COHESITY

WHITE PAPER

Improve cyber resilience with a digital jump bag™

How to rapidly restore a Minimum Viable Response Capability and strengthen incident response

TABLE OF CONTENTS

Forward

James Blake
VP Cyber Resiliency
Strategy

For over 30 years, I've been on the front lines of cyber response to destructive cyberattacks and data theft. My experience ranges from running incident responses to wiper attacks from nation-states to leading cyber risk management at the world's largest bank.

During this time, I've learned the value of having a "jump bag." The term originally referred to a physical container holding essential hardware and software necessary to pick up on the way to a physical location that suffered an attack. This jump bag had the essentials to quickly investigate the incident, gather evidence, and mitigate threats. As well as hardware and software, it contained items like printouts of the contact list of key stakeholders inside the organization and third parties, the crisis management plan, workflows for the types of incidents I was likely to respond to, and a mobile phone. The idea was to be prepared to respond immediately: rushing around to find everything you need while under the pressure of an incident wastes valuable time and leads to forgetting something essential. The jump bag contained a mixture of tooling, details of processes, and a method to allow communication.

Today, we live in a world of remote acquisition, endpoint and extended detection and response (EDR/XDR), virtual machines, and cloud instances. Jump bags can still be physical containers we take on-site. But now, the greatest utility can be found in preparing a digital jump bag™. This protected and trusted repository provides rapid access to not only the tools required for remote acquisition and analysis but also any other digital assets required for a positive outcome during an incident response and recovery.

Executive summary

The digital jump bag™ is the foundation of a clean room—a secure and isolated environment where the security operations team can perform the necessary investigatory steps to understand how an attack happened. They also use a clean room to perform remedial steps before recovery to eradicate the threat and help prevent reoccurrence. What goes in the digital jump bag depends on an organization's maturity, structure, processes, and tooling.

At its core, the digital jump bag enables an organization to rapidly restore a Minimum Viable Response Capability (MVRC)– a streamlined set of essential tools, documents, and processes required to effectively respond to a cyberattack. The MVRC ensures organizations can rapidly contain breaches, restore critical business operations, and minimize downtime during a cyber incident.

The **Cohesity Clean Room solution** supports this modern approach to help organizations combat destructive cyberattacks. It offers flexibility to adapt to diverse needs and supports continual improvement of operational cyber resilience capability over time.

In this white paper, we'll recommend what organizations should consider including in their digital jump bag as they build a more robust and agile incident response strategy.

Commonly unaddressed issues in cyber resilience

Destructive cyberattacks often involve the evasion of the security tooling used within the victim organization, with EDR/XDR evasion capabilities being baked into many of the common Ransomware-as-a-Service (RaaS) platforms that are responsible for the vast majority of the ransomware attacks we see today. By their very nature, EDR/XDR solutions sit on the endpoint, which, when not evaded, provide excellent visibility of processes, network connections, and file systems.

Incident response best practices, such as the SANS Institute Six Step Incident Response Lifecycle, NIST SP800-61 Computer Security Incident Handling Guide, RE&CT Framework, and MITRE D3FEND, all advocate containing the spread of an incident through isolation of infected networks and hosts. In the world of endpoint controls, at best, this leaves an organization with only the information it has already collected to investigate the incident.

However, as we face a constantly adapting adversary, we may not always know what information we need to collect to understand an attack ahead of time. We can find ourselves blinded by the fact that our investigation and response capability has now become an unreachable island. Similarly, remote forensic imaging of volumes in an impacted host becomes impossible if we've cut off the connectivity.

On top of security tooling, many other systems are involved in the investigation, mitigation, and recovery phases of incident response. These can be impacted by destructive cyberattacks like ransomware and wipers, yet are frequently overlooked as being critical in many business impact analyses. I have been involved in incidents where incident responders couldn't get inside their buildings because physical access controls had been impacted. Many organizations found themselves unable to communicate with the press, regulators, law enforcement, cyber insurers, or impacted data subjects due to their voice-over-IP and email servers being hit. Many tabletop ransomware exercises undertaken by organizations do not sufficiently capture these impacts created by the adversary's targeted techniques. After all, the attackers want to ensure organizations struggle to respond and recover from incidents.

With RaaS platforms baking in exploits for recently patched vulnerabilities in as little as five days, we need to identify these in systems and get them patched before returning systems into production. Otherwise, the same adversary, or another affiliate using the same RaaS platform, will roll back in.

We also need to identify the initial access vector which gives us the first system impacted, so-called "patient zero," then work forward through the incident. Understanding how the adversary is maintaining persistence, escalating privileges and finding other artifacts of the attack is required to make sure any recovery is to a secure state. Response teams must also understand the nature of any data that may have been compromised to comply with regulatory obligations for notification.

