ESG First Look

How Cyber Shield Features within Cobalt Iron Compass Enable Ransomware Recovery

Date: October 2021 **Author:** Vinny Choinski, Senior Analyst; and Tony Palmer, Senior Validation Analyst

Cyber-recovery Data Protection Challenges

The percentage of IT/information security executives and managers that believe **cyber-risk is greater than it was 2 years ago**.[1]

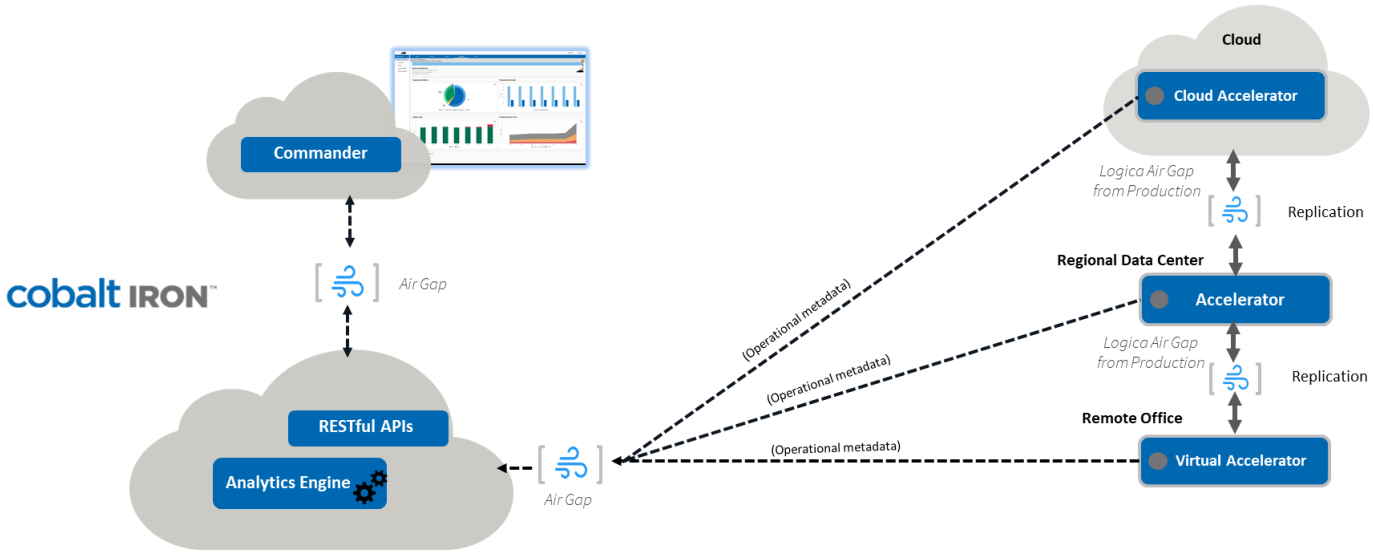
The percentage of data protection professionals that identified **loss of employee productivity as a major impact that could result from application downtime or lost data**.[2]

IT executives are noticing an increasing risk of cyber-attacks. And this risk is leading them to build more comprehensive data protection and cyber-resiliency strategies in an effort to protect their organizations from the detriments of application downtime and lost data. ESG research also shows that loss of employee productivity is the most cited impact that respondents believe could result from application downtime or lost data, followed by other challenges such as diversion of IT resources from business-critical projects, loss of customer and employee confidence, loss of revenue, and more.

Cobalt Iron Compass Overview

Compass is a SaaS platform that plugs in and embeds various backup, storage, and cloud technologies to deliver enterprise backup in a software-as-a-service model. The Compass architecture is a new technical approach to data protection that harnesses analytics and automation to drive down cost and complexity while delivering reliable, secure, immutable data and ransomware protection as well as valuable data insights to the business.

Figure 1. Cobalt Iron Compass Overview



Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *Cybersecurity in the C-suite and Boardroom*, February 2021.
[2] Source: ESG Research Report, *Real-world SLAs and Availability Requirements*, October 2020.

