RSA® ARCHER® SUITE
Integration Guide

Digital Defense Frontline VM 6.0 - RSA Archer Integration 6.6

Internal Use - Confidential

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:https://community.rsa.com/community/rsa-customer-support.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and Dell are either registered trademarks or trademarks of Dell Corporation ("Dell") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go towww.emc.com/legal/emc-corporation-trademarks.htm.

License agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on RSA.com. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

For secure sites, Dell recommends that the software be installed onto encrypted storage for secure operations.

For customers in high security zones, Dell recommends that a full application sanitization and reinstallation from backup occur when sensitive or classified information is spilled.

Note on Section 508 Compliance

The RSA Archer® Suite is built on web technologies which can be used with assistive technologies, such as screen readers, magnifiers, and contrast tools. While these tools are not yet fully supported, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for RSA Archer.

The RSA Archer Mobile App can be used with assistive technologies built into iOS. While there remain some gaps in support, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for the RSA Archer Mobile App.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. Use of the software described herein does not ensure compliance with any laws, rules, or regulations, including privacy laws that apply to RSA's customer's businesses. Use of this software should not be a substitute for consultation with professional advisors, including legal advisors. No contractual obligations are formed by publication of these documents.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright 2010-2019 Dell, Inc. or its subsidiaries. All Rights Reserved.
September 2019

Internal Use - Confidential

Table of Contents

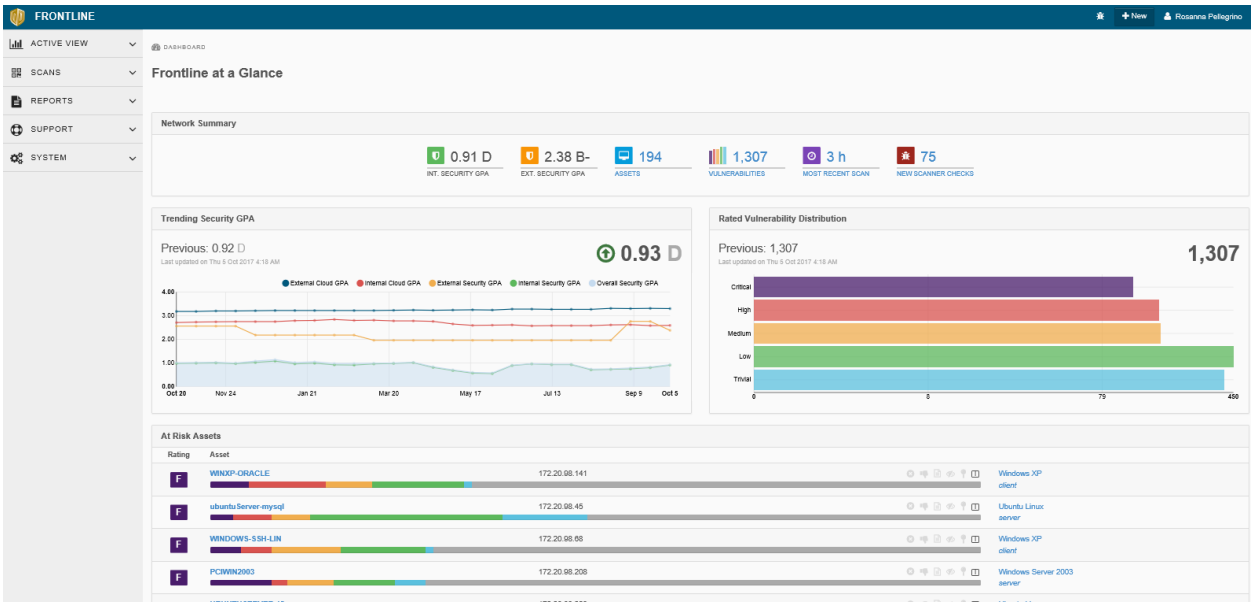
Internal Use - Confidential

Chapter 1: Overview of Digital Defense

About Digital Defense

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.



Key Features and Benefits

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.

Internal Use - Confidential

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.

