

MILITÄRISCHE AES 256-BIT VERSCHLÜSSELUNG ZUM SCHUTZ VON MOBILEN DATEN

ENDGERÄTE-VERWALTUNG PER FERNZUGRIFF

USB-MALWARE-SCHUTZ



SICHERE, KONTROLLIERTE USB-STICKS FÜR ANSPRUCHSVOLLE UNTERNEHMENSANWENDUNG

IronKey Enterprise S200 kombiniert USB-Sticks mit AES 256-Bit Hardwareverschlüsselung mit den IronKey Enterprise Management Services. So können Sie die Sicherheitsrichtlinien von Tausenden von Endgeräten - auch für Remote-Anwender - über das Internet fernsteuern. Die integrierte starke Authentifizierung erlaubt es Organisationen, IronKey USB-Sticks als zuverlässige Basis für sicheren Fernzugriff und virtuelle Desktops zu nutzen.

Bestleistung und Wahrung von Daten

IronKey Enterprise S200 ist weiter entwickelt als je zuvor. Dieser USB-Stick kombiniert absolut sichere Verschlüsselung mit Spitzenleistung und Zuverlässigkeit - hochwertigste Fertigungskomponenten bewahren Daten bis zu 10-Mal länger, als konventionelle USB-Sticks. Daher eignen sich IronKey S200 USB-Sticks ideal für Power-User, die täglich hohe Ansprüche in Bezug auf Datensicherung stellen oder Anwendungen darauf nutzen.

Der einzige USB-Stick mit FIPS 140-2 Level 3 Standard

IronKey USB-Sticks entsprechen den strengen Sicherheitsanforderungen der US-Regierung nach FIPS 140-2 Level 3. Das beinhaltet nicht nur das Verschlüsselungsmodul, sondern auch die Platine, den Speicher und das Authentifizierungssystem. Alle Benutzerdaten auf einem IronKey Enterprise USB-Stick werden mit AES 256-bit Hardwareverschlüsselung verschlüsselt. Diesen starken Algorithmus setzen auch das U.S.-Militär und U.S.-Regierungsbehörden zum Schutz von streng geheimen Daten ein.

Aktiver Schutz vor Malware

Böswillige Codes und Viren, die durch austauschbare Datenträger verbreitet werden, infizieren jährlich Millionen von Computern. Der mehrstufige, aktive Schutz von IronKey vor Malware stoppt die Verbreitung von Malware und Würmern. Pro-Aktiver Schutz verhindert die Änderung von AutoRun-Dateien und erlaubt es Administratoren, per Fernwartung zu kontrollieren, auf welchen Computern IronKey USB-Sticks genutzt werden dürfen. Ein integrierter Malware-Scanner schützt den USB-Stick, wenn Dateien verschoben oder geöffnet werden. Zusätzlich verhindert ein Nur-Lese-Modus das Überspringen von Malware eines befallenen PC auf den USB-Stick.

Verwaltung und Umsetzung von Sicherheitsrichtlinien über das Internet

Der IronKey Enterprise Remote Management Service lässt Sie mit Leichtigkeit tausende von IronKey USB-Sticks verwalten und Sicherheitsrichtlinien für jeden Stick einstellen - einschließlich Passwortstärke, Anzahl von Passwort-Eingabeversuchen und installierten Anwendungen.

Verlorene und gestohlene USB-Sticks aus der Ferne abschalten und zerstören

Eine Hauptkomponente des IronKey Enterprise Remote Management Service ist der Silver Bullet Service mit leistungsfähigen Optionen zur Unterbindung des Zugriffs auf nicht mehr vertrauenswürdige Sticks - sei es wegen Verlust, Diebstahl oder ehemalige, bzw. nicht vertrauenswürdige Angestellte.

- **Blockieren** – verhindert Datenzugriff auf dem USB-Stick, bis der Status überprüft werden kann
- **Abschalten** – Schließt den Anwender vollständig aus, wenn der Stick wieder angeschlossen wird
- **Zerstören** – gibt dem IronKey USB-Stick den Befehl zur Selbstzerstörung

„IronKey Enterprise ist ein mächtiges und effektives Mittel, um Kontrolle über mobile Datenbestände zu erlangen und zu bewahren.“

Information Security Magazine, Februar 2009

WELCHER IRONKEY IST DER RICHTIGE FÜR SIE?

	ENTERPRISE	PERSONAL	BASIC
Remote Terminate bei Verlust oder Diebstahl	✓		
Zugriffskontrolle und-widerruf	✓		
Tracking von Nutzeraktivität und Events	✓		
Wiederherstellung und Wiederinbetriebnahme	✓		
Remote-Steuerung per Internet	✓		
Umsetzung von Sicherheitsrichtlinien	✓		
Automatischer Virensan	✓		
RSA SecurID®, CRYPTOCard, Einmalpasswort	✓		
Web Privacy und Identitätsschutz*	✓	✓	
Eingebauter Schutz vor Malware	✓	✓	✓
Automatische Hardware-Verschlüsselung	✓	✓	✓
Zweikanal-Hochleistungsarchitektur	✓	✓	✓
Robust, manipulationssicher & wasserdicht	✓	✓	✓