With the Compass platform, backup and storage technologies are completely managed, configured, maintained, monitored, and continually optimized with best practices, allowing the power of these technologies to be experienced without the complexities. Metadata is constantly collected from Compass Accelerators and sent to the Compass Analytics Engine where it is transformed into real-time intelligence, displayed in Commander, and leveraged to enhance overall automation and recoverability. Key solution elements of the Compass solution include:

- Commander: an easy-to-use, efficient web interface providing a simple and intuitive user experience to monitor, manage, survey, and analyze all of the Compass-protected systems. RESTful APIs are integrated to connect with many elements.
- Analytics Engine: a machine learning-based engine that delivers data protection efficiency through metadata analysis. Using this metadata, Compass provides improved operations, proactive problem avoidance, and automated efficiencies through 22 worldwide cloud data center locations in a SaaS model.
- Accelerator: a converged, integrated, and scalable enterprise-class data protection system, which lives where your data resides and is constantly monitored, maintained, and enhanced. Each Accelerator, whether physical or virtual, on-premises or in the cloud, can stand alone or work with a replicated Accelerator to further enhance data protection.
- Agents and APIs: connect with and protect systems and applications. They include a comprehensive list of file systems, applications, and databases. API integrations allow coordinated systems management with business tools such as ServiceNow, Ansible, Chef, Puppet, vRealize, and others.

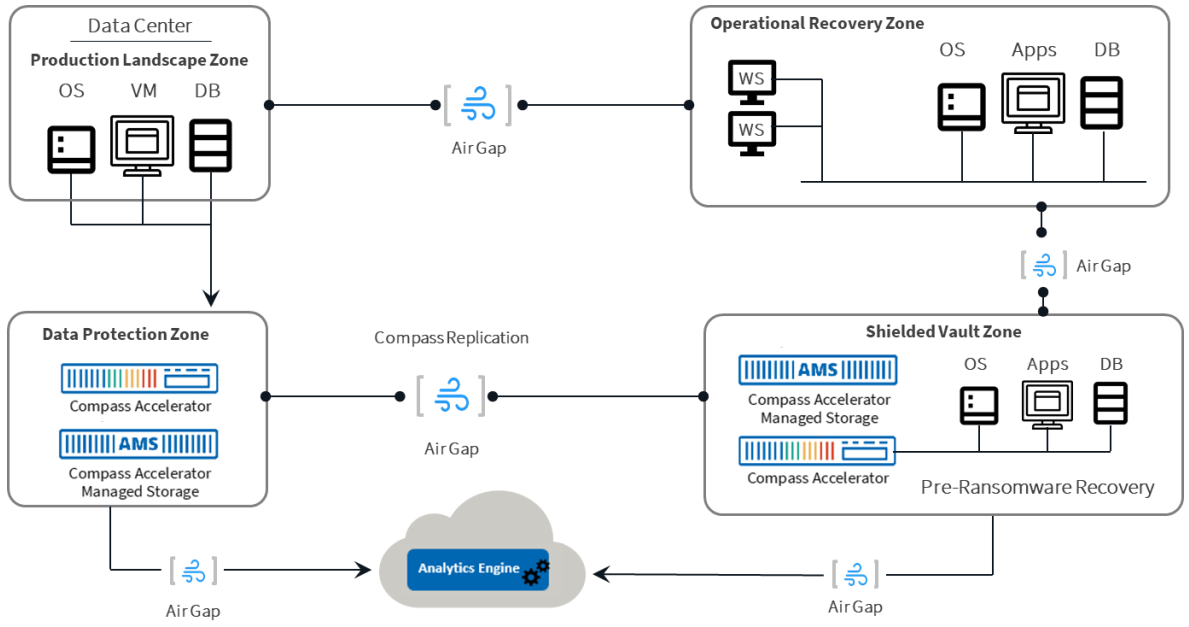
ESG Demo Highlights

ESG performed a detailed evaluation of the Compass Cyber Shield features by participating in an interactive demo hosted by Cobalt Iron subject matter experts. The evaluation focused on highlighting the solution's cyber-recovery capabilities.

Cyber Shield Overview

So, what is Cyber Shield? Its's a name for the features within Compass that were in the architecture from the beginning, are enhanced/hardened with each release, and help customers create cyber-resilient workflows in their data protection environments.

