

# SafeNet Data-at-Rest Schutz ProtectDrive™ 8.4

*Niedrige Betriebskosten, leichte Verwaltung.*

## Hauptmerkmale

Unterstützung einer breiten Palette von Tokens und Smart Cards, einschließlich CAC Active Directory™ oder ADAM-basierte Zentralverwaltung oder lokale Verwaltung Multi-Boot-Unterstützung für bis zu vier bootfähige, gesicherte Partitionen; nicht-Windows®-Partitionen sind zulässig

100%-ige Festplattenverschlüsselung für:

- Lokale und remote angebundene Server, Netzwerklautwerke, Arbeitsplätze und Laptops
- Benutzerdaten, Systemdateien, ausgeblendete Dateien, vorläufige Dateien
- Registrierungseinstellungen, Ruhezustandsdateien

Passwortbasierter, entferntbarer Schutz für Datenträger  
Starker

Verschlüsselungsalgorithmus und Schlüsselstärke mit sicherer Schlüsselverwaltung

Starke Authentifizierung mit optionaler passwortgestützter Fallback-Option

Single Sign-On für Pre-Boot-Authentifizierung, Windows®-Anmeldung und andere Startanwendungen

große Benutzergruppen  
Effizientes und sicheres Recovery für Daten und Remote-Passwörter  
Sichere Protokollierung von Pre-Boot-Ereignissen wie Anmeldeversuchen und Passwortänderungen  
Unterstützung für Ruhezustand  
Minimaler Verarbeitungsoverhead

## Einzigartiger Vorteil der Zwei-Faktoren-Authentifizierung

ProtectDrive™ ist die einzige Data-at-Rest-Lösung, die von einem Sicherheitsunternehmen angeboten wird, das auch Zwei-Faktoren-Authentifizierungstools wie Tokens und Smart Cards entwickelt. Dies garantiert Endbenutzern eine reibungslose Interoperabilität – sowohl jetzt als auch in der Zukunft. Darüber hinaus läuft ProtectDrive™ mit einer breiten Vielfalt von Drittlösungen. Bei Einrichtung der Zwei-Faktoren-Authentifizierung können Benutzer nur dann von der Pre-Boot-Umgebung ProtectDrive™ zur Windows®-Umgebung gelangen, wenn sie erfolgreich vorweisen können, dass sie entweder etwas haben (nämlich einen Token) oder etwas wissen (eine PIN).

## Sichere und verwaltbare Wechseldatenträger

Wechseldatenträger wie USB-Memorysticks und tragbare Festplattenlaufwerke sind heutzutage allgegenwärtig. Die Überwachung all dieser Geräte entspräche der Registrierung sämtlicher ausgedruckter Seiten Papier. Für kleine Mengen ist dies durchaus machbar, mit zunehmender Nutzung wird es jedoch sehr kostspielig und schwer zu verwalten.

ProtectDrive™ bietet passwortbasierten Schutz für Wechseldatenträger und führt den "sicheren Unternehmensdatenträger" ein.

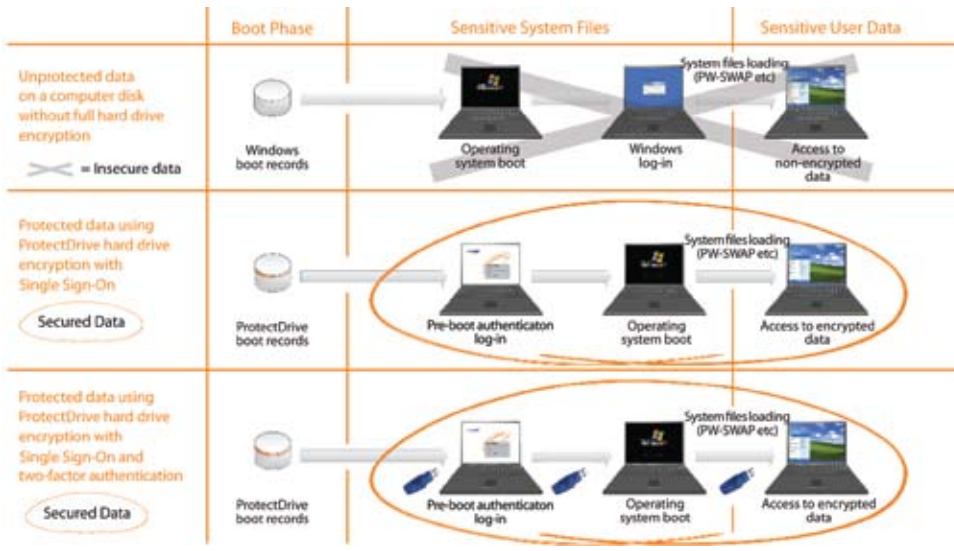
Nachdem ein Speichermedium einmal von einer Person innerhalb des Unternehmens verwendet wurde, um Informationen zu speichern, wird es automatisch zu einem sicheren Unternehmensdatenträger. Nur Benutzer innerhalb des Unternehmens, die das Passwort kennen, können auf den Datenträger zugreifen. Mitarbeiter, denen explizit das entsprechende Recht eingeräumt wurde, können ihn auch außerhalb des Unternehmensumfelds verwenden. In Kombination mit Port-Management und Gerätekontrolle, das die Konfiguration zulässiger Gerätetypen ermöglicht, lassen sich Wechseldatenträger kontrollieren. Das Ergebnis: sichere Datenträger mit minimaler



## Verwaltung durch die IT-Abteilung und maximaler Benutzerakzeptanz.

Am häufigsten von ProtectDrive™ -Kunden genannte Vorteile:

- Überlegene Betriebskosten gegenüber robuster Microsoft® Active Directory™- oder ADAM-Integration; keine zusätzliche Schulung erforderlich und niedrigere laufende Verwaltungskosten
- Gute Akzeptanz durch Endnutzer, da Betrieb äußerst leistungsfähig und transparent ist
- Keine Synchronisierungsprobleme - ProtectDrive™ verwendet Active Directory™ oder ADAM nativ, wodurch sichergestellt wird, dass bei Verlust eines Laptops das Sicherheitsprofil auf dem neusten Stand ist
- Einzelner Verwaltungspunkt; Administratoren brauchen keine neuen Anwendungen zu erlernen, um ProtectDrive™ zu verwalten und unternehmensweit einzuführen
- Gesicherte Einhaltung von Regulierungen durch ProtectDrive™-Verschlüsselung der gesamten Festplatte
- Verhindert Datendiebstahl über Wechseldatenträger wie USB-Memorysticks durch unzuverlässige Mitarbeiter
- Eliminiert zusätzliche Ausgaben für die Entsorgung von Festplatten
- Schützt sowohl Server als auch Arbeitsplätze



## Technische Spezifikationen

### Verschlüsselungsalgorithmen

- DES, 3DES, IDEA, AES-128, AES-192, AES-256

### Sicherheitszertifikate

- Common Criteria EAL2 und ITSEC E1
- Common Criteria EAL4-Konformität im Gange
- Datenverschlüsselungsmodul FIPS 140-2 Level 2-zertifiziert

### Unterstützte Plattformen

- Microsoft Windows XP, 2000 Client und Server, 2003 Server
- Citrix Winframe und Metaframe

### Unterstützte Zwei-Faktoren-Authentifizierung

- SafeNet® iKey™ 1000
- SafeNet® iKey™ 2032
- U.S. DoD Common Access Card (CAC)
- und viele mehr: setzen Sie sich für Details bitte mit uns in Verbindung

### Minimale Systemanforderungen

- 10 MB freier Speicherplatz

### Software-Management-Tools

- Active Directory, RIS, SMS, Tivoli, TNG und andere

## Geringe Implementierungs- und Verwaltungskosten

Warum Betriebskosten (TCO) erwähnen, bevor wir über Technologie reden? Immerhin sind wir vor allem für beispielsweise die Sicherung der Telekommunikation von Air Force One und den tagtäglichen Schutz von Milliarden von Banküberweisungen bekannt.

Aber heutzutage ist ein kugelsicherer Schutz nur eine von mehreren grundlegenden Anforderungen. Wenn die IT-Abteilung eine Festplattenverschlüsselungssoftware nicht effizient implementieren und verwalten kann, oder wenn sich Endbenutzer weigern, Sicherheitsmaßnahmen umzusetzen, weil diese zu mühselig sind, können Kosten leicht eskalieren. Unter diesen Bedingungen leidet die Sicherheit.

Um auf diese Bedenken einzugehen, ermöglicht ProtectDrive™ eine kostengünstige Verwaltung durch Nutzung von Microsoft® Active Directory™ oder ADAM als Verwaltungsplattform. Diese Eliminierung einer zusätzlichen Verwaltungsplattform ist eine einfache, elegante Lösung, die Implementierungen beschleunigt und den Schulungsbedarf minimiert.

Unser Ansatz bietet Organisationen die Möglichkeit, vorhandene Software, Hardware, Prozesse und Wissen einzusetzen, um die Festplattenverschlüsselungsfunktion zentral zu verwalten. Eine Schulung von Endbenutzern ist nicht erforderlich. Für die Implementierung und die laufende Verwaltung ist für Administratoren lediglich eine grundlegende Schulung und ein Basiswissen erforderlich. Eine einfache und automatisierte netzwerkbasierte Implementierung über MSI-Installationspakete oder Active Directory™ GPO ermöglicht eine schnelle und kostengünstige Implementierung, selbst in sehr großen Umgebungen. Das Ergebnis: eine schlanke, unternehmensweite Implementierung ohne Widerstand durch die Benutzer.

## Unsere bewährte Erfolgsgeschichte

ProtectDrive™ ist skalierbar und wurde bereits von führenden Regierungsbehörden, Unternehmen und kleinen Firmen in aller Welt implementiert – von Installationen auf Einzelcomputern bis hin zu Netzwerken mit Zehntausenden von Benutzern. Die anspruchsvollsten Kunden entscheiden sich für ProtectDrive™, weil es Daten umgehend („on the fly“) ver- und entschlüsselt. Hierfür werden starke Verschlüsselungsalgorithmen wie AES-256 verwendet. Ver- und Entschlüsselung werden transparent durchgeführt, eine Interaktion mit dem Endbenutzer ist nicht erforderlich.

**Unternehmenssitz:**  
 4690 Millennium Drive, Belcamp, Maryland 21017 USA  
 Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,  
 Email: info@safenet-inc.com

**Hauptsitz für Europa, Naher Osten und Afrika:**  
 Tel.: + 44 (0) 1276 608 000, E-Mail: info.emea@safenet-inc.com

**Hauptsitz für den Asien-Pazifik-Raum:**  
 Tel.: +852 3157 7111, E-Mail: info.apac@safenet-inc.com

Die Adressen aller Niederlassungen und alle Kontaktinformationen finden Sie unter:  
[www.safenet-inc.com/company/contact.asp](http://www.safenet-inc.com/company/contact.asp)

©2008 SafeNet, Inc. Alle Rechte vorbehalten. SafeNet und das SafeNet-Logo sind eingetragene Warenzeichen von SafeNet. Alle anderen Produktnamen sind Warenzeichen ihrer entsprechenden Eigentümer.  
 PB-ProtectDrive8.2-10.03.08



[www.safenet-inc.com](http://www.safenet-inc.com)