Analysis of encrypted systems isn't enough. Typically, ransomware gangs deploy encryptors right at the very end of their attack cycle, in the last few minutes or hours of an attack that could have been dwelling inside of our infrastructure for anything from a handful to hundreds of days. Encryption is very noisy, and likely to trigger security controls and user detection. By this time, it is too late. This need to be built for speed is one of the reasons encryptors often aren't built for integrity, resulting in large amounts of data loss for those who pay ransoms for decryption keys. Limiting the scope to encrypted systems, without identifying how the adversary got in and continues to dwell inside your network, is a recipe for disaster.

Organizations that take this approach will often recover dozens of times, only to become reinfected again and again. This “doom loop” cycle is resolved by properly investigating the incident, and using the insights gained to remediate the threats.

Just ask yourself, how would your last tabletop exercise result have differed if you had no telephones or email, had been locked out of your buildings, and had no access to identity and access management systems at the onset of the event?

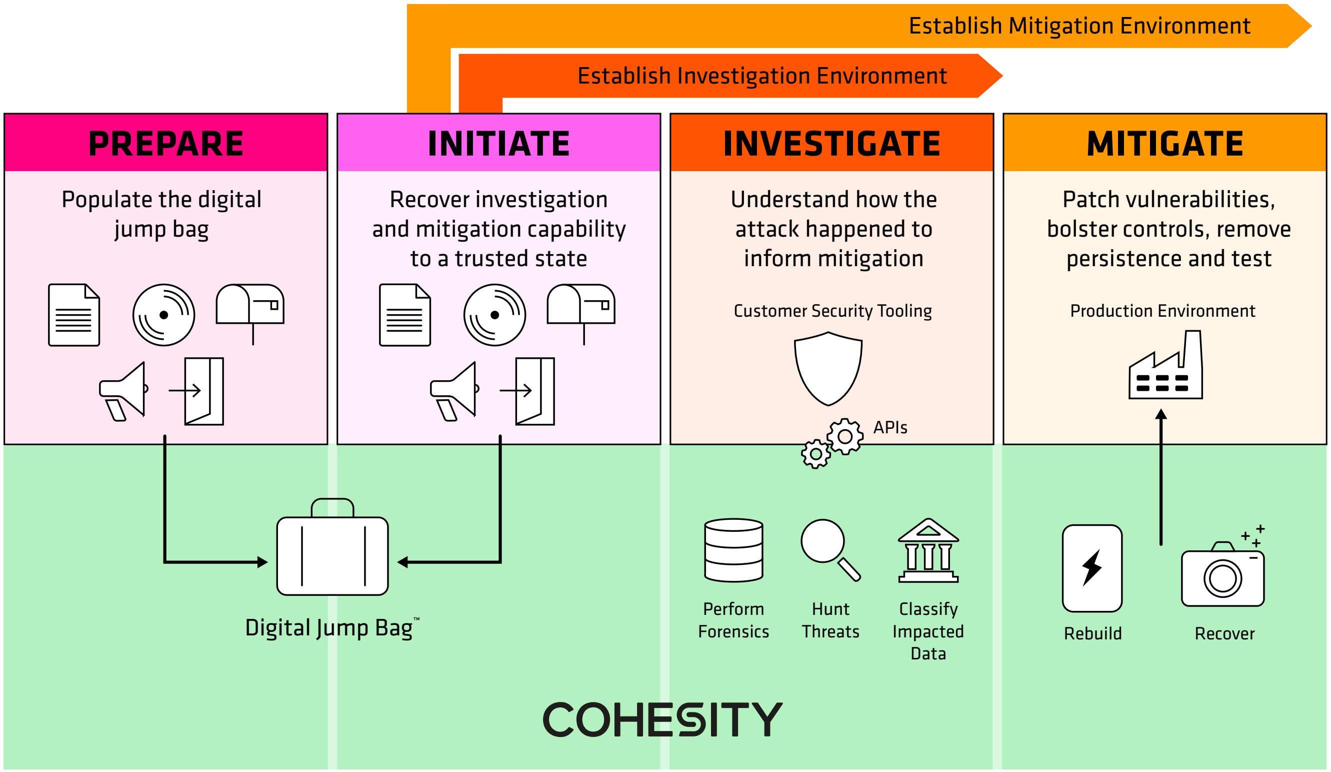
How the digital jump bag fits into the Cohesity Clean Room Solution

The digital jump bag is the foundation for the entire Cohesity Clean Room solution, supporting the critical stages of incident response and recovery to allow organizations to restore clean data back into production, shown below.

