TEST REPORT

Tolly.

#214102

December 2014

Commissioned by
Attachmate Corporation

Attachmate® Reflection® 2014

Feature Evaluation vs. IBM Personal Communications 6.0, OpenText HostExplorer 14.0 and Rocket Software BlueZone 6.1

EXECUTIVE SUMMARY

Legacy IBM host-based applications, whether running on IBM mainframes or AS/400 minicomputers, operate on the most critical business data in enterprises. Today's user interfaces have advanced significantly since the golden age of the mainframe and it is important to take advantage of modern user-interface constructs and productivity enhancements to streamline access to critical enterprise data. Similarly, regulatory standards like PCI require secure access for connections both inside and outside the corporate network.

Attachmate Corp. commissioned Tolly to evaluate its Reflection 2014 terminal emulation solution vs. three other offerings focusing on user interface, productivity, secure access and mobile experience. The Attachmate solution delivered significant benefits in all areas evaluated in Feb. 2014. See Table 1.

...<continued on next page>

THE BOTTOM LINE

Attachmate Reflection 2014 provides:

1. A modernized user experience that enhances productivity on desktop, laptop and tablet devices
2. Superior security and protection of sensitive host data over the network and on the desktop
3. Reflection Security Gateway (RSG) (optional add-on) to secure access to host applications and centrally manage emulation desktop clients

Terminal Emulation Solutions: Feature/Function Summary

Area	Terminal Emulation Solution			
	Attachmate Reflection 2014	IBM Personal Communications 6.0	OpenText HostExplorer 14	Rocket Software BlueZone 6.1
Modern User Experience with Legacy Host Applications	**Four interface modes, multiple sessions in one instance of the application**	**One interface mode, one session per application instance**	**One interface mode, one session per application instance**	**One interface mode, one session per application instance**
Securing Access To Legacy Hosts	**FIPS 140-2 validated SSL/TLS. Info privacy support, trusted locations, User Account Control (UAC), Reflection Security Gateway for central session management, user access control and as the security proxy**	**FIPS 140-2 validated SSL/TLS. No info privacy, trusted locations or UAC support**	**FIPS 140-2 validated SSL/TLS. No info privacy, trusted locations or UAC support**	**Rocket Software not on the FIPS 140-1 and FIPS 140-2 Vendor List[2]. No info privacy, trusted locations or UAC support**
Optimizing the Mobile User Experience[2]	**TouchUx interface for Windows tablets and Citrix XenApp with iPad or Android devices**	**No specific client interface for touchscreen**	**No specific client interface for touchscreen**	**No specific client interface for touchscreen**

Notes: 1) FIPS validation was according to http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm 2) See the Mobile User Experience section for alternative solutions provided by each vendor for mobile devices.

Source: Tolly, February 2014

Table 1

© 2014 Tolly Enterprises, LLC

Executive Summary (cont.)

The rich feature set of Attachmate Reflection 2014 provides significant benefits for end-users, IT admins and those responsible for the overall security of the legacy host systems.

The Attachmate terminal emulation solution implements a wide range of user interface and productivity features that optimize the user experience on traditional PCs as well as provide support for touch screen-oriented systems like Windows 8.1 on PCs and tablets.

Behind the scenes, features like the Attachmate Customization Toolkit assist system admins in pre-deployment tasks. Finally, a robust set of features bolster front-end security to back-end mainframe systems. These include FIPS-validated cryptography, information management features, integration with Microsoft User Account Control (UAC) and more.

Attachmate Corporation

Reflection 2014

User Interface, Productivity, Security and Mobile User Features

Tested February 2014

Modern User Experience with Legacy Hosts

Area	Function	Terminal Emulation Solution Windows Client			
		Attachmate Reflection 2014	IBM Personal Communications 6.0	OpenText HostExplorer 14	Rocket Software BlueZone 6.1
Interface Modes	Classic	✔	✔	✔	✔
	Ribbon	✔	✘	✘	✘
	Browser	✔	✘	✘	✘
	Touch	✔	✘	✘	✘[1]
Multiple Session Support	Windows	✔	✔	✔	✔
	Tabs	✔	✘	✘	✘
Productivity Features	MS Office Integration	✔	✘	✔	✘
	Auto-complete	✔	✘	✘	✘
	Auto-expand	✔	✘	✘	✘
	Spell check/auto-correct	✔	✘	✘	✔
	Screen History	✔	✘	✔	✔
	Search	✔	✘	✘	✘
	Built-in Web browser	✔	✘	✘	✘
Application Integration	Microsoft .NET API Support	✔	✘	✘	✘
Enterprise Deployment Tools for IT Admins	Customization toolkit	Attachmate Customization Toolkit (ACT) for creating custom MSI configuration prior to deployment	Configuration definitions files and group policies	OpenText Tools (Sconfig tool, Profile Space Editor Management Console, Profile Publishing Wizard)	Modify setup.ini to customize options. Use MSIEXEC command to install specific components.

