

# FAQ

## Computrace Produkte

<b>PRODUKTE &amp; FUNKTIONEN</b> .....	<b>1</b>
PRODUKTE.....	1
FUNKTIONEN .....	2
IT Asset Management .....	2
Ferngesteuerte Datenlöschung.....	2
Geolokation Tracking .....	10
Wiederbeschaffung nach einem Diebstahl .....	11

## PRODUKTE & FUNKTIONEN

### PRODUKTE

	IT Asset Management	Remote Datenlöschung	Geolokation Tracking	Diebstahl Wiederbeschaffung
Computrace One	●	●	●	●
Computrace Mobile	●	●	●	
Computrace for Netbooks	●			●
Computrace Data Protection	●	●	●	
Absolute Track	●		●	

**Gibt es eine Consumer-Version der Computrace Produkte, die ich für meinen Computer zu Hause kaufen kann?**

Ja. Die gleiche Technologie, die Installationen von Computern innerhalb einer Organisation schützt ist mit LoJack® für Laptops von Absolute® Software für den Heimgebrauch erhältlich. LoJack für Laptops kommt bald nach Europa. Um Ihr Interesse anzumelden, schreiben Sie uns bitte eine E-Mail: [Lojack@emea.absolute.com](mailto:Lojack@emea.absolute.com)

## FUNKTIONEN

### IT Asset Management

#### **Was ist IT Asset Management und was bedeutet es für mich?**

IT asset management (Systemverwaltung) ist eine Strategie oder ein Plan, den eine Organisation umsetzt, so dass sie alle ihre elektronischen Systeme (Computer, Handheld-Geräte, etc.) verwalten kann. Die Verwaltung dieser Systeme ermöglicht es dem Unternehmen, den Überblick darüber zu behalten, wo die Geräte sind und wie sie verwendet werden.

Es ist auch eine zentrale Methode der Systemwartung vorgesehen, da sie es IT-Teams ermöglicht zu wissen, welche Art von Software, Hardware oder Programmen sich auf jedem Rechner befinden und wann diese aktualisiert oder entfernt werden müssen. Geräte können nicht durch Bestandsabweichung (Asset-drift) verschwinden, wenn eine Organisation in der Lage ist, diese zu verfolgen. Und wenn der Verteilungsbereich auch gemietete Geräte enthält, kann jedes Gerät schnell lokalisiert und Daten gelöscht werden, so dass das Ende der Mietzeit nicht überschritten wird.

Die meisten IT Asset Managementpläne enthalten eine Reihe von Regeln, die im Falle eines Diebstahls oder einer Datenschutzverletzung zu befolgen sind, um sicherzustellen, dass die Organisation Staatliche- und Unternehmensvorschriften einhält. Für weitere Informationen sehen Sie im Abschnitt Einhaltung gesetzlicher Bestimmungen dieser FAQ nach.

#### **Wie können Computrace Produkte mir helfen, meine IT-Systeme zu verwalten?**

Mit Computrace Produkten, können Sie alle Ihre elektronischen Systeme einfach mit einer einzigen Schnittstelle (unabhängig davon, ob ein Gerät innerhalb oder außerhalb Ihres LANs ist) innerhalb des Absolute Kundencenters verwalten. Sie können Veränderungen in den Systemdaten, einschließlich der Benutzeridentifikation, dem physischen Standort und die Installation von Software/Hardware, die nicht den Staatlichen- und Unternehmensvorschriften entspricht, überwachen. Die meisten unserer Produkte bieten Ihnen erweiterte Berichtsfunktionen. Computrace Plus versorgt Sie mit wesentlichen Berichten.

### Ferngesteuerte Datenlöschung

#### **Was ist Datenlöschung?**

Bei der Datenlöschung handelt es sich um eine Remotelöschfunktion, mit der Kunden sensible Daten auf gestohlenen oder verloren gegangenen Zielcomputern löschen. Wenn Ihr Computer gestohlen wurde, können Sie eine Datenlöschanforderung einstellen, mit der sensible Daten auf einem Computer gelöscht werden, sobald der Computer sich das nächste Mal im Kontrollzentrum meldet. Weiterhin kann diese Funktion für die Verwaltung des Gerätelebenszyklus verwendet werden, um sicherzustellen, dass Computer am Ende ihrer Lebenszeit oder ihres Leasingzeitraums keine sensiblen Daten mehr enthalten.