Let's review what's happening in each of these stages.

Prepare

In this stage, we choose what goes into the digital jump bag, such as network or hypervisor configurations that support tiers of interdependent systems that would be restored in the Mitigation environment. See the section "What are the potential components of your digital jump bag?" for suggestions to enable the subsequent stages.


Establish Mitigation Environment
Establish Investigation Environment
PREPARE
Populate the digital jump bag
INITIATE
Recover investigation and mitigation capability to a trusted state
INVESTIGATE
Understand how the attack happened to inform mitigation
Customer Security Tooling
APIs
MITIGATE
Patch vulnerabilities, bolster controls, remove persistence and test
Production Environment
Digital Jump Bag™
Perform Forensics
Hunt Threats
Classify Impacted Data
Rebuild
Recover
COHESITY

Initiate

In this stage, we recover the MVRC where the necessary tools for communication, collaboration, and incident investigation are recovered from the digital jump bag to a trusted state inside the isolated clean room environment. The digital jump bag also establishes the Investigation and Mitigation environments.

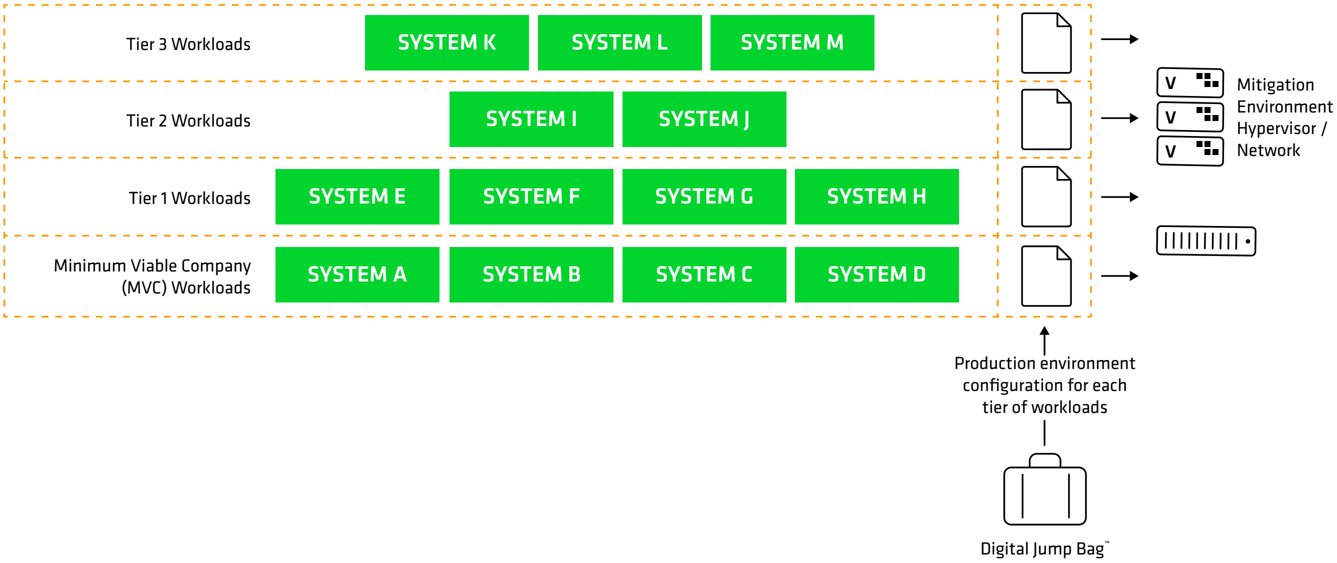
Investigate

Security operations use the security tools recovered into a trusted state within the isolated clean room along with native Cohesity capabilities for data classification, threat hunting, and file system forensics to understand the entire end-to-end incident timeline. As security tooling is recovered to a trusted state inside the clean room and Cohesity's security capabilities aren't subject to the defence evasion techniques used against endpoint controls, the challenges of evasion and isolation due to containment are overcome. Cohesity's Data Security Alliance provides a rich set of security vendor tooling that are incumbent in my Security Operations Centres that are preconfigured to work alongside Cohesity solutions.

Mitigate

IT operations use what the security operations team has uncovered about the incident to recover then clean, or choose to rebuild systems to a trusted state. Whereas the Investigation stage does not involve a full recovery of systems with interdependencies, the Mitigation stage does.

Customers often reuse their development environments as the Mitigation environment for the duration of incident recovery. Interdependent systems are brought up in the Mitigation environment with network configurations that match production environments. These network or hypervisor configurations are stored for each tier of interdependent systems in the digital jump bag. This is shown below.



