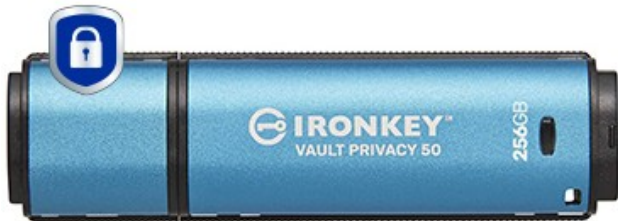


Kingston Technology IronKey Vault Privacy 50 USB flash drive

Artikel	21286182
Herstellernummer	IKVP50/256GB
EAN	0740617329100
Kingston Technology	



Die Kingston IronKey™ Vault Privacy 50 Serie umfasst hochwertige USB-A und USB-C®-Sticks, die mit einer FIPS 197-zertifizierten AES-256-Bit-Hardwareverschlüsselung im XTS-Modus Sicherheit für Unternehmen bieten, einschließlich Schutzmaßnahmen gegen BadUSB mit digital signierter Firmware und gegen Brute-Force-Passwortangriffe. Der VP50 wurde für Sicherheit auf Unternehmensniveau einem Penetrationstest unterzogen***** (Pen Tested). Da es sich um verschlüsselte Speicher unter physischer Kontrolle des Benutzers handelt, bietet die VP50-Serie einen wesentlich besseren Datenschutz als das Internet oder Cloud-Dienste.

Der Vault Privacy 50 unterstützt die Multi-Passwort-Option (Admin, Benutzer und einmalige Wiederherstellung) mit Komplex- oder Passphrasen-Modi. Dadurch lässt sich der Zugriff auf die Daten besser wiederherstellen, wenn eines der Passwörter vergessen wurde. Mit dem herkömmlichen Komplexmodus sind Passwörter mit 6 bis 16 Zeichen unter Verwendung von 3 von 4 Zeichensätzen zulässig. Der neue Passphrase-Modus unterstützt numerische PINs, Sätze, Wortlisten oder sogar Liedtexte mit 10 bis 64 Zeichen. Der Administrator kann ein Benutzer- und ein einmaliges Wiederherstellungspasswort aktivieren oder zur Wiederherstellung des Datenzugriffs das Benutzerkennwort zurücksetzen. Zur Erleichterung der Passworteingabe kann das „Auge“-Symbol aktiviert werden, sodass das eingegebene Passwort angezeigt wird, was für weniger Tippfehler und somit für weniger fehlgeschlagene Anmeldeversuche sorgt. Der Brute-Force-Angriffsschutz sperrt Benutzer- oder einmalige Wiederherstellungspasswörter nach 10 ungültigen, hintereinander eingegebenen Passwörtern und kryptolöscht nach 10-maliger fehlerhafter Eingabe hintereinander den USB-Stick.

Zum Schutz vor potenzieller Malware auf nicht vertrauenswürdigen Systemen können sowohl der Administrator als auch der Benutzer den Schreibschutz für den USB-Stick aktivieren. Außerdem schützt die integrierte virtuelle Tastatur Passwörter vor Key- und Screenloggern.

Unternehmen können die USB-Sticks der VP50 Serie mit einer Produkt-ID (PID) für die Integration mit Standard-Endpoint-Management-Software anpassen und konfigurieren und somit die IT- und Cybersicherheits-Anforderungen des Unternehmens mithilfe von Kingstons Personalisierungsprogramm erfüllen.

Kleine und mittlere Unternehmen können die Admin-Rolle zur lokalen Verwaltung ihrer USB-Sticks verwenden, z. B. zum Konfigurieren oder Zurücksetzen von Benutzer- oder einmaligen Wiederherstellungs-Passwörtern von Mitarbeitern, zur Wiederherstellung des Datenzugriffs auf gesperrten USB-Sticks und zur Einhaltung von Gesetzen und Vorschriften, wenn forensische Untersuchungen erforderlich sind.

Der Vault Privacy 50 bietet schnelle Dual-Channel-Leistung für alle Speicherkapazitäten. Der USB-Stick ist wasserdicht gemäß IPX8-Klasse****, TAA-konform und wird in den USA montiert.

Hardwareverschlüsselter USB-Stick für mehr Datenschutz

Schützen Sie wichtige Daten mit FIPS 197-zertifizierter XTS-AES-256-Bit-Verschlüsselung. Integrierter Schutz gegen BadUSB, Brute-Force-Angriffe und Penetrations-getestet für Sicherheit auf Unternehmensniveau.

Multi-Passwort-Option für die Datenwiederherstellung

Aktivieren Sie Administrator-, Benutzer- und einmalige Wiederherstellungspasswörter. Der Administrator kann ein Benutzerkennwort

zurücksetzen und ein einmaliges Wiederherstellungspasswort erstellen, um dem Benutzer wieder den Zugriff auf die Daten zu ermöglichen. Der Brute-Force-Angriffsschutz sperrt Benutzer- oder einmalige Wiederherstellungspasswörter nach 10 ungültigen, hintereinander eingegebenen Passwörtern und kryptolöscht nach 10-maliger fehlerhafter Eingabe hintereinander den USB-Stick.

