

## Schützen von Legacy-Host-Anwendungen durch moderne Sicherheitsmaßnahmen

---

### INHALT

Moderne Ansätze zur Sicherheit .....	1
Legacy-Host-Anwendungen ohne Sicherheitstechnologie .....	2
Legacy-Host-Sicherheit der ersten Generation: SSL direkt zum Host .....	2
Legacy-Host-Sicherheit der nächsten Generation: Mehrschichtarchitektur .....	2
Vorteile des Sicherheitsframeworks von Attachmate .....	3
Nicht intrusive mehrstufige Sicherheit für Legacy-Host-Anwendungen .....	5

---

# Schützen von Legacy-Host-Anwendungen durch moderne Sicherheitsmaßnahmen

Unter dem Druck, für Datenschutz zu sorgen und vertrauliche Informationen zu sichern, haben Unternehmen in jüngster Zeit ausgefeilte IT-Sicherheitsinfrastrukturen aufgebaut. Sie setzen auf eine „Defense in Depth“-Strategie, also mehrstufige Verteidigung mit verschiedenen Schutzebenen. Leider kommen bei der Absicherung der Systeme, in denen die meisten wichtigen Daten gespeichert sind, häufig antiquierte und unzureichende Sicherheitsverfahren zum Einsatz.

Es gibt jedoch eine Möglichkeit, diese entscheidenden Legacy-Hosts in die moderne Sicherheitsarchitektur einzubeziehen. In diesem Whitepaper wird die Entwicklung der Sicherheitstechnologie für Legacy-Host-Anwendungen betrachtet; zudem erhalten Sie Informationen über die Vorteile eines zeitgemäßen Ansatzes für den Schutz von Green-Screen-Anwendungen.

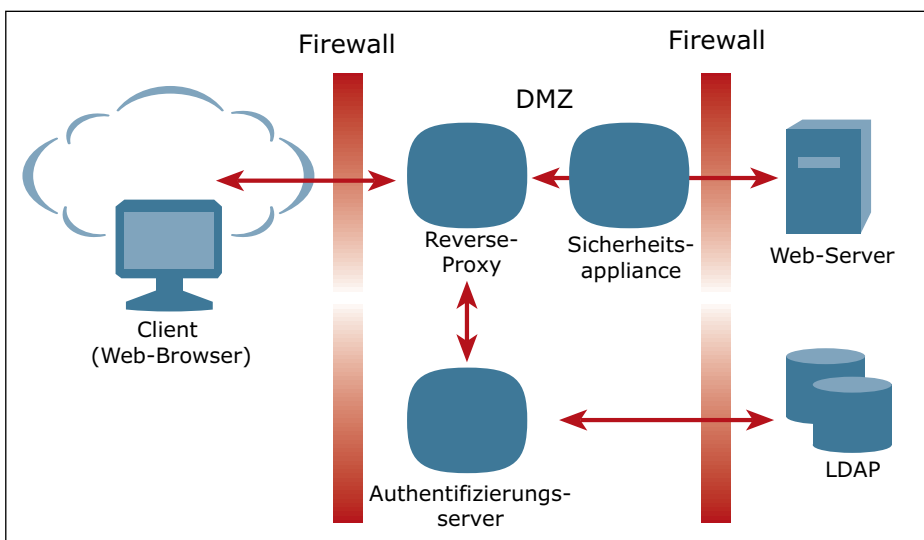
## Moderne Ansätze zur Sicherheit

Bei fortschrittlicher Netzwerksicherheit wird – entsprechend dem Defense-in-Depth-Prinzip des Rundumschutzes – ein mehrstufiger Ansatz verfolgt. Moderne Unternehmen setzen verschiedene Instrumente ein, um sich gegen vielfältige Bedrohungen zu wappnen.

