

# Schutz von Karteninhaber-Kontodaten

## Wie Reflection-Software die PCI-Compliance erleichtert

### INHALT

Die zwölf PCI-Anforderungen .....	1
Wie Reflection Ihre Host-zentrischen Sicherheitsprobleme löst .....	2
Mit Reflection Compliance erreichen .....	3
Größerer Funktionsumfang, schnellere Compliance .....	5

# Schutz von Karteninhaber-Kontodaten

## Wie Reflection-Software die PCI-Compliance erleichtert

2004 schlossen sich die größeren Kreditkartenunternehmen – darunter Visa, MasterCard und American Express – zusammen und schufen den Payment Card Industry Data Security Standard (PCI DSS). Alle Unternehmen, die Karteninhaber-Kontodaten speichern, verarbeiten oder übertragen, müssen diesen Standard erfüllen. Der Zweck besteht darin, mithilfe strenger Sicherheitskontrollen branchenweiten Datenschutz für Kunden zu gewährleisten.

Eine Reihe von Compliance-Fristen haben Unternehmen in Zugzwang gebracht, die zwölf umfassenden PCI DSS-Anforderungen zu erfüllen. Manche dieser Anforderungen sind verhältnismäßig leicht umzusetzen, wie z.B. Antivirussoftware auf dem neuesten Stand zu halten, andere sind komplex und anspruchsvoll, beispielsweise die Protokollierung der Zugriffe auf Netzwerkressourcen und Karteninhaberdaten.

In diesem Beitrag wird beschrieben, wie Sie mit Terminalemulatoren, Anwendungen zur Dateiübertragung und SSH-Clients und -Servern von Attachmate® Reflection® PCI DSS-konform werden können. Nach Beendigung der Lektüre wissen Sie, mit welchen Reflection-Produkten Sie bestimmte PCI-Anforderungen erfüllen können – und wie das geschieht. Ebenso verstehen Sie dann, dass Reflection über Terminalemulation und Dateiübertragung hinaus Compliance in Bereichen ermöglicht, die Sie vielleicht noch nicht in Erwägung gezogen haben.

### Die zwölf PCI-Anforderungen

Der PCI DSS umfasst zwölf Anforderungen, die gewährleisten sollen, dass Karteninhaberdaten sicher und die Daten verarbeitenden Netzwerke und Systeme gut geschützt sind. Die zwölf Anforderungen lassen sich in folgende Gruppen unterteilen:

<b>Einrichten und Verwalten eines sicheren Netzwerks</b>
1. Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten 2. Änderung von Herstellervorgaben für Systemkennwörter und andere Sicherheitsparameter
<b>Schutz von Karteninhaberdaten</b>
3. Schutz von gespeicherten Karteninhaberdaten 4. Verschlüsselung der Übertragung von Karteninhaberdaten über nicht gesicherte, öffentliche Netzwerke
<b>Verwalten eines Programms zur Bewältigung von Sicherheitsrisiken</b>
5. Verwendung und regelmäßige Aktualisierung von Antivirusprogrammen 6. Entwicklung und Wartung sicherer Systeme und Anwendungen
<b>Implementieren strikter Zugriffssteuerungsmaßnahmen</b>
7. Beschränkung des Zugriffs auf Karteninhaberdaten auf das Nötigste 8. Zuweisung einer eindeutigen Benutzerkennung für jede Person mit Rechnerzugang 9. Beschränkung des physikalischen Zugriffs auf Karteninhaberdaten
<b>Regelmäßiges Überwachen und Testen von Netzwerken</b>
10. Protokollierung und Überwachung aller Zugriffe auf Netzwerkressourcen und Karteninhaberdaten 11. Regelmäßige Prüfung von Sicherheitssystemen und -prozessen
<b>Einführen und Einhalten einer Informationssicherheitsrichtlinie</b>
12. Einführung und Einhaltung von Richtlinien in Bezug auf Informationssicherheit

Reflection-Produkte erleichtern die Einhaltung der Anforderungen 1, 2, 4, 6, 7, 8 und 10.

## Wie Reflection Ihre Host-zentrischen Sicherheitsprobleme löst

Damit Sie besser verstehen, wie Reflection-Produkte die PCI-Compliance erleichtern können, enthält dieser Abschnitt eine Zusammenfassung der größten Host-zentrischen Sicherheitsprobleme und eine Beschreibung, wie Reflection-Produkte diese lösen.