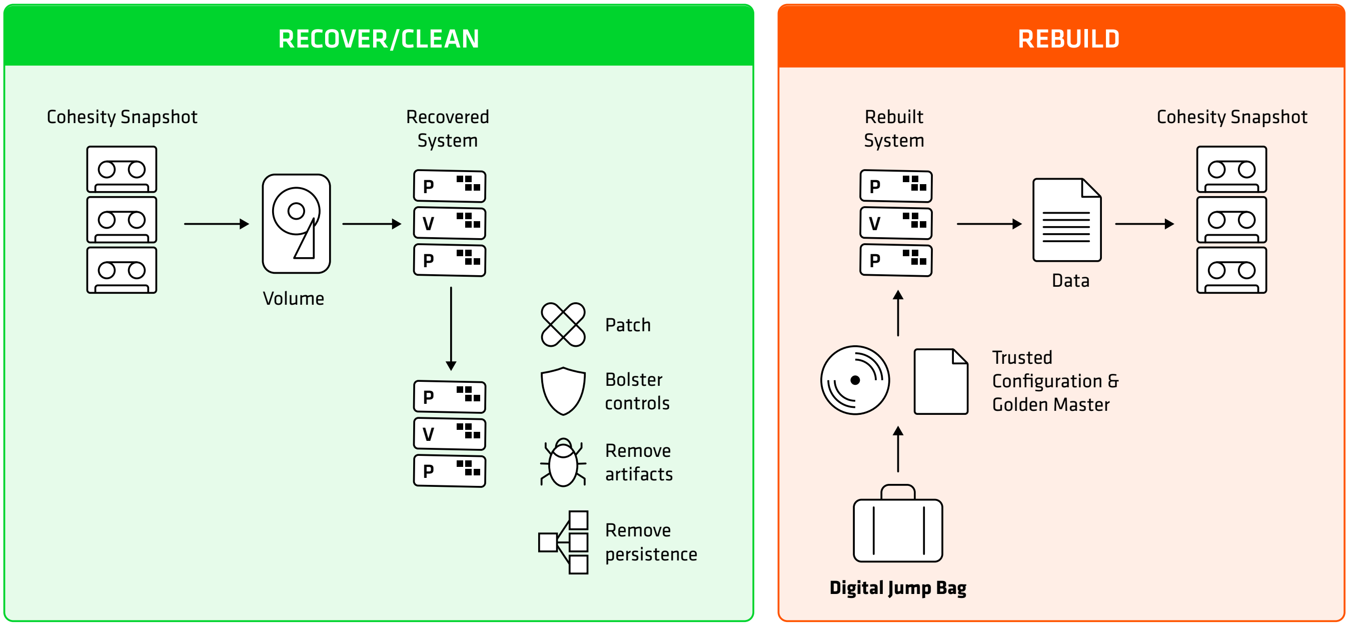
Cohesity Clean Room alignment to incident response best practices.

With the Cohesity Clean Room solution, the strategy of whether to “recover and clean” or “rebuild to trusted state” can be applied universally, or chosen on a per system basis during an incident based on level of remediation effort and residual risk of threats. Let’s review a brief description of each option:

- **Recover and clean**: Systems are recovered from their snapshot, and the mitigation steps outlined by the security operations team in their Investigation stage are undertaken. As data isn’t typically used to carry malicious payloads, data recovery can often occur in parallel with the system rebuilding, further driving down ultimate recovery times.
- **Rebuild systems to a trusted state**: The digital jump bag will contain known-good configurations, installation scripts, and golden master install images. Once rebuilt, data will be recovered from snapshots on the rebuilt systems.

The section “**Using the jump bag to establish the Minimum Viable Response Capability**” details the comparison of each approach.

Having an environment that serves the security operations team’s investigatory needs and an environment that allows the IT operations team to ensure that recovery is to a secure state by applying mitigations helps organizations achieve an effective and appropriate shared responsibility model for cyber resilience. This approach optimizes the speed of secure recovery by ensuring that IT and security operations assets can be fully utilised.