## Mehrere Sicherheitsmaßnahmen

Eine moderne mehrschichtige Architektur umfasst eine Reihe von Sicherheitsmaßnahmen:

- **Verschlüsselung.** Daten werden bei der Übertragung im ungeschützten Netzwerk außerhalb des Sicherheitsperimeters verschlüsselt.
- **Zentralisiertes Identitätsmanagement.** Über ein LDAP-Repository im Unternehmen werden Identitätsdaten für alle Benutzer verwaltet.
- **Zentralisierte Zugriffssteuerung.** Am Perimeter werden Authentifizierungs- und Autorisierungsrichtlinien auf den gesamten Datenverkehr zwischen Clients und Servern angewendet.
- **Zentralisiertes Auditing.** Der Zugriff auf Netzwerkressourcen wird am Zugriffssteuerungspunkt zentral überwacht.
- **Zentralisierte Bedrohungsüberwachung.** Der ein- und ausgehende Datenverkehr wird am Sicherheitsperimeter analysiert – mit Eindringlingserkennung, Inhaltsinspektion und anderen Schutzverfahren zur Abwehr möglicher Angriffe oder unbefugter Zugriffe auf vertrauliche Daten.



In einer modernen Sicherheitsarchitektur ist das Defense-in-Depth-Konzept umgesetzt – enthalten sind verschiedene Schichten mit Reverse-Proxy-Element, Authentifizierung sowie Autorisierung in der DMZ. Netzwerkrichtlinien werden mit der Sicherheitsappliance durchgesetzt (Ausführung von Inhaltsinspektion, Eindringlingserkennung usw.); Back-End-Server erhalten einen geschützten Bereich.

## Zentralisierte Sicherheitsverwaltung

Der Einsatz mehrerer Sicherheitsmaßnahmen ist wichtig, nicht weniger bedeutend ist jedoch die Art und Weise, wie diese Sicherheitsmaßnahmen verwaltet werden. In einem dezentral strukturierten Unternehmen sind möglicherweise verschiedene Anwendungen und Server vorhanden, die von unterschiedlichen Geschäftsbereichen kontrolliert werden. Für ein zentrales Sicherheitsteam kann es schwierig sein, die an jedem der Serverknoten im Back-End angewendeten Sicherheitsverfahren zu überwachen und durchzusetzen.

Die oben beschriebene moderne Architektur ermöglicht eine zentralisierte Sicherheitsverwaltung. Der gesamte Netzwerkverkehr zwischen Clients und Back-End-Servern muss durch eine DMZ (demilitarisierte Zone), die vom zentralen Sicherheitsteam kontrolliert wird. So entsteht ein zentraler Steuerungspunkt zum Anwenden, Überwachen und Durchsetzen der unternehmensweiten Sicherheitsrichtlinien – unabhängig von den spezifischen eingesetzten Sicherheitsverfahren an den einzelnen Back-End-Knoten.

### Legacy-Host-Anwendungen ohne Sicherheitstechnologie

Der Zugriff auf Legacy-Host-Anwendungen erfolgte bisher in der Regel über häufig verwendete ungesicherte Ports, etwa Port 23 bei Telnet und TCPA oder Port 102 bei INT1 und TPO. Mit dieser Vorgehensweise sind verschiedene Sicherheitsrisiken und Schwierigkeiten verbunden:

- **Keine Vertraulichkeit von Daten oder Kennwörtern.** Ohne Verschlüsselung sind Daten und Kennwörter ungeschützt.
- **Schwache Authentifizierung.** Bei vielen Hosts sind nur Kennwörter mit acht Zeichen ohne Unterscheidung von Groß- und Kleinschreibung möglich.
- **Dezentralisierte Authentifizierung.** Hostbasierte Authentifizierung lässt sich oft nur schwer in LDAP einbinden; für gewöhnlich läuft sie getrennt von den Identitätsmanagementsystemen ab, die in übrigen Unternehmensbereichen verwendet werden.
- **Dezentralisierte Zugriffssteuerung.** Zugriffssteuerung erfolgt nur am Host, daher wird der Zugang zu Unternehmensressourcen nicht zentral kontrolliert.
- **Dezentralisiertes Auditing.** Der Zugriff auf Hosts wird nur durch die Hosts selbst überwacht.

