

Analytics-Driven Automation in Cobalt Iron Compass®

“We eliminated about 80% of the time we previously spent managing our backup solution since deploying Cobalt Iron.”

— Travis Cooper
VP and IT Manager
Capital City Bank

Backup and Recovery at a Crossroads

Today's enterprises face daunting challenges in their ongoing quest to safeguard mission-critical data. Data protection is typically the largest application running in the data center, but ironically, it's often an afterthought in IT budgets. A backup administrator's task might seem straightforward—store data, protect it from threats both natural and human, and restore it as quickly as possible when needed—but it's anything but simple.

In these challenging times, it's never been more important for companies to protect data from cyber criminals and ensure effective deployment, operation, and administration of backup systems. Even though they might now be working from home, the onus is still on backup administrators to make sure these critical requirements are covered. But there's good news, in the form of automation and analytics tools built into a next-generation, enterprise software-as-a-service (SaaS) backup solution.

The Compass Difference

Cobalt Iron uniquely addresses these challenges with Compass, its industry-leading enterprise backup platform. Compass enables analytics-driven automation for complex enterprises with terabytes or petabytes of data to manage.

Delivering data protection in a SaaS model, Compass embeds various backup, storage, cloud, and other technologies. Compass' patented software orchestrates these technologies and also adds industry-changing automation and analytics capabilities that transform the business backup experience. Unlike a traditional technology product purchase, Compass customers pay for an enterprise backup outcome.

Compass uniquely solves enterprise backup challenges in the following ways:

- ▶ Compass automates up to 90% of backup operations and backup infrastructure management tasks. With most daily backup management tasks eliminated, administrators are freed to work on higher-value projects and overall costs are reduced.
- ▶ Compass applies analytics-based optimization, keeping all software current (OS, Compass software, backup tooling software, backup catalog software, storage firmware levels, etc.) and continually applying best practices for workload protection, backup tooling, infrastructure, and operations.



SMART.
SECURE.
AUTOMATED.

Third-Party Validation Cloud Backup



- ▮ Cyber Shield™, a set of native security features built into every Compass deployment, implements deep layers of data security including industry-leading ransomware protection, a shield of protection over the backup landscape, authentication control, logical air gap, data immutability, containment, and data governance.
- ▮ Compass provides a single, unified experience for orchestration of multicloud backup infrastructure and operations across on-premises data centers, remote offices, and public clouds.
- ▮ Compass reduces the total cost of enterprise backup ownership through operational automation, extreme scalability, extreme infrastructure optimization, data reduction, and licensing efficiencies.
- ▮ Compass fully leverages the functionality, reliability, scalability, performance, and cost efficiencies of various backup and storage products, public cloud services, VTL, and other technologies. Since these technologies are plugged directly into the Compass platform, they are seamlessly managed, configured, maintained (including software updates), monitored, and continually optimized with best practices. In other words, Compass customers are able to experience the power of these technologies without the complexities.

The Compass Automation Advantage

As we've mentioned, enterprise backup environments are notorious for requiring tremendous care and feeding, with administrators having to spend too much time on mundane tasks just to sustain the many moving parts of the backup operation. Freeing people from these tasks, therefore, is a key benefit of backup automation—but there are many other advantages as well:

Principle of least privilege

The fewer people and entities that have access to data and infrastructure, the more secure those assets are. Compass automation removes a tremendous amount of access and vulnerability at every level.

Operational efficiencies

Since they're spending less time on low-skill tasks, skilled resources can be redirected to opportunities more valuable to the business. In addition to lowered operational expenses, automation often drives more production from the infrastructure—leading in turn to capital expense savings as well.

Policy Domain for Standard Backups/Archives

Name:Policy Domain for Standard Backups/Archives

Protection Type:Files and Operating System Objects

Retention Policies

	Name	Limit Copies	Limit Deleted	Keep Backup	Keep Deleted	Keep Archive
>	Default management class for Standard Backups/Archives	10 versions	1 version	365 days	No limit	No limit
>	Management Class for 10-year retention	1 version		3650 days	3650 days	3650 days
>	Management class for PMP Dump Backups/Archives - 7 Day Reten...	No limit	No limit	7 days	7 days	No limit
>	Management class for VM workstation Backups/Archives	1 version	1 version	30 days	No limit	No limit
>	Management class for Zabbix dump Backups/Archives - 7 Day Ret...	7 versions	7 versions	7 days	7 days	30 days
>	Management class for image Backups/Archives	10 versions	1 version	365 days	No limit	No limit
>	Management class for mysql database backups	No limit	No limit	7 days	7 days	30 days
>	Management class for single copy Backups/Archives	1 version	1 version	30 days	No limit	No limit

Consistent results on time, every time

Policy-based automation not only ensures operations and processes are executed as expected, but according to consistent patterns across the organization as dictated by the needs of the business.