### Sicherheit für Server

Auf Host-Systemen werden Karteninhaberdaten gespeichert und Anwendungen ausgeführt, um den Zugriff auf diese Daten zu ermöglichen. Host-Systeme können auch Dateiserver sein, auf denen Karteninhaberdaten in Dateiform gespeichert sind, die über öffentliche Netzwerke übertragen werden müssen. Da die Daten vertraulich behandelt werden müssen, ist es erforderlich, dass Unternehmen den Zugriff auf diese Daten beschränken und diese während der Übertragung im Netzwerk verschlüsseln.

**Reflection-Lösung:** Reflection for Secure IT ist eine Produktfamilie von Secure Shell-Clients und -Servern für Windows® und UNIX. Mit Reflection for Secure IT-Servern können Sie sichere, verschlüsselte Tunnel für Daten während der Übertragung einrichten – einschließlich der Kommunikation von Client-basierten Emulatoren, Dienstprogrammen zur Dateiübertragung oder anderen Anwendungen, die das TCP/IP-Protokoll verwenden.

Außerdem erfüllt Reflection for Secure IT noch eine weitere entscheidende Sicherheitsfunktion: die Protokollierung von Zugriffen, einschließlich solcher mit Administratorrechten, auf Systemkomponenten. Wenn Sie die Konfiguration für Audit Logging aktivieren, liefert Reflection for Secure IT Schlüsselinformationen (wer hat wann über den SSH-Server auf das System zugegriffen) an standardmäßige Protokollierungsanwendungen auf dem Host-System.

### Sicherheit für Arbeitsstationen

Benutzer und Systemadministratoren verwenden häufig Client-basierte Programme, um auf Host-Anwendungen und -Dateien zuzugreifen. Die für den Zugriff auf Host-Systeme verwendeten Benutzer-IDs und -kennwörter sowie die vertraulichen Daten, die zwischen der Arbeitsstation und dem Host-System ausgetauscht werden, müssen allesamt vor neugierigen Blicken geschützt werden.

**Reflection-Lösung:** Die Terminalemulatoren von Reflection for the Web und Reflection for Windows unterstützen eine Vielzahl von Verschlüsselungstechnologien (einschließlich SSH und SSL/TLS) und Authentifizierungsmethoden (z.B. Kerberos), die den auf dem Host-System aktivierten Funktionen entsprechen. Dank dieser Unterstützung können sich Datenschutzbeauftragte sicher sein, dass sowohl Benutzerkonto-Anmeldedaten (z.B. Kennwörter) als auch vertrauliche Informationen (z.B. Karteninhaberdaten) beim Austausch zwischen Host und Terminalemulationsbildschirm verschlüsselt werden.

## Info zu Reflection-Produkten

### Reflection for Windows

Reflection Terminalemulationsprodukte (sowie Attachmate EXTRA!® und INFOConnect® Terminalemulatoren) stellen sichere Verbindungen zu Anwendungen auf Systemen von IBM, HP, UNIX, Unisys, OpenVMS, Tandem und CRS/GDS her. Diese bewährten Produkte mit großem Funktionsumfang bieten eine vollständige Optionspalette zu Verschlüsselung, Authentifizierung und Datenintegrität.

### Reflection Secure FTP

Reflection Secure FTP ist im Lieferumfang der Reflection-, EXTRA!- und INFOConnect-Produkte enthalten und ist eine stabile Software zur Übertragung von Dateien zwischen Benutzer-Arbeitsstationen und Host-Systemen.

### Reflection for the Web

Reflection for the Web ist eine Terminalemulations-Software, mit der sichere Verbindungen zwischen Browserbenutzern und Anwendungen auf Systemen von IBM, HP, UNIX, Linux, OpenVMS, Unisys und CRS/GDS hergestellt werden. Dank der leistungsfähigen Funktionen im Bereich Benutzerauthentifizierung, Benutzerautorisierung, Audit Logging, Verschlüsselung und Zugriffssteuerung können Sie voll funktionierende Host-Anwendungen sicher über das Internet bereitstellen.

### Reflection for Secure IT

Reflection for Secure IT ist eine Produktfamilie von Secure Shell-Clients und -Servern für Windows- und UNIX-Umgebungen – allesamt dafür konzipiert, Daten während der Übertragung zu schützen. Mit den Funktionen im Bereich Verschlüsselung, Authentifizierung, Überwachung und Datenintegrität von Reflection for Secure IT können Sie über verschlüsselte Verbindungen vertrauliche Daten übertragen, Remote-Server verwalten und auf Firmenanwendungen zugreifen.

