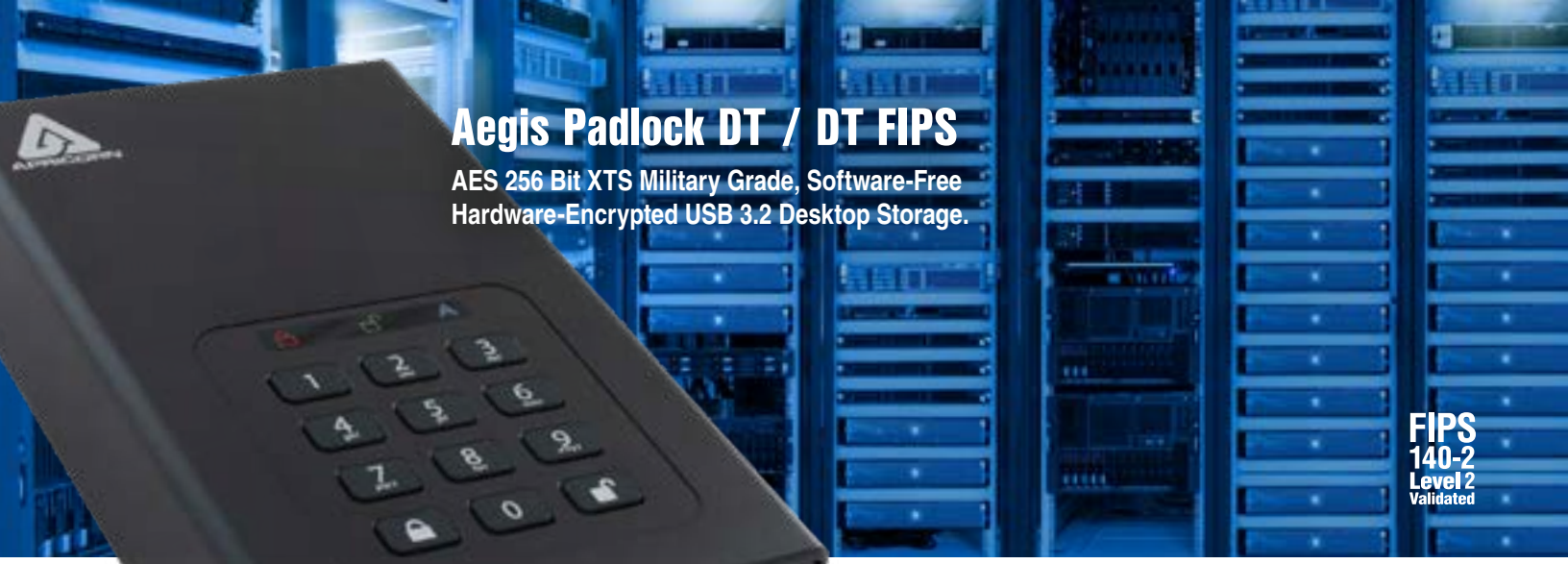

Aegis Padlock DT / DT FIPS

AES 256 Bit XTS Military Grade, Software-Free Hardware-Encrypted USB 3.2 Desktop Storage.

FIPS 140-2 Level 2 Validated

Highest Capacities Out There.

The Ultimate Backup Device. Available in 10 Capacities Ranging from 2TB to a Whopping 22TB, The Padlock DT and DT FIPS are the Perfect Choice for Daily Backups and Multi-User Collaborations.

Go big.

The Padlock DT continues to set the standard for securing massive amounts of data in a standalone desktop device. Ideal for daily, weekly, and monthly backups, as well as serving as the "1" in the "3-2-1" data resiliency method. Additionally, the Padlock DT continues to raise the bar for introducing the highest storage capacities of any hardware-encrypted USB storage device.

Desktop versatility.

Available in 10 HDD storage capacities to align perfectly to your data storage requirements. Whether it's for daily use or long term encrypted archiving, the Padlock DT is large enough to handle the load, and small enough to carry in a laptop bag. Unlike the other Aegis Secure Drives, the Padlock DT is our only model that doesn't run on USB bus power, but rather, is powered via a 12v AC adapter (included).

OS agnostic.

Like all Aegis secure drives, the Padlock DT is software-free and completely hardware-encrypted, making it completely cross-platform compatible. With its numeric keyboard and internal encryption chipset, 100% of its authentication and encryption processes take place on the fly within the device itself. None of these processes involve, nor are they ever shared with any host computer.

FIPS or no FIPS.

Some industries and institutions (legal, medical, educational, healthcare, etc.) are required to incorporate FIPS validation in their encryption processes when it comes to protecting the client data they possess. Some industries aren't required. That's why we offer the Padlock DT in both FIPS and non FIPS versions. Either way, the internal components operate the same and the security levels are equal.

APRICORN

Aegis Padlock DT / DT FIPS

AES 256-Bit XTS FIPS 140-2 level 2 Validated Hardware-Encrypted USB 3.2 Gen-1 with Type A Connector. Durable Aluminum Outer Enclosure with 10k Press Tested Wear-Resistant Polymer-Coated Rubberized buttons. Software-Free / Locked-Down FIrmware to Prevent Introduction of Malware Such as BadUSB

aegisware

Our patented firmware delivering the industry's most advanced feature set– the heart and soul of every Apricorn device.

Separate Admin and User Modes / PINs
Admin (Device Configuration) Mode and User Access Mode. The Admin mode controls the universal programmable settings of the device and can only be accessed with the Admin PIN. The User mode is for general external drive usage like read /write, unlock / lock, and certain other functions. The User mode is accessible via a User PIN or the Admin PIN.