Notes: 1) BlueZone desktop client does not have a specific mobile touch interface. But it is able to provide the function keys (PA1, PA2, PF01, PF02, etc.) on the screen. Thus, it is usable on a touchscreen Windows device.

Source: Tolly, February 2014

Table 2

The evaluation compared current versions of terminal emulation solutions from Attachmate, IBM, OpenText and Rocket Software. While vendors also provide solutions to allow end users accessing the legacy host using Web browsers, this report focus on the Windows desktop clients. See Table 4 for details. The solutions were evaluated in three broad categories: 1) User Experience, 2) Secure Access, and 3) Mobile User Experience.

Modern User Experience

Where legacy mainframes offered a single, "green screen", interface, Windows users have long grown accustomed to having flexible and multi-faceted application interfaces. Thus, it is important to understand the options that each vendor provides for bringing modern interface elements to legacy mainframe applications. See Table 2 for all detailed results for this section of the report.

Interface Modes

Different users work differently. Thus, providing a flexible user experience typically provides a better user experience. In addition to the "classic" interface of mainframe 3270/5250 terminals, Attachmate also delivers the terminal emulation experience wrapped in the familiar "web browser"-style screen as well as the "ribbon" interface that has been standard on Microsoft Office products in recent years. Among competitors tested, none provide a browser-type experience.

Secure Access to Legacy Hosts

Function	Terminal Emulation Solution Windows Client			
	Attachmate Reflection 2014	IBM Personal Communications 6.0	OpenText HostExplorer 14	Rocket Software BlueZone 6.1
FIPS 140-2 validated SSL/TSL, SSH Cryptography	✔	✔	✔	?[1]
Information Privacy	✔	✘	✘	✘
Trusted Locations	✔	✘	✘	✘[2]
Microsoft User Account Control (UAC) Integration	✔	✘ (access control by group policies)	✘ (access control by password)	✘
Add-on Product: Central Session Management with LDAP Integration for User Access Control and Security Proxy with Authorization from the Central Session Management Application	✔ (Attachmate Reflection Security Gateway)	✘[3]	✘[3]	✘[3]

Note: 1) Attachmate, IBM and OpenText are on the list of all vendors with a validated FIPS 140-1 and FIPS 140-2 cryptographic module (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm).. Rocket Software BlueZone's datasheet mentioned "Supports security standards using state-of-the-art encryption and FIPS-certified cryptography". Rocket Software is not on the FIPS validated list. It is possible that they used third party or open source software like OpenSSL.
2) Password protected encrypted scripts to provide unauthorized modification or execution of confidential data.
3) Other vendors may provide partial functionality but not the full functionality of the Attachmate Reflection Security Gateway. See the Central Session Management: Attachmate Reflection Security Gateway (RSG) section for detail.

Source: Tolly, February 2014

Table 3

Additionally, Attachmate offers TouchUx mode designed for touch screen devices with Windows 8.1 and access via Citrix XenApp for Android and Apple iOS. The interface includes larger buttons and an optional transparent full keyboard with all function keys. IBM, OpenText, and Rocket Software BlueZone's Windows clients do not provide specific user interface for touchscreen devices.

Multiple Sessions

Sometimes, users need to access multiple hosts at the same time. Attachmate supports multiple sessions as tabs or windows in one application instance. IBM, OpenText and Rocket Software BlueZone support one session per application instance, so users will have to use multiple instances for multiple sessions.

Productivity Features

Users have come to expect native PC applications to provide productivity features like spell-check and auto-complete. Such features, however, were never native to mainframe systems. Fortunately, Attachmate's solution implements such features along with integrating Reflection with Microsoft Office thereby allowing mainframe screens to be exported to Microsoft Office documents. IBM and Rocket Software BlueZone do not provide similar support while OpenText implements a portion of these features.

Screen history and application search help users document and find previously typed or displayed information. Only Attachmate provides these features while OpenText and Rocket Software BlueZone provide only the screen history feature. IBM does not provide these two features.