## Wie fordere ich eine Datenlöschung an?

1. Melden Sie sich am **Kundencenter** (<http://cc.absolute.com>) mit Ihrem Anmeldenamen und ihrem Kennwort an.
2. Wählen **Sie Datenlöschung**.
3. Wählen **Sie Datenlöschung anfordern**.

## Für welche Produkte steht die Datenlöschung zur Verfügung?

Die Datenlöschung ist mit den meisten Absolute Software-Produkten erhältlich. Für weitere Informationen lesen Sie bitte den Abschnitt Produkte von dieser FAQ.

## Wird eine Vorabautorisierung benötigt, bevor ich die Datenlöschung nutzen kann?

Ja. Die Datenlöschung muss zuerst für Ihr Konto autorisiert werden, bevor sie benutzt werden kann.

## Wie funktioniert die Vorabautorisierung für die Datenlöschung?

Die Zeichnungsberechtigten Ihres Unternehmens müssen zunächst eine Vorabautorisierungsvereinbarung ausfüllen und an Absolute zurücksenden, bevor die Datenlöschfunktion freigegeben werden kann. Das Formular ist im Dokumentationsbereich des Absolute Kundencenters verfügbar. Diese Vereinbarung bestimmt die Personen, die zur Ausführung von Datenlöschbefehlen befugt sind (sie werden als "Administratoren für Datenlöschung" bezeichnet) sowie Ihre bevorzugte Authentifizierungsmethode für die Datenlöschung. Bei Eingang der ausgefüllten Vorabautorisierungsvereinbarung, versorgt Absolute den oder die in der Vereinbarung aufgeführten Administratoren für Datenlöschung mit der Möglichkeit, Datenlöschanforderungen innerhalb Ihres Kundencenterkontos auszuführen.

## Welche Authentifizierungsmethoden für die Datenlöschung gibt es?

Absolute bietet zwei verschiedene Methoden zur Authentifizierung der Datenlöschung:

- RSA SecurID Token.
- Per E-Mail gesendete Autorisierungscode

Sie müssen bei der Einrichtung Ihres Kundencenter-Kontos und beim Ausfüllen der Vorabautorisierungsvereinbarung angeben, welche Methode Sie verwenden möchten.

Wenn RSA SecurID-Token als die Authentifizierungsmethode gewählt wurden, senden wir Ihnen die Token an die in der Vereinbarung angegebenen Administratoren für Datenlöschung. Sobald sie diese erhalten, lässt sich die Datenlöschung ohne weitere Beteiligung von uns einrichten. Beachten Sie, dass die RSA SecurID-Token einen zusätzlichen Aufwand verursachen und direkt von Absolute Software gekauft werden müssen.

## Was sind RSA SecurID® Schlüssel/Token und wie funktionieren sie?

Die RSA SecurID® Lösung ist das weltweit führende 2-Faktoren-System zur Benutzerauthentifizierung, dem Tausende von Organisationen weltweit den Schutz ihrer wertvollen Netzwerkressourcen anvertrauen. Ein RSA SecurID® Authentifikator funktioniert wie eine Geldautomatenkarte. Netzwerk- und Desktopbenutzer müssen sich mit zwei einzigartigen Faktoren identifizieren—etwas, was sie wissen und etwas, was sie

# FAQ

haben-, bevor Sie die Zugriffsberechtigung erhalten. Die Verwendung von RSA SecurID® Authentikatoren ist nicht komplizierter als die Eingabe eines Kennwortes, aber viel sicherer. Jedem Endbenutzer wird ein Token zugewiesen, das alle 60 Sekunden einen neuen, nicht vorhersagbaren Code generiert. Der Benutzer kombiniert diese Nummer mit einem Kennwort/einer persönlichen Geheimnummer, um Zugriff auf geschützte Ressourcen zu erhalten.