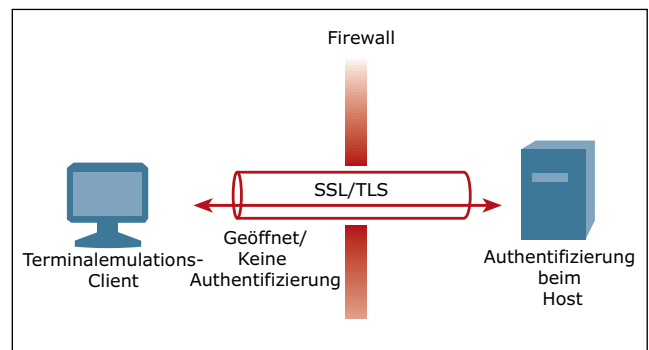
### Legacy-Host-Sicherheit der ersten Generation: SSL direkt zum Host

Legacy-Host-Sicherheitsarchitekturen der ersten Generation basieren auf direkten SSL-Verbindungen vom Client zum Host. Der wesentliche Vorteil dabei: Daten und Kennwörter werden verschlüsselt.

Der verschlüsselte Tunnel vom Client zum Host bewirkt aber leider auch, dass andere Sicherheitsmaßnahmen unbrauchbar werden, da die Überwachung des Netzwerkverkehrs und die Anwendung jeglicher Art von Zugriffssteuerung in der DMZ erschwert werden.

Dies sind einige der Einschränkungen einer einfachen Architektur mit SSL-Verbindung direkt zum Host:

- **Schwache dezentralisierte Authentifizierung.** In den meisten SSL-Umgebungen erfolgt die Authentifizierung vollständig am Host, daher sind viele Hosts lediglich durch Kennwörter mit acht Zeichen ohne Unterscheidung von Groß- und Kleinschreibung geschützt. Host-Authentifizierung läuft üblicherweise getrennt von den in anderen Unternehmensbereichen verwendeten Identitätsmanagementsystemen ab.



Host-Sicherheit der ersten Generation basiert auf SSL-Verschlüsselung des Datenstroms direkt zum Host, die Authentifizierung erfolgt jedoch erst dann, wenn die Verbindung zum Host hergestellt wurde – so haben Unbefugte freie Bahn bis zur Anmeldeseite des Hosts.

- **Dezentralisierte Zugriffssteuerung.** Zugriffssteuerung erfolgt nur am Host, daher wird der Zugang zu Unternehmensressourcen nicht zentral kontrolliert.
- **Nicht authentifizierter SSL-Datenverkehr wird unmittelbar an den Host weitergeleitet.** Aufgrund des verschlüsselten SSL-Tunnels ist es nicht möglich, die Verbindung in der DMZ zu überwachen; Unbefugte können daher ohne Hindernisse bis zur Anmeldung beim Host gelangen. Das zentrale Sicherheitsteam muss Datenverkehr durch die DMZ zulassen, ohne den Client oder die Art des Datenverkehrs zu kennen, da der Datenverkehr verschlüsselt ist.
- **Dezentralisiertes Auditing.** Der Zugriff auf Hosts wird nur durch die Hosts selbst überwacht.
- **Keine zentralisierte Bedrohungsüberwachung am Perimeter.** Der ein- und ausgehende Datenverkehr kann nicht mit Inhaltsinspektion oder anderen Sicherheitsverfahren analysiert werden, da der Inhalt verschlüsselt ist.
- **Dezentralisierte Steuerung der Sicherheitsfunktionen.** Authentifizierung, Zugriffssteuerung und Auditing können nur bei jedem einzelnen Host angewendet werden; für das zentrale Sicherheitsteam ist es deshalb schwierig, die Einhaltung unternehmensweiter Sicherheitsrichtlinien zu überwachen und durchzusetzen.

Alles in allem sorgt eine SSL-Verbindung direkt zum Host für Verschlüsselung, kann aber eine zentralisiert durchgeführte Zugriffssteuerung und die Durchsetzung anderer Sicherheitsrichtlinien erschweren.

### Legacy-Host-Sicherheit der nächsten Generation: Mehrschichtarchitektur

In einer modernen Mehrschichtarchitektur kann die Terminalemulations-Software Attachmate® Reflection®, EXTRA!® und INFOConnect® mit Sicherheitskomponenten von Reflection for the Web eingesetzt werden, um geschützten Zugriff auf klassische Green-Screen-Anwendungen zu bieten.

