

Data Protection Comparison

Review of current data protection solutions and how they compare on key features and components to keep your data safe.

Trivalent Protect™ employs a unique protection process of encryption, shredding, dispersal with secure storage and recombination, resulting in data becoming unusable and completely unrecoverable to unauthorized users.

Full Disk Encryption is designed to protect data on a device when it is powered off or in hibernation mode (based on configuration). If the device is stolen or lost in these modes, Full Disk Encryption will keep data encrypted. However, when the device is powered on either in sleep mode or during runtime Full Disk Encryption already has unlocked the drive(s) making all data vulnerable.

Trivalent Protect will safeguard data regardless of device state - powered off or powered on whether the device is lost, stolen or in the event of a breach over the network. In addition, software based Full Disk Encryption introduces a significant performance hit, whereas Trivalent Protect has minimal impact on device performance.

Data Protection Comparison Chart

SOLUTIONS	FEATURES					
	Encryption	Shredding	Protection at Runtime	No Performance Latency	Fast Bootstrap & Bootdown	NIAP/CSfC Certification
Trivalent (File Level)	✓	✓	✓	✓	✓	✓
Dell Endpoint (File Level)	✓			✓	✓	
Windows BitLocker (Full Disk)	✓					✓
WinMagic (Full Disk)	✓					
ViaSat (Self-Encrypting)	✓			✓	✓	

Current data protection mechanisms are clearly not working, or are too hard to implement effectively. Trivalent provides real data protection that is easy to use.

Trivalent Protect deploys in minutes, works seamlessly with existing infrastructure, and never puts your data at risk again.

Secure Data-at-Rest

Special Forces can now protect top secret data with a complete software solution to support tactical and strategic missions.

Trivalent Protect™ is the only NSA approved file security solution under the CSfC program fully supported in the USA.



NEXT GENERATION DATA PROTECTION

Data security that is applied directly at the file level, with protection techniques that supersede traditional encryption and infrastructure security methods.

Trivalent's Data Protection Platform protects mission-critical data at rest (DaR) in the file system of a device so it remains safe from unauthorized use.

Critical and classified information on Getac devices will:



Meet Government (i.e. DoD, Intelligence Community) Top Secret and layered protection file encryption requirements



Security Always Stays with the Data: in both connected and disconnected modes and scales to meet mission needs



Cost Effective: Commercially sustainable and dedicated support in the USA

About Trivalent

Founded in 2010, Trivalent's next generation data protection stays with data to keep information safe and industries thriving. Trivalent supports the classified or sensitive data protection needs of Government agencies (DoD and Intelligence communities) and companies in regulated markets, such as Healthcare and Financial Services.