Jeder RSA SecurID® Authentikator verfügt über einen einzigartigen, symmetrischen Schlüssel mit einem leistungsstarken Algorithmus, der jedes Mal einen neuen, zeitabhängigen Code erstellt. Nur der RSA® Authentifizierungsmanager weiß, welche Nummer zu einem bestimmten Zeitpunkt für die spezifische Benutzer/Authentikator-Kombination gültig ist. Mehr Informationen finden Sie unter <http://www.rsa.com>.

## **Was ist ein Autorisierungscode und wie funktioniert er?**

Bei einem Autorisierungscode handelt es sich um einen einzigartigen Code, der als Antwort auf eine Anforderung beim Kundencenter an die in den Akten vorliegende E-Mail Adresse des Administrators für Datenlöschung gesendet wird. Der Autorisierungscode ist nach seiner Ausgabe zwei (2) Stunden gültig und kann nur für einen Datenlöschvorgang verwendet werden. Außerdem kann der Autorisierungscode nur von dem anfordernden Administrator für Datenlöschung genutzt werden. Für per E-Mail gesendete Autorisierungscodes wird keine Gebühr erhoben.

## **Kann ich von RSA Secure ID® Token zu Autorisierungscodes oder umgekehrt wechseln?**

Ja, aber Sie können nur eine Authentifizierungsmethode auswählen. Administratoren für Datenlöschung können nicht beide Methoden gleichzeitig verwenden. Um die Authentifizierungsmethode zu ändern, wenden Sie sich unter <http://www.absolute.com/support> an den **Global Support von Absolute**.

## **Wie fordere ich einen Autorisierungscode an?**

Als ein berechtigter Administrator für Datenlöschung, können Sie einen Autorisierungscode wie folgt anfordern:

- Im Kundencenter wählen Sie Datenlöschung.
- Wählen Sie Autorisierungscode für die Datenlöschung.
- Sie erhalten Ihren Autorisierungscode per E-Mail.

## **Wie teuer ist die Datenlöschung?**

Für die Verwendung von Autorisierungscodes wird keine Gebühr erhoben. Für RSA SecurID® Token wird eine Gebühr für alle Token erhoben, inklusive aller Erneuerungen und Ersatz-Token. Sie müssen separate Token für jeden Administrator für Datenlöschung erwerben. Erkundigen Sie sich bei Ihrem Absolute Vertriebsmitarbeiter über die Preise.

## **Können die Daten über Festplatten/magnetische Medien wiederhergestellt werden, nachdem sie gelöscht wurden?**

Nein. Die Daten können nicht wiederhergestellt werden.

## Wie funktioniert die Datenlöschung?

Der für die Datenlöschung verwendete Algorithmus geht weit über die Empfehlungen des amerikanischen National Institute of Standards and Technology hinaus. Weitere Informationen finden Sie in der

### **Sonderveröffentlichung NIST Special Publication 800-88: Guidelines for Media Sanitization: Empfehlungen des National Institute of Standards and Technology**

([http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)). Dieses Dokument beschreibt die notwendigen Spezifikationen für das Löschen von Festplattenspeicherdaten, um eine dauerhafte Löschung aller zuvor auf diesem magnetischen Medium enthaltenen Daten sicherzustellen.

Wenn die meisten Computer eine Datei löschen, entfernt der Computer die Inhalte der Datei nicht wirklich, sondern trennt lediglich die Verbindung zwischen Datei und Dateiverzeichnissystem. Die Inhalte der Datei verbleiben jedoch auf den Festplattensektoren. Diese Daten verbleiben dort, bis das Betriebssystem die gleichen Sektoren wieder verwendet und mit neuen Daten überschreibt. Bis die alten Daten überschrieben sind (was Monate oder sogar länger dauern kann), können sie durch Programme wiederhergestellt werden, die Festplattensektoren direkt lesen (z. B. forensische Software). Selbst wenn ein Sektor überschrieben wird, kann das Phänomen der Datenremanenz (verbleibende physische Datendarstellung gelöschter Daten) gelöschte Daten forensisch wiederherstellbar machen.

