATURES

- Single, centralized dashboard for all environments
- Connect to hundreds of Repositories
- Apply Classifications – Tag and Label as needed
- Perform Global Search and Discovery across all unstructured and structured datasets
- Perform Migrations, ROT analysis and full data governance – with all datasets in mind
- Train the ML Libraries with your own datasets – hone classifications and execution of governance policies

HOW IT WORKS

Data Identification Manager is deployed via Data443's private cloud, your cloud, or on premises. With only a remote connection to the datasets needed, Data Identification Manager offers immediate deployment and rapid time to value.

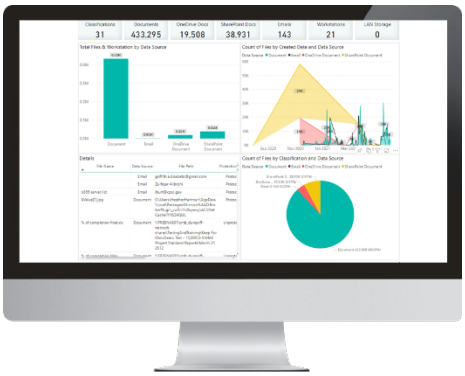
Utilizing our patent-pending archive extraction, parsing and indexing technologies, our indexers rapidly analyze and compress the inbound datasets and immediately present them as available for search and queries. Any additional tasks – such as existing searches, governance actions, and retention policy execution – are available to be executed upon ingest. OCR Capabilities are executed when content warrants, and originals are stored in near-store fashion if needed. Resultant content is additionally indexed for search capabilities.

Any data movement, consolidation or extraction may be executed at batch intervals or in a continuous mode.

Sample image of Data Identification Manager's location data

BENEFITS

- Search panel is purpose built for privacy and governance requirements
- Ingesting of additional file repositories ensures audit compliance for long term retention requirements – including roll offs of any data set as required.
- Rapid data consolidation, ROT analysis and management
- Specific IT security and data policy enforcement – across the entire data estate
- Select user roles and permissions based on your customizations
- Search and extraction are based on the entire data estate that in attached to the platform



Sample Dashboard of Data Identification Manager platform

ABOUT DATA443

Data443 Risk Mitigation is a leader in data security and privacy management – a critical element of IT security protecting access to All Things Data Security™ across the enterprise and in the cloud. Data443 provides the necessary visibility and control needed to protect at-scale, obtain compliance objectives, and enhance operational efficiencies.

101 J Morris Commons Lane, Suite 105,
Morrisville, NC 27560

data443.com
info@data443.com

Toll Free
+1 855-DATA-443 (855-328-2443)

US
+1 919 526 1070

UK
+44 203 7693 700

WHITEPAPER

COMPARING DATA DISCOVERY & FILE ANALYSIS SOFTWARE SOLUTION

Data and privacy management (DPM) technologies are now expected to be available from the same product suite to protect enterprises from rising penalties for failing to meet privacy and compliance requirements. As the types, categories, locations, and processors of sensitive data continue to proliferate, every organization needs a comprehensive DPM solution that provides protection across all data stores. In addition, every DPM solution should leverage existing IT investments that support meeting governance and compliance demands.

The DPM platform itself should also provide constant and consistent classification and discovery capabilities to ensure continuous protection. The move to remote/hybrid work requires that effective discovery/classification be in place for endpoints, email, all cloud providers, and SaaS application solutions.

Ensuring data privacy also requires a consistent platform to protect the data, with centralized policy management applied to all data and with policy changes applied quickly across all data sets. The key: automating these processes.

This overview will explore and compare Data443's Data Identification Manager to other vendor solutions by BidID and Varonis.

BIGID ENTERPRISE

Getting the DPM solution choice right is necessary to protect the business and not all solutions are created equal. In many ways, tasks such as discovery, governance and classification, form the foundation for DPM, and the quality and breadth of this functionality are critical to success. The chart and text below identify how Data443 Data Identification Manager and BigID Enterprise compare across the most important aspects of this functionality.

	Data443	BigID
Cloud data drives	✓	?
Databases	✓	✓
Email	✓	
Endpoints	✓	
Data in flight	✓	✓
Data at rest	✓	✓
Structured data	✓	✓
Unstructured data	✓	✓

DATA SECURITY & PRIVACY MANAGEMENT

is critically important for protecting businesses from risk as well as compliance and legal issues due to loss or misuse of private or sensitive data. However, effective data privacy management requires a platform that has the capabilities to handle these complexities.