Figure 2. Cyber-resilient Data Protection Workflow Overview



Source: Enterprise Strategy Group

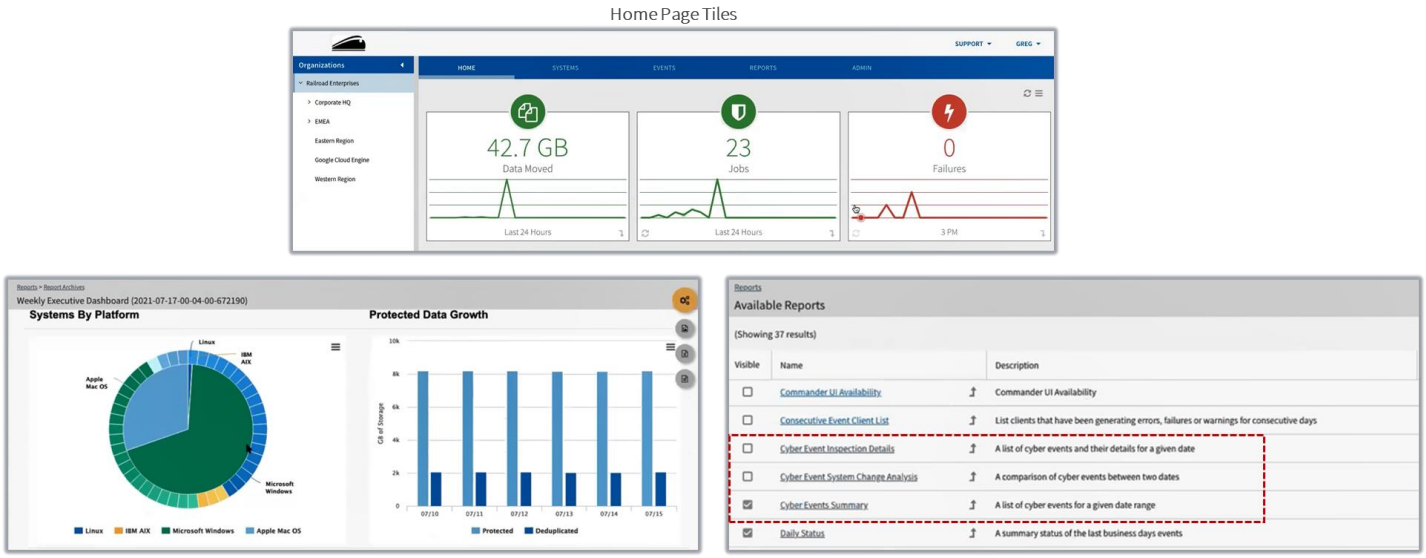
These features include the logical and physical separation of the Compass SaaS management interface from the actual data protection infrastructure, as well as the ability to create immutable data protection copies and logically or physically airgap those copies when necessary. Probably most important is the ability to identify anomalous data protection images and reliable recovery points. Key Cyber Shield features include:

- Analytics: provides the ability to analyze past data patterns to make assumptions and drive optimal decisions. Compass analytics also provide cyber event impact analysis, which includes identification of possibly infected systems and files, recommended object recovery lists, and recommended recovery points.
- Inaccessibility: eliminates almost all typical ransomware attack vulnerabilities in backup landscape.
- Immutability: creates read-only access after write—immutable by default data protection copies.
- Physical and Virtual Air Gap: enhances security measures by providing physical and virtual fault isolation zones.
- Encryption: provides the ability to protect data against unauthorized data exposure and data theft.
- Vault: creates an operational zone that isolates visibility and access to the data protection infrastructure.
- Data Governance: gives comprehensive visibility and auditing of backup operations over time. This allows you to prove what happened during a cyber event.

Data Protection Visibility and Insight

Next, ESG explored the monitoring and reporting capabilities of the Compass solution. As shown in Figure 3, we navigated the user interface pages to demonstrate the intuitive top-down approach to data protection visibility the solution provides.

