# Kaseya®

UNITRENDS
FIPS

FIPS Mode for Unitrends

Cyber resilience for regulated, compliance-driven environments

FIPS Mode for Unitrends empowers IT teams to deliver strong, compliance-aligned data protection for organizations operating in regulated industries, including government, health care, financial and legal sectors.

Available at no additional cost, this optional mode introduces FIPS 140-3 validated encryption across Unitrends Recovery Series Gen 10 backup appliances and Unitrends Backup virtual appliances (deployed locally on VMware or Hyper-V). It also supports Unitrends Windows and next-gen Linux agents, ensuring your data is protected end to end against theft or breach.

FIPS Mode combines more than 35 years of data protection innovation with FIPS 140-3 validated cryptography so organizations can meet compliance and regulatory mandates without sacrificing the performance, simplicity or seamless continuity Unitrends is known for.
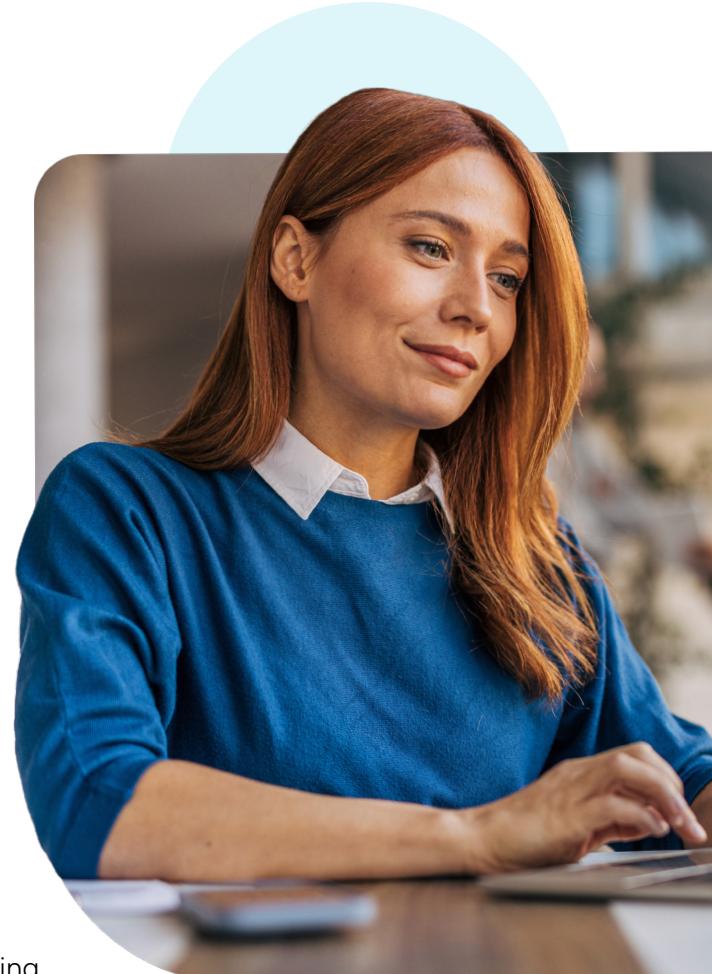
Secure by design

Simplicity and security work hand in hand. The FIPS image is available for any Unitrends Gen 10 Recovery Series appliance and Unitrends Backup virtual appliances.

Key benefits include:

Built for regulated environments: Deliver data protection that ensures compliance with FIPS 140-3 standards for federal and high-security environments.

Hardened platform: Encryption implemented using FIPS 140-3 validated cryptographic modules, secure key management, and integrated ransomware and anomaly detection capabilities.

Streamlined management: Unitrends physical appliances deploy turnkey, with hardware and software pre-integrated and optimized.

Compliance beyond backup

FIPS Mode supports secure backup, recovery and retention workflows specifically designed for compliance-focused organizations.

Backup: Incremental Forever backups optimize speed and storage utilization, protected by FIPS 140-3 validated encryption for both Unitrends Windows and next-gen Linux agents.

Recovery assurance: Automated testing validates recoverability of backups and benchmarks RTO/RPO objectives, helping assess alignment with internal SLAs.

Restore: Supports file recovery, image-level recovery, application (Exchange, SQL) recovery and metadata (backup copy) recovery.

Security and verification in a ransomware world

FIPS Mode enhances the robust security stack of Unitrends with cryptographic controls validated by NIST, ensuring data is safeguarded against emerging cyberthreats.

Every layer of Unitrends FIPS Mode is designed to support compliance objectives while helping secure backup data against sophisticated attacks.

Security capabilities include:

- Hardened backup appliances and agents
- Ransomware and anomaly detection
- Two-factor authentication (2FA)

FIPS components overview

Component	Cryptography level	Description
Unitrends Recovery Series Gen 10 appliances	FIPS 140-3 Inside*	End-to-end protection for local backup, recovery and replication
Unitrends Backup virtual appliance **	FIPS 140-3 Inside*	End-to-end protection for local backup, recovery and replication
Unitrends Windows agent	FIPS 140-3 Inside*	Collects and transmits encrypted data using FIPS-validated cryptography
Unitrends next-gen Linux agent	FIPS 140-3 Inside*	Collects and transmits encrypted data using FIPS-validated cryptography

See the Appendix: Technical References for a full list of certificates.

**To utilize FIPS Mode, the Unitrends Backup virtual appliance must be deployed locally in a VMware or Hyper-V virtual environment.*

Unbreakable cyber resilience built on layered security and validated cryptography

FIPS Mode is purpose-built for cyber resilience, combining the turnkey Unitrends platform with the assurance of FIPS-validated encryption to deliver secure, compliant continuity.

IT teams can benefit from:

Unified continuity: Protect Windows, Linux and application workloads with a fully integrated hardware and software solution.

Automated testing: Recover with confidence using verified backups. Know in advance the impact of an outage with RTO/RPO testing and reporting.

Training and support: Leverage Unitrends' award-winning, 24/7/365 technical support and on-demand training for seamless adoption.

With Unitrends FIPS Mode, IT teams can confidently protect data in regulated industries while maintaining the same reliability, automation and recovery performance that define Unitrends.

Appendix: Technical references

FIPS Mode utilizes the following validated module(s):

Unitrends Recovery Series Gen 10 appliances, Unitrends Backup virtual appliance, Unitrends Windows agent, Unitrends next-gen Linux agent

FIPS 140-3 Inside **Certificate #5040**

These components ensure FIPS-validated controls at the cryptographic library level, verified through NIST's Cryptographic Module Validation Program (CMVP).