RSA[®] ARCHER[®] GRC Platform Implementation Guide

Digital Defense Frontline VM 6.0

Jeffrey Carlson, RSA Partner Engineering Last Modified: October 16th, 2017





Solution Summary

Digital Defense's Frontline Vulnerability Manager[™] (Frontline VM) is the industry's most comprehensive, accurate, and easy to use vulnerability management software. Backed by security research expertise (DDI VRT[™]), and a highly intuitive user interface touted by customers as simple, insightful, and immediately actionable, Frontline VM delivers unparalleled excellence from deep, accurate network and host assessments all the way to intelligent integration with SIEMs and security workflow management systems. Together, Frontline RNA[™] and Frontline VM yield the industry's lowest false positive rate – critical to effective vulnerability discovery, productive remediation guidance, and ultimately, true cyber risk reduction.

The Digital Defense Frontline VM integration with RSA Archer allows you to combine the power of Frontline's device discovery and vulnerability detection with RSA's Vulnerability Management features to view your devices and their vulnerabilities in the context of the business risk they pose to your organization.

Partner Integration Overview	
RSA Archer Solution	IT Security Vulnerabilities Program
RSA Archer Use Case	IT Security Risk Management
RSA Archer Applications	Vulnerability Scan Results, Devices
Uses Custom Application	No
Requires On-Demand License	No





Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Digital Defense Frontline VM with the RSA Archer GRC Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Digital Defense Frontline VM Configuration

By integrating Digital Defense Frontline VM with RSA Archer, organizations can derive the following benefits:

• Complete an accurate detailed analysis of devices on network via integration

The end user will be able to take advantage of Digital Defense's scan-to-scan host correlation combined with the functionality of the RSA products. Digital Defense's scan-to-scan host correlation ensures that RSA products receive the most accurate and up-to-date information about hosts that have been scanned, allowing the user to make better, more informed decisions when coupled with information presented by the McAfee products.

Digital Defense's scan to scan host correlation identifies over 25 host characteristics that also include applications that are installed on the host, which helps our mutual customers insure that their host security investments are protecting the environment and data.

• Deliver an effective path to remediation

Effectively improve risk posture, remediation efforts identified and prioritized help plan remediation thru recommendations with rule based policies within RSA Archer.

• Communicate, collaborate and transform

Ever changing breach landscape, counter measures can be deployed based on risk evaluation information contextualized by Frontline and integrated within RSA Archer.

Before integrating Frontline VM with RSA Archer it is first necessary to generate an API key. Perform the steps below to do so.



Generate Frontline VM API Key

The following instructions describe how to generate an API key to access Frontline VM data.

To generate a **Frontline VM** API key:

- 1. Log in to Frontline VM.
- 2. In the site header, select your name and choose **My profile**.
- 3. On the API Tokens tab, select Create new token.
- 4. In the **Add New Token** dialog, type the token name (it can be whatever you like) and select **OK**.
- 5. Your token is created.

Below your token name, **Click to show key** displays your API key, which you need to integrate Frontline VM with RSA Archer.

Service Reminder	×
Protect your token. Do not share your token with other application integrations or users.	
API Key will appear in this box	
0	Dk

Note: An API key is equivalent to a user's password. Do not use a key with more than one product integration. If you believe a key is compromised, delete the token from Frontline VM immediately by selecting and the resulting checkmark to confirm.



RSA Archer GRC Configuration

Configuring the Devices Application

Before importing the necessary data feeds for importing vulnerability information, it is first necessary to make a number of changes to the existing Devices application within Archer. To add the **DDI Device ID** field to the **Devices** application perform the following steps:

- 1. Click the down arrow next to the tools icon in the menu bar.
- 2. In the Application Builder section, choose Applications:



- 3. Choose the **Devices** application name from the list.
- 4. Click on the **Fields** tab next to **General.**
- 5. Click on the **Add New** link in the upper right of the **fields** table:

Manage Application: Devices							X
Save Apply Delete							🖂 Email
General Fields Layouts	Navigation Menu	Workflow	Advanced Wor	kflow Calculation	ns Adminis	tration	
▼ Fields						Add New	1
Drag a column name here to group the	items by the values with	in that column.					
Name 🛦	Field Type	Access	Active ▼	Last Updated	Updated By	Actions	
# Server Drives	Numeric	Public	~	12/22/2016 9:22 AM	Archer, Eric	1	
% of Non-Compliance	Numeric (Calculated)	Private	~	12/22/2016 9:22 AM	Archer, Eric	D 🗊	
Activated Plans	Related Records	Public	~	12/22/2016 9:27 AM	Archer, Eric	2	
Alternate Administrator(s)	Cross-Reference	Public	~	12/22/2016 9:27 AM	Archer, Eric	🖻 🗊	
Antivirus Signatures	Sub-Form	Public	~	12/22/2016 9:27 AM	Archer, Eric	🖻 🗊	
Applications	Cross-Reference	Public	~	12/22/2016 9:27 AM	Archer, Eric	1	

- 6. Choose the **Create a new Field from scratch** radio button.
- 7. Choose the **Text** field type. Click **OK**.
- 8. Enter **DDI Device ID** for the name. Complete any other fields required by your organization.
- 9. Click **Save** above the **General** tab.