Zu Reflection for the Web gehören die folgenden Komponenten:

- Reflection Management Server zur Steuerung von zentralisierten Client-Konfigurationen. Die Einbindung in eine zentralisierte Identitätsmanagement-Infrastruktur im Unternehmen ist möglich.
- Reflection Security Proxy für den Empfang des SSL-Datenverkehrs von Clients und den Empfang der vom Verwaltungsserver ausgegebenen Autorisierungstokens.
- Reflection Metering Server zur Verfolgung der Anzahl von Verbindungen sowie ggf. zur Aufzeichnung aller Hosts und Ports, zu denen die Benutzer eine Verbindung aufbauen, und zur Erfassung der Gesamtverbindungsdauer.
- Reflection Thin-Client-Emulation mit VT-, TN3270-, TN5250-, NS/VT- und FTP-Sitzungen innerhalb von SSL.

Die moderne mehrstufige Sicherheitsarchitektur von Attachmate besteht aus folgenden Schichten:

- **Zentralisiertes Identitätsmanagement.** Bevor der Zugriff auf einen Host erfolgen kann, müssen Benutzer sich bei Reflection Management Server authentifizieren. Die Anmeldedaten werden anhand des im Unternehmen verwendeten Identitätsmanagementsystems überprüft – dies kann z. B. LDAP, Active Directory oder ein Portal sein.
- **Zentralisierte Zugriffssteuerung.** Bevor die Sitzung genehmigt wird, prüft Reflection Management Server, ob der Administrator dem Benutzer Zugang zur Host-Sitzung gewährt hat. Zugriffsrechte können über die Mitgliedschaft in einer LDAP-Gruppe kontrolliert werden.
- **Durchsetzung der Zugriffssteuerung am Perimeter.** Reflection Security Proxy prüft unter Verwendung der speziellen Reflection-Autorisierungstechnologie mit sicheren Tokens, ob der Benutzer zum Aufbauen einer

Verbindung mit dem Host berechtigt ist. Erst danach wird die Verbindung durch die DMZ geleitet, sofern die Autorisierung erfolgreich war. Nicht autorisierte Benutzer kommen niemals durch die DMZ.

- **Verschlüsselung.** Der Terminalemulations-Client von Reflection stellt eine SSL-Verbindung zu Reflection Security Proxy her. Dabei werden Verschlüsselungsstärken bis 256-Bit-AES unterstützt, der Verschlüsselungscode entspricht FIPS 140-2.
- **Zentralisiertes Auditing.** Da die Authentifizierung und Autorisierung von Benutzern am Perimeter erfolgt, wird der Zugriff auf sämtliche Netzwerkressourcen zentral überwacht und protokolliert – durch Reflection Management Server.
- **Zentralisierte Bedrohungsüberwachung am Perimeter.** Eine bei der Einrichtung von Reflection Security Proxy häufig verwendete Option ist die Entschlüsselung des gesamten Datenverkehrs mit anschließender Übermittlung zum Host durch einen geschützten Netzwerkbereich in reinem Textformat per Telnet. Jeder Datenverkehr zum und vom Host kann dabei mit Eindringlingserkennung, Inhaltsinspektion und anderen Sicherheitsfunktionen überwacht werden.

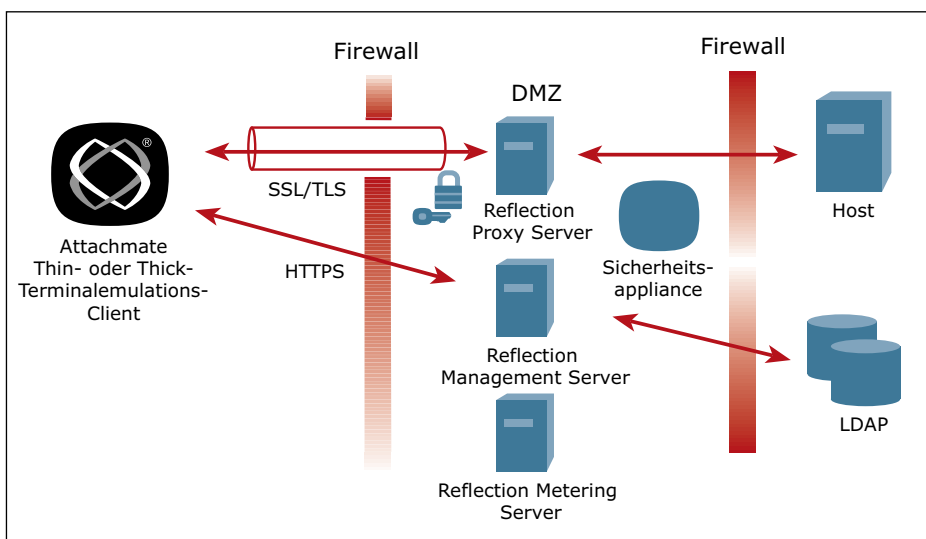
### Vorteile des Sicherheitsframeworks von Attachmate

