druva

SHI

Accelerating Incident Response and Recovery with the Power of Data

A cyber breach represents one of the most challenging periods in any professional's career. When an organization suspects a cyberattack, IT and security experts must execute a coordinated series of actions to analyze and rapidly respond to the incident. This process gets to be challenging due to the limited information available to effectively analyze the breach incident.

While traditional security tools focus primarily on the perimeter and production environment, these tools don't provide full-picture visibility into the data, which could lead to prolonged and incomplete digital forensics and incident analysis. Legacy backup approaches typically resort to brute force recovery, but modern incident response (IR) demands a comprehensive analysis even before recovery becomes a viable option. When analyzing a cyber incident, IT and Security professionals need access to both clean copies of data and critical insights from data to pull together a complete picture of the breach's scope, impact, and remediation strategies.

Drawing on the extensive experience in assisting customers with detection, response, and recovery from cyber attacks, Druva has developed a data-powered approach to IRR efforts to address these gaps. By operationalizing the detection, response, and recovery stages of the NIST Cybersecurity Framework, Druva's data-powered IRR workflow provides a prescriptive approach to leverage protected data and insights, accelerating incident response and remediation.

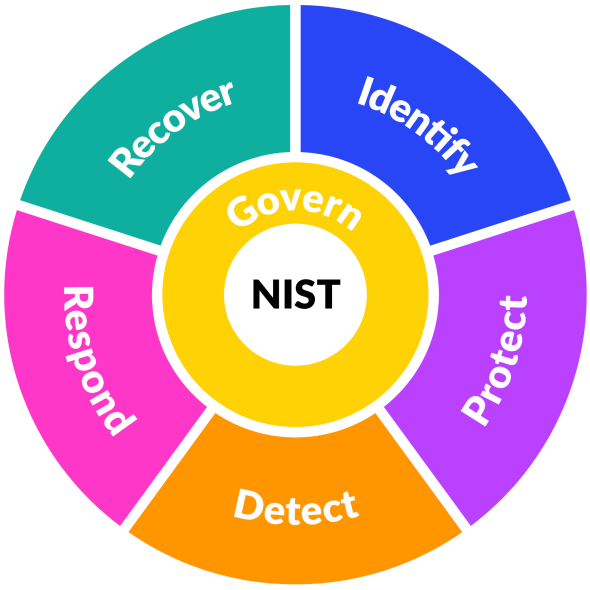
This paper analyzes the key aspects of NIST CSF 2.0 and Druva's data-powered IRR workflow, empowering you with the knowledge and tools needed to effectively respond and recover from cyber risks.

Understanding NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework (CSF) 2.0 offers a structured, risk-based approach that aligns with industry best practices, guiding organizations to meet regulatory and compliance requirements.

This framework serves as a resource for organizations seeking to effectively manage and improve their cybersecurity posture. It outlines six key pillars: **Identify, Protect, Detect, Respond, Recover, and Govern**.

These pillars collectively empower organizations to first identify and understand their data assets and risks, implement appropriate preventive measures, swiftly detect potential threats or breaches, respond effectively to incidents, and ensure robust recovery processes are in place. The Govern pillar iterates on the people and processes across these core functions to meet evolving IT priorities. By integrating these pillars, organizations can establish a holistic security approach tailored to their specific organizational goals, risk tolerances, and management strategies.



