



Degarmo Technologies

Keeping you connected

KEEPING YOU CONNECTED

PRODUCT BROCHURE

DT Endpoint Backup

Continuous Cloud Backup for Every Managed Endpoint.

Servers have been protected by backup for decades. Laptops and workstations — where your employees actually create data — are largely unprotected. DT Endpoint Backup closes that gap with continuous, automatic cloud backup for every managed device.

Continuous

AUTOMATIC BACKUP ON
EVERY FILE CHANGE

30 Days

FILE VERSION HISTORY
PER DEVICE

< 1 Hour

RECOVERY TIME
OBJECTIVE (RTO)

Zero

RANSOM PAID ON
SUCCESSFUL
RECOVERY



THE PROBLEM

Your Endpoints Are Your Biggest Backup Gap

Servers are backed up. Laptops are not. That is where your business data actually lives.

Where Business Data Actually Lives

Research consistently shows that 70% or more of business-critical data lives on employee devices — not on servers or cloud storage. Sales proposals, financial models, client communications, project files — all created and stored locally on laptops and workstations that have no backup protection. When those devices fail, that data is gone.

140K

HARD DRIVES FAIL
EVERY WEEK IN THE US

70M

DEVICES LOST OR
STOLEN GLOBALLY EACH
YEAR

66%

RANSOMWARE TARGETS
ENDPOINT DATA
DIRECTLY

94%

BUSINESSES THAT LOSE
DATA DON'T SURVIVE 2
YEARS

What DT Endpoint Backup Protects

User Profile & Documents

All user profile folders — Documents, Desktop, Downloads — are protected by default. Additional folders are configured per your environment.

Local Business Data

Any data stored locally that is not synced to a file server or cloud drive — the most vulnerable data in your environment.

Project & Creative Files

Large project files, design assets, and work-in-progress data that employees save locally for performance reasons.

Configuration & Settings

User-specific application configurations that would need to be manually recreated after a device failure.



HOW IT WORKS

Continuous, Automatic Cloud Backup for Every Managed Device

The moment a file changes, it is protected — with recovery managed end to end by Degarmo Technologies.

How DT Endpoint Backup Works

- 1 Continuous File Monitoring.** A lightweight agent monitors designated folders for any file changes. The moment a file is saved, modified, or created, a new version is captured and queued for upload.
- 2 Encrypted Cloud Upload.** All backup data is encrypted in transit and at rest — sent to our secure cloud infrastructure with redundant storage across multiple geographic regions.
- 3 30-Day Version History.** Every version of every file is retained for 30 days — enabling point-in-time recovery to any previous state, not just the most recent backup.
- 4 Managed Recovery.** Degarmo Technologies manages all restore operations — locating the correct version, initiating the transfer, and verifying successful recovery on your behalf.

Recovery Scenarios

Scenario	Recovery Method	RTO	RPO
Accidental file deletion	Point-in-time restore from archive	< 1 hour	< 15 min
Ransomware encryption	Restore from pre-infection version	< 2 hours	< 15 min
Hardware failure	Full profile restore to new device	< 4 hours	< 15 min
Lost or stolen device	Cloud restore to replacement device	< 4 hours	Last sync
Accidental overwrite	Previous version restore	< 30 min	Last save
No backup (comparison)	Data permanently lost	Days–weeks	N/A



RECOVERY & COMPLIANCE

Fast Recovery. Documented Protection. Compliance Evidence.

DT Endpoint Backup satisfies both business continuity and compliance requirements.

Compliance Framework Alignment

Framework	Requirement	Coverage
HIPAA Security Rule	§164.308(a)(7) — Contingency Plan	✓ Backup & recovery documentation
PCI DSS v4.0	Req. 12.3 — Recovery Plans	✓ Documented endpoint backup program
NIST CSF — Recover	RC.RP — Recovery Planning	✓ Tested recovery procedures + evidence
CMMC Level 1	MP.1.118 — Media Protection	✓ Backup of CUI on endpoints

Managed Backup Program

Agent Deployment

We deploy and configure the backup agent across all managed endpoints — with folder policies tailored to your data environment.

Backup Monitoring

We monitor backup success rates and alert on failures — ensuring every device is protected without you having to check.

Recovery Management

All restores are handled by our team — from identifying the correct version to verifying successful recovery.

Monthly Compliance Reports

You receive documented evidence of backup status and recovery testing — ready for auditors and cyber insurance underwriters.



GET STARTED

How Much Data Would You Lose Today?

Degarmo Technologies can assess your current endpoint backup coverage and show you exactly which devices and data sets are at risk — at no cost. Most businesses are surprised by how much is unprotected.

◆ **Free Endpoint Backup Assessment**

◆ **Deployment in Days**

◆ **Same-Day Support**

Start the conversation today.

Visit degarmo.tech · Oklahoma City, OK · Veteran-Owned MSSP

degarmo.tech
support@degarmo.tech