Im Folgenden werden die Vorteile des mehrstufigen Sicherheitsframeworks von Attachmate skizziert.

#### Zentralisierte Sicherheitsverwaltung

Ein wesentlicher Vorteil der Sicherheitsarchitektur von Attachmate ist die Möglichkeit der zentralisierten Steuerung des Netzwerkverkehrs zwischen den Clients und dem Host. Zusätzlich zu einer evtl. auf dem Host selbst durchgeführten Authentifizierung können mit Reflection Schichten für Authentifizierung,

Autorisierung und Auditing in der DMZ eingerichtet werden, wo eine zentrale Steuerung und Überwachung möglich ist. Die praktischen und logistischen Probleme, die mit der separaten Durchsetzung von Sicherheitsrichtlinien an jedem einzelnen Back-End-Host einhergehen, werden so erheblich verringert.



Bei Host-Sicherheit der nächsten Generation gibt es einen Zugriffssteuerungspunkt vor dem Host. Benutzer müssen sich authentifizieren, bevor sie ins interne Netzwerk gelangen. Der Steuerungspunkt kann durch Einbindung in ein unternehmensweit eingesetztes Identitätsmanagementsystem wie LDAP zentral verwaltet werden.

### **Integration in das vorhandene Identitätsmanagementsystem**

Der Verwaltungsserver von Reflection for the Web schützt frühere Investitionen in ein Identitätsmanagementsystem.

Reflection kann in Kombination mit allen gängigen LDAP-Servern eingesetzt werden:

- Active Directory
- Novell
- iPlanet/Netscape/SunOne
- IBM Directory Server
- IBM RACF
- OpenLDAP
- Andere mit RFC 2256 kompatible LDAP-Server

Reflection ist nicht intrusiv; Lesezugriff auf das LDAP-Verzeichnis reicht aus. Der Zugang zu den Hosts lässt sich problemlos unter Verwendung der vorhandenen Struktur von LDAP-Benutzern und -Gruppen steuern.

Reflection kann außerdem in Kombination mit verbreiteten Portal- und Webauthentifizierungstools eingesetzt werden:

- WebSphere Portal
- BEA WebLogic Portal
- Plumtree Portal
- Netegrity SiteMinder

Anders als bei einigen Produkten anderer Hersteller ist es bei Reflection nicht notwendig, im Hostzugriffsprogramm Benutzer und Gruppen separat vom Unternehmensverzeichnis zu definieren. Reflection ermöglicht vielmehr eine unkomplizierte Integration in das bestehende Identitätsmanagementsystem und die Nutzung der darin verfügbaren Funktionen.

### **Spezielle Autorisierungstechnologie mit sicheren Tokens zur Durchsetzung der Zugriffskontrolle**

Mitbewerber bieten verschiedene Produkte für einfache SSL-Gateways oder SSL-Umleitungen. Sämtliche dieser Produkte haben jedoch einen Mangel: Sie akzeptieren Verbindungen von jedem SSL-kompatiblen Client, ohne zu prüfen, ob der Benutzer für den Zugang zum Host autorisiert ist.

Bei Mitbewerberprodukten erfolgt die Authentifizierung, bevor eine Sitzung für berechtigte Benutzer gewährt wird; ein unbefugter Benutzer mit SSL-fähigem Client kann jedoch die Authentifizierung umgehen und einfach eine Verbindung zum Gateway oder Redirector aufbauen – hier fehlt eine Prüfung der Autorisierung für den Hostzugang. Stattdessen wird die Verbindung automatisch zum Host weitergeleitet. So haben unbefugte Benutzer freie Bahn bis zum Host.