* Sicherer Browser, Integrierter Identitätsmanager und VeriSign® Identity

The World's Most Secure Flash Drive

TECHNISCHE DATEN

Kapazität	1GB, 2GB, 4GB, 8GB oder 16GB
Geschwindigkeit*	Lesen bis zu 27MB/Sek. Schreiben bis zu 24MB/Sek.
Abmessungen	75mm X 19mm X 9mm
Gewicht	25 Gramm
Wasserdicht	MIL-STD-810F
Temperatur	Betrieb: 0 °C, +70 °C Lagerung: -40 °C, +85 °C
Stoßfestigkeit	16G RMS
Hardware	USB 2.0 High Speed
Verschlüsselung kompatibel mit Betriebssystemen	Windows 2000 SP4, Windows XP SP2+, Vista, Macintosh OS X 10.4+, Linux 2.6+
Hardwareverschlüsselung	Daten: AES Cipher-Block Chained mode Encryption Keys: 256-bit Hardware PKI: 2048-bit RSA Hashing: 256-bit SHA FIPS Standard: 140-2 Level 3
Erfüllt Abschnitt 508	

VORTEILE des IronKey Enterprise

- Gespeicherte Daten sind mit militärischer AES 256-BIT Hardwareverschlüsselung geschützt
- Keine Installation von Software oder Treibern
- Einfacher Einsatz und Anwendung
- Auf Ihre Unternehmensrichtlinien anpassbar
- Verwaltung per Fernzugriff

Sichere Verwaltung aller IronKey Enterprise USB-Sticks Ihres Unternehmens über das Internet.

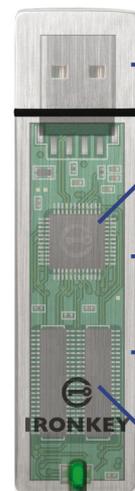


Leicht in bestehende EDV-Landschaft zu integrieren

Die IronKey Enterprise Lösung wurde für die nahtlose Integration in viele der marktführenden EDV-Systeme und Sicherheitssoftware für Endgeräte entwickelt. IronKey Enterprise S200 USB-Sticks unterstützen PKI-basierte digitale Identitäten und Einmalpasswörter. Somit können IronKey USB-Sticks als starke Zwei-Faktor-Authentifizierung für Unternehmensanwendungen genutzt werden.

Verwaltung von Richtlinien und Lebenszyklen

Eine intuitive und sichere Online-Benutzeroberfläche dient IronKey-Administratoren zur Umsetzung von Anwendersicherheitsrichtlinien auf IronKey Enterprise S200 USB-Sticks im Unternehmen. Administratoren können den gesamten Lebenszyklus von Einsatz und Wartung, einschließlich Bereitstellung, Betreuung und Updates, effizient verwalten.



ROBUSTES METALLGEHÄUSE
Wasserdicht
Manipulationssicher

**PERMANENTE AES 256-BIT
HARDWARE-VERSCHLÜSSELUNG**
FIPS 140-2 LEVEL 3 Standard

STARKE AUTHENTIFIZIERUNG
RSA SecurID®
VeriSign® Identity Protection
CRYPTOCard
Digitale Zertifikate

MOBILE ANWENDUNGEN
Sicherer Browser
Verschlüsselte Sicherung
Identitätsmanager

ULTRASCHNELLER SPEICHER
Dual-channel SLC Flash

Selbständige Passwort-Wiederherstellung

IronKey bietet optional die selbständige Online-Passwort-Wiederherstellung mit fortschrittlicher gegenseitiger Authentifizierung zur Überprüfung der Identität des Mitarbeiters.

Entsperren und Rücksetzen von USB-Sticks durch den Administrator

IronKey Enterprise verwendet Public-Key-Authentifizierung, um autorisierten Administratoren Datenzugriff auf USB-Sticks von Mitarbeitern zu gewähren, ohne Passwörter als Hintertür zu verwenden. Administratorenrechte können per Fernzugriff widerrufen werden.

Mobile Sicherheitssoftware

IronKey Enterprise USB-Sticks können optional mit einem Paket von Anwendungen und Diensten versehen werden, das eine sichere mobile Version von Mozilla Firefox, den IronKey Passwortmanager und den IronKey Secure Sessions Dienst beinhaltet. IronKey System-administratoren können diese Anwendungen nach Bedarf aktivieren und deaktivieren.

Sichere Plattform für Virtualisierungen

Schneller Zugriff, hohe Zuverlässigkeit, Schutz auf Hardware-Ebene und die große Speicherkapazität machen IronKey USB-Sticks zur idealen Plattform für den Einsatz von sicheren virtuellen Desktops und mobilen Anwendungen.

 **IRONKEY**

Designed and

Assembled
in the USA



Sicheres Konzept

Das IronKey-Team aus renommierten Experten für Verschlüsselung, Authentifizierung und Internetsicherheit hat die IronKey USB-Sticks und Onlinedienste entwickelt, um hoch entwickelten Angriffen, einschließlich Brute-Force (systematische Zeichenrekombination), USB-Sniffing, Hardware-Demontage, Differential Power Analysis und Chip-Inspektion, standzuhalten.

©Copyright 2009 IronKey, Inc. Alle Rechte vorbehalten. Kopien, ganz oder teilweise, nur mit schriftlicher Erlaubnis von IronKey. IronKey und das IronKey-Logo sind eingetragene Marken der IronKey, Inc. Windows und alle anderen Warenzeichen sind Eigentum der jeweiligen Inhaber. Technische Änderungen vorbehalten. *Lese- und Schreibgeschwindigkeiten wurden unter Laborbedingungen getestet. Die tatsächliche Geschwindigkeit kann abweichen. Die angegebene Kapazität ist ein Näherungswert, der nicht vollständig als Speicherplatz verfügbar ist.