Attachmate Reflection also provides a built-in Web browser which is displayed in the application so users can work with both host and web applications simultaneously. On top of this component, Attachmate's .NET API and macro capabilities (Visual Basic for Applications) allow for integration of host, web and desktop applications. This allows users to have information from host screens automatically pre-fill web forms, for example.

API Support

The user experience for corporate developers is enhanced by API support. Unlike competing solutions, Attachmate provides support for Microsoft's strategic .NET framework application programming interface (API) which allows tight integration/customization between the terminal emulation solution and the Microsoft .NET environment.

Deployment Tools

Finally, Attachmate and OpenText provide extensive GUI-based toolkits to assist system administrators in deployment tasks where other solutions require administrators to modify configuration files manually or using command lines.

Secure Access To Legacy Hosts

While legacy hosts implement access security, those hosts were almost always deployed on private networks and were not subject to the type of attacks that take place regularly today. Attachmate provides a significant set of features that enhance security external to the host. See Table 3 for all detailed results for this section of the report.

FIPS 140-2 Validated SSL/TSL, SSH

Like IBM and OpenText, Attachmate provides FIPS 140-2 validated cryptography. Rocket Software BlueZone also claims FIPS compliance but was not on the FIPS validated vendor list. See Test Methodology section for FIPS information.

Information Privacy

Attachmate provides information privacy features designed to protect sensitive information like social security and credit card numbers. For example, the sensitive information could automatically hide on the screen. This capability assist organizations to be compliant with regulatory standards like PCI-DSS and HIPAA/HITECH.

Trusted Locations

The trusted locations feature controls where host configurations, macros and other product customizations are stored. By controlling the allowed location, administrators can protect users from running dangerous macros and connecting to hosts for which they should not have access.

User Account Control

By leveraging the User Account Control (UAC) mechanism built into Windows, administrators can lock down user rights in Attachmate Reflection. By using UAC, internal support personnel can quickly access restricted functions in the product by providing their administrative credentials and diagnose and repair problems more quickly than in the other solutions reviewed.

Central Session Management: Attachmate Reflection Security Gateway (RSG)

Finally, Attachmate's unique Reflection Security Gateway (RSG) integrates with LDAP/Active Directory to allow granular session control.

For the central management server of RSG, Tolly engineers verified that it could use LDAP queries for user access control and session profile management. Administrators could assign customized sessions to LDAP user groups. Users could then log into the central management server's Web portal, login with their LDAP credentials and double click the assigned session. The Attachmate Reflection software then automatically launched with the customization. Microsoft Active Directory users were used in the tests.

For the security proxy server component of RSG, Tolly engineers verified Attachmate's patented secure token authorization which only allowed authorized users from the central management server to connect to the legacy host. Unauthorized users could not connect to the host using the proxy.

Other vendors provide partial functionality of the Attachmate RSG. For example, as a proxy server, Rocket Software's BlueZone Security Server could authenticate users using their Active Directory credentials. But it does not check the user's authorization to access the host session. Take a realistic scenario for example. Alice works in Payroll and Bob works in Customer Service. Both Alice and Bob have valid Active Directory logins. Bob is supposed to only have access to the Customer Service application on the host. With Attachmate RSG, administrators can control the session connectivity using LDAP groups, so Bob can connect to the Customer Service app but cannot connect to the Payroll app through RSG. With the BlueZone Security Server, Bob is able to connect to both apps as he has the valid credentials to pass the BlueZone Security Server. Therefore, there is risk to providing access to a broader set of users than is required. This limitation was identified from researching BlueZone's documentation but has not been verified by Tolly engineers.

Mobile User Experience

With the increasing prevalence of touch-based operating systems and tablets, mobile/touch user experience becomes more important. Typically, the on-screen keyboards provided by operating systems do not include function keys required to interact with host applications, like F1 to F12. So vendors need to provide alternative, efficient ways for the input.

Attachmate Reflection desktop client provides a specific user-interface mode called TouchUx that is optimized for tablets and Windows touch devices. This mode makes interacting with host applications much more productive than traditional user-interfaces by enlarging key buttons to press and providing a full terminal emulation keyboard that can be transparently overlaid across the terminal. A peek key allows the user to temporarily hide the keyboard to see the host application without the keyboard overlay.

To support Apple iPad and Google Android tablet environments, Citrix XenApp environment can be used to communicate with legacy host applications.

Other than the Windows client, vendors provide alternative solutions for mobile devices. Rocket Software "Rocket Mobile TE" could work between the client and the host and allow users to access the host using a Web browser with mobile friendly interface.

