



USB- Flashspeicher

DataTraveler Vault Privacy - Managed

Was spricht für einen zentral verwalteten USB-Stick?

- Administratoren erhalten ein leistungsstarkes Tool, mit dem der USB- Flashspeicher auch per Fernzugriff integriert, aktualisiert und verwaltet werden kann.
- Die Datensicherheit und Zuverlässigkeit der zentral verwalteten USB-Sticks von Kingston Technology bieten in Kombination mit der serverbasierten Managementsoftware „SafeConsole for Kingston“ von BlockMaster größere Transparenz, Sicherheit und Kontrolle.

Was ist der DTVP-M?

- Der DTVP-M ist ein USB-Stick mit vollständiger Hardwareverschlüsselung, der mit der Managementsoftware „SafeConsole for Kingston“ von BlockMaster zentral verwaltet werden muss.
- Alle gespeicherten Daten sind durch hardwarebasierte 256-Bit-AES-Verschlüsselung (Advanced Encryption Standard) im CBC-Modus (Cipher Block Chaining) geschützt.
- Er überträgt Dateien mit bis zu 24 MB/s (Lesegeschwindigkeit) und 10 MB/s (Schreibgeschwindigkeit) und ist mit Speicherkapazitäten von 2–32GB erhältlich.
- Das robuste Aluminiumgehäuse ist bis ca. 1,2 m wasserdicht.
- Der Speicher ist mit Windows Vista, Windows XP und Windows 7 kompatibel.
- Es gibt mehrere Personalisierungsoptionen wie Co-Logo, Seriennummern, kundenspezifische Farbe, vorinstallierte Inhalte usw. sowie den Aufdruck des Unternehmenslogos oder -namens zur Stärkung der Corporate Identity oder für das Asset-Tracking.
- Fünf Jahre Garantie und 24/7 Kundensupport runden das Angebot ab.



Potenzielle Kunden:

- Unternehmen, die auf die Verschlüsselung aller Daten bestehen und die auf den sicheren Transport aller sensiblen Daten Wert legen.
- Unternehmen, die einen sicheren USB-Stick benötigen, der einfach zu verwalten ist und eine bessere Produktivität und Zusammenarbeit bietet.
- Datensicherheits-Lücken sind teuer; potenziell rufschädigend, führen zu großem Verwaltungsaufwand und erfordern manuelle Sicherheitsüberprüfungen.

Vorteile:

- **Vollständig durchgesetztes Management**
Der DTVP-M muss mit der Serversoftware „SafeConsole for Kingston“ von BlockMaster verwaltet werden. Alle erweiterten Funktionen können auf diese Weise einfach konfiguriert und verwaltet werden. Dies schließt u.a. das Zurücksetzen des Kennworts per Fernzugriff und das Gerätemanagement ein.
- **Sicherheit für Unternehmen**
Alle gespeicherten Daten sind durch hardwarebasierte 256-Bit-AES-Verschlüsselung (Advanced Encryption Standard) im CBC-Modus (Cipher Block Chaining) geschützt.
- **Security Assurance Program von Kingston Technology**
Kingston Technology arbeitet mit SYSS zusammen, einem unabhängigen Testunternehmen, das sich auf Penetrationstests für sichere USB-Flashspeicher in Unternehmen spezialisiert hat.
- **Schneller, hochwertiger Speicher**
Kingston Technology verwendet für seine Produkte nur hochwertige Flashspeicher, um größtmögliche Übertragungsgeschwindigkeiten, gute Integrität und eine lange Lebensdauer zu gewährleisten.
- **Schutz vor Brute-Force-Angriffen**
Der Speicher wird nach zehn fehlgeschlagenen Anmeldeversuchen gesperrt und der Kodierungsschlüssel gelöscht. Um den Speicher wieder verwenden zu können, ist ein neues Kennwort erforderlich, wobei alle Daten gelöscht werden.
- **Sperrung bei Inaktivität**
Wird der Speicher über längere Zeit nicht verwendet oder am Arbeitsplatz vergessen, erfolgt automatisch die Sperrung.
- **Fünf Jahre Garantie**
Neben der legendären Zuverlässigkeit von Kingston Technology erhalten Sie fünf Jahre Garantie und 24/7 technischen Support für den DTVP-M.