Neuer Passphrase-Modus

Wählen Sie zwischen dem Passwortmodus Komplex oder Passphrase. Passphrasen können eine numerische PIN, ein Satz mit Leerzeichen, eine Liste von Wörtern oder sogar Text sein – mit einer Länge von 10 bis 64 Zeichen.

Einstellungen für den dualen Schreibschutzmodus

Vermeiden Sie Malware-Angriffe mit einem erzwungenen Schreibschutzmodus, der vom Administrator für den Benutzer eingerichtet wird, oder einem sitzungsbasierten Schreibschutzmodus, der vom Administrator oder Benutzer eingerichtet wird.

Lokale Verwaltung von USB-Sticks für KMU

Verwenden Sie die Admin-Rolle, um Benutzer- und Einmal-Wiederherstellungspasswörter von Mitarbeitern lokal zu verwalten, den Datenzugriff auf gesperrte Laufwerke wiederherzustellen und Gesetze und Vorschriften einzuhalten, wenn Forensik erforderlich ist.

Zusätzliche Sicherheitsfunktionen

Sorgen Sie für weniger fehlgeschlagene Anmeldeversuche und Frust durch Aktivierung der Taste „Auge“, um das eingegebene Passwort anzeigen zu lassen. Verwenden Sie eine virtuelle Tastatur, um die Passworteingabe vor Keyloggern und Screenloggern zu schützen.

Zusammenfassung

Die Kingston IronKey™ Vault Privacy 50 Serie umfasst hochwertige USB-A und USB-C®*-Sticks, die mit einer FIPS 197-zertifizierten AES-256-Bit-Hardwareverschlüsselung im XTS-Modus Sicherheit für Unternehmen bieten, einschließlich Schutzmaßnahmen gegen BadUSB mit digital signierter Firmware und gegen Brute-Force-Passwortangriffe. Der VP50 wurde für Sicherheit auf Unternehmensniveau einem Penetrationstest unterzogen***** (Pen Tested). Da es sich um verschlüsselte Speicher unter physischer Kontrolle des Benutzers handelt, bietet die VP50-Serie einen wesentlich besseren Datenschutz als das Internet oder Cloud-Dienste.

Der Vault Privacy 50 unterstützt die Multi-Passwort-Option (Admin, Benutzer und einmalige Wiederherstellung) mit Komplex- oder Passphrasen-Modi. Dadurch lässt sich der Zugriff auf die Daten besser wiederherstellen, wenn eines der Passwörter vergessen wurde. Mit dem herkömmlichen Komplexmodus sind Passwörter mit 6 bis 16 Zeichen unter Verwendung von 3 von 4 Zeichensätzen zulässig. Der neue Passphrase-Modus unterstützt numerische PINs, Sätze, Wortlisten oder sogar Liedtexte mit 10 bis 64 Zeichen. Der Administrator kann ein Benutzer- und ein einmaliges Wiederherstellungspasswort aktivieren oder zur Wiederherstellung des Datenzugriffs das Benutzerkennwort zurücksetzen. Zur Erleichterung der Passworteingabe kann das „Auge“-Symbol aktiviert werden, sodass das eingegebene Passwort angezeigt wird, was für weniger Tippfehler und somit für weniger fehlgeschlagene Anmeldeversuche sorgt. Der Brute-Force-Angriffsschutz sperrt Benutzer- oder einmalige Wiederherstellungspasswörter nach 10 ungültigen, hintereinander eingegebenen Passwörtern und kryptolöscht nach 10-maliger fehlerhafter Eingabe hintereinander den USB-Stick.

Zum Schutz vor potenzieller Malware auf nicht vertrauenswürdigen Systemen können sowohl der Administrator als auch der Benutzer den Schreibschutz für den USB-Stick aktivieren. Außerdem schützt die integrierte virtuelle Tastatur Passwörter vor Key- und Screenloggern.

Unternehmen können die USB-Sticks der VP50 Serie mit einer Produkt-ID (PID) für die Integration mit Standard-Endpoint-Management-Software anpassen und konfigurieren und somit die IT- und Cybersicherheits-Anforderungen des Unternehmens mithilfe von Kingstons Personalisierungsprogramm erfüllen.

Kleine und mittlere Unternehmen können die Admin-Rolle zur lokalen Verwaltung ihrer USB-Sticks verwenden, z. B. zum Konfigurieren oder Zurücksetzen von Benutzer- oder einmaligen Wiederherstellungs-Passwörtern von Mitarbeitern, zur Wiederherstellung des Datenzugriffs auf gesperrten USB-Sticks und zur Einhaltung von Gesetzen und Vorschriften, wenn forensische Untersuchungen erforderlich sind.

Der Vault Privacy 50 bietet schnelle Dual-Channel-Leistung für alle Speicherkapazitäten. Der USB-Stick ist wasserdicht gemäß IPX8-Klasse****, TAA-konform und wird in den USA montiert.

Hardwareverschlüsselter USB-Stick für mehr Datenschutz

Schützen Sie wichtige Daten mit FIPS 197-zertifizierter XTS-AES-256-Bit-Verschlüsselung. Integrierter Schutz gegen BadUSB, Brute-Force-Angriffe und Penetrations-getestet für Sicherheit auf Unternehmensniveau.

