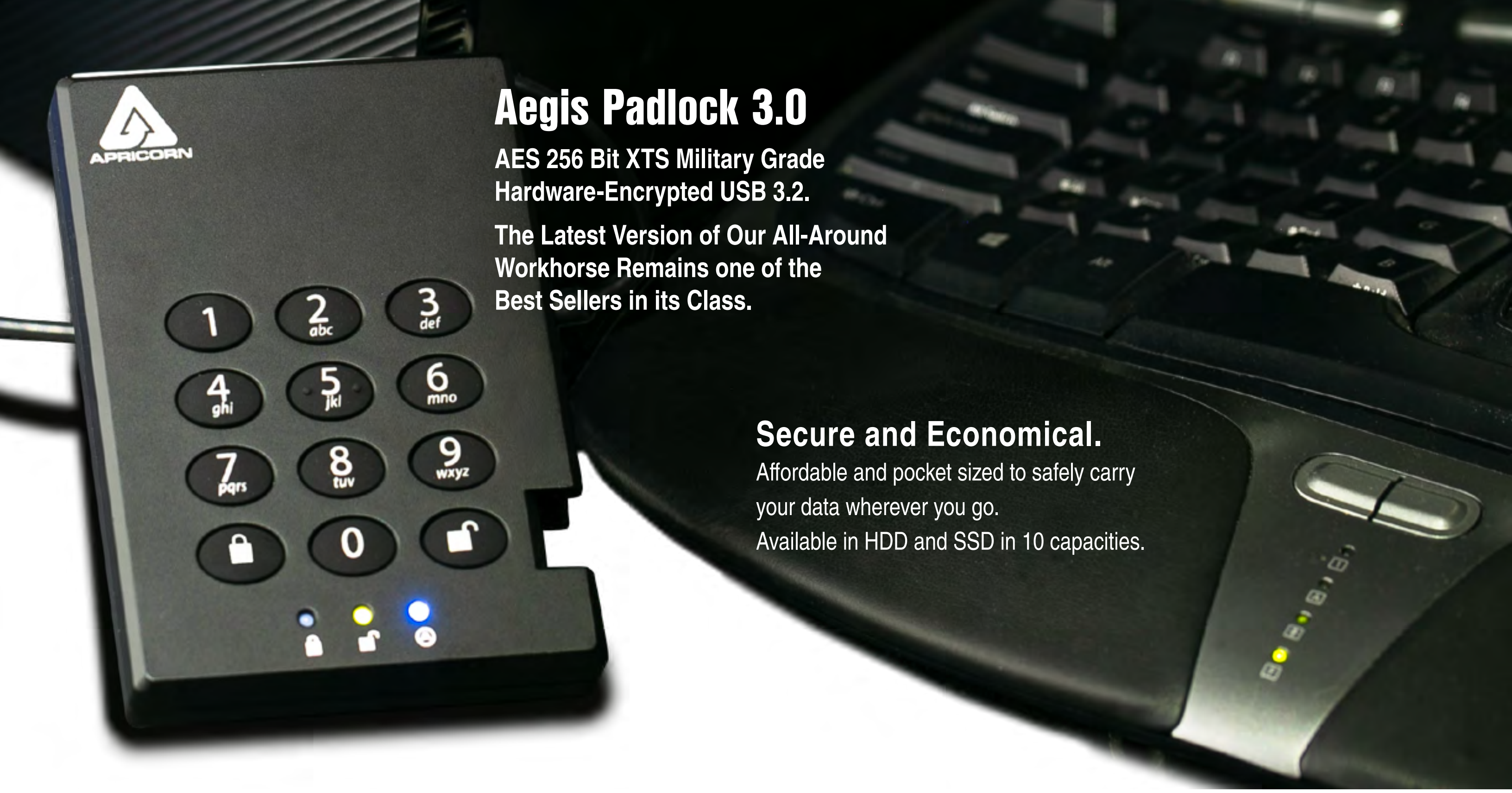

Aegis Padlock 3.0

AES 256 Bit XTS Military Grade Hardware-Encrypted USB 3.2.

The Latest Version of Our All-Around Workhorse Remains one of the Best Sellers in its Class.

Secure and Economical.

Affordable and pocket sized to safely carry your data wherever you go.
Available in HDD and SSD in 10 capacities.

Classics get imitated.

Prior to the USB 3 version being introduced in 2013, the USB 2 Padlock model introduced many of the features such as its onboard keypad and built-in rugged USB cable that have since become standards, both in our portable modelsas well as within our industry. Today, the Padlock 3 remains the most reliable, super secure hardware-encrypted USB drive out there for the money.

The Practical choice.

For those who aren't bound by regulations requiring FIPS validated devices, the Padlock 3 brings the exact same security levels as its FIPS counterpart, the Padlock Fortress, without the added expense of a FIPS validated device. Equally perfect for large corporate deployments and single proprietors, the Padlock 3 remains the go-to for economical data security worldwide.

All OSs welcome.

Like all Aegis secure drives, the Padlock 3 is software-free and completely hardware-encrypted, making it completely cross-platform compatible and OS agnostic. Since 100% of its authentication and encryption processes take place on the fly within the device itself, none of the CSPs are ever shared with its host computer. All it needs is a powered USB port and storage file system.

Built for collaboration.

A single Padlock 3 device can store one Admin PIN and up to four additonal User PINs to allow multiple authorized persons to access the device with their own unique passwords. Transfer and store data offline securely, assured that the device's contents won't be at risk of compromise while at rest or in transit.

©2023 Apricorn. 12191 Kirkham Rd., Poway, CA. 92064 | 800.458.5448 | apricorn.com

APRICORN

Aegis Padlock 3.0

AES 256-Bit XTS PUB 197 Validated Hardware-Encrypted USB 3.2 Gen-1 with Hardwired Type A Connector

Durable ABS Outer Enclosure and Hardened Epoxy Potting to Protect Internal Componentry.

10k Press Tested, Polymer-Coated Wear-Resistant Rubberized Button Keypad

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: 500GB, 1TB, 2TB
SSD: 256GB, 512GB, 1TB, 2TB, 4TB
8TB, 16TB

INTERFACE

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

DIMENSIONS and WEIGHT

120mm x 84.5mm x 19mm | 176 g
4.7” x 3.3” x 0.75” | 6.2oz

POWER SUPPLY

100% bus powered

TRANSFER RATE

HDD: up to 159MB/s*
SSD: up to 360MB/s*

SYSTEM COMPATIBILITY

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

STANDARDS / CERTIFICATIONS

TAA COMPLIANT, IP66, NATO OTAN RESTRICTED (PENDING)

CONFIGURABLE VCI RoHS FC CE

OPERATING TEMPERATURE RANGES

-40° to 158°F (-40°C to 70°C)

OPERATING HUMIDITY RANGES

95% @ temps under 131°F (55°C)

SHOCK SSD

NON-OPERATING: 1500G .5ms
OPERATING: 1500G .5ms

SHOCK HDD

NON-OPERATING: 1000G @1ms
OPERATING: 300G @2ms

ECCN / HTS / CAGE CODE

5A992.c / 8523.51.0000 / 3VYK8

SKU NUMBERS

SSD: A25-3PL256-500, A25-3PL256-1000, A25-3PL256-2000, A25-3PL256-S256, A25-3PL256-S512, A25-3PL256-S1000, A25-3PL256-S2000, A25-3PL256-S4000, A25-3PL256-S8000, A25-3PL256-S16TB

WARRANTY

3-Year Limited

PACKAGE CONTENTS

Aegis Padlock 3.0, (1) 18” Type-A Y-connector extender cable, (1) Travel Pouch, 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