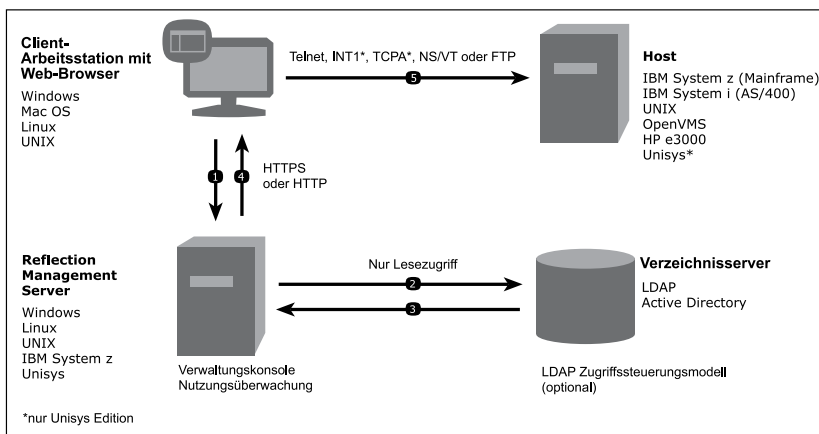
Die Reflection Secure FTP-Clients (in den Reflection-Emulationsprodukten enthalten) unterstützen ebenfalls eine Reihe von Verschlüsselungstechnologien und Authentifizierungsmethoden. Diese Technologien und Methoden sorgen dafür, dass Dateien mit vertraulichen Informationen nicht von unbefugten Benutzern aufgerufen werden können und innerhalb des Netzwerks verschlüsselt werden.

### Sicherheit für den Systemzugriff

Über Client-Terminalemulatoren kann auf private Host-Daten zugegriffen werden – der Zugriff auf Emulationssitzungen muss also streng kontrolliert werden.

**Reflection-Lösung:** Reflection for the Web bietet eine Authentifizierungs- und Zugriffskontrolle, die auf vorhandene Benutzerverzeichnisse (z.B. Active Directory) zurückgreift. Benutzer können nur dann auf Emulationssitzungen zugreifen, wenn dies von einem Administrator genehmigt wurde.

Innerhalb einer Domäne können Benutzern und Gruppen individuelle Sitzungskonfigurationen zugewiesen werden. Diese Sitzungen werden über Links auf einer geschützten Webseite oder einem Portal aufgerufen. Beim Zugriff auf diese Seite werden Benutzer mit dem Benutzerverzeichnis abgeglichen und dürfen nur auf vorbestimmte Host-Sitzungen zugreifen.



- 1) Der Benutzer verbindet sich mit Reflection Management Server.
- 2) Der Benutzer authentifiziert sich bei einem Verzeichnisserver (LDAP/Active Directory) – optional.
- 3) Der Verzeichnisserver liefert die Benutzer- oder Gruppenidentifizierung.
- 4) Reflection Management Server sendet die Emulationssitzung an den authentifizierten Client.
- 5) Der authentifizierte Benutzer verbindet sich mit dem Host.

## Mit Reflection Compliance erreichen

In diesem Abschnitt wird erklärt, wie Reflection Sie bei der Erfüllung der PCI DSS-Anforderungen 1, 2, 4, 6, 7, 8 und 10 unterstützen kann.

### Anforderung 1: Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten

Abschnitt 1.1 der PCI DSS-Dokumentation sieht vor, dass bestimmte Protokolle – einschließlich Secure Sockets Layer (SSL) und Secure Shell (SSH) – die Firewall ohne besondere Berechtigung oder Protokollierung durchlaufen dürfen. Protokolle wie FTP, die als risikobehaftet gelten, bedürfen dagegen einer Berechtigung und Protokollierung, um die Firewall passieren zu dürfen.

In Abschnitt 1.2 wird vorgeschrieben, dass Firewalls konfigurationsgemäß sämtlichen Datenverkehr – mit Ausnahme von erforderlichen Protokollen für die Karteninhaberdaten-Umgebung – von nicht vertrauenswürdigen Netzwerken ablehnen müssen.

