

Zero Trust Doesn't Stop Hackers.
Zero Access® Does.





Today's enterprise networks are complex and dynamic. While capability may have bred the complexity, that complexity also breeds vulnerability. In other words, in a highly complex data environment, there's a lot more potential for security breaches.

That's why so many organizations have adopted a zero trust security model for accessing and managing IT resources such as applications, devices, or data. With this approach, a user attempting access to a resource is never trusted by default, even if they are already part of the corporate network. Access is granted only after successful validation using two or more methods of verification, or in other words multi-factor authentication.

Many IT solutions, including most backup and disaster recovery products, trumpet zero trust as the pinnacle of security. Zero trust architecture requires organizations to validate that users and their devices have the right privileges and attributes to access given resources.

While zero trust authentication does provide some level of security hardening, the approach still implies there is access to the allowed resources. That is, the whole point of the process is to grant access to the IT resources after verification. And when someone has access, no matter how legitimate, there's potential for error (or worse).

The best way to completely protect your IT resources, including data, is by not allowing any user or entity to get to them in the first place. In other words, Zero Access.

In fact, a zero trust approach might instill a false sense of confidence in an organization's security posture, leading to less scrutiny of those that do pass authentication processing. This means that if an account or credentials are

compromised, significant damage might be done before the breach is discovered.

The best way to completely protect your IT resources, including data, is by not allowing any user or entity to get to them in the first place. In other words, Zero Access.

A Zero Access approach takes security protection to a higher level than zero trust. Zero accessibility means users have no access at all to the IT resources. Let's take backup environments as an example.

A typical backup application requires:

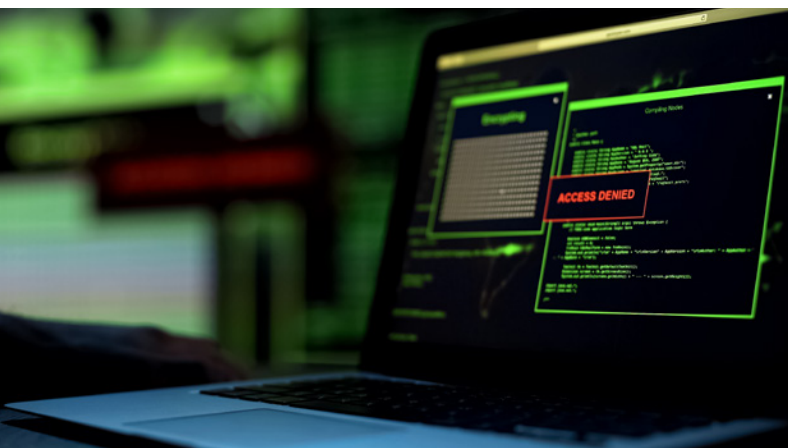
- the backup software,
- a backup server to run on,
- an operating system on that server,
- a backup catalog database,
- a backup network (which may be the same as the primary, production network),
- storage devices,
- reporting tools, monitoring tools, and maybe some security tools.

Each of these hardware and software components includes access for administering them. A backup product may offer multi-factor authentication (ie, zero trust) to access its software. But it is still allowing access to that backup software, and what about all of these other components that it needs to run? And that is just for a single backup server deployment. Many large environments require dozens, or maybe hundreds, of backup servers to protect their corporate data. That's a lot of vulnerabilities, even with a touted zero trust approach by the backup software!

Cobalt Iron® Compass® provides a much more secure, and simpler, approach to enterprise backup using a unique Zero Access architecture.

How is this possible and how is Compass different than zero trust backup solutions?

In most IT environments, administrators install an operating system and backup software on a standard server. They have logins for the operating system, logins for the backup software, logins for the database, logins for any reporting or security tools, and logins to the storage devices where all the backup information is stored. Humans must log in to all of these components, probably using active directory logins or admin logins that are used for other tasks. The fact that humans are logging in with credentials that are part of production systems means that if ransomware was to get access (or destroy access) to any of these credentials, it would get access (or destroy access) to the entire backup environment as well. And that's where the danger lies. Too many vulnerabilities, even with zero trust!



The Cobalt Iron Compass vaulted backup solution is different. Compass software automatically manages and monitors all of the hardware and software components of the backup environment. No access is needed or even allowed to any of the normal components of a backup environment that we discussed above. The Compass unique, Zero Access architecture makes it so no human ever needs to — or is

allowed to — access any of the normal components of a backup infrastructure. Instead, Compass analytics and automation software do the work that is typically done manually.

The essentials of Compass

It starts with the Compass Accelerator which contains the Compass backup technologies and is preconfigured as the backup target. The Compass Accelerator is delivered in a SaaS model that is simpler, and more secure, than even hyper-converged models in that it requires no ongoing management, and allows no access, after deployment. Compass tracks every aspect of backup operations, infrastructure, software updates, customer service levels, etc. such that the Compass backup infrastructure is audit ready at all times. The Accelerators serve as the backup infrastructure for an enterprise, replacing all other components and removing all vulnerabilities associated with those components.

The Compass Analytics Engine is a software component that lives in the cloud. The Analytics Engine uses automation and analytics to ensure all backup and data management tasks are carried out on all Accelerators according to customer-defined policies. Accelerators communicate with the Analytics Engine via hyper-secure connections.

Users experience Compass by logging in to the Compass Commander interface. Commander connects to the Analytics Engine and the Analytics Engine communicates with the Accelerator. That in-between layer prevents any human access to the Accelerator backup infrastructure. Commander allows users to establish policies (eg, retention periods, schedules, etc.) and have visibility (eg, dashboard into operations, reporting, etc.) into all aspects of their backup operations. Commander is accessed via zero trust, multi-factor authentication. However, even super-user privileges to Commander give Zero Access into the Accelerator backup infrastructure.

Zero trust will never stop bad actors, and you won't know they've hit you until it's too late. That's why Zero Access should be the backup model of the future.

Compass is the only backup solution out there to offer Zero Access, and it can replace any other backup products.

888-584-4766 • www.cobaltiron.com

cobalt IRON®

© 2024 Cobalt Iron, Inc. All rights reserved. Cobalt Iron, the Cobalt Iron logo, the Cobalt Iron agent logo, Compass, the Compass logo, "Data Protection Everywhere. Smart. Secure. Automated.", and Take Control of Your Data are trademarks of Cobalt Iron. All other trademarks or registered trademarks are the property of their respective owners. 100323