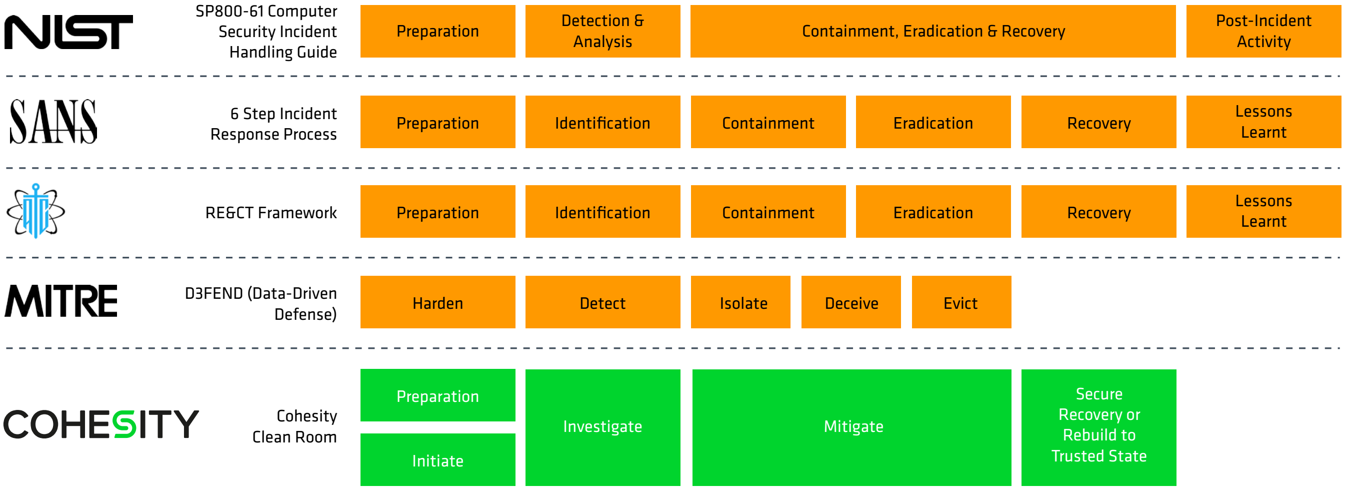


Cohesity Clean Room provides customers with the option to recover and clean workloads or rapidly rebuild to a trusted state.

Once systems have been rebuilt or recovered, functional and performance tests can be conducted on that tier of workloads. A snapshot is taken, and then the entire interdependent workload is restored to the production environment—safe in the knowledge that the full scope of the incident has been investigated, the threats mitigated, and performance and functionality are restored. These test cases can be stored in the digital jump bag for each recovery tier of interdependent workloads. Should something in investigation and mitigation have been missed, there is no need to go back to square one as the snapshot taken at the end of the Mitigation phase can be used as the foundation for further Investigation and Mitigation.

How the Cohesity Clean Room aligns with incident response best practices

The Cohesity digital jump bag and the Minimum Viable Response Capability align with the cyber incident response best practices outlined in the SANS Institute Six-Step Incident Response Lifecycle, NIST SP800-61 Computer Security Incident Handling Guide, RE&CT Framework and MITRE D3FEND. With this approach, organizations that already follow these methodologies can easily integrate the Cohesity Clean Room solution into their existing workflow. Customers looking to improve their incident response and recovery maturity can adopt the Cohesity Clean Room solution to operationalize these best practices.



NIST	SP800-61 Computer Security Incident Handling Guide	Preparation	Detection & Analysis	Containment, Eradication & Recovery			Post-Incident Activity
SANS	6 Step Incident Response Process	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
	RE&CT Framework	Preparation	Identification	Containment	Eradication	Recovery	Lessons Learnt
MITRE	D3FEND (Data-Driven Defense)	Harden	Detect	Isolate	Deceive	Evict	
COHESITY	Cohesity Clean Room	Preparation Initiate	Investigate	Mitigate		Secure Recovery or Rebuild to Trusted State	

Cohesity Clean Room alignment to incident response best practices

Bringing security and IT operations together to deliver resilience

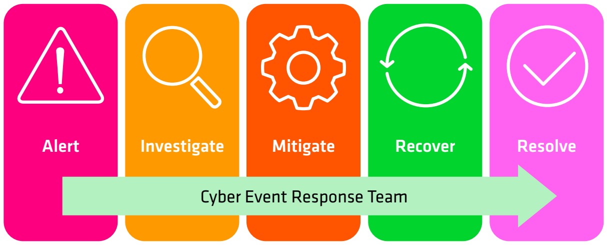
Cyber resilience is a team sport: it can't be delivered by IT operations in isolation, nor by security operations acting alone. Both teams need to have integrated processes and complementary tooling. Likewise, no one vendor can deliver cyber resilience. The Cohesity Clean Room solution is designed to allow the security operations team to leverage and own the Investigation environment, while IT operations own and utilize the Mitigation environment. This ownership and hand-off between the teams help ensure a clear shared responsibility model, minimising the opportunity for activities to fall down the cracks. The ability to iteratively revert previously mitigated snapshots back to the Investigation stage if some aspect of the attack is missed in initial investigation and mitigation, without having to start at the beginning, drives down investigation time and ultimate recovery.

