



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 reimaging 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 is 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.