First the solution must identify data across the entire IT "estate"—that is, look across cloud services, endpoints, servers, cloud applications and all other infrastructure that can store data. The business data estate also includes data at third-party providers.

KEY FINDINGS

- Data443 supports all activities across the entire data estate, whereas BigID lacks the visibility into endpoints and email systems, which can contain plentiful and highly sensitive data
- Data443 can engage directly with data owners and stewards. BigID has less ability to support this direct engagement. Engagement with these individuals improves results and leverages data knowledge to deliver better results.
- Data443 can support interactions at the user/device level, which will be increasingly important as the move to hybrid/remote work continues, and that will include key stakeholders.
- Only Data443 supports classic enterprise use cases such as assigning share and folder owners and determining data ownership based on classification and not simply on usage.
- The Data443 platform engages other important parts of enterprise infrastructure such as Microsoft MIP, SIEM tools/appliances, CyberArk access management, and ShareFile. Data443 works well with other components of the technology stack and is a team player, not a silo

CLASSIFICATION & GOVERNANCE

Best-in-class data stewardship is delivered with active classification and governance processes that, ideally, occur continuously. These major activities comprise many individual tasks that enable effective data privacy management throughout the entire data lifecycle. Automating these tasks is the only effective way to complete the substantial amount of work requires, and this should be augmented with human management as needed. These management tasks will be jointly completed by IT and other teams such as the compliance office.

	Data443	BigID
End user classification/governance	✓	
Data access governance	✓	
Governance alerts	✓	
Live classification	✓	
Manual classification	✓	?
High-risk classification	✓	✓
Data audit with classification information	✓	✓

KEY FINDINGS

- Data443 provides broad classification capability across all data sets, regardless of location, including end users. It also enables data stewards to provide input.
- Data443 has strong orchestration functionality.
- Data443 is built with a “classify all the time” approach that also enables an organization to move at its own pace and learn as it goes. BigID lacks live classification which can result in data gaps that put sensitive data at risk.
- One of the most important capabilities of Data443’s solution is the ability to take governance actions on data, not just classify it. This results in better enforcement of existing IT data security policies to reduce risk.
- Data443 provides alerts for governance problems as they are found, either to SIEM or other alert types. BigID does not have this functionality.
- BigID misses the key functionality to manage the governance and remediation of access. Data443 includes all identity repositories for this capability.
- Data443 leverages 900+ active taxonomies included with the product, available in 14 languages and powered by both fuzzy logic and machine-learning technologies.

DISCOVERY & COMPLIANCE

The output most organizations focused on is discovery and compliance information. Given the amount of data stored by modern organizations, automation of these activities is mandatory, and it enables full lifecycle data privacy management. With these capabilities the organization will find it easier to meet changing compliance demands. The emergence of inconsistent and overlapping global and local compliance rules demand a comprehensive automated solution.

	Data443	BigID
All-enterprise search and discovery	✓	
Customer e-discovery	✓	✓
Sensitive-data detection	✓	✓
Workflow for compliance response and reconciliation	✓	
Compliance with GDRP, HIPAA, PCI and other standards	Explicit and fuzzy	Explicit only

IDENTIFYING IMPORTANT DIFFERENCES

- Data443 can deliver the global discovery that is required, using both “crawl” and indexed approaches.
- BigID is limited in this area of functionality in terms of customer e-discovery and sensitive-data detection features.
- The Data443 solution has a built-in privacy request panel with workflows for compliance response and remediation, including for FOIA, GDPR, CCPA, e-discovery, litigation sup- port, and retention management demands.
- Data443’s product has the ability to work with “fuzzy” logic, which drives many new and emerging compliance demands. Without this functionality, it is likely that the business will fail to meet some compliance and governance demands. BigID can work only with explicit demands.
- Support for full archiving management is another key benefit that Data443 provides that BigID does not. This feature supports archiving for email, unstructured data, and many ECM platforms, and actions can be based on both condition and time.
- Identifying data that is duplicated or not necessary is essential for efficiency, and only Data443 has next- generation ROT (redundant, obsolete, or trivial) identification capabilities, including fingerprinting, obfuscation, and other display options.