So erleichtern Reflection-Produkte die Erfüllung von Anforderung 1:

#### Reflection for Windows

Alle Reflection for Windows-Produkte unterstützen die Verschlüsselung des Terminaldatenstroms über

ausreichende Sicherheitsprotokolle, einschließlich SSH und SSL/TLS.

#### Reflection Secure FTP

Das Reflection Secure FTP-Dienstprogramm unterstützt die Standard-FTP-, SFTP- und FTP/S-Client-Funktionalität über ausreichende Sicherheitsprotokolle, einschließlich SSH und SSL/TLS.

#### Reflection for the Web

Reflection for the Web unterstützt die Verschlüsselung des Terminaldatenstroms über ausreichende Sicherheitsprotokolle, einschließlich SSH und SSL/TLS.

Reflection for the Web beinhaltet außerdem Reflection Security Proxy für reinen Firewall-freundlichen Host-Zugriff. Hosts werden hinter Firewall und Proxy versteckt. Es kann über einen offenen Port der Firewall auf mehrere Hosts zugegriffen werden.

#### Reflection for Secure IT

Die SSH-Server von Reflection for Secure IT bieten einen serverseitigen Mechanismus zur Unterstützung von SSH-Verbindungen von Reflection Terminalemulations- und Dateiübertragungs-Clients.

### Anforderung 2: Änderung von Herstellervorgaben für Systemkennwörter und andere Sicherheitsparameter

Abschnitt 2.3 sieht vor, dass alle administrativen Zugriffe auf Hauptsysteme, die nicht über eine Bedienkonsole erfolgen, verschlüsselt sein müssen. SSH und SSL/TLS sind als ausreichende Protokolle aufgeführt.

So erleichtern Reflection-Produkte die Erfüllung von Anforderung 2:

#### Reflection for Windows

Reflection for Windows-Produkte können für den administrativen Zugriff auf Host-Systeme verwendet werden, der nicht über eine Bedienkonsole erfolgt. Alle Produkte unterstützen die Verschlüsselung des Terminaldatenstroms über ausreichende Sicherheitsprotokolle, einschließlich SSH und SSL/TLS.

#### Reflection for the Web

Reflection for the Web unterstützt die Verschlüsselung des Terminaldatenstroms über ausreichende Sicherheitsprotokolle, einschließlich SSH und SSL/TLS.

Reflection Security Proxy bietet außerdem verschlüsselte Verbindungen zu Host-Systemen wie Unisys, die über keine native Verschlüsselungsunterstützung verfügen.

#### **Reflection for Secure IT**

Reflection for Secure IT Secure Shell-Clients verfügen über Dienstprogramme für interaktive und geskriptete Remote-Administrationsaufgaben über das SSH-Protokoll.

Die SSH-Server von Reflection for Secure IT bieten einen serverseitigen Mechanismus zur Unterstützung von SSH-Verbindungen von Reflection Terminalemulations-Clients.

#### **Anforderung 3: Schutz von gespeicherten Karteninhaberdaten**

In Abschnitt 3.3 ist festgelegt, dass Primary Account Numbers (PANs) bei Anzeige verdeckt werden sollten.

So erleichtert Reflection® for IBM® 2007, ein Windows-basierter Terminalemulator, die Erfüllung von Anforderung 3:

#### **Reflection for IBM 2007**

Reflection for IBM 2007 umfasst eine konfigurierbare Datenschutzfilterfunktion, mit der in Verlaufsfeinstern, gedruckten Berichten und Zwischenablagen angezeigte PANs verdeckt werden können.

Hinweis: Die Terminalemulations-Software Attachmate EXTRA! bietet dieselbe Funktionalität.

#### **Anforderung 4: Verschlüsselung der Übertragung von Karteninhaberdaten über nicht gesicherte, öffentliche Netzwerke**

Anforderung 4 sieht vor, dass vertrauliche Informationen während der Übertragung über Netzwerke verschlüsselt sein müssen, da Hacker Daten während der Übertragung mühelos abfangen, ändern und umleiten können. In Abschnitt 4.1 wird außerdem vorgeschrieben, dass starke Kryptografie und Sicherheitsprotokolle verwendet werden müssen, um vertrauliche Karteninhaberdaten während der Übertragung zu schützen.