As soon as security operations have finished investigating a workload in the Investigation environment, it can be handed off to IT operations and the Mitigation environment for rebuilding, recovery, and cleaning. This ensures the most efficient use of IT and Security operations resources.

Respond faster, recover smarter: Cohesity CERT (Cyber Event Response Team)

Many organizations lack the expertise or resources for effective cyber incident response. To minimize impact, we've enhanced our world-class data security solution with a dedicated Cyber Event Response Team (CERT) service.

Cohesity CERT provides expert-led, rapid recovery from cyberattacks, ensuring your data is restored and your business resumes operations with minimal downtime.



Cohesity CERT is available to all customers as part of their Cohesity subscription.

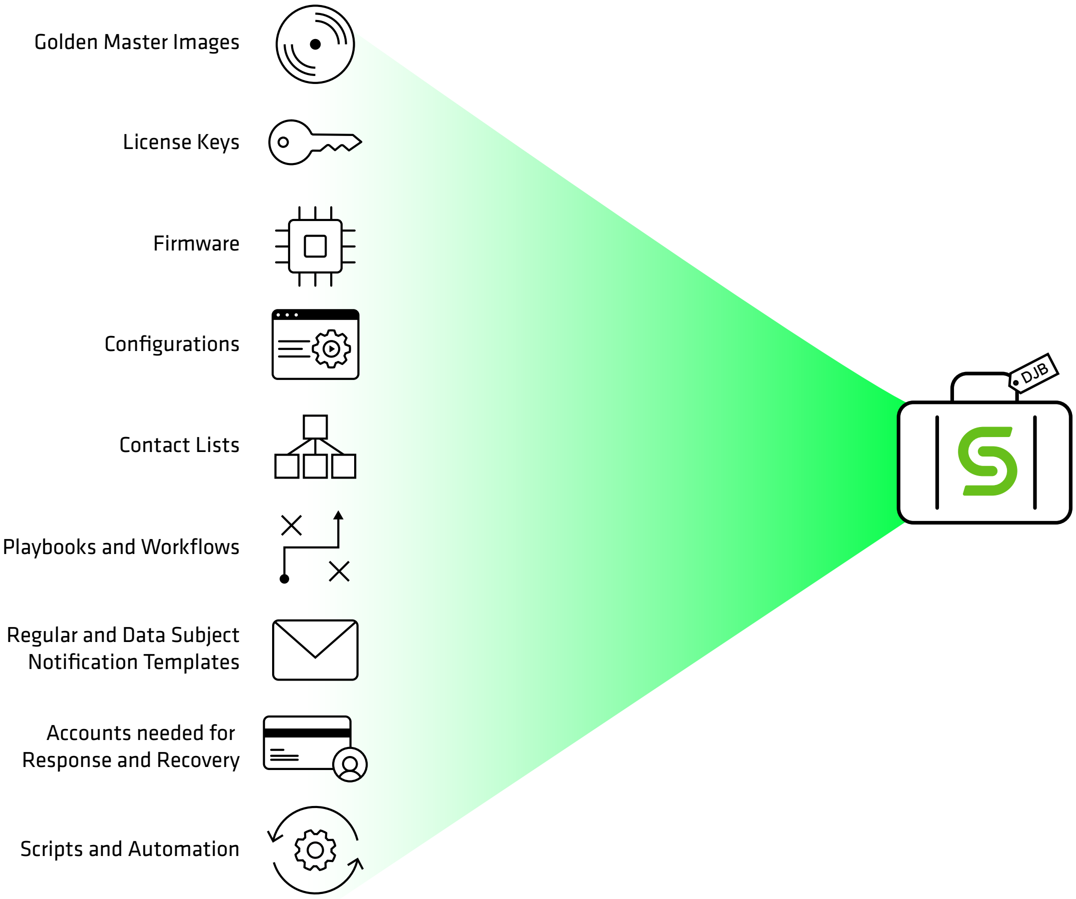
What are the potential components of your digital jump bag?

The contents of your digital jump bag depend on your individual triage, investigation and mitigation processes, and the tools you use to achieve them.

In general, we see the following items commonly included in our customer's digital jump bags:

Documentation

- A contact list including internal stakeholders and external entities such as law enforcement, information sharing and analysis centers, insurance companies, retained incident responders, and regulators.
- Network diagrams.
- Potentially a backup or dump of the organization's configuration management database.
- A copy of the incident response runbook/workflow.
- Contracts and policy documents concerning retained incident response services and cyber insurers.
- User manuals for applications and tools.