Requirements

Components	Requirement
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

Prerequisites (ODA and system requirements)

Components	Recommended Software
Operating System	Windows Server 2012 R2 or 2016 Standard or Datacenter editions.
Database Server	Microsoft SQL Server 2016 SP 1 (64-bit) or 2016 Enterprise Edition (64-bit) or 2017 (64-bit) or greater Note: SQL Express is not supported
Services Server	Java Runtime Environment (JRE) 8 (64-bit)
RSA Archer	RSA Archer 6.6 and later
Pre-Requisite Applications	N/A

Internal Use - Confidential

Chapter 2: Configure Digital Defense

This section provides instructions for configuring the [Partner Product] with the RSA Archer 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 [Partner Product] 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.

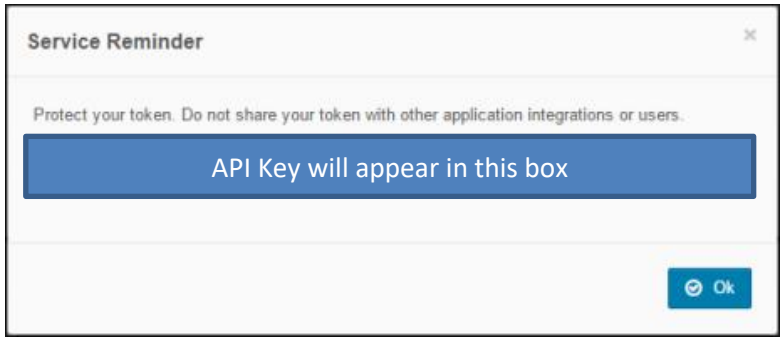
Configure Digital Defense

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

Task 1: Generate 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.



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.*

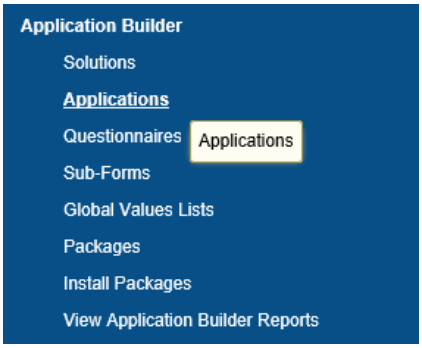
Internal Use - Confidential

Configure RSA Archer

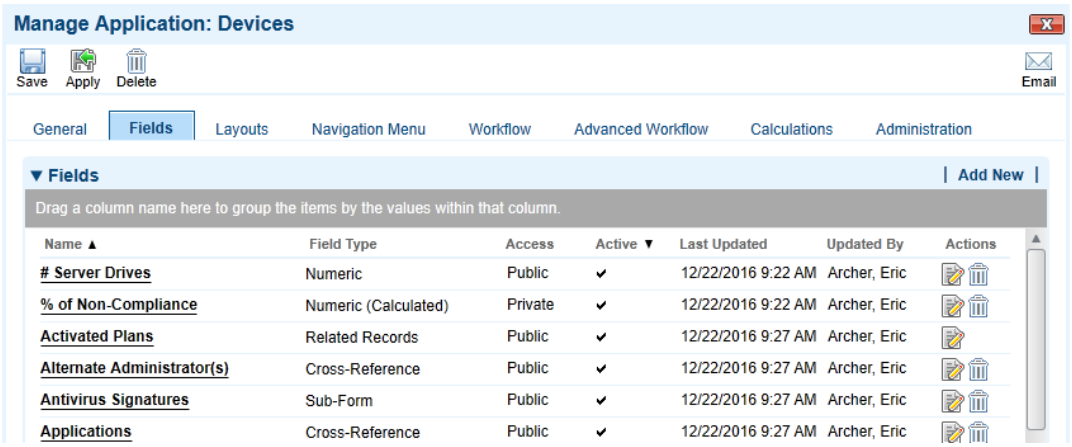
Task 1: Configuring the Devices Application

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 tool's 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:



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.