So erleichtern Reflection-Produkte die Erfüllung von Anforderung 4:

#### **Alle Reflection-Produkte**

Alle Implementierungen der SSH- und SSL/TLS-Protokolle in Reflection-Produkten verwenden starke Kryptografie – einschließlich Triple DES- und AES-Algorithmen – zur Verschlüsselung von Karteninhaberdaten, die über das Netzwerk übertragen werden. In den meisten Fällen wurden diese kryptografischen Implementierungen von einer autorisierten dritten Partei gemäß FIPS 140-2 validiert.

#### **Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen**

In Abschnitt 6.1 der PCI-DSS-Anforderungen ist festgelegt, dass man immer die neuesten vom Hersteller bereitgestellten Sicherheitspatches innerhalb eines Monats nach Veröffentlichung installiert haben muss.

Damit Sie immer auf dem aktuellen Stand hinsichtlich der sich ständig verändernden Sicherheitsbedrohungen sind, sollten Sie mit einem Partner zusammenarbeiten, der die führenden Sicherheitswarndienste beobachtet und Sie bei relevanten Sicherheitsrisiken benachrichtigt.

Die Sicherheitsexperten von Attachmate führen einen Technical Notes-Katalog (verfügbar auf unserer Support-Website), in dem alle veröffentlichten Sicherheitsrisiken erläutert sind. Wenn ein Attachmate-Produkt betroffen ist, können Attachmate-Kunden mit Wartung die entsprechenden Sicherheitspatches sofort herunterladen.

#### **Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten auf das Nötigste**

Dieser Anforderung zufolge darf nur Benutzern, die geschäftlich auf Karteninhaberdaten zugreifen müssen, dieser Zugriff erteilt werden. Weiterhin sollte die Standardkonfiguration für Benutzer, die nicht explizit autorisiert sind, auf „Alle Zugriffe ablehnen“ eingestellt sein.

So erleichtert Reflection for the Web die Erfüllung von Anforderung 7:

#### **Reflection for the Web**

Alle Host-Systeme bieten ein gewisses Maß an Autorisierungs- und Zugriffssteuerung. Erhöhen Sie die Sicherheit noch zusätzlich: Mit Reflection for the Web können Sie die Dienstprogramme, z. B. Terminalemulatoren und Dateiübertragungs-Dienstprogramme, steuern, die auf Ihre Hosts zugreifen.

So funktioniert es: Benutzer müssen sich auf einer Website anmelden, auf der Links zu Terminalemulations- und Dateiübertragungssitzungen bereitgestellt sind. Authentifizierungs- und Zugriffssitzungen können über einen bestehenden Zugriffskontrolldienst (z. B. Active Directory) verwaltet werden. Der Zugriff lässt sich auf Benutzer- oder Gruppenebene kontrollieren. Nach der Standardeinstellung von Reflection for the Web wird unbefugten Benutzern der Zugriff verweigert.

#### **Anforderung 8: Zuweisung einer eindeutigen Benutzererkennung für jede Person mit Rechnerzugang**

Diese Anforderung fällt in die Zielkategorie „Implementieren strikter Zugriffssteuerungsmaßnahmen“ und sieht vor, dass sich Benutzer identifizieren müssen, bevor sie Zugriff auf Karteninhaberdaten erhalten. Außerdem wird eine Reihe von Authentifizierungsmethoden vorgeschlagen und die Verwendung einer 2-Faktoren-Authentifizierung für den Remote-Zugriff vorgeschrieben.

So erleichtert Reflection for the Web die Erfüllung von Anforderung 8:

### **Reflection for the Web**

Indem vor den Zugriff auf Terminalemulations- und Dateiübertragungs-Dienstprogramme noch eine Authentifizierungs- und Autorisierungsstufe eingeschoben wird, können mit Reflection for the Web die eindeutigen IDs, die innerhalb eines bestehenden Benutzerverzeichnisses zugewiesen wurden, für die Zugriffssteuerung verwendet werden.

Neben kennwortbasierter Authentifizierung unterstützt Reflection for the Web auch digitale Zertifikate und öffentliche Schlüssel.

### **Anforderung 10: Protokollierung und Überwachung aller Zugriffe auf Netzwerkressourcen und Karteninhaberdaten**

Protokollierungsmechanismen und die Möglichkeit der Nachverfolgung von Benutzeraktivitäten sind gemäß den PCI-DSS-Anforderungen von entscheidender Bedeutung. Anforderung 10 schreibt vor, welche Ereignisse zur Überwachung protokolliert und welche spezifischen Überwachungspfade pro Ereignis aufgezeichnet werden müssen.

