Managed Data Detection & Response (DDR)

24x7x365 security monitoring of backups, expert analysis, and support from Druva Incident Response for threat monitoring, investigation, response, and cyber recovery.

The Challenge

The evolving tactics of cybercriminals continuously test the efficacy of traditional security defenses, which primarily focus on the perimeter and critical applications in the production environment. Security teams face the daunting task of optimizing their security posture while balancing budget, risk, and operational efficiency. Cyber attacks are more prevalent than ever before, with threat actors increasingly targeting backups as they often represent the last line of defense. Despite heightened investments in security, significant gaps remain in monitoring and securing backup environments, leaving organizations vulnerable to data breaches, ransomware attacks, and operational disruptions.

Backups offer more utility than recovery alone. Monitoring this environment provides insights and alerts that can lead to earlier detection of a threat. However, simply adding another monitoring and alerting tool is insufficient, as it adds to the existing challenge of filtering through the noise of false positives. What organizations truly require is a comprehensive solution that not only analyzes, correlates, and triages incidents effectively, but also enables decisive action the moment a threat is detected. Without the ability to rapidly contain malicious activity, attackers can delete, exfiltrate, or encrypt data before response teams can mobilize. Closing this gap is critical to safeguarding organizational assets and ensuring resilience in today's complex threat landscape.

The Solution — Druva's Managed Data Detection & Response

Druva's Managed DDR (Data Detection and Response) is a fully managed service designed to enhance your organization's security posture by integrating 24x7 advanced security monitoring and threat detection capabilities across your backup environment. Leveraging a single SaaS platform, Druva has an aggregated view across all your workloads– including data across SaaS apps like Microsoft 365 and Google Workspace, to cloud workloads like AWS, the data center, end-user devices, and more.

Druva Incident Response (IR) team expertly triages alerts and analyzes anomalous activity to eliminate false positives. Once a threat has been verified, Druva's IR team works with customers and partners to proactively protect customer data by locking down access to the environment. The team provides expedited support during the entire incident response and recovery process, streamlining the workflows and mitigating the impact of incidents while accelerating the response and recovery efforts.

Key Features

- **24x7x365 Real-Time Monitoring**: Continuous monitoring of your backup environment to detect threats early.
- **AI-Powered Threat Detection**: Utilizes advanced machine learning algorithms to identify suspicious activities and potential security risks, enhancing detection accuracy and speed.
- **Expert Analysis by Druva Incident Response**: Druva experts analyze each threat for validity and provide data insights for any anomalous behavior, enabling customers to stay ahead of emerging threats.
- **Automated Incident Response and Containment**: MDDR with Safe Mode enables you to quickly lock down your environment to minimize reinfection when ransomware incidents are detected by halting restores/downloads,

preventing data deletion, restricting admin and API access, and preserving immutable audit trails. Pre-built response workflows and SIEM/SOAR integrations ensure seamless forensic readiness.

- **Expedited Support and Cyber Recovery Assistance**: Provides assistance to customers throughout the cyber recovery process to minimize downtime and prevent data loss.

Managed DDR In Action

The following is a real-world scenario that took place with a Druva customer.

- **U.S. holiday weekend, 1:00 AM** — A threat actor secured a footprint in the customer network, compromised the active directory, and secured a footprint on customer assets. After compromising SSO servers, the threat actor secured SSO credentials and navigated to various SSO-connected SaaS services, including backup systems. The threat actor leveraged administrative credentials and attempted to compromise backups, deploying ransomware and initiating mass encryption, seeking to take advantage of the upcoming holiday in the hopes of delayed detection.
- **2:00 AM** — Within an hour, Druva's incident response team detected backup data anomalies, investigated the activity, and contacted the customer to confirm the incident. Druva locked down access to the customer tenant and secured critical data. Following its rapid response playbook, the team reviewed security access and enhanced controls like login timeouts and geo-IP fencing. They expedited support and used advanced cyber recovery tools, including Curated Snapshots and quarantining, to isolate infected backups and restore clean data by filtering out malware. Despite 40% of the customer's data being targeted, Druva successfully restored terabytes of data within 24 hours.
- **2:00 PM, following day** — Customer's security team then took over and initiated verification of the restored data, and began to recover applications. Thanks to Druva's IR team detecting the threat within the first hour of the attack, it enabled the customer to quickly limit the scope of the impact on their data. Rather than starting their response hours or days later, the early warning enabled them to mitigate the cyber threat and restore their data within the same day.

The Benefits

- **Autonomous Protection**: Continuous monitoring and AI-powered threat detection provide an additional layer of protection, helping to identify and mitigate threats before they cause significant damage.
- **Faster Incident Response**: Early detection and comprehensive incident response capabilities allow organizations to quickly manage and contain security incidents, minimizing impact and reducing recovery time.
- **Cost-Efficient Simplicity**: Druva IR acts as an extra set of eyes on customer data, working with the customer's team and our partners to provide the same level of monitoring they would get with a third-party solution — all within their existing coverage. This eliminates the need for additional infrastructure and resource support, providing robust security without additional costs, and reducing operational expenses (OpEx).

Druva's Managed DDR service is currently available to customers (refer to product documentation for specifics). It has successfully detected and mitigated real-world threats by alerting customers and streamlining their response and recovery workflows. Our Managed DDR service is delivered as part of the Druva platform, based on a fully Software-as-a-Service (SaaS) architecture, eliminating the need for customers to manage physical infrastructure, require additional resource support, or incur additional monitoring costs. As a result, customers remove the headache of working with multiple vendors and have a single source of truth. Simply put, Druva does it all for you.

druva Sales: +1-800-375-0160 | 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