Resources for the Initiate stage: Collaboration and communication

- Communication with internal stakeholders and external third parties such as law enforcement, information sharing and analysis centers, insurance companies, retained incident responders, regulators, the press, and impacted data subjects is likely needed. To establish this capability, a digital jump bag could contain the following:
  - Known-good router and switch firmware and configuration to allow secure connectivity. Alternatively, the organization may maintain trusted stand-by equipment.
  - Firewall software and configuration to restrict ingress and egress to just the resources needed for response and recovery (including access to Cohesity Helios.)
  - The base operating system installation media and license keys used as the foundation for rebuilding other systems, including ones in the Investigation and Mitigation environments.
  - Automation and orchestration scripts, which can be anything from Windows Answerfiles for unattended installation, through Ansible playbooks, through to Terraform Infrastructure-as-a-Code.
  - Voice-over-IP management (VoIP) server software and configuration. It is important to realize that this is not the entire production VoIP environment. It only has lines related to response and recovery activities. The production VoIP configuration will be returned online after investigation, and any threats found have been mitigated.
  - Email server software and configuration. Like the VoIP server, this is not a production capability. It just allows communication by the resources involved in response and recovery activities.
  - Other collaboration tools used by the organization, like ticketing, conferencing, or similar, can be included in the jump bag.
  - Templates for regulator and impacted data subject notification

Resources for the investigation stage environment

The security operations team typically owns the environment used during the Investigation Stage. It’s focused on understanding the end-to-end attack timeline so the organization can make informed decisions about recovering production capability while protecting from reinfection and reattack. Systems are investigated inside the organization using a mixture of the native security operations capability of Cohesity to perform tasks like data classification, threat hunting, and file system forensics and by Cohesity supporting other security operations tooling. Threat hunting using Cohesity isn’t impacted by incident containment. It is passive, so it is not visible to the adversary and isn’t subject to evasion techniques common to endpoint security solutions. In the Investigation stage environment, systems are typically investigated in isolation.

- Installation media and configurations for security software. This allows the reinstallation of tooling to a trusted state inside the isolated clean room environment, ensuring confidence that the tooling and response activities are not being evaded or disrupted.
- Security tooling can be reinstalled to a trusted state inside the clean room. This tooling is highly dependent on the preferences of your security incident response team but typically contains at least some of the following:
  - Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) tools include Palo Alto Networks, Cisco XDR, and CrowdStrike
  - Forensic capture and analysis tools like Dissect, Flare, Redline, Sleuth Kit, Autopsy, CyLR, and Unix-like Artifacts Collector (UAC)
  - Indicators of Compromise and evidence-sharing tools, like Cortex, Kuiper, and MISP
  - Event log analysers like Event Log Explorer, Event Log Observer, Hayabusa, LogonTracer, or Windows Event Log Analyzer (WELA)
  - Vulnerability scanners, such as Qualys, Rapid7 neXpose, Tenable Nessus, or OpenVAS

  - Packet Capture and Analysis Software, such as Wireshark
  - Netflow/SFlow Analysers
  - Memory capture and analysers like Volatility, Memoryze, Orochi, Rekall, and WindowsSCOPE.
  - Sandboxes, malware reverse engineering, and analysis tools, like Cuckoo, CAPA, CAPE, Ghidra, Joe Sandbox, Mastiff, Radare 2, and Valkyrie Comodo.
  - Web browser history forensic tools like Internet History Forensics
  - Many of the above tools are available inside security software distributions such as Kali Linux, and SANS Institute SIFT Workstation. These can be stored inside the digital jump bag rather than installing each tool.

Resources for the Mitigation stage environment

The IT operations team typically owns the Mitigation environment. In the Mitigation environment, system operating systems and applications are rebuilt from trusted install media and configurations contained in the digital jump bag or are recovered from backup snapshots and cleaned using the information gained by security operations during the Investigation stage. Remedial steps are taken to mitigate threats such as the patching of vulnerabilities, the application of missing controls or rules to prevent or detect future attacks of the same time, and any persistence mechanisms, malicious accounts, or other attack artifacts are removed. In the Mitigation environment, interdependent systems to deliver a product or services are brought together and rebuilt or mitigated, until finally performance and functionality can be tested by restoring data from a backup snapshot. A snapshot is taken at this point in time, and the systems are recovered into the production environment.

- If the organization takes a “rebuild” rather than a “recover and clean” approach, the digital jump bag will contain the required installation media and configurations for the application stack.
- The network or hypervisor configuration required for the current interdependent workload. This allows the Mitigation environment to replicate that of the production environment—that the workload will ultimately be recovered into.
- Test cases for the workloads.