SUMMARY & KEY TAKEAWAYS

The Data443 solution, in comparison, contains a more modern approach to help organizations meet the challenge of current and future data privacy management – including capabilities around breadth, reporting and remediation.

The Data443 better positions to support the move to hybrid and remote work, with the ability to find and protect data on endpoints and in email systems. With the inclusion of classification and discovery abilities, Data Identification Manager proves the stronger solution – BigID’s lack of live classification functionality within the offering can further put organizations at risk and the absence of alert functionality is highly problematic.

The Data443 solution provides build-in workflows for compliance response and reconciliation, substantially reducing the number of resources necessary to complete projects, enabling faster completion.

VARONIS SECURITY PLATFORM

Choosing the wrong solution for this critical initiative can leave an organization with a big data knowledge gap. What follows is a competitive analysis of the solutions from Data443 and Varonis, examining their capabilities across three critical areas of functional capability. The better a solution can perform these tasks, the better the organization can protect its sensitive and private information. This chart shows how Data443 and Varonis compare.

	Data443	Varonis
Cloud data drives	✓	Limited
Databases	✓	
Email	✓	
Endpoints	✓	
Data in flight	✓	
Data at rest	✓	✓
Structured data	✓	
Unstructured data	✓	Limited

KEY FINDINGS

- Data443 can find and protect data in many more locations, such as every major cloud provider, laptops and desktops, and hundreds of SaaS services/applications.
- Varonis has very limited data identification capabilities and a comparatively small library of patterns. Data443 has more than 900 built in, in 14 languages, enabling a better false detection rate and more-accurate reporting and governance controls.
- New data types in new locations are increasingly important, and only Data443 can find them.
- Varonis has a substantial blind spot for user data on end user devices, and this is increasingly problematic as remote and hybrid work become the norm.
- Risks created when information is sent to others (both inside and outside the organization) make Data443's ability to discover sensitive information in all major email plat- forms (and archives if needed) a major advantage.
- Varonis lacks interaction with data owners, whereas Data443 engages data owners and stewards actively and continuously training its machine learning (ML) with your own data.
- Data443 assigns data ownership based on classification accuracy and other forward generation vectors (including ML), not only legacy methods such as who uses the data.
- In terms of integration, Data443 was first in many cases and continues to natively integrate with Microsoft MIP, SIEM tools, CyberArk access management, Dropbox and others.

CLASSIFICATION & GOVERNANCE

Effective data stewardship means that classification and governance are active tasks that must happen regularly or even continuously. Classification has many new subtasks that are essential to ensuring effective data privacy management as data moves through the lifecycle. The best setup is automated engines with human supervisory management – and the burden should not always be directly on IT.

	Data443	Varonis
End-user classification/governance	✓	
Data access governance	✓	✓
Governance alerts	✓	✓
Live classification	✓	
Manual classification	✓	
High-risk classification	✓	
Data audit with classification information	✓	✓

MAJOR DIFFERENCES

- Varonis has very limited classification functionality, with very few built-in sensitivity lists to pick from.
- Data443 can obtain visibility and feedback from non-datacenter data sets (end users, SaaS platforms, unstructured data sets) to support more accurate decision-making on classifications, a capability Varonis lacks.
- Varonis classification functionality often delivers false positives from regular expressions, which increases costs and results in bad execution.
- Data443 has more than 900 mature prebuilt classification schemas in 14 languages that support a "classify all the time" mentality, enabling organizations to take an iterative approach and reducing the demands and limitations of doing it all at once.

DISCOVERY & COMPLIANCE

Active and automated discovery and policy compliance functionality is essential to completing a full lifecycle data privacy deployment. This enables better response to changing compliance demands, and the emergence of mismatched and overlapping global and local compliance rules requires a modern solution that can respond to them.