>> Weitere Informationen zur Managementsoftware „SafeConsole for Kingston“ finden Sie auf der Rückseite.



Management Software

SafeConsole for Kingston

Was ist „SafeConsole for Kingston“?

- Eine Managementsoftware, die ausschliesslich für ausgewählte USB-Flashspeicher verwendet werden kann. (SafeConsoleReady-Geräte)
- Eine kleine, eigenständige Webserver-Software, die Sie unternehmensintern betreiben.

Funktionen:

- Management aller Ihrer „SafeConsole Ready“ Geräte
- Durchsetzung starker, komplexer Kennwörter; Festlegung eigener Richtlinien
- Wenn Mitarbeiter ihr Kennwort vergessen haben, kann es mittels eines “Herausforderung/Antwort”-Verfahrens zurückgesetzt werden
- FileRestrictor ermöglicht das Blockieren und/oder Kopieren von Dateien, abhängig von festgelegten Dateieindungen.
- Device Audit Trail: Alle Aktivitäten auf dem Speicher (Anmeldungen, Abmeldungen, Sperrungen, Verwendung usw.) werden überprüft und protokolliert.
- File Audit Trail: Alle Aktivitäten bezüglich der Dateien (Erstellen, Löschen usw.) werden überprüft und protokolliert.
- Schutz vor Malware, z. B. standardmäßiger Schutz vor dem Conficker-Wurm
- Publisher ermöglicht die sichere Distribution von Dateien und Anwendungsprogrammen
- EasyShare: Ausgewählte Dateien können ohne die Weitergabe des Hauptkennworts sicher durch einen temporären Pin freigegeben werden.



Potenzielle Kunden:

- Alle Benutzer von DTVP-M und DT4000-M USB-Flashspeicher von Kingston Technology

Vorteile:

- Reduziertes Risiko von Datensicherheits-Lücken
- Leicht per Fernzugriff die Löschung, erneute Bereitstellung und Authoursierung aller im Einsatz befindlichen USB-Sticks veranlassen.
- Einfaches Rollout im Unternehmen durch anwenderfreundliche Plug-and-Play Installation
- Wiederherstellung der gesicherten Dateien vom zentralen Server auf einen neuen USB-Stick bei Verlust oder Diebstahl.
- Problemloser Datenaustausch zwischen Anwendern über gemeinsam nutzbare Bereiche
- Sichere Verteilung mobiler Anwendungen und Dateien per Push-Übertragung über das Internet auf die USB-Sticks

Weitere Funktionen:

- **Kennwortrichtlinie**
Konfiguration komplexer Kennwörter nach selbst definierten Kriterien, einschließlich Kennwortlänge und Zeichenarten
- **Kennwortzurücksetzung per Fernzugriff**
Administratoren können per Fernzugriff mittels des “Herausforderung/Antwort”-Verfahrens die Kennwörter von Anwendern zurücksetzen.
- **ZoneBuilder**
Anwender können mit ihrem eigenen Anwenderkonto und denen von Mitarbeitern vertrauenswürdige Bereiche einrichten. Wird der USB-Stick in diesem vertrauenswürdigen Bereich in einen USB-Anschluss gesteckt, wird er automatisch entsperrt.
- **Gerätemanagement und Inaktivitätssperre**
Verwaltung der Sticks auf Grundlage der Häufigkeit von Anmeldungen und des Status des USB-Sticks; Anpassung der Nachricht, die angezeigt wird, wenn ein verloren gegangener oder gestohlener Speicher angeschlossen wird, zentrale Festlegung des Timeouts bei Inaktivität.
- **Publisher (Datenübertragung)**
Zentrales Management der Bereitstellung von Dateien und mobilen Anwendungen, z. B. Antivirenprogramme, VPN, Firefox, Chrome und Skype. Sichere automatische Push-Übertragung von Unternehmensdaten auf den USB-Stick, z. B. Preislisten, Datenblätter oder Unternehmenshandbücher
- **Sicherung und Datenüberprüfung**
Automatische Verschlüsselung aller auf dem Speicher befindlichen Daten ohne Beeinträchtigung der Produktivität
Administratoren können per Fernzugriff Daten wiederherstellen bzw. den Inhalt eines verloren gegangenen USB-Sticks einfach erneut erstellen.

