Modern Evidence Collection

SOLVING THE CHALLENGE OF DATA COLLECTION IN A WORK FROM HOME WORLD

F-Response is a Registered Trademark of Agile Risk Management LLC. For more information on F-Response, or any of part of the solution presented in this paper please contact us on the web at www.f-response.com.

June 20, 2023

Table of Contents

Table of Contents 2
The Challenge 3
The Solutions 4
F-Response Product Options 5
How F-Response Classic (Enterprise, Consultant + Covert, Consultant) works: 7
How F-Response Universal works: 8
How F-Response Collect Works: 9
Demonstration 10
Contact Us 11
Legal Notices 12

The Challenge

The COVID19 pandemic changed the way we work completely. While some organizations are trying to return to a fully staffed office, most are accepting the fact that Work from Home ("WFH") is going to be a part of all operating strategies going forward. For forensics, incident response, and e-discovery professionals, this presents a new challenge, acquiring data from employees regardless of their present location, both on and off the Virtual Private Network ("VPN"). This includes:

Cloud Workspaces

Many organizations have transitioned to cloud services for collaboration and office document management. Tools like Office365 and Google Workspaces have become ubiquitous, and as such, employees rarely need to connect to a VPN to access, create, and manage organizational documents.

Mobile Workforce

Even with a VPN, employees are often in remote locations competing for bandwidth with other members of the family or on shared WIFI. This leads to higher latency connections and slower response times, as well as instability of network operation.

Temporal Variations

Employees are spread further than ever before. Time zones don't line up nearly as clean as they used to, making finding, and accessing their data sources for collection, especially a covert collection, exceedingly difficult.

The Solutions

F-Response offers several software solutions for accessing and collecting data from remote machines.

Scenario #1

If your remote subject machine(s) are ONLY accessible via VPN, on fast, low latency connections, and your primary use case is ad hoc interactive investigating:

> Use F-Response "Classic," Enterprise, Consultant + Covert, or Consultant Edition

Scenario #2

If your remote subject machine(s) are on or off the VPN, on fast, low latency connections, and your primary use case is ad hoc interactive investigating:

> Use F-Response Universal

Scenario #3

If your remote subject machine(s) are on or off the VPN, on potentially unstable or high latency connections, and your primary use case is image/data collection with automatic resumption: (Imaging/Collecting without interaction)

> Use F-Response Collect

F-Response Product Options

The following further breaks down the F-Response software options highlighted prior:

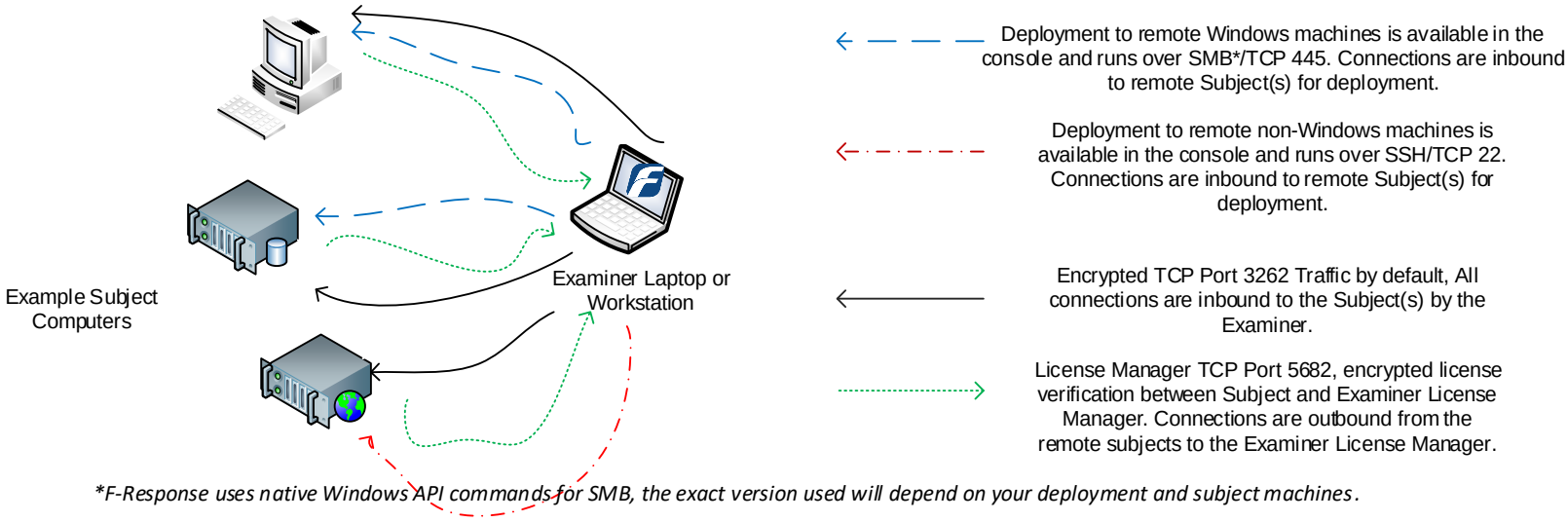
	F-Response Classic (Enterprise, Consultant + Covert, Consultant)	F-Response Universal	F-Response Collect
Networking	• Works best in a LAN/WAN[1] (requires fast, low latency network for optimal performance) • Requires direct access to the remote machine.	• Works best in a LAN/WAN[1] (requires fast, low latency network for optimal performance) • Requires remote subject machine(s) to access Universal Server directly.	• Works in ALL network configurations (LAN/WAN/VPN/Internet)[2]. • Requires remote subject machine(s) to access Collect Server directly.
Features	• Interactive access to the remote subject machine(s) disks, volumes, and memory. (Windows only) • A simple imaging option is available. • Compatible with 3rd Party Imaging/Analysis tools	• Interactive access to the remote subject machine(s) disks, volumes, and memory (Windows only) • A simple imaging option is available. • Compatible with 3rd Party Imaging/Analysis tools	• Offers collection (imaging) of remote targets, including disks, volumes, memory (Windows), files, folders, MFTS, custom content. • **Automatic Resumption** • No interaction
Licensing	• 1 or 3-years options • Dongle-Based	• 1 or 3-year options. • Server-based (downloadable software)	• 1 or 3-year options. • Server-based (downloadable software)

[1]Can also be used over the internet provided there is a VPN in place and the remote subject machine(s) are accessible via TCP/IP.

[2] Server must be accessible via TCP/IP using standard HTTPS protocols.