Um sicherzustellen, dass eine Datei korrekt gelöscht wurde, müssen die Datensektoren dieser Datei überschrieben werden. Es ist nicht ausreichend, die Festplatte zu löschen oder zu formatieren, da es zahlreiche Programme gibt, mit denen "verlorene" Daten auf Festplatten wiederhergestellt werden können. Diese Spezifikation erfordert, dass jeder einzelne Sektor auf einem magnetischen Speichermedium drei Mal neu überschrieben wird: einmal mit einem festen Wert (0x00), dann mit seinem Komplementärwert (0xff) und schließlich einmal mit Zufallswerten. Unser Datenlöschalgorithmus geht über diesen Standard hinaus, indem er die Daten 7 Mal überschreibt (nicht nur 3 Mal) und zudem Zusatzvorgänge durchführt. Der Algorithmus:

1. Überschreibt den Zielsektor 7 Mal – die ersten 6 Mal mit einem alternierenden Muster von 1s und 0s und beim letzten Mal mit einem Zufallswert
2. Schreibt Zufallswerte in die Datei
3. Ändert die Dateiattribute auf "Verzeichnis"
4. Ändert Dateidatum/Zeitstempel und gibt einen festen Wert dafür ein
5. Stellt für die Dateigröße "0" ein
6. Ändert den Dateinamen und gibt einen zufällig erstellten Dateinamen ein
7. Entfernt den neuen Dateinamen aus dem Verzeichnis

# FAQ

## **Entspricht die Datenlöschung dem Standard 5220.22-M des US-Verteidigungsministeriums zum Löschen von Daten auf Festplatten?**

Nein. Es gibt keine ausschließlich auf Software beruhenden Lösungen, die diesem Standard entsprechen, da er die physische Zerstörung des Speichermediums erfordert (Zerstückeln, Verbrennen, Mahlen oder Schmelzen des Plattenlaufwerks).

## **Entspricht der Datenlöschalgorithmus auf Windows Mobile Geräten den Empfehlungen des Dokuments NIST 800-88 Media Sanitization Guidelines zum Löschen von Daten auf Flash-Speichergeräten?**

Ja. Der Datenlöschalgorithmus für Windows Mobile Geräte geht über diese Richtlinien hinaus.

## **Woher weiß ich, ob der Datenlöschvorgang erfolgreich war?**

Der Datenlöschvorgang endet in der Erstellung einer Audit-Protokolldatei, die überprüft, welche Dateien gelöscht wurden. Das Auditprotokoll wird im Kontrollzentrum zur Verfügung gestellt (nur für Windows PCs: Außer Sie verwenden eine Richtliniendatei und geben **"kein Booten ohne Protokolldatei"** im Befehl vor).

## **Wenn ich eine Datenlöschung auf einem gestohlenen Computer ausführe, kann ich sagen, auf welche Dateien nach dem Diebstahl zugegriffen wurde?**

Wenn Sie eine Datenlöschung durchführen, können Sie das Datum von Erstellung, Änderung und Zugriff in die Protokolldatei aufnehmen (nur für Windows PCs). Ist diese Einstellung aktiviert, zeigt die Protokolldatei diese Datumsattribute neben dem Namen jeder gelöschten Datei an.

Die Einbeziehung dieser Attribute erhöht die Größe der Protokolldatei.

Hinweis: Ein nach dem Diebstahlsdatum liegendes Zugriffsdatum für eine Datei gibt nicht unbedingt an, dass die Datei nach dem Diebstahl kompromittiert wurde. Nicht erkannte Malware, Antivirus- und Spyware-Scans, automatische Backups und ähnliche Anwendungen können die Änderung des Zugriffsdatums auslösen.

