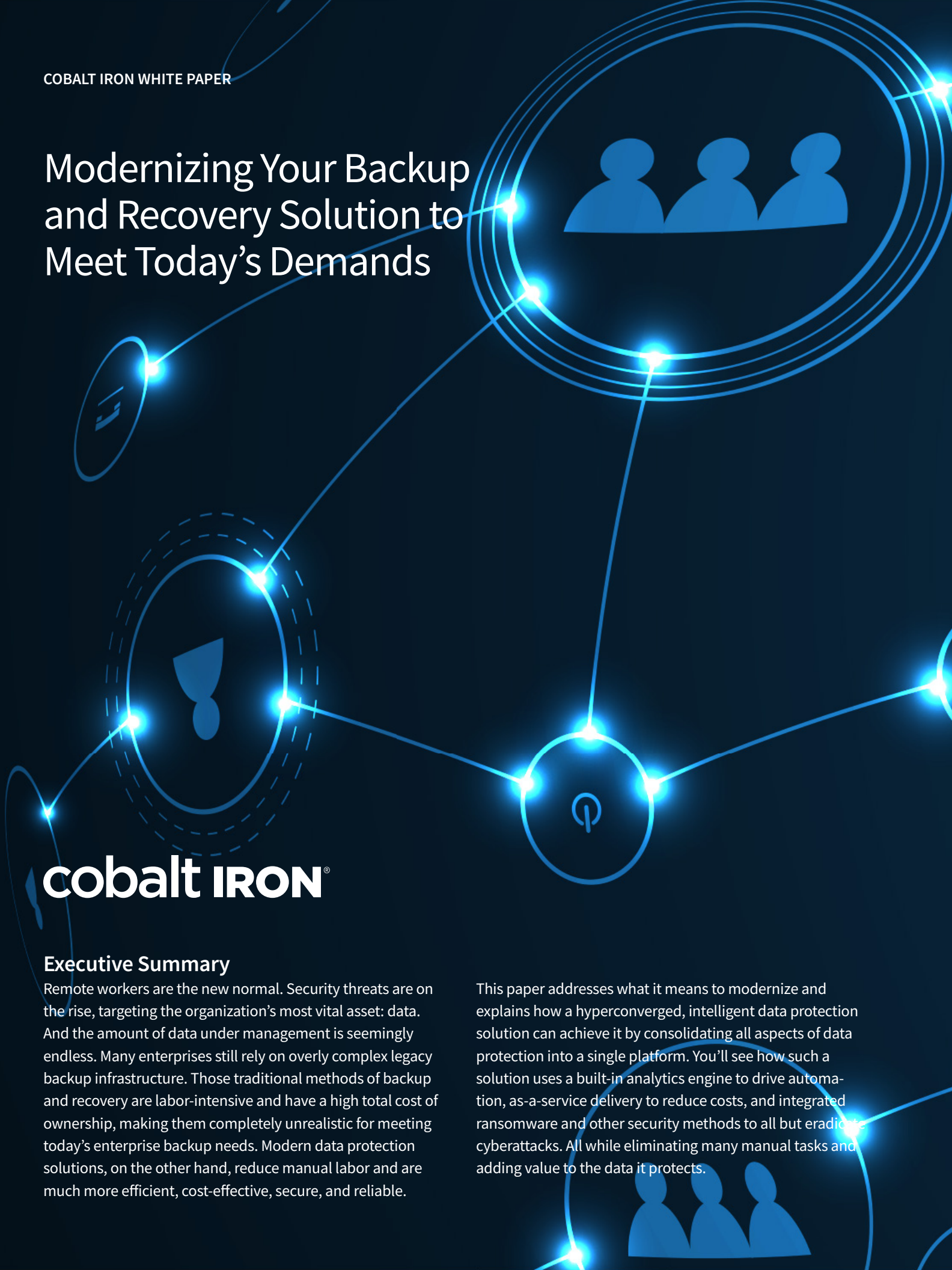


Modernizing Your Backup and Recovery Solution to Meet Today's Demands

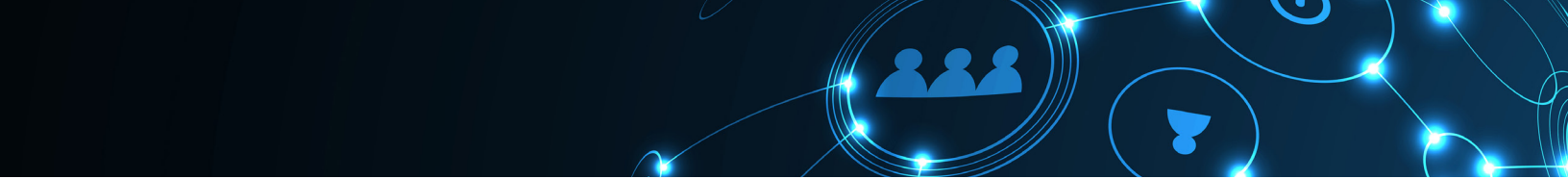


cobalt IRON®

Executive Summary

Remote workers are the new normal. Security threats are on the rise, targeting the organization's most vital asset: data. And the amount of data under management is seemingly endless. Many enterprises still rely on overly complex legacy backup infrastructure. Those traditional methods of backup and recovery are labor-intensive and have a high total cost of ownership, making them completely unrealistic for meeting today's enterprise backup needs. Modern data protection solutions, on the other hand, reduce manual labor and are much more efficient, cost-effective, secure, and reliable.

This paper addresses what it means to modernize and explains how a hyperconverged, intelligent data protection solution can achieve it by consolidating all aspects of data protection into a single platform. You'll see how such a solution uses a built-in analytics engine to drive automation, as-a-service delivery to reduce costs, and integrated ransomware and other security methods to all but eradicate cyberattacks. All while eliminating many manual tasks and adding value to the data it protects.



Yesterday's backup methods don't fit today's needs. With the amount of administration and management that goes into daily enterprise backup operations, the sheer volume of data, the ever-evolving cybersecurity threats, and the mass move to remote workflows, traditional data protection solutions just aren't viable anymore.

Today's enterprise backup environments need a data protection solution that's more affordable and more hands-off. Not only that, but it should be scalable and agile and offer better data visibility. It must simplify operations and integrate with other solutions. And it must be an all-encompassing, secure solution that not only protects the data at rest and in flight, but also protects you from outside threats.

What does modern data protection look like?

Modern data protection has several key markers that make it the best option for today's backup environments.

Hyperconvergence

It starts with a hyperconverged data protection platform, which delivers the entire data protection solution — data protection software, compute, storage, operating system, security, analytics, APIs, administrative functions, and a user interface — in a single architecture. Most traditional data protection solutions require you to buy all of those components separately and then cobble them together. Not so with hyperconverged data protection.

With hyperconvergence, traditional backup and recovery evolves away from discrete software and hardware components with disparate, multipoint systems. Consolidating all the functional elements of data protection into a single hyperconverged data protection platform drives simplicity, eliminates inefficiency, and lowers total cost of ownership for data centers. A hyperconverged platform includes the ability to plug and play into data protection that supports multiple backup and recovery-access software tools in a one-to-many configuration. And you can access all data protection resources in the hyperconverged architecture via a single administrative interface.