Trust and excellence

Continually tuned automation builds trust in the organization's infrastructure, operations, and processes, further supporting operational excellence and business efficiencies.

“Cobalt Iron Compass provides the broader set of core backup and recovery features that enterprises expect and demand. It simultaneously delivers the new set of anti-ransomware features enterprises want.”

— DCIG

Key Backup Automation Features Built In

Comprehensive backup automation

With Compass, customers never have to log into a backup server again. Compass automates most infrastructure and operational tasks associated with backup. This includes:

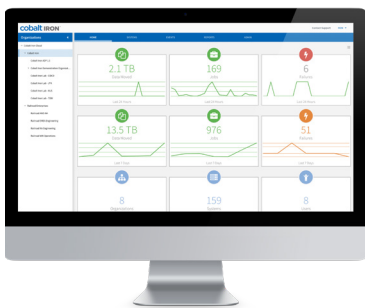
- ▮ Keeping backup server software at the latest validated release levels.
- ▮ Automated configuration, maintenance, monitoring, reporting, best practices tuning, and other administrative tasks.
- ▮ Constant health monitoring and predictive failure analysis of backup server and environment.
- ▮ Proactive problem determination and remediation.
- ▮ Defect identification, management, and resolution with vendors as needed.
- ▮ Automation assistance with file system client installs.
- ▮ Automation of all backup, replication, data migration, scheduling, policy, maintenance, and other backup operations. As an example of the power of Compass automation, certain actions (e.g. policy or schedule changes) in the Compass Commander portal may result in automated updates to hundreds or even thousands of clients.
- ▮ For security and other business reasons, restore continues to be an operation managed directly by the customer.

Automation of storage system tasks

Compass installs storage firmware software and maintains storage controller software levels, ensuring that customers never have to touch this complex part of storage sub-system management. Compass sets up and configures storage arrays to maximize their optimal characteristics. As workloads change over time, Compass changes and tunes the settings of the storage array to maintain optimal operations.

Storage metrics for controllers, drive channels, drives, volumes, and interfaces are continuously collected, monitored, and analyzed. These metrics include:

- ▮ Asset information including tracking of customer hardware and software infrastructure resources for cost accounting, auditability, and operational optimization.
- ▮ Continual views of license conformance to maintain constant audit-ready status.
- ▮ Health indicators and error codes for devices, components, software, and operations, to continually monitor status and health to maintain uninterrupted service.
- ▮ Performance metrics including numerous latency, throughput, read and write Input/Output Operations per Second (IOPs), and other metrics to provide a continuous view of the operational performance of the service.
- ▮ Capacity metrics on storage utilization, consumption, and availability for business planning.



ANALYTICS-DRIVEN AUTOMATION IN COBALT IRON COMPASS

Compass also manages encryption for key usage and rotation within multiple encryption contexts per storage subsystem.

In addition, Compass monitors and tracks storage system hardware issues to resolution. These include:

- ▮ Both predictive failure analysis and complete component failures
- ▮ Problem determination and remediation
- ▮ Defect management and resolution with vendors
- ▮ Coordinating hardware component replacements
- ▮ Installing software, firmware, and microcode updates