## **Muss ich das gesamte Laufwerk löschen oder kann ich bestimmte Dateien oder Verzeichnisse wählen?**

Der Datenlöschdienst steht in 3 Varianten zur Verfügung:

1. **Bestimmte Dateien/Verzeichnisse (nur PCs):** Der Benutzer erstellt eine Richtliniendatei, um bestimmte Dateien, Dateitypen und/oder Verzeichnisse anzugeben, die gelöscht werden sollen. Der Computer bleibt nach dem Datenlöschvorgang funktionsfähig, vorausgesetzt, der Benutzer löscht keine Verzeichnisse des Betriebssystems und verwendet nicht die Option "kein Booten". Sie könnten sich beispielsweise dafür entscheiden, den gesamten Inhalt des Verzeichnisses "Meine Dokumente" sowie alle Word-, Excel-, PowerPoint- und PDF- Dokumente zu löschen - unabhängig davon, wo sie sich auf der Festplatte befinden.
2. **Alle Dateien außer Betriebssystem:** Alle Dateien mit Ausnahme der Dateien des Betriebssystems werden von der Festplatte entfernt – der Computer bleibt nach dem Datenlöschvorgang funktionsfähig.
3. **Alle Dateien einschließlich Betriebssystem:** (nicht für Windows Mobile Geräte) Alle Dateien, die nicht zum Betriebssystem gehören und bestimmte Betriebssystemdateien werden von der Festplatte entfernt. Nach dem Löschen aller Dateien, die nicht zum Betriebssystem gehören,

# FAQ

beginnt die Datenlöschung mit einer Sektorenlöschung auf Sektor 0. Gelöscht werden alle Benutzerdateien (inklusive Programme und Daten) und ausreichend viele Dateien des Betriebssystems, um ein Booten des Computers zu verhindern. Es kann sein, dass sich nach der Datenlöschung noch Betriebssystemdateien auf der Festplatte befinden. Der Computer ist nach Abschluss des Datenlöschvorgangs nicht mehr funktionsfähig.

Im Falle einer vollständigen Datenlöschung inklusive der Dateien des Betriebssystems handelt es sich um einen Vorgang in 2 Phasen: Zunächst werden alle Dateien mit Ausnahme der Betriebssystemdateien entfernt, dann wird eine Protokolldatei hochgeladen, die alle gelöschten Dateien auflistet, und anschließend die Datenlöschung des Betriebssystems gestartet. Da der Computrace-Agent nach dem Löschen der Betriebssystemdateien nicht mehr anrufen kann, wird die Datenlöschung auf abgeschlossen gesetzt, nachdem die Löschung der Dateien abgeschlossen ist, die nicht zum Betriebssystem gehören.

## **Kann die Datenlöschung die Benutzerprofile von Windows XP und Windows Vista löschen?**

Ja. Die Datenlöschung kann alle Windows XP Benutzerprofile löschen, indem sie einen Eintrag in "C:\Dokumente und Einstellungen\" verwendet. Windows Vista Benutzerprofile können gelöscht werden, indem ein Richtliniendateieintrag von "C:\Benutzer\" verwendet wird. Vergessen Sie nicht den Backslash ("\") nach dem Ordernamen.

## **Was ist eine Richtliniendatei für Datenlöschungen und wie verwende ich sie?**

Bei einer Richtliniendatei für Datenlöschungen handelt es sich um eine Liste mit Einträgen, die bestimmte Dateien, Dateitypen und/oder Ordner angeben, die gelöscht werden sollen. Sie können auch die Optionen "kein Booten mit Protokolldatei" oder "kein Booten ohne Protokolldatei" in einer Richtliniendatei verwenden, wenn Sie zunächst Dateien an einem bestimmten Speicherort löschen möchten, bevor die vollständige Datenlöschung erfolgt. Richtliniendateien werden nur auf Windows Computern unterstützt.

## **Kann die Datenlöschung gesperrte Dateien von Windows PCs entfernen?**

Ja. Beim ersten Löschversuch markiert der Datenlöschdienst alle gesperrten Dateien wie beispielsweise geöffnete Word-Dokumente, die beim nächsten Neustart an einen sicheren Speicherort verschoben werden. Dann erzwingt die Datenlöschung einen Neustart, um die Dateisperrungen zu entfernen und fährt nach dem Neustart mit dem Löschen der Dateien fort.