Test Setup & Methodology

Test Environment

All PC client testing took place using a Microsoft Windows 7 system. The Microsoft tablet test was taken using Microsoft Windows 8.1 running on an ASUS Transformer Book T100 . Apple iPad testing was run with iOS 7.

Connectivity with remote legacy (mainframe) system was via cable modem connection.

Test Methodology

Modern User Experience

Interface Modes

Engineers evaluated the availability of various methods for the user to interact with the legacy host. They are defined as follows: 1) Classic. "Green Screen" 3270-style terminal interface, 2) Ribbon. Interface that integrates the "ribbon-style" interface of recent versions of Microsoft Office programs for terminal emulation functions. 3) Browser. Terminal emulator with a browser-style, tabbed interface. 4) Touch. Specific designed interface and keyboard to work with touch-based operating system on PC or tablet/phablet (phone/tablet hybrid).

Multiple Session Support

Engineers evaluated the availability of multi-session support for emulation sessions. They are defined as follows: 1) Windows. Capability of running multiple

instances of the solution for different connections, 2) Tabs. Capability to put multiple connection sessions into tabs and switch between them.

Productivity: MS Office Integration

Engineers evaluated whether users could export the current screen and screen history to Microsoft Office documents (e.g. Word, PowerPoint, Outlook, etc.) directly from the solution under test.

Productivity: Auto-Complete

Engineers evaluated the availability of productivity tools that would reduce the keystrokes required by users as well as improve the quality of input. They are defined as follows: 1) Auto-complete. Suggest completion of word after typing a few letters, 2) Auto-expand. Automatically expand abbreviations into full words. 3) Spell-check. Monitor and correct words as is standard in word processing software.

Screen History

Engineers evaluated the capability to capture prior host screens and review information seen earlier.

Search

Engineers evaluated the search function in the solution to search words in the current screen, screen history, configuration settings or Internet.

Application Integration: Microsoft .NET API Support

Engineers researched the availability of product support for the Microsoft .NET application programming interface. (Note: Some products offered support for other, older interfaces but that was beyond the scope of this study.)

Deployment Tools

Engineers evaluated the availability of tools provided by solution vendors that would help system administrators customize the terminal emulation solution and roll it out to groups of users.

Secure Access To Legacy Hosts

FIPS 140-2 Validated SSL/TSL, SSH

Engineers researched whether the solution had been FIPS validated. Tolly did not provide validation but referred to public US government information[1].

Information Privacy

Engineers evaluated the availability of information privacy features such as whether the solution could automatically

Solutions Under Test

Attachmate Reflection 2014	R1 (15.6.636.0)
Attachmate Reflection Security Gateway 2014 (Central management server, proxy server)	R1 (12.0.166)
IBM Personal Communications	Version 6.0.8 for Windows 20130811 S
OpenText HostExplorer for Win32	14.0.0.354
Rocket Software BlueZone	6.1

Source: Tolly, February 2014 Table 4

[1] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

hide Social Security numbers, credit card numbers, etc.

Trusted Locations

Engineers evaluated the availability of defining trusted locations. By this, it is meant the solution can only access files (e.g. saved sessions, macros, etc.) in specific folders.

User Account Control

Engineers evaluated whether the solution implemented the Microsoft User Account Control (UAC) feature. So when a user tries to access restricted functions, administrators could easily use the UAC pop up to grant the access.

Central Session Management: Attachmate Reflection Security Gateway

Engineers evaluated the features and functions available in the Attachmate Reflection Security Gateway (RSG) which is an add-on product to Attachmate Reflection. Specifically, the central management server and the security proxy server components in RSG were evaluated.

Tolly notes that other vendors may also offer some of the functions found in the Attachmate management offering.

Mobile User Experience

Touch Screen Device User Experience

Engineers evaluated whether the solution provides specific designed interface and keyboard to work with touch screen devices like iPad, Android tablets and Windows 8 tablets (may need Citrix Receiver to work on iOS and Android devices). The default on-screen keyboards on these devices do not provide function (or "attention identifier - AID") keys like F1 to F12. So the solution should provide such keys to work with legacy hosts.

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 25 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at: http://www.tolly.com

Interaction with Competitors

In accordance with Tolly's Fair Testing Charter, Tolly personnel invited representatives from the competing vendors to participate in the project. Rocket Software declined and OpenText responded. Tolly provided the test plan but received no feedback. After testing, Tolly provided OpenText its results but received no comments by the original publication date of March 2014 as Tolly document #214102.

For more information on the Tolly Fair Testing Charter, visit:

http://www.tolly.com/FTC.aspx

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

214154 bu-6 wt--2014-11-18-VerB