Im Unterschied dazu ist bei Reflection Security Proxy ein Nachweis über die Authentifizierung und Autorisierung der Clients erforderlich, damit der Zugang zum Host gewährt wird. Bei Authentifizierung eines Clients gegenüber Reflection Management Server wird vom Server geprüft, ob der Benutzer für die angeforderte Sitzung autorisiert ist. Danach wird dem Client ein zeitlich begrenztes, digital signiertes Token zugewiesen, das den gewünschten Zugang gewährt. Der Reflection Security Proxy verifiziert die digitale Signatur des Tokens unter Verwendung von Kryptografie mit öffentlichem Schlüssel, bevor die Verbindung an den Host weitergeleitet wird.

Wenn ein unbefugter Benutzer versucht, eine SSL-Verbindung zu Reflection Security Proxy aufzubauen, ohne dass zuvor eine Authentifizierung und Autorisierung durch den Verwaltungsserver erfolgt ist, wird der Zugriff auf der Proxy-Ebene verweigert. Der unbefugte Benutzer hat keine Möglichkeit, eine Netzwerkverbindung zum Host herzustellen.

### **Zugang zu mehreren Hosts über einen Port**

Es gibt verschiedene Mitbewerberprodukte für einfache SSL-Gateways oder SSL-Umleitungen, die einem Back-End-Host einen abhörenden Port zuweisen. Wenn Sie mehrere Back-End-Hosts betreiben, müssen Sie mehrere abhörende Ports öffnen – und damit auch mehrere Ports in der Firewall.

Reflection Security Proxy ermöglicht Clients das Aufbauen von Verbindungen zu mehreren Hosts über nur einen abhörenden Port. Mit einer einzigen Öffnung in der Firewall, z. B. bei Port 443, können Sie Zugang zu allen Hosts gewähren und später weitere Hosts hinzufügen, ohne etwas an der Firewall zu verändern. So wird die Konfiguration einfacher, und der Verwaltungsaufwand für das Sicherheitsteam wird reduziert.

### **Alternativszenario: Durchgängige Verschlüsselung mit Zugriffssteuerung am Perimeter**

Ein häufig eingesetztes Konzept bei Architekturen für den sicheren Host-Zugriff besteht darin, dass verschlüsselter Datenverkehr vom Client zum Reflection Security Proxy in der DMZ vorgeschrieben ist und dann die Übertragung von Daten im Textformat durch den geschützten Bereich zum Host zugelassen wird. Dieser Ansatz ermöglicht die Inhaltsinspektion beim Datenverkehr zum und vom Host.

Manchmal kann es jedoch Gründe für SSL-Verbindungen vom Client direkt bis zum Host geben. Unter Umständen möchten Unternehmen die Nachrichtenintegrität zwischen Client und Host sichern oder Richtlinien einhalten, die eine uneingeschränkte Verschlüsselung vorsehen. Eine

einfache Architektur mit SSL-Verbindung direkt zum Host ermöglicht eine durchgängige Verschlüsselung, bringt jedoch alle oben genannten Nachteile mit sich: Zugriffssteuerung kann nicht am Perimeter erfolgen; Sicherheitselemente lassen sich nicht zentral verwalten, überwachen und prüfen.

Mit der Reflection-Sicherheitsarchitektur ist durchgängige Verschlüsselung ebenso möglich wie eine zentrale Verwaltung, Überwachung und Überprüfung. Diese Konfiguration lässt sich einfach mit einem Kontrollkästchen auf Client-Seite einrichten.

Reflection Security Proxy erfordert mittels sicherer Token-Autorisierung einen Nachweis über die Authentifizierung der Clients für den Zugang zum Host. Erst nach Validierung des sicheren Tokens wird dem Client gestattet, eine SSL-Verbindung bis zum Host zu öffnen.

Die entstehende SSL-Verbindung ist wirklich durchgängig; es handelt sich nicht nur um eine SSL-Verbindung vom Client zu Security Proxy und eine separate SSL-Verbindung von Security Proxy zum Host.