## **Kann die Datenlöschung gesperrte Dateien von Windows Mobile Geräten entfernen?**

Nein.

## **Welche Sicherheitsmaßnahmen sind vorgesehen, um sicherzustellen, dass nur autorisierte Benutzer eine Datenlöschung starten können?**

Nur die in der Vorabautorisierung als Administratoren für Datenlöschung bezeichneten Personen sind berechtigt diesen Dienst anzufordern. Diese Administratoren für Datenlöschung müssen die Authentifizierungsmethode verwenden, die zur Ausführung des Befehls notwendig ist.

# FAQ

Hier ist ein Überblick über die vorhandenen Beschränkungen:

- Die Seite zur Datenlöschanforderung wird solange nicht in Ihrem Kundencenterkonto angezeigt, bis Sie eine vollständige und unterschriebene Vorabautorisierungsvereinbarung übermittelt haben.
- Sie müssen ein berechtigter Administrator für Datenlöschung sein, so wie er in der Vorabautorisierungsvereinbarung angegeben ist.
- Sie müssen Administrator-Zugriff auf das Kundencenter haben.
- Sie müssen die entsprechende Authentifizierungsmethode (RSA SecurID Schlüssel oder Authentifizierungscode) verwenden. Diese sind jeweils mit dem bestimmten Kundencenter Anwender verknüpft und sind zwischen verschiedenen Benutzern auf einem Konto oder zwischen verschiedenen Konten NICHT austauschbar.
- Das Kennwort, das sie ins Formular zur Datenlöschanforderung eingeben, muss mit dem Kennwort für den aktuell angemeldeten Benutzer im Kundencenter übereinstimmen.
- Ihr Wert des RSA SecurID-Token (Zeitabhängig) muss, wenn er in das Formular zur Datenlöschanforderung eingegeben wurde, mit dem auf dem Absolute SecurID-Server für Ihr bestimmtes Kundencenter Benutzerprofil, übereinstimmen

Sind alle oben ausgeführten Bedingungen erfüllt, wird die Datenlöschung so eingestellt, dass sie beim nächsten Computrace Agent Anruf auf diesem Computer durchgeführt wird.

Zusätzlich zu diesen Sicherheitsvorkehrungen wird den Zeichnungsberechtigten der Vorabautorisierungsvereinbarung eine E-Mail gesendet, wenn die Datenlöschung angefordert, gestartet und vollständig durchgeführt wurde.

## **Kann Absolute auf meinem Computer ohne mein Einverständnis eine Datenlöschung durchführen?**

Nein. Wir können keine Datenlöschung durchführen, da dafür Unterlagen erforderlich sind, die nur der Kunde besitzt (RSA SecurID Token, Autorisierungscode, Anmeldung/Kennwort, etc.).

## **Kann ich die Datenlöschung testen?**

Ja. Wenden Sie sich an Ihren Absolute Vertriebsmitarbeiter, um dies einzustellen.

## **Sind meine Daten geschützt, wenn der Dieb den Computer nie mit dem Internet verbindet?**

Nein. Aber nach unserer Erfahrung findet die große Mehrheit gestohlener Computer schnell wieder den Weg zurück ins Internet. Dies ist in der Regel der Grund, warum sie gestohlen werden. Zu diesem Zeitpunkt können Sie die Datenlöschanforderung aktivieren.

## **Wozu ist eine Datenlöschung notwendig, wenn ein Dieb das Betriebssystem neu installiert und die Daten also ohnehin gelöscht werden?**

Interne Diebstähle machen die Mehrzahl aller Laptop-Diebstähle aus. In solchen Fällen kennt der Benutzer alle Kennwörter und muss das Betriebssystem nicht neu installieren. In Fällen internen Datendiebstahls ist die Datenlöschung die perfekte Lösung.

