Advanced Services for Ransomware Recovery

The Druva Professional Services team ensures your organization has first-hand access to our rich expertise during the design and deployment of Druva's solutions. We work directly with your IT and security teams to enhance your organizational readiness and capabilities to respond and recover confidently from future ransomware events.

Organizations face greater risks than ever

Even with the best technology and processes in place, it's only a matter of time before ransomware or some other disaster strikes. With increasingly diverse types of ransomware attacks and malware threats on the rise, the importance and strategic value of data protection is more important than ever.

Cloud data protection can enhance the role and value of traditional data protection by eliminating security vulnerabilities, enhancing threat detection, and automating recovery. Yet, with ongoing security and IT skill gaps, many organizations need and seek help to validate their cyber recovery readiness and minimize downtime and data loss from a potential ransomware attack.

Assess your organization's ransomware recovery strategy and readiness

No organization or platform is immune to threats or attacks. The Druva Professional Services team provides a thorough evaluation of risks to your data protection environment, tests and validates your cyber recovery strategy, and helps you to bolster your defense against ransomware wherever your data resides. This assessment will improve your business resilience by highlighting both alignment and gaps across both security and IT teams.

How Druva Professional Services provide support

Our teams will align with you on business direction, priorities, challenges, and key initiatives/goals, before determining the steps forward to improve your cyber resilience with Druva. We support customers across the following key areas:

Discovery

The Professional Services team begins by thoroughly reviewing the customer's existing environment, to gain a comprehensive understanding of their cyber recovery readiness. As part of this process, we examine the customer's current recovery and restore processes, highlighting strengths and areas for improvement.

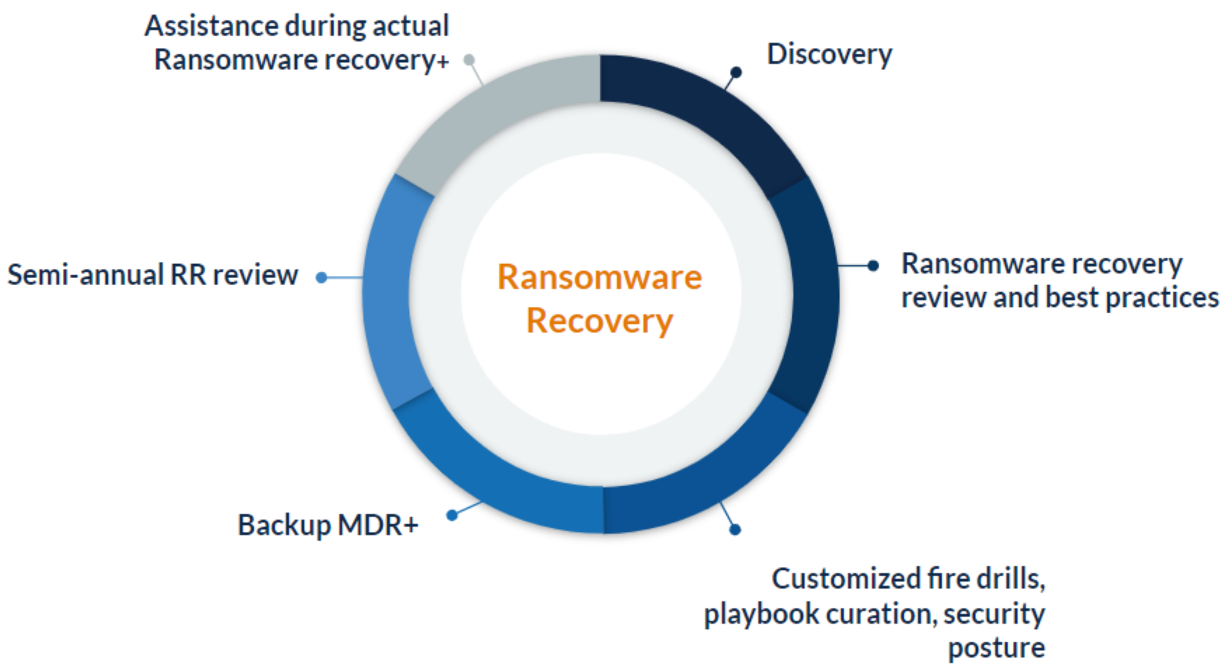
Tools and best practices

To ensure effective cyber recovery in the event of a ransomware infection, we review the customer's existing tools and playbooks and evaluate their efficacy in dealing with a potential incident. We provide recommendations on enhancing these tools and practices to bolster recovery efforts, employing industry best practices and leveraging Druva's capabilities.

Customer awareness and education

The Druva Data Resiliency cloud not only ensures air-gapped data protection, but can play a role in ransomware detection, response, and cyber recovery. The Druva Professional Services team works with your IT and security teams to create a shared understanding of how Druva can augment and improve readiness and cyber recovery using existing tools. Examples include better defining how the organization should respond to data or user anomaly alerts found on the Druva Security Command Center, or how security teams can quickly quarantine backup snapshots during an investigation period, scan them, and isolate infected files.

By combining a structured review of requirements and capabilities with the expertise to answer any technical question, the Professional Services team helps customers accelerate time-to-value.


Assistance during actual Ransomware recovery+
Discovery
Ransomware Recovery
Ransomware recovery review and best practices
Semi-annual RR review
Backup MDR+
Customized fire drills, playbook curation, security posture

Security posture and response readiness

Druva's Professional Services consultants work with customers to identify gaps in their security posture monitoring and incident response processes. We help improve these processes and integrate data from Druva with existing SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) tools using pre-built integrations and APIs.

Recovery readiness and tabletop exercises

We collaborate with the customer and their partners to identify gaps or weaknesses in their recovery plans. Through customized "fire drill" testing that includes a series of tabletop exercises, we simulate real-world scenarios to enhance readiness. This proactive approach ensures that the customer is well-prepared to handle ransomware incidents effectively.

Backup MDR (Managed Detection and Response)

Druva's support team monitors the customer's data backup platform in real time for unusual, potentially harmful data activity such as bulk deletions and other critical events, and will reach out to maintain security and enable swift recovery.

Real-time ransomware recovery assistance

In the unfortunate event of a ransomware attack, Druva Professional Services consultants and our support team collaborate closely with the customer and other related parties to assist with incident response and data recovery. This is included by default for any Druva customer. Our goal is to help customers recover clean data, minimize data loss, and accelerate the return to normal business operations.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the industry's leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.