Configuring the Vulnerability Scan Results Application

Before importing the necessary data feeds for importing vulnerability information, it is first necessary to make a number of changes to the existing Devices application within Archer. To add the **DDI Vuln Instance ID** field to the **Vulnerability Scan Results** application perform the following steps:

- 1. Click the down arrow next to the tools icon in the menu bar.
- 2. In the Application Builder section, choose Applications:



- 3. Choose the Vulnerability Scan Results application name from the list.
- 4. Click on the **Fields** tab next to **General.**
- 5. Click on the **Add New** link in the upper right of the **fields** table:
- 6. Choose the **Create a new Field from scratch** radio button.
- 7. Choose the **Text** field type. Click **OK**.
- 8. Enter **DDI Vuln Instance ID** for the name. Complete any other fields required by your organization.
- 9. Click **Save** above the **General** tab.

As part of the integration it is also necessary to mark the **Security Analyst** field as **not required** in order for the Data Feed to run without errors. To do this, perform the following steps:

- 1. Follow steps 1-4 above
- 2. Click on the **Security Analyst** field in the fields table.
- 3. Choose the **Options** tab. In the **Options** section of the page, **uncheck** the box next to **Required Field**.



Manage Field: Securi	ity Analyst	X	
Save Apply Delete		M Email	
General Options	Help Text Access		
▼ Display Control			
Control:	O Dropdown A dropdown list that allows only one selection.	1	
	Radio Buttons A group of radio buttons that allows only one selection. States: Values		
	Check A group of checkboxes that allow either single or multiple selections.	1	
	Listbox A listbox that allows either single or multiple selections.		
	Values Popup A control that allows either single or multiple selections.		
▼ Options			
Required Field:	quired Field: Require users to supply a value for this field before saving the record.		
Auditing Information:	ing Information: Display auditing (last modification) data next to this field. Include user name, date and time of last edit.		
Search Results:	Search Results: V Display this field in advanced search and search results.		

4. Click Save above the General tab.

Importing and Configuring the Frontline VM Devices Data Feed

Digital Defense Device records are created in RSA Archer via a preconfigured Data Feed. This Data Feed loads the host information from an XML file that is pulled from the Digital Defense APIs using a customer-specific API key. To configure the Data Feed, perform the following steps:

1. On your RSA Archer Server, browse to Administration -> Integration -> Data Feeds:

Integration				
Data Feeds				
Data Publica	tions			
Data Imports	Data Feeds			
Review Job Queues				
Obtain API Resources				
Management Reporting				
Master Reports Listing				

- 2. Select **Import** and browse to the Data Feed file (Digital_Defense_Frontline_VM_Devices.dfx5).
- 3. Click on the **Transport** tab.
- 4. In the **Data Request Properties** section, locate the Header Parameter **X-API-Token**. Replace the Xs in the **Value** field with your Frontline VM API Token.

Data Request Properties				
Configure the HTTP site to connect to retrieve the data source. Include any header parameters that are required.				
* Data Request URI:	st URI: https://frontline.cloud/customApi/archer/hosts/			
Header Parameters:	Key	Value		
	X-API-Token	x0000000000000000000000000000000000000		





- 5. Click **Save** above the **General** tab. Review the mappings on the **Data Map** tap if needed.
- 6. Set a schedule for the feed by clicking the **Schedule** tab. The Frontline VM Devices feed should be scheduled to run and complete **before** the Frontline VM Vulnerabilities feed.

Importing and Configuring the Frontline VM Vulnerabilities Data Feed

Digital Defense Frontline VM Vulnerability records are created in RSA Archer via a preconfigured Data Feed. It will also create the appropriate cross references to existing device records as needed. This Data Feed loads the vulnerability information from an XML file that is pulled from the Digital Defense APIs using a customer-specific API key. To configure the Data Feed, perform the following steps:

1. On your RSA Archer Server, browse to Administration -> Integration -> Data Feeds:

Integration				
Data Feeds				
Data Publicat	tions			
Data Imports	Data Feeds			
Review Job Queues				
Obtain API Resources				
Management Reporting				
Master Reports Listing				

- Select Import and browse to the Data Feed file (Digital_Defense_Frontline_VM_Vulnerabilities.dfx5).
- 3. Click on the **Transport** tab.
- 4. In the **Data Request Properties** section, locate the Header Parameter **X-API-Token**. Replace the Xs in the **Value** field with your Frontline VM API Token.

▼ Data Request Properties				
Configure the HTTP site to connect to retrie	ve the data source. Include any header parameters that are required.			
* Data Request URI:	Data Request URI: https://frontline.cloud/customApi/archer/vulnerabilities/?minLevel=High			
Header Parameters:	Кеу	Value		
	X-API-Token	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		

- 5. Click **Save** above the **General** tab. Review the mappings on the **Data Map** tap if needed.
- 6. Set a schedule for the feed by clicking the **Schedule** tab. The Frontline VM Vulnerabilities feed should be scheduled to run **after** the Frontline VM Devices feed.