Using the jump bag to establish the Minimum Viable Response Capability

When using the digital jump bag to establish the systems within the MVRC, a customer has two choices: Recover a pre-built system or rebuild from trusted sources.

- **Maintain the Minimum Viable Response Capability:** Build the systems needed for the MVRC and perform a volume-level backup on them, which are stored in the digital jump bag. If a cybersecurity incident that impacts systems needed for response and recovery or evasion of security tooling is suspected, the snapshots are recovered to establish the Minimum Viable Response Capability.
- **Rebuild from resources in the digital jump bag**: Here, trusted configurations and golden master images for the systems required for the MVRC are held in the digital jump bag. In the event of a cybersecurity incident that impacts systems needed for response and recovery or evasion of security tooling is suspected, the digital jump bag is mounted. These systems are rebuilt using scripts or orchestration tooling.

Each strategy has pros and cons, outlined in the table below:

Maintain a Minimum Viable Response Capability, back it up, and restore the snapshot after an incident.	
Pros:	**Cons:**
Quick access to functional systems during response	Patching and updates require more steps (rebuild, update/patch, backup), which require ongoing resources. These steps may introduce errors that impact response and recovery. Suppose an organization has been unable to keep IT systems secure and has been impacted by the incident. What is the guarantee that the Minimum Viable Response Capability systems that have been built and backed up will not have the same problems?
Ability to restore only required components	Occupies exponentially more space in the digital jump bag, incurring licensing costs
	It may need to be updated and patched during a response, causing delays
	May introduce infrastructure dependencies
Requirements:	
Perform successful test building MVRC from the digital jump bag	
Take a backup of MVRC, enable legal hold to preserve it for legal purposes, replicate, and archive offsite	

<table>
<tr><th colspan="2">Rebuild the Minimum Viable Response Capability from trusted sources after an incident</th></tr>
<tr><th>Pros:</th><th>Cons:</th></tr>
<tr><td>Relatively easy to maintain sources, as when there is a new version of an operating system, application, or configuration, this is simply exported to the jump bag.</td><td rowspan="4">Requires time to rebuild the infrastructure</td></tr>
<tr><td>Very portable via replication and archival</td></tr>
<tr><td>More adaptable to hardware and platform changes</td></tr>
<tr><td>The backup footprint in the digital jump bag is significantly lower (i.e. one Windows Server 2025 image is around 3.6 GB and may be shared among different systems, whereas each server in the Minimum Viable Response Capability that used that image would require around 35 GB).</td></tr>
<tr><th colspan="2">Requirements:</th></tr>
<tr><td colspan="2">Establish a process for populating and updating the digital jump bag</td></tr>
<tr><td colspan="2">Practice different scenarios of using the contents</td></tr>
<tr><td colspan="2">Keep necessary hardware on hand, or define a process to securely wipe existing hardware</td></tr>
</table>

Conclusion

In the face of increasingly sophisticated and destructive cyberattacks, organizations must move from reactive recovery to strategic resilience. This entails integrating a comprehensive digital jump bag into their incident response strategy to be better positioned to respond quickly to cyberattacks. A well-prepared digital jump bag enables the MVRC and serves as the foundation of a clean room—equipping security teams with the essential tools, processes, and documentation needed to investigate incidents, contain threats, and restore operations with minimal disruption.

The Cohesity Clean Room solution provides a trusted environment that speeds incident response and supports investigations while minimizing the risk of secondary attacks.

Thanks to a modular design, Cohesity rapidly creates an isolated environment, supporting the response and recovery process and allowing teams to collaborate in mitigating threats faster.

About Cohesity

Cohesity is the leader in AI-powered data security. Over 12,000 enterprise customers, including over 85 of the Fortune 100 and nearly 70% of the Global 500, rely on Cohesity to strengthen their resilience while providing Gen AI insights into their vast amounts of data. Formed from the combination of Cohesity with Veritas' enterprise data protection business, the company's solutions secure and protect data on-premises, in the cloud, and at the edge.

Backed by NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud, and others, Cohesity is headquartered in San Jose, CA, with offices around the globe. To learn more, follow Cohesity on LinkedIn, X, and Facebook.

Learn how Cohesity can accelerate your journey to modern data security at www.cohesity.com.

Recommended reading

We think you'll find the following white papers, guides, and blogs helpful.

- Building cyber resilience in a world of destructive cyberattacks
- Modern data security and management topologies: A guide for IT leaders
- Introducing the Cohesity clean room design
- A field guide for AI-powered data security: How to deliver breakthrough business outcomes
- An executive's guide to modern data security and management

Learn more at Cohesity

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000056-002-EN 4-2025