Admin Forced Enrollment
Eliminates factory default PIN vulnerability by forcing the enrollment of an Admin PIN prior to use. As with all Apricorn Aegis secure devices, there are no default passwords, and no backdoors. In order to use any Apricorn secure drive, the Admin must first establish a complex PIN.

User Forced Enrollment
Beyond the admin PIN, one additional PIN can be generated to access the device's data. This User PIN can be set up by the admin at initial setup, or the device can be deployed in a state of User Forced Enrollment, allowing the user to establish his or her own PIN prior to use.

Data Recovery PINs
Programmed by the admin at time of setup to permit regaining access to the drive by creating a state of User Forced Enrollment in which a new User PIN can be created without affecting the drive's existing data or the Admin PIN.

Two Read-Only Modes
Universal Read Only: set by the admin from within the admin mode and can't be modified or disabled by anyone but the admin. The second (User) mode can be set and disabled by a user but can also be enabled or disabled by the admin.

Programmable PIN Length
Admin designates minimum and maximum PIN lengths (between 6 and 16 Characters). The longer the PIN, the more secure the data on the device becomes. For example, the odds of brute force success go from 1/10,000,000 with a 7-digit PIN to 1/100,000,000 with an 8 digit PIN. In cases where the User sets up his or her own PIN from User Forced Enrollment, the Admin can still affect User password length requirements

Unattended Auto Lock
Programmable length of time of inactivity permitted before drive locks itself. All Aegis Secure Drives will automatically lock once disconnected from a computer's USB port or the power to that USB port is interrupted, or after a pre-programmed period of inactivity.

Lock Override
Allows drive to remain unlocked during USB port re enumeration (Virtual Machine, Remote Boot). Designated for specific cases in which the drive needs to remain unlocked through USB port re-enumeration such as during reboot, or passing through a virtual machine.

Self-Destruct PIN
When programmed and activated, performs a crypto-erase and becomes new access PIN. The last line of defense for data security when the device's physical security is at risk. The Self-Destruct PIN defends against these physically compromising situations by erasing the drive's contents, leaving it in normal working order appearing yet to be deployed

Brute Force Defense
Programmable number of consecutive invalid PIN attempts permitted (4-20) before crypto-erase. If the device comes under a physical brute force attack, once the programmed number (between 4 and 20) of consecutive incorrect password entries has been attempted, the device will delete its own encryption key and destroy the ability to decrypt its stored data.

Provision Lock
Patented setting where the admin can designate whether the device will permit itself to be reset by a User or after a brute force attempt. If Provision Lock is enabled, any attempt at complete reset will "brick" the device for good.

Aegis Configurator™ Compatible
Windows-Based app that quickly sets up multiple devices simultaneously. Create custom profiles and mass configure multiple devices in a matter of seconds using the Aegis Configurator. To configure an expanded number of devices, use the Powered Aegis Configurator Hub bundle.

TECHNICAL SPECIFICATIONS

CAPACITIES
HDD: 2TB, 4TB, 6TB, 8TB, 10TB, 12TB, 16TB, 18TB, 20TB, 22TB, 24TB

INTERFACE
USB 3.2 GEN. 1; TYPE A Connector
backward compatible with USB 1 and 2

DIMENSIONS and WEIGHT
4.5" x 7.2" x 1.5" | 3 lbs-1.6oz

POWER SUPPLY
12v AC external required

TRANSFER RATE
HDD: up to 159MB/s*

BUFFER SIZE
8MB

SYSTEM COMPATIBILITY
WINDOWS, MAC OS, LINUX, ANDROID, CITRIX
any that supports a USB mass storage device

STANDARDS / CERTIFICATIONS
FIPS 140-2 LEVEL 2 (CERT # 4528) TAA COMPLIANT, NATO OTAN RESTRICTED (PENDING)

OPERATING TEMPERATURE RANGES
-40° to 140°F (-40°C to 60°C)

OPERATING HUMIDITY RANGES
up to 50% @ temps under 131°F (55°C)

SHOCK HDD
NON-OPERATING: 250G @2ms
OPERATING: 70G @1ms

ECCN / HTS / CAGE CODE
5A992.c / 8471.70.5065 / 3VYK8

SKU NUMBERS
HDD FIPS: ADT-3PL256F-2000, ADT-3PL256F-4000, ADT-3PL256F-6000, ADT-3PL256F-8000, ADT-3PL256F-10TB, ADT-3PL256F-12TB, ADT-3PL256F-16TB, ADT-3PL256F-18TB, ADT-3PL256F-20TB, ADT-3PL256F-22TB, ADT-3PL256F-24TB

HDD NON-FIPS: ADT-3PL256-2000, ADT-3PL256-4000, ADT-3PL256-6000, ADT-3PL256-8000, ADT-3PL256-10TB, ADT-3PL256-12TB, ADT-3PL256-16TB, ADT-3PL256-18TB, ADT-3PL256-20TB, ADT-3PL256-22TB, ADT-3PL256-24TB

WARRANTY
3-Year Limited

PACKAGE CONTENTS
Aegis Padlock DT, (1) 18" Type-A USB cable, 12v AC adapter, Multi-Language Quick-Start Guide

* To achieve these speeds, your computer's internal harddrive must also be an SSD; all transfer rates will be limited by computer's internal HDD
One gigabyte (GB) = one billion bytes; accessible capacity will be less and actual capacity depends on the operating environment and formatting.

APRICORN