Third-Party Validation Best Practices



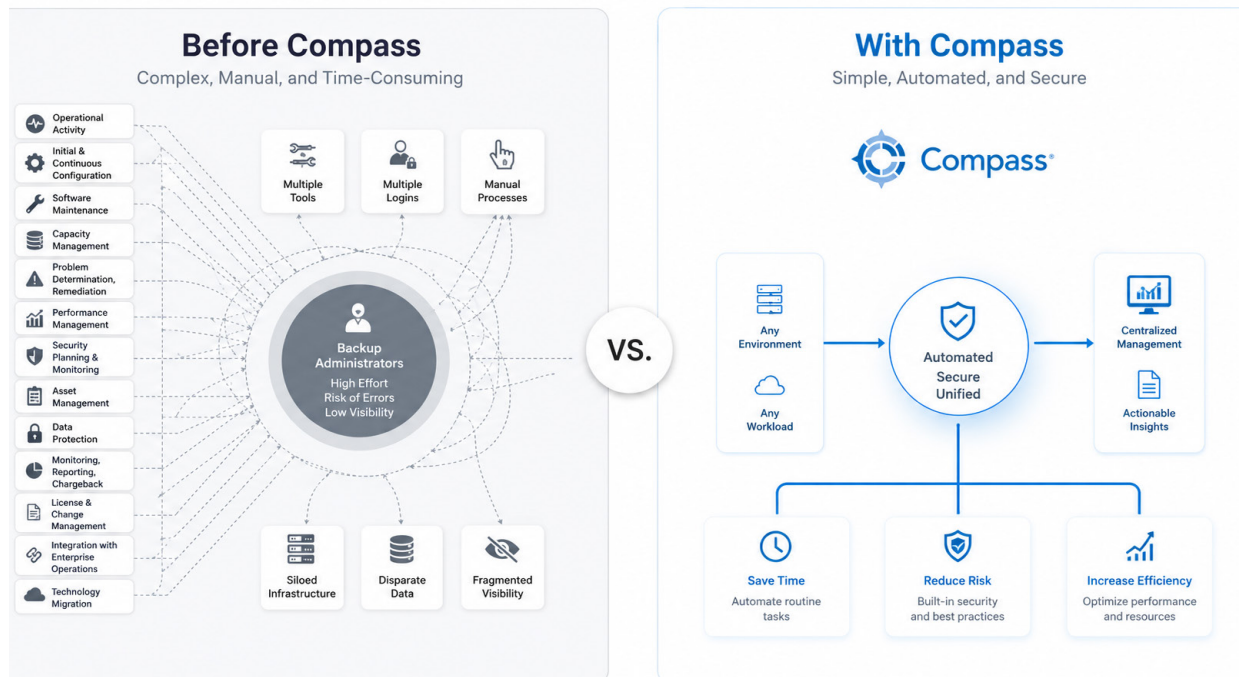
Automated management of other backup infrastructure

Compass manages servers, operating system, backup catalog software, and other backup infrastructure and provides:

- ▮ Automated monitoring, reporting, and optimization of capacity, performance, and health of all backup infrastructure components.
- ▮ Automated currency of all backup infrastructure components.

Automation of Compass platform and product

In addition to the automation described above for customer environments, Compass also includes a tremendous amount of internal automation around its own internal build, test, and deployment processes. Although this automation is not experienced externally by customers, it allows Compass to evolve continually and rapidly.





Industry-Defining Analytics

Compass analytics are informed by the system's extensive data collection and monitoring on backup infrastructure and operations, as well as on environmental conditions. Through the automation capabilities described previously, Compass constantly monitors and analyzes metrics, conditions, and events associated with backup infrastructure, operations, and environment.

The ever-expanding set of Compass analytics includes:

- **Simple capacity analytics**—Compass continually tracks free and utilized resources with historic and predictive analytics including trending at all levels, out-of-space projections, and future modelling based on past growth rates.
- **Performance analytics**—including out-of-bounds performance metrics on storage, servers, networks, and backup operations.
- **Health analytics**—including analysis of exhaust (metadata and metrics) for errors, recurring transient errors, out-of-bounds health metrics, predictive failure analysis, problem avoidance, etc.
- **Cyber-attack detection and other security analytics**—including monitoring various metrics, conditions, and events and analyzing for indications of ransomware or other security attacks. Specific examples of security analysis include: data or deduplication rate anomalies, file type anomalies, abnormal operational behaviors, any unauthorized access attempts into the Compass Commander portal, and any access attempts into any of the Compass infrastructure components.

Many of these analytics are internally optimizing, meaning Compass may make adjustments to its own operational and infrastructure management based on conditions, behaviors, and events it detects across the entire Compass universe.

Also, it is important to note that Compass is continually evolving and learning. Cobalt Iron regularly adds additional automation and analytics to the Compass platform, which makes them immediately available to customers.

Analytics-driven automation in the Cobalt Iron Compass solution is defining the future of enterprise backup.

Third-Party Validation Anti-Ransomware

