CyberFortress™
Defense to Recovery. No Gaps.

SOLUTION BRIEF

Docker Backup and Restore

Backup, monitoring, threat detection, and guided response for Docker environments. One collector, one console, built for managing many customers.

Docker workloads escape conventional backup

Critical data in Docker environments lives in volumes, bind mounts, database containers, Compose files, and locally built images. Server backups don't see these parts or what's going wrong inside them: restart loops, vulnerable images, suspicious processes, ransomware activity. Trinity understands Docker natively and brings protection and detection together in one place.

What Trinity delivers

Docker-aware backup

Volumes, bind mounts, Compose files, container configuration, networks, and local images, plus application-consistent dumps for PostgreSQL, MySQL, MariaDB, and MongoDB. Scheduled or on demand, with a preview of size and contents first.

Controlled recovery

Restore everything or just the volumes you need. Trinity stops affected containers, restores verified data, and brings them back up. Checksums validate every recovery point.

Continuous monitoring

One view per host: resources, container health, volume growth, network activity, SSH attacks, and full backup history. Image CVE scanning highlights critical vulnerabilities with fix guidance.

AI-assisted response

Alerts arrive with summaries, likely causes, and a remediation plan: stop a compromised container, block a malicious IP, pause and preserve. Nothing runs without administrator approval, and every action is logged.

Before any on-demand backup runs, Trinity shows you exactly what it will protect and how large it will be. Every recovery point is verified with checksums, sensitive values are redacted before data leaves your host, and reporting is honest by design: a backup that skipped items shows as degraded, never as a success.

1
Lightweight collector
One install command per host. It backs up, monitors, and remediates, and keeps itself updated.

60s
Always current
Hosts check in about every minute with health and security telemetry.

10 yrs
Retention range
Policies from 1 day to 10 years, with immutable recovery points where supported.

Up and running in three steps

1

Add the host

Pick the customer, name the host, and choose a backup policy in the Trinity console.

2

Run one command

Paste the generated install command on the host. The collector registers securely and starts as a service.

3

Protected

The host checks in within a minute, backups run on schedule, and the collector updates itself from then on.

Built to be trusted

Backup software only earns its keep on the worst day. Trinity is engineered so that what you see in the console is what you can actually recover:

- Compliance-mode immutability locks recovery points so no one, not ransomware and not even an administrator, can delete or alter them until the window expires
- Sensitive environment values are redacted before data leaves the host
- Stalled or failed jobs retry automatically; overdue backups raise alerts
- Optional email alerts for failed or degraded backups and restores
- Every recovery point carries a manifest and checksums, verified on restore
- Encrypted storage and time-limited signed transfer links by default
- Backups run at reduced priority so production workloads come first

Why it matters

- ✓ Recover application data in minutes, not a full host rebuild
- ✓ Ransomware resilience through locked, verified recovery points
- ✓ Catch operational and security problems before customers do
- ✓ Less tool sprawl: backup, monitoring, and response in one platform
- ✓ Shorter investigations with consolidated telemetry and AI assistance

REQUIREMENTS

Linux AMD64 with Docker Engine and systemd. Root or sudo to install. Outbound HTTPS to Trinity and object storage. Restores, deletions, and remediation always require admin privileges.

See Trinity protect your first host in minutes

Talk to a CyberFortress specialist about Trinity Docker Cyber Resilience.

cyberfortress.com