Figure 3. Compass Monitoring and Reporting Capabilities



Source: Enterprise Strategy Group

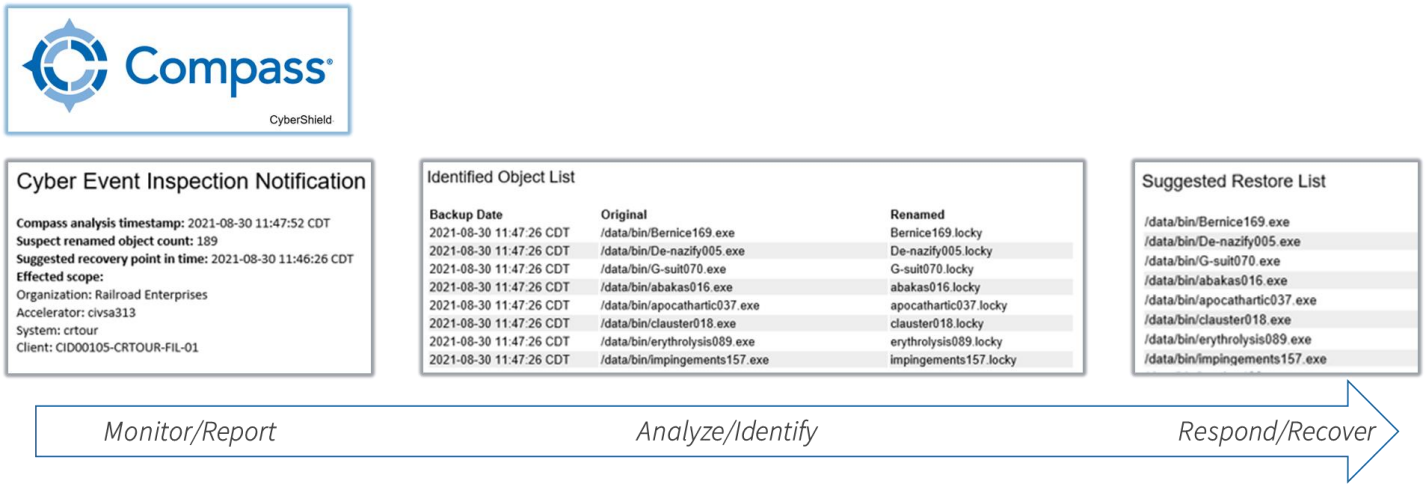
The top of Figure 3 shows the home page, which provides at-a-glance solution status and data trends. The *Data Moved* tile can be used to monitor irregularities in data transfers between backup jobs. The summary dashboard in the bottom left provides a visual representation of weekly trends like *Protected Data Growth*. The bottom right of Figure 3 shows a sample of the many pre-defined reports available in Compass with cybersecurity-specific reports highlighted in the red callout box.

Cyber-recovery Process

Finally, ESG reviewed a recently executed cyber-recovery scenario that simulated an actual Cobalt Iron customer's successful ransomware recovery in the field. At a high level, Cobalt Iron engineers ran a modified ransomware executable that encrypted a set of approximately 200 backup files stored in a Compass solution. As shown in Figure 4, we leveraged a Cyber Event Inspection Notification that was triggered by the event and was automatically sent via email from the solution.

The left side of the figure displays the suspected scope of the cyber-attack and includes the organization, the Accelerator, the system, and the client that were affected. The middle of the figure shows a detailed list of the backup files that were encrypted by the simulated ransomware attack. We used the ***Suggested Restore List*** on the right to recover the files to their original good state on the protected production client. Alternate recovery location options are also available.

Figure 4. Ransomware Recovery Response Process



Source: Enterprise Strategy Group

First Impressions

ESG research found that four of every five IT and information security executives believe there to be more cyber-risk now than two years ago.[3] In fact, the majority (70%) of organizations ESG surveyed reported experiencing at least one ransomware attack over the previous 12 months, and frighteningly, 18% of those organizations reported experiencing ransomware attacks on a daily basis.[4] With this heightened risk must come heightened security. If organizations are looking to become more cyber-resilient, they will need to invest in a solution that can demonstrate a field-tested approach to successful cyber-recovery.

ESG's first impression is that Cobalt Iron Compass is an enterprise-scale, Saas-based data protection platform that is designed to protect customer data, automate operations, provide predictive analytics, and more. The Compass architecture is positioned to safely back up an organization's most critical data and, most importantly, recover that data no matter what caused the data integrity issue. Organizations looking to gain confidence in their data protection strategy with a near-autonomous and simplified backup solution should take a deeper look into Cobalt Iron Compass.

[3] Source: ESG Research Report, *Cybersecurity in the C-suite and Boardroom*, February 2021.
[4] Source: ESG Research Report, *Tape's Place in an Increasingly Cloud-based IT Landscape*, January 2021.