# FAQ

In Fällen externer Diebstähle installiert der Dieb oft das Betriebssystem neu. Manchmal wird dabei die Festplatte neu formatiert, manchmal auch nicht. Wird das Betriebssystem ohne eine Neuformatierung der Festplatte neu installiert, werden die Dateien, aus denen sich das Betriebssystem zusammensetzt, ersetzt. Doch Dateien mit sensiblen Daten werden nicht vollständig ersetzt und sind über die Standard-Dateitabelle oder mit vielen weit verbreiteten forensischen Tools erschließbar. Die Datenlöschung entfernt diese Dateien und stellt sicher, dass die Daten nicht wiederhergestellt werden können

Eine Datenlöschung auf einem gestohlenen Computer bietet dem Kunden auch ein Auditprotokoll darüber, welche Dateien gelöscht wurden. Diese Überprüfung ist für die Richtlinienbefolgung sehr wichtig.

Bei einer Neuinstallation des Betriebssystems mit Neuformatierung der Festplatte ist es schwieriger, auf Überreste der Originaldateien auf dem Computer zuzugreifen, da sich Dateitabellenstruktur und Sektorgröße auf der Festplatte ändern können. Es ist jedoch trotzdem möglich, auf dem gestohlenen Computer die Daten eines bestimmten Sektors zu löschen.

## **Wie lange dauert die Durchführung einer Datenlöschung auf einem Windows PC?**

Die für die Datenlöschung notwendige Zeit ist von mehreren Faktoren auf dem Zielcomputer abhängig:

- Anzahl der Dateien
- Anzahl der Dateien > 100 Kbytes
- HDD Geschwindigkeit
- Prozessorgeschwindigkeit
- Verfügbarer Arbeitsspeicher (RAM)
- Installierte Antivirus-Software

Aufgrund der Gründlichkeit des Datenlöschalgorithmus dauert das Löschen von Dateien länger als eine normale Datenlöschung (auf Ebene des Betriebssystems). Die Löschengeschwindigkeit auf einem Windows XP Computer mit Pentium M 1.8Ghz CPU und 504 MB RAM beträgt ca. 100 MB/Minute. Eine "typische" Datenlöschung kann 2 Minuten bis mehrere Stunden dauern, je nach Computer und zu löschendem Datenvolumen.

Wenn Sie sich über die Geschwindigkeit Ihrer Datenlöschung Sorgen machen, empfiehlt Absolute die Erstellung einer Richtliniendatei mit den wichtigsten Dateien, die zuerst gelöscht werden sollen.

## **Kann eine Datenlöschung gestoppt werden?**

Nachdem der Datenlöschvorgang begonnen hat, kann er nicht mehr gestoppt werden. Wird ein Computer während des Vorgangs neu gestartet, wird der Datenlöschvorgang dort fortgesetzt, wo er unterbrochen wurde. Wurde eine Datenlöschung auf einem gestohlenen Computer programmiert, jedoch noch nicht begonnen, können Sie den Datenlöschvorgang im Kundencenter stoppen.

# FAQ

## **Werden auch verborgene Dateien von Windows-PCs gelöscht?**

Ja.

## **Kann ich nur die Datenlöschung kaufen?**

Nein – Die Datenlöschung steht als technische Funktion ausgewählten Absolute Software Produkten zur Verfügung.

## **Sollte die Datenlöschung im Bereich der Software-Konformität eingesetzt werden, beispielsweise für die Entfernung nicht autorisierter Software?**

Dies ist nicht empfehlenswert. Die Datenlöschung wurde vorrangig für die Entfernung sensibler Daten auf verlorenen oder gestohlenen Computern entwickelt. Wird sie verwendet, um Anwendungen wie limewire.exe zu entfernen, kann dies den Rechner instabil machen, da Verknüpfungen für Anwendungen und unterstützende DLLs nicht berücksichtigt werden. Die Verwendung der Datenlöschung für Konformitätszwecke lenkt auch die Aufmerksamkeit auf unsere Anwendung, was ihren 'geheimen Charakter' beeinträchtigt und die Wiederbeschaffungsanwendungen für den Endnutzer offensichtlicher macht.

## Geolokation Tracking

### **Was bedeutet geolokation tracking?**

Mit Geo-Standortverfolgung können Sie die geographische Lage ihrer Computer sehen.

