



In today's business environment, data creates
value—so it's more important than ever to
protect it as a vital business asset





Seagate Secure™

Reliable Data Protection Solutions

Always-on data protection

In today's business environment, data creates value. So, it's more important than ever to protect it as a vital business asset. Data managers need sustainable, long-term security solutions that minimize risk with the least impact on productivity. But greater value means greater threats, and software based security measures alone are no longer sufficient to ensure your data stays under your control. In fact, software-only solutions intensify the pressure on the data storage lifecycle, making end-to-end security both more important and more difficult. That's why security analysts recommend a broad range of solutions, including hardware-based encryption.

The self-encrypting drive (SED) was introduced in 2009 as a hardware-based data security measure. Seagate has embraced the standard and engineered it into an essential component of modern asset protection. Combined with its protected hardware lifecycle and integration of multiple levels of security protocols, this added layer gives Seagate Secure™ storage devices the edge.

Seagate leads the way in data security.

Seagate's long history with data storage has given us deep understanding and insight into data security. Seagate Secure SEDs protect your data at rest and make device retirement a breeze. For those with more stringent requirements, we also offer advanced government-grade security.

Data Security Lifecycle

All Seagate Secure™ devices are built using a secure supply chain

True data security begins before storage devices are put into use. Seagate focuses on maintaining holistic security solutions throughout the product lifecycle.

Security is embedded in the Seagate lifecycle

Data security starts long before you purchase your storage device—and persists indefinitely after you stop using it. All Seagate Secure™ devices are protected from attackers at every stage of the lifecycle—from the conceptual phase of design to their final retirement or reuse. You can rest assured attackers haven't accessed your device at any stage before you deploy it, and that your data is inaccessible after you retire your device.



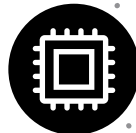
DESIGN

We ensure our hardware design process is closed to all but our own vetted workforce.



COMPONENT SOURCING

Every component of every device is sourced from trusted vendors.



MANUFACTURE

Each component is assembled in a secured facility.



DELIVERY

We engage only trusted vendors to deliver all Seagate Secure devices.



DEPLOYMENT

It's simple and straightforward to roll out our storage devices, minimizing the risk of security-related errors.



IN-USE

Our SEDs make sure your users—and only your users—can access your data.



RETIREMENT

Our Instant Secure Erase feature lets you eradicate all data in seconds for quick, painless device retirement.



Seagate Secure[™] delivers solutions you can depend on

Whether you need security at the Edge or a hardened data storage facility, Seagate has got you covered. Our **essential** feature set delivers protection that suits most needs, and we offer the **certified** level of service with federal information processing standards (FIPS) and Trade Agreement Act (TAA)-compliant solutions for government or enterprise customers running highly secure, data sensitive services and applications.

We offer two levels of service:

LEVEL 1: ESSENTIAL

LEVEL 2: CERTIFIED



LEVEL 1 - ESSENTIAL

INCLUDED—these features are available on Seagate Secure™ drives:

Secure Supply Chain

Each of our components is sourced securely from trusted sources.

- Seagate complies with the Open Trusted Technology Provider Standard (O-TTPS)
- Increasing trust of third-party processes to Seagate and O-TTPS security policies
- Ensuring customers receive authentic products, components, and firmware

Self-Encrypting Drive

Every device uses hardware-based encryption to protect against attacks.

- Secure data encryption using AES-256 standards and device root of trust
- Drive locks on power-down
- Industry-standard authentication key management interfaces

Secure Diagnosis & Download (SD&D)

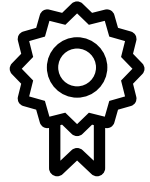
Your firmware is protected from attackers throughout its working life.

- Digitally signed firmware with rogue firmware detection.
- Locked diagnostic ports.
- Blocked cross-segment downloads.
- Secure boot process.

Instant Secure Erase

Administrators can instantly replace the encryption key on any device, rendering its data cryptographically erased and making retirement or reuse much easier.

- Fast, secure, and complete data erasure in seconds
- Internationally sanctioned erasure according to IEEE 2883 and NIST 800-88



LEVEL 2 - CERTIFIED

These features may be added to meet regulatory or other requirements:

FIPS 140-2 Level 2- and/or 140-3 Level 2-certified configuration

- Federal government encryption standard for sensitive, but not classified, data
- Required for Health Insurance Portability and Accountability Act (HIPAA)
- Tamper-evident labels

TAA compliant storage

- HDD and SSD product compliance.
- Meets origin requirements for U.S. government purchasing contracts.
- Adopted and recognized by over 100 designated nations.

Learn More

Seagate Secure storage devices deliver world-class data protection. We'd love to answer your questions or discuss solutions tailored to your unique needs. Please reach out to your Seagate sales representative any time.

Purchase Seagate Products

For all other Seagate Secure™ inquiries, please visit seagate.com/where-to-buy/