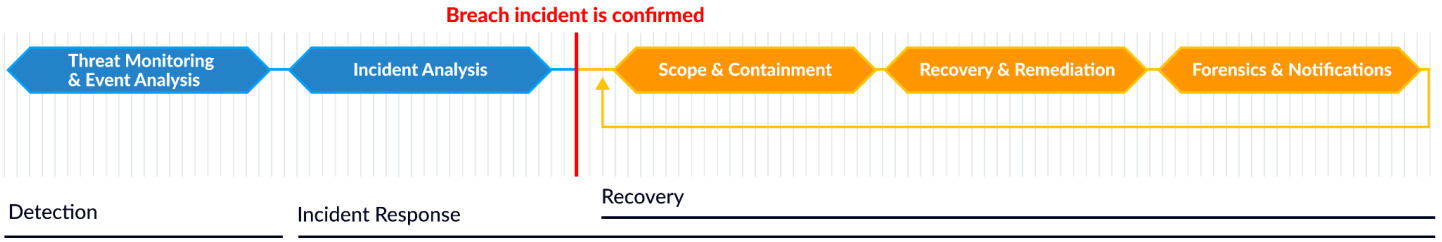
1. **Identify:** Organizations must understand the cybersecurity risks to their systems, applications, and data. Identifying risk enables organizations to prioritize their security investments and measure improvement in their cybersecurity posture.
2. **Protect:** Companies must train people, develop processes, and deploy technology to defend their environment from threats. Investing in cross-functional protection helps secure data, manage identity and access, and make infrastructure services resilient.
3. **Detect:** Organizations monitor their environments to identify cybersecurity events. Early detection enables them to respond to threats, mitigate damages, and limit the impact of incidents.
4. **Respond:** After detecting a cybersecurity incident, businesses must contain the incident, investigate its scope and impact, and initiate remediation efforts. An effective response plan can contain the business impact of the incident.
5. **Recover:** Organizations must restore the data, capabilities, and services that were affected. A robust recovery plan will minimize downtime, financial losses, and reputational damage.

6. **Govern:** Businesses must establish roles, responsibilities, and oversight for their cybersecurity plans and continually review those systems as the threat landscape is constantly evolving.

Among many notable changes, NIST CSF 2.0 introduced a sixth pillar: Govern. This pillar highlights the framework's responsiveness to the evolving landscape of infrastructures, cloud environments, IT priorities, and tactics employed by threat actors (TTPs). This adaptation underscores the framework's commitment to staying current and relevant. This is especially critical as it serves as a guide for organizations in tailoring an effective security strategy that safeguards their most critical assets while ensuring resilience from cyber threats.

Data-Powered Incident Response and Recovery (IRR)

Building on NIST CSF 2.0, Druva's data-powered IRR workflow focuses on the operational steps involved after a potential breach is suspected. The workflow complements existing security strategies with insights from protected data to accelerate detection, response, and recovery from cyber incidents.



Threat Monitoring and Event Analysis

Security teams, especially SOC, CERT, and IR teams, typically have good visibility into the alerts coming in from network, endpoints, and identity management. However, these alerts alone do not paint a full picture because they lack visibility into what's happening with the data – making the event analysis more complex, lengthy, and often incomplete. Effective event analysis requires insights into data changes and anomalies, to triangulate with all other information flowing in from the periphery.

As recent ransomware attacks have shown, backups are often first targeted by bad actors to deprive businesses of recovery as the last line of defense. So, it is essential to treat backup as a tier-1 application that's continuously monitored with any alerts feeding into SOC. Despite the importance of backups to the cyber resiliency strategy, security teams often lack visibility into the backup environment, thereby missing out on critical early indicators of potential attacks, including deleted backups and backup policy changes.

As a fully managed service, Druva continuously monitors the backup environment, looking for unusual administrator activities like mass deletions or significant policy changes. Druva monitors and alerts you when unusual data activity occurs across the environment. Because Druva centralizes data from all protected workloads to a single namespace, it detects unusual data activity across the environment. This spans laptops, SaaS apps, the data center, and the cloud in order for security teams to get a holistic view of their data. These alerts are seamlessly fed to your Security Information and Event Management (SIEM) system, enhancing the security team's visibility into the data environment.

Incident Analysis

When the security team determines that the alerts are for an actual incident, it then needs to investigate whether the incident is severe enough to be considered a breach. Unfortunately, security rarely has access to all the data they need for this incident analysis.

Druva addresses this gap by equipping the incident response team with comprehensive information about the data environment. Druva scans for sensitive and high-risk data on potentially compromised systems and generates detailed logs of data changes and activities over time. Additionally, Druva's Security Command Center highlights unusual administrator and user activities, and provides comprehensive logs of all accesses to backup data.

