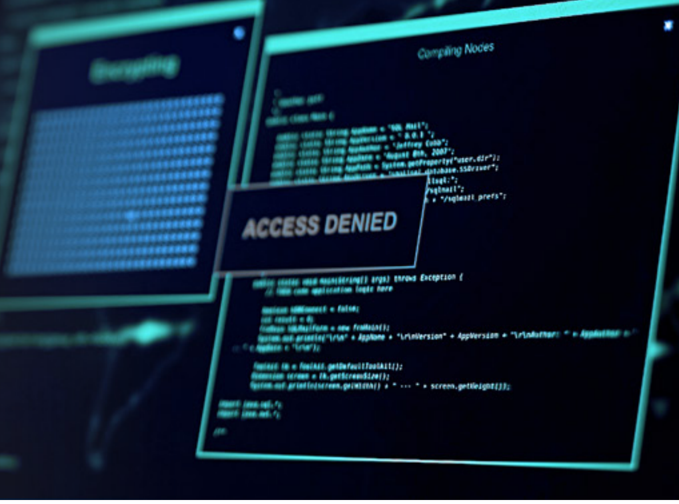
cobalt IRON®



Backup Environment Security Vulnerability Questionnaire

Review and answer the following key questions to improve your enterprise data protection. This self-assessment will help you understand and improve critical elements to your organization's backup data protection.

BACKUP ENVIRONMENT ACCESS CONSIDERATIONS	WITH COMPASS®	TYPICAL ENTERPRISE GRADE DEPLOYMENT	YOUR ENVIRONMENT?
Do you have a Zero Access® backup environment that eliminates access to backup server hardware and software components and backup data?	Yes	No. Even most hardened backup environments have dozens of vulnerabilities	
Who has access to the OS on your backup server(s)?	Nobody	Systems team and others	
Who has access to your backup server software?	Nobody	Backup team and others	
Who has access to your backup catalog database?	Nobody	Database team and others	
Who has access to your backup storage network?	Nobody	Network team and others	
Who has access to your backup storage repository?	Nobody	Storage team and others	
Is your backup storage isolated from your production network and the internet?	Yes	Regularly not, especially with NFS and SMB/CIFS attached storage	
Does your backup product include reporting, security, backup database, monitoring, and analysis capabilities inherently without introducing additional access vulnerabilities? If these are separate tools, who else has access through these to the backup environment?	Yes	Almost all backup products require separate tools for these functions with separate access from multiple teams	
Are backup operations and administration software automated to limit access, reduce vulnerabilities, and simplify operations?	Yes	Almost never	
Do you employ robust authentication including MFA to your interfaces for visibility and management without granting any access to actual backup components or backup data?	Yes	MFA and Zero Trust are often used but access is provided to backup components	
Is there OpenSSH access to your backup product or other components of your backup infrastructure?	No	Backup and other products commonly allow OpenSSH login access	

BACKUP VAULTING AND SECURITY ZONES	WITH COMPASS®	TYPICAL ENTERPRISE GRADE DEPLOYMENT	YOUR ENVIRONMENT?
Does your backup product(s) establish multiple, fault-tolerant, isolated security zones?	Yes	This is done only at great expense in the most restrictive environments	
Is your backup data always locked down and vaulted within your isolated security access zones?	Yes	This is rarely done and usually at great expense	
Does your backup deployment have multiple zones of logical airgap?	Yes	Single point of airgap is common but rarely multiple	

BACKUP DATA SECURITY	WITH COMPASS®	TYPICAL ENTERPRISE GRADE DEPLOYMENT	YOUR ENVIRONMENT?
Does your backup product(s) create multiple, automatically managed copies of backup data, including off-site copy(copies)?	Yes	Yes, most backup products are good at this	
Does your backup product perform data integrity checks on all data at ingest and recovery at both block and file level, and during replication/copy events?	Yes	Only a few backup products provide this	
Does your backup product perform encryption at all phases of your data being protected: on the source system, in-flight, to-storage, and at-rest?	Yes	Most perform some combination of source, in-flight, and at-rest. Very few provide to-storage encryption. Encryption options are commonly not turned on.	
Does your backup product perform automated, periodic encryption key management/rotation and TLS certificate management/rotation?	Yes	Almost none do	
Is your backup data immutable with additive ingest only to eliminate data overwrites, destruction, or mutation?	Yes	Very few backup environments are hardened to this degree	
Is your backup data inert (not possible to execute)?	Yes	Most backup products have inert repositories	
Is your backup data only able to be deleted based on defensible deletion retention policy only? With notifications of any retention policy changes?	Yes	Most products provide policy, but few provide notification on policy changes	
Do you have comprehensive data governance with audit readiness at all times for all aspects of your backup infrastructure and operations?	Yes	Backup audit readiness is very rare, typically just a few incomplete reports	
Do you maintain backup data locality policy control and enforcement to meet required regulations?	Yes	Most do not but can be done at great effort	

CYBER ATTACK MONITORING, DETECTION, ANALYTICS, REMEDIATION	WITH COMPASS®	TYPICAL ENTERPRISE GRADE DEPLOYMENT	YOUR ENVIRONMENT?
Is ransomware monitoring, detection, and notifications performed as part of your backup operations to identify data distortion patterns?	Yes	Sometimes, usually with separate tools	
Is DDoS detection and protection performed across your entire backup infrastructure and componentry?	Yes	Almost never	
Do you perform automated rejection and logging of all unauthorized activities across your entire backup environment?	Yes	Almost never	
Does your backup product provide cyber-attack event impact analysis?	Yes	Rarely, and using a separate tool	
Can your backup product analyze cyber events over time and across domains worldwide in your company to detect cyber-attack patterns?	Yes	Rarely, and using a separate tool	
Is your backup product able to identify potentially infected systems and files?	Yes	Becoming more common	
Is your backup product able to provide recommended clean recovery points?	Yes	Rarely, and often using a separate tool	
Does your backup product automatically update itself and the infrastructure it uses with new security patches to your OS, backup software, backup catalog, and storage devices?	Yes	No	
Does your backup product automatically deploy new security countermeasures based on new, emerging, attack patterns in the market as well as on other companies cyber event experiences?	Yes	No	

While eliminating all bad actors is impossible, Compass Zero Access® empowers you to fortify your backup environment, reducing risks and accelerating recovery. Schedule your free backup security consultation today!

Book Now!

cobalt IRON®

888-584-4766 • **www.cobaltiron.com**