Analytics and automation

Two other key attributes that go hand in hand are analytics and automation. Analytics are what make the solution intelligent, which in turn leads to autonomous operations that can be performed by the software itself, requiring no human intervention.

Intelligence is derived from the metadata, which is the natural byproduct of a modern data protection solution in its normal course of operation. Metadata feeds the platform's analytics engine to drive intelligent operations and tasks.

Importantly, if you're using a truly modern, hyperconverged data protection platform, the provider has no access to your data at all. The solution is hermetically sealed and encrypts not only data in flight and at rest, but the metadata used by the analytics engine. No human on the provider side can access your data directly.

And unlike solutions that act on a single metric, a modern solution looks at metrics in combination, which form a problem signature that allows the system to do something automatically and more intelligently — like repeat a backup of a file to ensure reliability or make adjustments to ensure the CPU or memory don't get overloaded. You can also tell the system to alert someone under certain parameters so they can take action on their own.

Finally, because the system is constantly and automatically kept up-to-date with the latest software, operating systems, and security patches across the backup infrastructure, you never have to worry about upgrades again.





Other important distinctions of a modern data protection solution

Built-in security. One of the most important aspects of modern data protection is that the security is embedded into the software — no add-on products or additional purchases needed. Completely integrated security guards against outside threats such as ransomware. The data stored, transmitted, and analyzed is all protected using the most advanced methods in the software industry. Any sign of malice from inside or outside the company is recognized and remediated quickly.

As-a-service delivery. It's a true as-a-service solution that turns ongoing data protection into an operational cost instead of a capital investment. But the benefit goes beyond the pricing model. As-a-service delivery provides smooth installation and configuration and allows you to transition quickly and easily into steady-state daily operations from day one — which makes for a painless onboarding experience.

Rapid recovery. It can quickly recover from any type of failure — hardware or software — anywhere in the environment. The ability to recover data at the file level or system level is not only scalable, but very fast. And the recovery system integrates with other solutions, like VMware's vCenter.