Mit Reflection wird dadurch erreicht, was kein anderes Produkt in der Branche parallel bietet:

- Durchgängige SSL-Verbindung mit SSL-Handshake des Clients direkt beim Zielhost
- Zentral verwaltete Zugriffssteuerung, durch die der Client den Proxy erst nach geprüfter Authentifizierung und Autorisierung überwindet

Bei dieser Konfiguration entfällt natürlich die Möglichkeit einer Inhaltsinspektion. [Anmerkung: Mit Reflection for the Web kann jedoch eine Inhaltsinspektion bei durchgängiger SSL-Verbindung durchgeführt werden. Informationen zur Einrichtung erhalten Sie beim technischen Kundendienst von Attachmate.]

### **Umfassende Plattformkompatibilität**

Reflection Management Server und Metering Server sind kompatibel mit den führenden Webservern und Anwendungsservern. Reflection for the Web wird mit Tomcat geliefert, kann jedoch auch auf IBM WebSphere, BEA WebLogic, Microsoft® IIS und anderen beliebten Serverumgebungen bereitgestellt werden. Reflection Security Proxy lässt sich auf jeder Plattform installieren, die Java unterstützt.

Auch Reflection for the Web kann auf jeder Plattform mit Java-Unterstützung installiert werden, beispielsweise Windows, Linux, Solaris, HP-UX oder z/OS.

Die Thin-Client-Emulatoren von Reflection for the Web sind auf allen Plattformen ausführbar, die Java unterstützen, etwa OS X, Linux und Windows. Alle gängigen Java-Client-Versionen werden unterstützt, beispielsweise Sun JRE 1.5 und frühere Versionen sowie Microsoft 1.1 VM.

Reflection for the Web unterstützt außerdem beliebte Webbrowser wie Internet Explorer, Mozilla, FireFox, Safari, Opera und Netscape. Um höchste Sicherheit und Plattformkompatibilität zu erreichen, wird vorhandenes Javascript unterstützt, es ist auf Endbenutzersystemen jedoch nicht erforderlich.

### **Nicht intrusive mehrstufige Sicherheit für Legacy-Host-Anwendungen**

Legacy-Host-Anwendungen wurden nicht für eine Welt mit modernen Sicherheitsarchitekturen und verbreitetem Netzwerkzugriff konzipiert. Mit Management Server und Security Proxy Server von Reflection for the Web ist es jedoch möglich, moderne mehrstufige Sicherheit auch auf klassische Green-Screen-Anwendungen auszudehnen – auf nicht intrusive Weise, ohne Veränderung an den Anwendungen oder ihren Hosts.

Die Reflection-Sicherheitsarchitektur bietet zahlreiche Vorteile:

- Vor dem Host können Sicherheitsschichten hinzugefügt werden.
- Die Sicherheitsfunktionen von Reflection sind nicht intrusiv; es ist nicht erforderlich, die Anwendungen oder Hostrechner dafür zu modifizieren.
- Für Thin- und Thick-Client-Emulatoren von Attachmate kann dieselbe Sicherheitsarchitektur verwendet werden.
- Reflection Management Server und Security Proxy sind kompatibel mit häufig verwendeten Load-Balancern, sodass für Redundanz gesorgt werden kann und Skalierung für große Bereitstellungen möglich ist.

## Informationen zu Attachmate

Attachmate hilft Unternehmen bei der Erweiterung, Verwaltung und Sicherung ihrer IT-Investitionen. Wir bieten eine große Bandbreite an Lösungen – von Terminalemulation, Legacy-Integration und PC-Lifecycle-Management bis hin zu innovativen Systemen und Sicherheitsmanagementwerkzeugen. Weltweit nutzen mehr als 65.000 Kunden unsere Technologie, um ihre IT-Anlagen auf neuartige Weise sinnvoll einzusetzen. Besuchen Sie die Website [www.attachmate.de](http://www.attachmate.de), um mehr zu erfahren.



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

**Europäische Zentrale**  
Niederlande  
TEL +31 71 368 1100  
FAX +31 71 368 1181

**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)