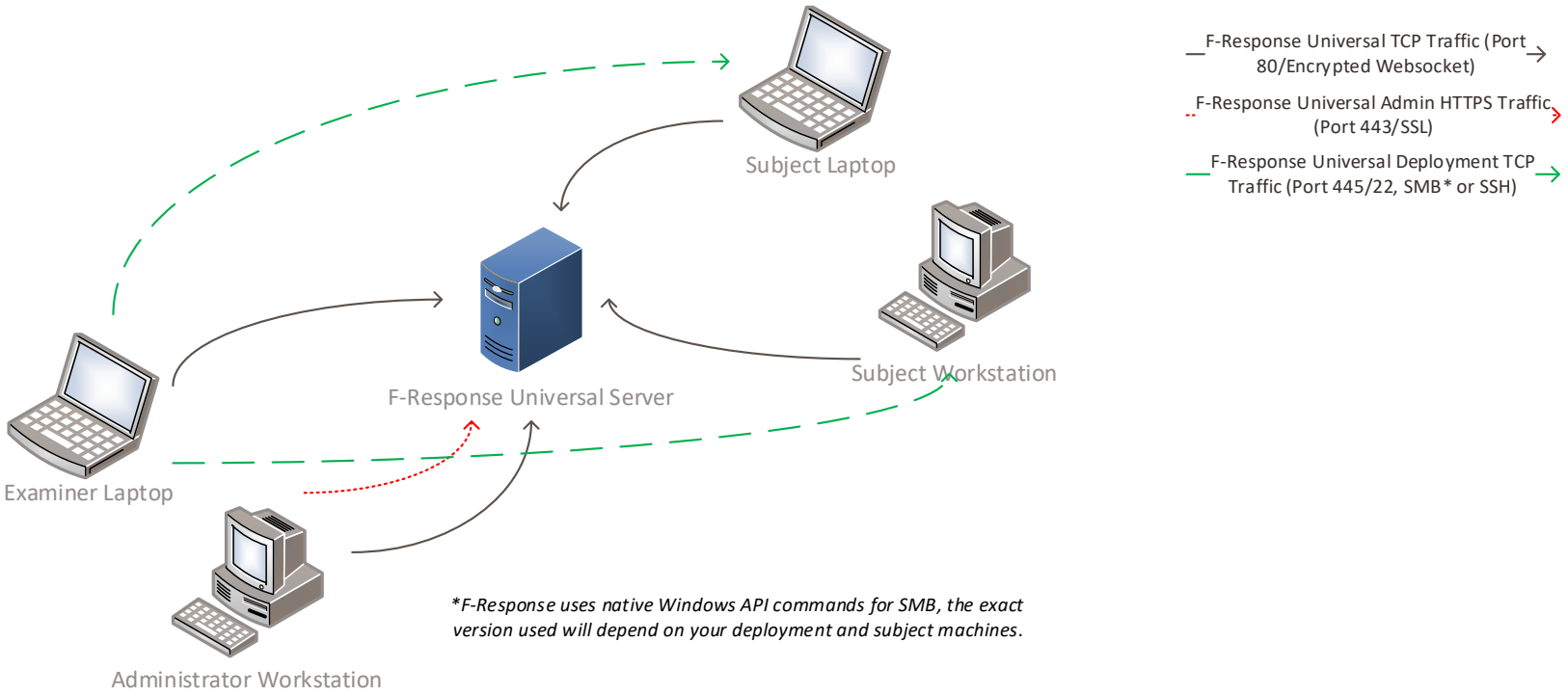
Notes	• Requires hardware license dongle on the examiner's machine.	• Server must be able to access license.f-response.com.	• Server must be able to access license.f-response.com.
PLATFORMS:	F-Response Classic (Enterprise, Consultant + Covert, Consultant)	F-Response Universal	F-Response Collect
Windows	• Windows (XP to present, 32 and 64 bit.) • Provides access to disks, volumes, and physical memory.	• Windows (XP to present, 32 and 64 bit.) • Provides access to disks, volumes, and physical memory.	• Windows (XP to present, 32 and 64 bit.) • Provides collection of disks, volumes, physical memory, MFTs, Profiles, and custom content images.
Linux	• All modern versions of Linux on x86 and x64. • Provides access to disks and volumes, as well as files and folders via SSH/SFTP.	• All modern versions of Linux on x86 and x64. • Provides access to disks and volumes, as well as files and folders via SSH/SFTP.	• All modern versions of Linux on x86 and x64. • Provides collection of disks and volumes, as well as home directories and custom content images.
Apple OSX	• Access to files and folders via SSH/SFTP.	• Access to files and folders via SSH/SFTP.	• Supports modern Apple OSX (ARM and Intel). • Provides collection of home directories and custom content images.
Solaris & AIX	• Access to disks and volumes.	• Not supported.	• Not Supported.

How F-Response Classic (Enterprise, Consultant + Covert, Consultant) works:

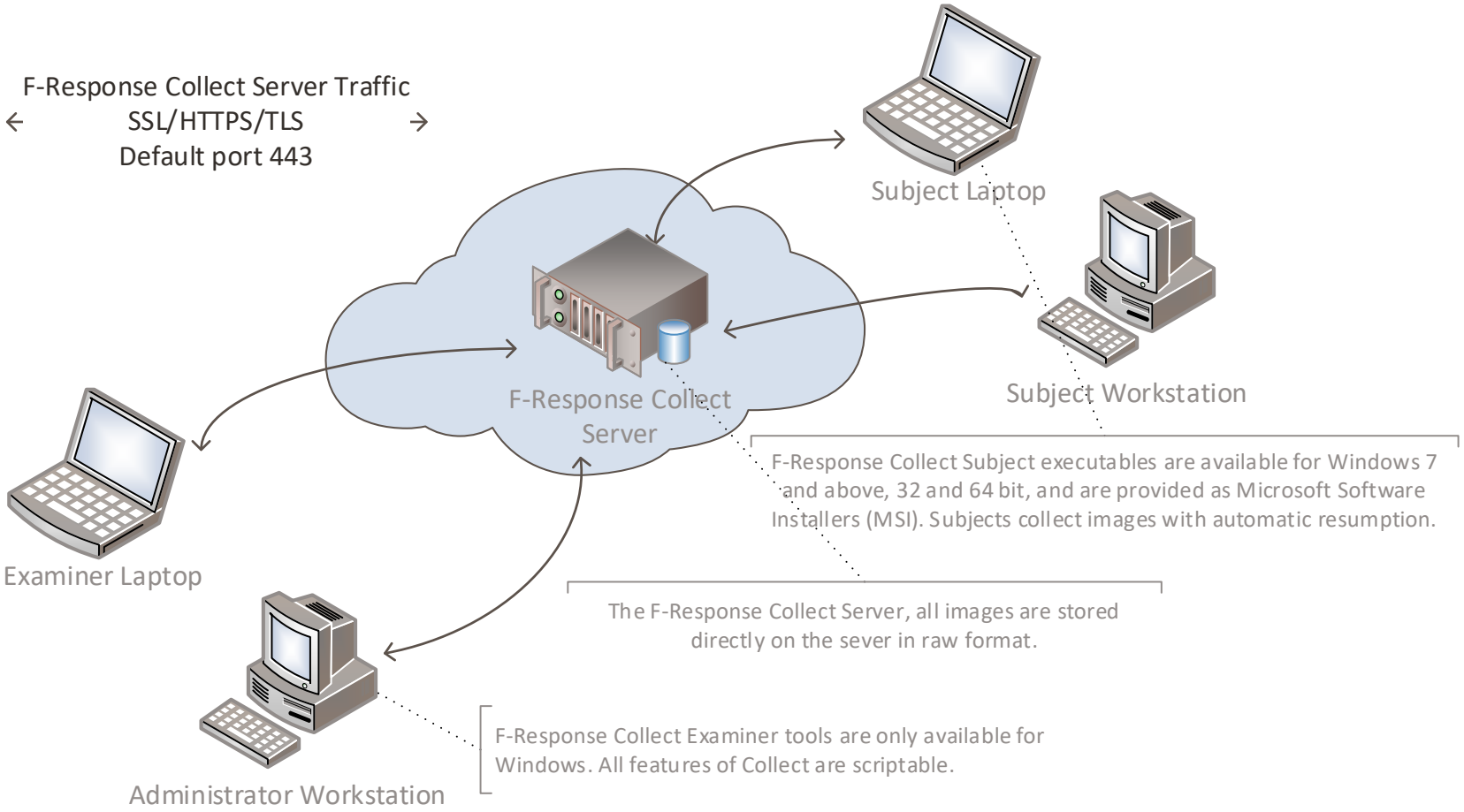


**F-Response uses native Windows API commands for SMB, the exact version used will depend on your deployment and subject machines.*

How F-Response Universal works:



How F-Response Collect Works:



Demonstration

F-Response offers several solutions to meet the challenge of data collection in a Work from Home ("WFH") world. We would be happy to provide a demonstration of any of them at your convenience. In that demo, you'll learn:

How F-Response works

We will walk you through the process top to bottom, explaining F-Response software, the solutions, and help zero in on what works for you.

How F-Response products are licensed

We will walk through the licensing model so there are no surprises. Explain renewals and the like, as well as go over what you get when you become an F-Response customer.

How F-Response can find the best path forward

The "Work from Home" world is challenging. It breaks a lot of standard conventions and requires some more flexible thinking. We've been in the business of remote forensics for over a decade. We know how to navigate these new challenges and can give you a cost-effective way to do just that.

Contact Us

Feel free to reach out and ask questions or schedule a live demonstration of any of the F-Response products mentioned in this document.

F-Response

Email: sales@f-response.com

Phone: 1-800-317-5497

Website: https://www.f-response.com/contact/contact-us

Legal Notices

Copyright

Copyright © 2023 Agile Risk Management, LLC DBA F-Response. All rights reserved. This document is protected by copyright with all rights reserved.

Trademarks

F-Response is a trademark of Agile Risk Management, LLC DBA F-Response. All other product names or logos mentioned herein are used for identification purposes only and are the trademarks of their respective owners.

Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners.

Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.