So erleichtern Reflection-Produkte die Erfüllung von Anforderung 10:

#### **Reflection for Secure IT**

Als Anbieter von serverbasierten Secure Shell-Diensten bietet Reflection for Secure IT stabile Protokollierungsfunktionen. Schlüsselereignisse während des Betriebs von Reflection for Secure IT-Servern, einschließlich eingehender Client-Verbindungen und -Authentifizierungen, werden in einer Reihe von konfigurierbaren Systemen, so auch Standard-Ereignisprotokollen des Betriebssystems, erfasst.

#### **Reflection for the Web**

Während Terminalemulations- und Dateiübertragungssitzungen protokolliert Reflection for the Web eingehende Zugriffsereignisse und -Details zu den Host-Systemen, mit denen sich die Benutzer verbinden.

### **Größerer Funktionsumfang, schnellere Compliance**

Es ist keine leichte Aufgabe, die umfassenden PCI DSS-Anforderungen zu erfüllen. Die Umsetzung kann Abteilungsgrenzen überschreiten, mehrere Teams einschließen und mehrere Systemplattformen betreffen. Der nötige Aufwand kann zeitraubend und teuer sein.

Leider gibt es keine einzelne Sicherheitslösung, die alle PCI-Compliance-Anforderungen abdeckt. Reflection-Produkte, die mehr PCI-Compliance-Funktionen als jede andere Terminalemulationslösung bieten, können jedoch eine breite Unterstützungsgrundlage bieten. Mithilfe von Werkzeugen, die auf Servern und Benutzer-Arbeitsstationen laufen, reduzieren Reflection-Produkte den Zeitaufwand für Compliance und unterstützen eine sicherere Informationsweitergabe.

Und das ist noch nicht alles: Sobald Sie Ihre PCI-Anforderungen erfolgreich erfüllt haben, ist es kein weiter Weg mehr für Ihr Unternehmen, weitere neuere Bestimmungen zu erfüllen.

## **Die Verbindung zu NetIQ**

Alle in diesem Dokument beschriebenen Reflection-Produkte eignen sich als Bestandteil einer gut geplanten Strategie zur Erfüllung der PCI-Anforderungen. Wenn Sie jedoch alle PCI DSS-Anforderungen erfüllen, verwalten und überwachen möchten, ist NetIQ, ein Geschäftsbereich von Attachmate, der richtige Ansprechpartner für Sie.

NetIQ ist einer der Marktführer in den Bereichen Compliance, Überwachung und IT-Prozessautomatisierung. NetIQ wurde von Gartner im Bereich Sicherheitslösungen als führend eingestuft und versorgt mit Sicherheits- und Überwachungstechnologien (inkl. Security Information and Event Management - SIEM) eine Vielzahl der größten Unternehmen und Regierungen weltweit.

Die Lösungen von NetIQ® decken so wichtige Bereiche wie Systemsicherheit, Netzwerküberwachung, Richtlinienverwaltung und Zugriffssteuerung ab und können schnell und problemlos zur Compliance-Unterstützung bereitgestellt und eingesetzt werden. Außerdem fertigen die Sicherheitsexperten von NetIQ in Zusammenarbeit mit Ihren IT- und Compliance-Teams eine maßgeschneiderte Lösung an, die Ihre individuellen Ziele erfüllt und sich für Ihre vorhandene Infrastruktur eignet.

Weitere Informationen zu den Lösungen von NetIQ finden Sie unter [www.netiq.de](http://www.netiq.de).



**Hauptsitz**  
1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL +1 206 217 7500  
FAX +1 206 217 7515

**Europäische Zentrale**  
Niederlande  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

**Österreich**  
TEL +43 1 595 4335 0  
FAX +43 1 595 4335 11  
[www.attachmate.at](http://www.attachmate.at)  
[info-at@attachmate.com](mailto:info-at@attachmate.com)

**Schweiz**  
TEL +41 43 399 2090  
FAX +41 43 399 2099  
[www.attachmate.ch](http://www.attachmate.ch)  
[InfoCH@attachmate.com](mailto:InfoCH@attachmate.com)

**Deutschland**  
TEL +49 89 99 351 0  
FAX +49 89 99 351 111  
TEL +49 2102 4965 0  
FAX +49 2102 4965 65  
TEL +49 711 67 968 0  
FAX +49 711 67 968 33  
[www.attachmate.de](http://www.attachmate.de)  
[info-de@attachmate.com](mailto:info-de@attachmate.com)