Using Frontline VM with RSA Archer

The integration of Digital Defense Frontline VM with RSA Archer IT Security Risk Management enables customers to have a complete analysis of digital asset within their environment an accurate view of the risks. Organizations can proactively identify, track status and manage the repair of critical vulnerabilities.

Audit Management 👻	🍰 Executive Dashboard 🔻	SHOW ALL		۹	· * -	👤 Sys	tem 🔻 (
can-05571 Vulnerability Sca	n Results						8
🖥 NEW 🗋 COPY 📄 SAVE 🖉 I	DIT 🗓 DELETE 🛛	Record 1 of 1	តំំំ RELATED	RECALCULATE	EXPORT	🖶 PRINT	🖾 EMAIL
► ABOUT	First Published: 10/16/201	7 2:19 PM Last Updated: 1	0/16/2017 2:20 PM				
▼ GENERAL INFORMATION							- 1
Scan Result ID: Scan-0557	I		Status:				- 1
Source: Frontline \	M	ŀ	ssue Status:				
Device Name: Srv2012St	Web.qa.targetfarm-2.ddi 6772708	Add Secu	rity Analyst:				
IP Address: 172.20.97.	25	NetBIOS	Hostname: Srv20	12StdWeb.qa.targetfa	arm-2.ddi		
DNS Hostname:		Po	ort Number: 65536	i/tcp			
Operating System:		Bu	isiness Unit:				
Date First Found: 4/19/2017		Date	Last Found: 4/19/2	2017			
Response Type:		Vulner	ability Scan:				
Scan Results Remediation	n						
VULNERABILITY SCAN INFORMA	lion						
Vulnerability ID:		Devic	e Criticality: Not Ra	ted			
CVE ID: CVE-2015-	:478		Severity:				
Category:			BugTraq ID:				
CVSS Base Score: 7.2		CVSS Tem	poral Score:				
Title: MS15-119:	Security Update for Winsock to Address E	levation of Privilege					
Description: The remot could allow privileged Windows : Server 200 core instal	: Windows host is affected by a 'Elevation an attacker with unprivileged access to th ser Microsoft has rated this flaw 'Importa 0 - Windows 10 Version 1511 - Windows 7 8 R2 - Windows Server 2012 - Windows Se ation) - Windows Vista - Windows Vista x6	of Privilege' flaw which ne affected component ont' and released a fix fo - Windows 8 - Windows rver 2012 (Server Core i 4 Edition	could compromise to leverage input v r this in Microsoft : 8.1 - Windows RT nstallation) - Windo	it's security posture. alidation flaws to upg Security Bulletin 'MS1 - Windows RT 8.1 - W ows Server 2012 R2 -	The vulnerabil grade their priv 15-119', Affecte indows Server Windows Serve	lity in questic vileges to tha ed Products A 2008 - Windo er 2012 R2 (s	on tofa Are:- ows erver

Having the ability to know and report what devices are on your network and how they are vulnerable allows organizations to manage business critical hosts. With the consolidated view, the individual risks can be mapped to multiple hosts, and in addition knowing what vulnerabilities are found within each hosts.



🖍 🗐 Audit Management 👻	Executive Dashboard 🔻 🚦 SH	IOW ALL	۹	≪ -	👤 System	•	7
Srv2012StdWeb.qa.targ	etfarm-2.ddi_6772708	Devices				(×
🖥 NEW 🔁 COPY 📄 SAVE 🗡 EDIT	T DELETE	ភ្នំ RELATED		EXPORT	🖶 PRINT 🖾	EMAII	L
-▼ VULNERABILITY ASSESSMENT SUMMA	RY						•
Number of High Risk 0 Vulnerabilities:		Scan-Based Risk Rating:					
VULNERABILITY SCAN RESULTS					Add New	_	
Scan Result ID	Title	Category	Severity	•			
<u>Scan-05454</u>	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure						
<u>Scan-05571</u>	MS15-119: Security Update for Winsock to Address Elevation of Privilege			_			
<u>Scan-05599</u>	MS15-120: Security Update for IPSec to Address Denial of Service						
<u>Scan-05717</u>	MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service			_			
<u>Scan-05776</u>	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass						
► HISTORY LOG						_	
► ATTACHMENTS						_	
							Ŧ
RSA Archer GRC Version 6.2 P1						Ú.	

This many to many relationship gives the RSA Archer Platform an entire vulnerability lifecycle – by providing complete and accurate information for remediation and verification.



Certification Environment for RSA Archer GRC

Date Tested: October 11th, 2017

Certification Environment					
Product Name Version Information Operating System					
RSA Archer GRC	6.2	Virtual Appliance			
Digital Defense Frontline VM	6.0	SaaS			