Multi-Passwort-Option für die Datenwiederherstellung

Aktivieren Sie Administrator-, Benutzer- und einmalige Wiederherstellungspasswörter. Der Administrator kann ein Benutzerkennwort zurücksetzen und ein einmaliges Wiederherstellungspasswort erstellen, um dem Benutzer wieder den Zugriff auf die Daten zu

ermöglichen. Der Brute-Force-Angriffsschutz sperrt Benutzer- oder einmalige Wiederherstellungspasswörter nach 10 ungültigen, hintereinander eingegebenen Passwörtern und kryptolöscht nach 10-maliger fehlerhaften Eingabe hintereinander den USB-Stick.

Neuer Passphrase-Modus

Wählen Sie zwischen dem Passwortmodus Komplex oder Passphrase. Passphrasen können eine numerische PIN, ein Satz mit Leerzeichen, eine Liste von Wörtern oder sogar Text sein – mit einer Länge von 10 bis 64 Zeichen.

Einstellungen für den dualen Schreibschutzmodus

Vermeiden Sie Malware-Angriffe mit einem erzwungenen Schreibschutzmodus, der vom Administrator für den Benutzer eingerichtet wird, oder einem sitzungsbasierten Schreibschutzmodus, der vom Administrator oder Benutzer eingerichtet wird.

Lokale Verwaltung von USB-Sticks für KMU

Verwenden Sie die Admin-Rolle, um Benutzer- und Einmal-Wiederherstellungspasswörter von Mitarbeitern lokal zu verwalten, den Datenzugriff auf gesperrte Laufwerke wiederherzustellen und Gesetze und Vorschriften einzuhalten, wenn Forensik erforderlich ist.

Zusätzliche Sicherheitsfunktionen

Sorgen Sie für weniger fehlgeschlagene Anmeldeversuche und Frust durch Aktivierung der Taste „Auge“, um das eingegebene Passwort anzeigen zu lassen. Verwenden Sie eine virtuelle Tastatur, um die Passworteingabe vor Keyloggern und Screenloggern zu schützen.

Kingston Technology IronKey 256GB Vault Privacy 50 AES-256 verschlüsselter, FIPS 197, 256 GB, USB Typ-A, 3.2 Gen 1 (3.1 Gen 1), 230 MB/s, Kappe, Schwarz, Blau

Kingston Technology IronKey 256GB Vault Privacy 50 AES-256 verschlüsselter, FIPS 197. Kapazität: 256 GB, Geräteschnittstelle: USB Typ-A, USB-Version: 3.2 Gen 1 (3.1 Gen 1), Lesegeschwindigkeit: 230 MB/s, Schreibgeschwindigkeit: 150 MB/s. Formfaktor: Kappe. Passwortschutz. Gewicht: 15 g. Produktfarbe: Schwarz, Blau

Merkmale

Lieferumfang		Leistungen	
Menge pro Packung	1 Stück(e)	Kapazität	256 GB
Sonstige Funktionen		Geräteschnittstelle	USB Typ-A
		USB-Version	3.2 Gen 1 (3.1 Gen 1)
		Lesegeschwindigkeit	230 MB/s
Ursprungsland		Schreibgeschwindigkeit	150 MB/s
		Kompatible Betriebssysteme	Windows 11, 10, macOS 12.x – 15.x
Betriebsbedingungen		Logistikdaten	
Betriebstemperatur	0 - 50 °C	Anzahl Produkte pro Versandkarton	8 Stück(e)
Temperaturbereich bei Lagerung	-20 - 85 °C	Breite des Versandkartons	135,9 mm
Gewicht und Abmessungen		Länge des Versandkartons	203,2 mm
		Höhe des Versandkartons	69,8 mm
Breite	21,9 mm	Gewicht Versandkarton	358,34 g
Tiefe	77,9 mm	Warentarifnummer (HS)	84717070
Höhe	12 mm	Design	
Gewicht	15 g		
Verpackungsdaten		Formfaktor	Kappe
		Produktfarbe	Schwarz, Blau
Verpackungsbreite	129,5 mm	Schutzfunktion	Wasserdicht
Verpackungstiefe	12,9 mm	Schlüsselanhänger	Ja
Verpackungshöhe	184,2 mm	Internationale Schutzart (IP-Code)	IPX8
Paketgewicht	35,02 g	Wasserdicht bis	1,2 m
Verpackungsart	Sichtverpackung	Zertifizierung	FIPS 197

Sicherheit

PIN_gesicherter Zugang	Ja
Passwortschutz	Ja
Unterstützte Sicherheitsalgorithmen	256-bit AES-XTS, FIPS 197
Hardwareverschlüsselung	Ja
Schreibschutzschalter	Ja
Read-only-Funktion	Ja
Verteidigung für Brute-Force-Angriff	Ja
Benutzer- und Admin-Rollen	Ja
Management-Funktionen	Passwort zurücksetzen

Preisänderungen und Irrtümer vorbehalten. Alle Produkte solange der Vorrat reicht.