### **Welche Art von Technologie ist erforderlich, um meine IT-Systeme geographisch zu orten?**

Die GPS- oder Wi-Fi-Technologie ermöglicht es Ihnen, Ihre Systeme auf einer Google™-Karte (siehe Beispiel unten) zu verfolgen. Sie können aktuelle und historische Standorte innerhalb von etwa 33 Fuß sehen. Die Verwendung der GPS-Technologie erfordert einen GPS-Empfänger.

### **Welche Systemvoraussetzungen gibt es für die Wi-Fi-Triangulation?**

- Momentan nur für Windows-Clients verfügbar (keine Unterstützung für Mac-Computer)
- Der Computrace Agent muss installiert sein
- Der Client muss einen WLAN-Netzwerkadapter haben
- Der WLAN-Netzwerkadapter muss eingeschaltet sein und mindestens ein Wi-Fi-Netzwerk muss sichtbar sein

### **Welche Systemvoraussetzungen gibt es für GPS?**

- Verfügbar für Windows, Windows Mobile und BlackBerry Clients
- Der Computrace Agent muss installiert sein
- Der Client muss einen unterstützten GPS-Empfänger besitzen:
  - Windows: Notebook muss ein mobiles Gobi Breitbandmodul haben
  - Windows Mobile: alle offenen GPS-Empfänger
  - BlackBerry: alle offenen GPS-Empfänger

# FAQ

Wenn der Client sowohl Wi-Fi-Triangulation und GPS unterstützt, wird zuerst per GPS der Standort bestimmt, wird aber, falls erforderlich, auf die Wi-Fi-Triangulation zurückgreifen.

HINWEIS: Computrace Mobile Geo-Standortbestimmung ist nur mit der GPS-Technologie verfügbar.

## Wiederbeschaffung nach einem Diebstahl

### **Was meinen Sie mit "Wiederbeschaffung nach einem Diebstahl"?**

Genau das, was es sagt - wir werden helfen, um Ihren Computer wiederzubeschaffen, wenn er gestohlen wurde. Ist dies der Fall ist, wird das Absolute Wiederbeschaffungsteam mit der örtlichen Polizei zusammenarbeiten, um ihn zu lokalisieren und ihn an Sie zurückzugeben.

### **Wie funktioniert das?**

Wenn Ihr Computer gestohlen wurde, kontaktieren Sie uns. Das nächste Mal, wenn Ihr Computer eine Verbindung zum Internet herstellt, wird er unauffällig in den Diebstahlmodus gesetzt, indem sich die Kontaktrate des Agenten von einmal pro Tag auf alle 15 Minuten erhöht. Dieser erhöhte Kontakt ermöglicht es dem Absolute Diebstahl Wiederbeschaffungsteam mit einer Vielzahl forensischer Verfahren, einschließlich des Mitschneidens von Tastatureingaben, Registry- und Datei-Scannens, Geo-Standortbestimmung und anderer Ermittlungstechniken, zu bestimmen, wer Ihren Computer hat und was sie mit ihm tun.

Am wichtigsten ist, dass wir unsere Technologie nutzen werden, um genau den physischen Standort des Computers herauszufinden und eng mit der örtlichen Polizei zusammenarbeiten, um ihn wiederzubeschaffen.

### **Mein Computer wurde gestohlen! Was soll ich tun?**

Sie müssen eine Diebstahlmeldung wie folgt aufgeben:

1. Melden Sie sich am **Kundencenter** (<http://cc.absolute.com>) mit Ihrem Anmeldenamen und ihrem Kennwort an.
2. Wählen **Sie Diebstahlmeldung**.
3. Wählen **Sie eine Neue Diebstahlmeldung**.
4. Wählen Sie den gestohlenen Rechner aus und stellen Sie die folgenden Informationen zur Verfügung:
  - Wie ging der Computer verloren
  - Die Einzelheiten der von Ihnen eingereichten Diebstahlanzeige bei der Polizei

### **Was, wenn mein Computer verloren geht?**

Wenn Ihr Computer verloren geht, können Sie die Funktion zur Geo-Standortbestimmung innerhalb des Kundencenters verwenden, um das Gerät zu orten.