Infinitely scalable. Even though it's hyperconverged, a modern data protection solution has building blocks that let you scale as your data grows. A lot of today's traditional solutions hit a brick wall in terms of scalability, but a hyperconverged data protection platform is virtually limitless.

Cloud support. It is cloud-enabled, with the ability to protect data in the top cloud environments, on prem, or in any combination thereof.

Virtual backup. It also protects virtual environments, which is a critical capability with so many companies moving to remote work these days.

Multisystem, legacy backup. It can back up multiple different types of systems including legacy workloads — unlike other solutions, which might not back up legacy applications and operating systems such as AIX or Db2.

Easy integrations. Through APIs, it integrates easily with other solutions — like customer ticketing and help desk systems or IT workflow management software such as ServiceNow, Chef, Puppet, Ansible, and Remedy. You can also customize what's sent through those APIs for reporting and audit capabilities.

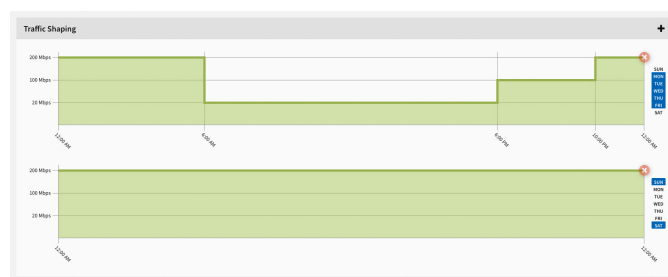
Customized database support. On the database and application side, a modern data protection platform pays attention to the many specific characteristics of a database or application, like SAP HANA, and tunes itself to accommodate those file types and the types of data that come from specific applications. Other solutions treat data more generically.

Multitenancy. It has multitenant capabilities, so you can customize what can be seen and who can see it down to a very granular level.

Custom billing. It allows customizable billing and reports so that you can bill other departments or, if you're a managed service provider, your customers.

Storage choices. Because it's hyperconverged, a modern data protection platform can provide storage as part of the solution, or it can manage and protect whatever storage you choose.

Visibility. Dashboards and reports give you a real-time look at all the data under protection to drive faster recovery time. Plus, it confirms that everything is indeed being protected and ensures you're meeting your SLAs.



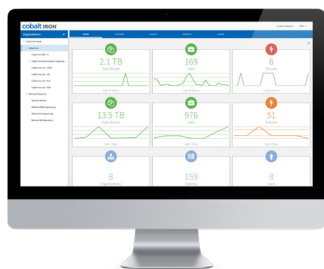
Traffic shaping. From a network perspective, it performs traffic shaping to optimize network performance and ensure data protection operations don't burden the network if there's other activity going on. When bandwidth is available, the solution takes advantage of it to get optimum performance. When it's not, it tones down its access to the network.

Components

Technologically speaking, there are three major components that make up a modern data protection solution:

A hyperconverged appliance. A single piece of hardware is the heart of the hyperconverged data protection platform. Inside the appliance is everything you need for your backup and recovery operation, including compute resources, storage, an operating system, and components for administration, orchestration, reporting, monitoring and alerting, and data acquisition. All in one box that arrives preconfigured and ready to plug in to your network. From there, the provider takes over, and within hours, you have a productive data protection solution. It beats the traditional methods, where you spend weeks or months acquiring hardware, installing software, configuring, testing, tweaking, etc.; not to mention the maintenance.

Analytics engine. The hyperconverged appliance feeds the analytics engine, which has APIs, a data protection abstraction layer, and a mechanism that directs the system's actions based on the metadata being collected.



Interface. A simple, centralized workspace gives you total command over the entire enterprise backup environment. Your users get a unified view and centralized management through an interface that requires no complex training or technology skills.

Conclusion

Cobalt Iron Compass® is the only solution in the market that meets all these criteria and more.

The importance of consolidating many data protection solutions into a single platform cannot be overstated when talking about modernizing enterprise backup. Cobalt Iron is the first to have a true

hyperconverged platform for data protection that combines compute, storage, security, an administrative interface, an operating system, APIs, and analytics into a single system that embraces one-to-many backup and recovery-access tools.

Compass not only improves upon the data it's protecting, but it

also guards against outside threats like ransomware. More differentiators? Compass integrates with other solutions and embraces other data protection tools. It eliminates administrative and maintenance tasks that take a lot of time and resources. And its ability to support both public and private clouds, including the top five major clouds, is unprecedented in the data protection industry.

With Compass, there's no need to add on security components, customize in order to integrate, or buy other things to support cloud. It's an all-in-one solution. And it's all delivered as a service for reduced cost of ownership and better ability to scale.



The importance of consolidating many data protection solutions into a single platform cannot be overstated when talking about modernizing enterprise backup.