Druva helps IT bring data insights to security's incident analysis, making it more accurate and more streamlined. When incident analysis confirms a breach, the organization must pivot to address the next three phases of the response. This process is iterative, requiring continuous refinement as more information about the breach becomes available.

Scope and Containment

Once the breach has been confirmed, the incident response team needs to concentrate on determining the scope and gestation period of the malware. Their tasks include identifying the gestation, scope and timeline of the threat, isolating the affected resources to prevent the further spread and assess what data was compromised and/or exfiltrated.

Since breaches revolve around data, the IR team needs as much information about the data on compromised systems as possible. As a fully air-gapped solution, Druva solves this challenge by providing uninterrupted access to all protected data. Affected backups are automatically quarantined to prevent reinfection. With threat hunting, incident response and recovery teams can search across all protected data for malware signatures and delete that malware in the backup and on the active system

Recovery and Remediation

Meanwhile, IT needs to recover the data, the systems, and the applications to get the business up and running again. This is the recovery and remediation phase. IT will need to balance two conflicting priorities — recovering as quickly as possible and recovering as safely as possible, requiring close collaboration with the security team to ensure the backup data and the recovery environment are both clean and secure.

Druva supports this effort in several key ways:

1. **Ensuring Clean Backups:** Druva operates as a separately managed service independent of the customer environment. This separation ensures that any malware affecting the customer cannot infiltrate Druva. Druva's data storage architecture and microservices design prevent malware from running within its environment. Additionally, Druva quarantines all backups from infected systems and conducts thorough threat hunting to remove malware.
2. **Providing Safe, Clean Recoveries:** Druva scans all data being recovered for malware and encrypted files. It also offers sandbox recoveries both on-premises and in the cloud, allowing organizations to validate the cleanliness of their data before reintroducing it into production. Furthermore, Druva's Curated Recovery process identifies the most recent good versions of files across multiple backups, ensuring that the recovery is both safe and current.

While an organization manages the scope and containment along with recovery and remediation, it is equally important to conduct thorough forensics and notification processes.

Forensics and Notifications

During this phase, the organization requires detailed information about the data impacted by the breach to formulate an appropriate business response plan. This includes accurate insights into the event pipeline, the affected data, and the current state of the data environment.

Unfortunately, this information is often difficult to obtain. Druva addresses this challenge in two ways. First, Druva enhances visibility across the data environment with its sensitive data governance, which scans all systems to identify where sensitive data resides and whether it has been affected by the breach.

Second, Druva provides a unified view of your entire environment, including laptops, data centers, SaaS applications, and other cloud-based applications. This comprehensive visibility allows you to understand what data was affected and assess the current state of the data environment effectively.

Managed Data Detection and Response

Recognizing the critical role that backup insights play in early detection and effective response to cyber attacks, Druva also offers a Managed Data Detection and Response (DDR) service to its customers at no additional cost. Fully managed by Druva, it enhances customers' security posture with:

- **24x7x365 monitoring of backups** for early threat detection.
- **Expert analysis by Druva incident response and recovery** to provide data insights for anomalous behavior.
- **Pre-built response runbooks and automatic lockdown of backups** to safeguard data.
- **Expedited support and expert assistance** to customer IR teams during cyber recovery.

With Druva, businesses can gain confidence throughout their IRR workflows with access to a single source of truth and CloudOps experts to assist in incident remediation and recovery.

Accelerate Incident Response and Recovery with Druva

Responding to a breach can be overwhelming. Druva uses the power of data to bridge the gap between IT and Security, and accelerate incident response and recovery. Druva helps minimize downtime, data loss, and breach impacts by leveraging the power of data to complement existing security strategies.

See why Druva was recognized as a 2024 Gartner® Peer Insights™ Customers' Choice for Enterprise Backup & Recovery Software Solutions with our 30-day self-service free trial. No credit card required.

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

Americas: +1 888-248-4976
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 leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on LinkedIn, X (formerly Twitter), and Facebook.