	Data443	Varonis
All-enterprise search and discovery	✓	
Customer e-discovery	✓	✓
Sensitive data detection	✓	✓
Workflow for compliance response and reconciliation	✓	
Compliance with GDRP, HIPAA, PCI and other standards	Explicit and fuzzy	Explicit only
IT Governance actions	✓	

Data443 has numerous advantages here:

- Varonis' solution focuses on the discovery part of the process only and is limited by the basic capabilities of its tools, namely in on-premises and file systems only.
- Data443 provides a "global" discovery, including all cloud, 200+ database types and 300+ SaaS leaders, including Salesforce, Zoom, WebEx, Snowflake and others.
- The automated governance action capabilities of Varonis are limited and provide little value in automated compliance management
- Data443 offers strong support for compliance reports and remediation, supporting key regimes such as FOIA, GDPR and CCPA, plus workflows surrounding e-discovery and retention management – including archiving, retention and request portals with over 40K customers using it today.
- Many new compliance and governance standards are still being developed, thus introducing vague requirements, but Data443 can adapt to these nonexplicit directives as they develop.
- Data443 solves the problem of archiving data across all data types and sources based on conditions such as policy, sensitivity, classification, age, and other factors.
- Strong policy enforcement and reporting are key capabilities of Data Identification Manager – this technology detects governance failure conditions (permissions, access control and data sensitivity) and executed actions (SIEM, email alert, data encryption, permissions removal, etc).
- Identifying data that is duplicate or not necessary is essential for efficiency, and Data443 has next-generation ROT – Redundant, Obsolete or Trivial – identification capabilities, including fingerprinting, obfuscation and other options.

SUMMARY & KEY TAKEAWAYS

The Data443 solution is designed with current and future data privacy demands in mind. Unlike Varonis' solution, which is focused primarily on legacy on-premises reporting use cases, the Data443 solution supports all aspects of the data privacy management life cycle.

Data443 possesses a substantial advantage based on the ability to look across the IT estate for private or sensitive data, not just in on-premises file shares. The inability of the Varonis solution to find private data in cloud services, SaaS solutions, or endpoints is a substantial drawback and can leave organizations with large gaps in their data inventory and potentially noncompliance risks for privacy laws.

Organizations need a comprehensive data privacy platform that not only locates all sensitive data but also provides auto- mated and effective tools for protecting it. The system must also be dynamic and meet new or changing compliance, legal, and governance demands. Finally, the privacy platform that meets forthcoming regulatory requirements must also seamlessly integrate with existing IT infrastructure—not be a new technology silo to manage.

DATA IDENTIFICATION MANAGER MIGRATION CASE STUDY

THE CHALLENGE

This Real Estate customer had the good fortune of already having a team in place that put an emphasis on well-structured and well-maintained data. They had employed the use of OpenText's ECM platform several years prior. Where their problem arose is a common story: a clean and effective migration from their shared drives to OpenText never became a priority.

Even the most well-intentioned ECM vendor will stress the importance of proper platform use moving forward, but migrating past data is not always an urgent aspect of the project. This created a snowball effect, in which new data moving forward often stems from legacy data; if legacy data does not move over to the new destination, neither does the new data.

Their commitment to OpenText was present, but they needed a way to properly migrate their data. With most user seats sitting unused and only the off file being dropped into OpenText, they needed to improve ROI on their ECM platform.

As the nature of their industry would dictate, this customer also produced a wide array of physical paper documents – legacy documents that took up more than their share of real estate.

They also faced another common industry problem: the transition from physical to digital documents via scanning can be a tedious task in and of itself. Compounding the issue is the fact that attributing metadata to these new files was a manual task.

THE SOLUTION

Data Identification Manager allowed them to capture and attribute their metadata through inheritance. Scanned documents no longer need to be analysed and tagged individually.

This customer created their predefined destination folder in OpenText, attributed metadata tags to that folder and migrated the scanned documents for those documents to reflect the metadata defined at the container level. Data Identification Manager automated the tedious task of incorporating meaningful context.

INDUSTRY

- Real Estate

ABOUT THE COMPANY

This Real Estate organization builds and manages large commercial properties globally. Their portfolio of properties represents more than 50 million square feet of office, retail, hotel, industrial, land, and multi-residential assets in key markets across Canada, the United States, and Europe.

With Data Identification Manager, this customer now has the solution in place that addresses the ingestion of compelling content. This aided work productivity since manual efforts including naming, finding, and sorting of data were further automated.

The scope of the project expanded as the list of business units affected by these circumstances continues to become clearer. Data Identification Manager continues to work with the growing number of stakeholder and ensure that each issue is treated individual and addresses their concerns specifically.

ABOUT DATA443

Data443 Risk Mitigation is a leader in data security and privacy management – a critical element of IT security protecting access to All Things Data Security™ across the enterprise and in the cloud. Data443 provides the necessary visibility and control needed to protect at-scale, obtain compliance objectives, and enhance operational efficiencies.