Internal Use - Confidential

Task 2: Configuring the Vulnerability Scan Results Application

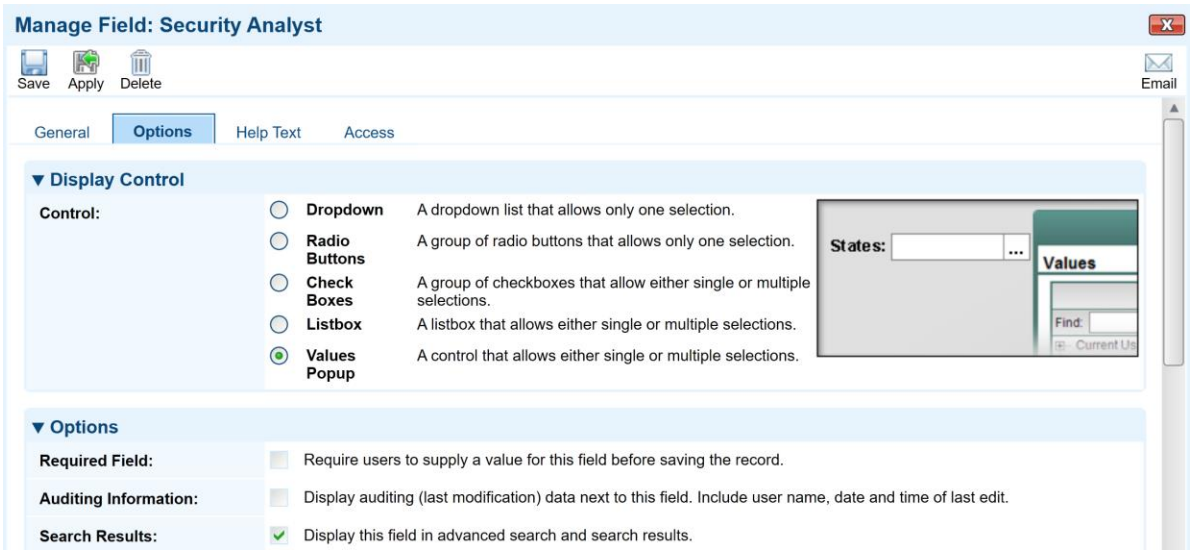
Before importing the necessary data feeds for importing vulnerability information, it is first necessary to make a number of changes to the existing Devices application within Archer. To add the **DDI Vuln Instance ID, Source, and Status** field to the **Vulnerability Scan Results** application perform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

1. Click the down arrow next to the tool's 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.

Task 3: Mark the Vulnerability Analyst field as not required

As part of the integration it is also necessary to mark the **Vulnerability 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 **Vulnerability 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**.



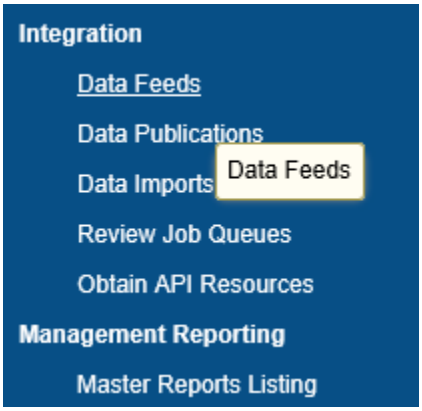
4. Click **Save** above the **General** tab.

Internal Use - Confidential

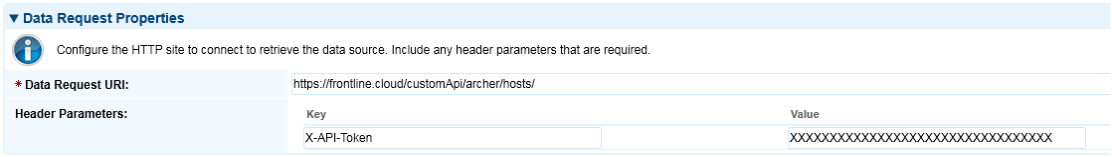
Task 4: Importing and Configuring the Frontline VM Devices Data Feed

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:**



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.



5. Click **Save** above the **General** tab. Review the mappings on the **Data Map** tap if needed, the key field definition should be **DDI Device ID.**
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.

Task 5: Importing and Configuring the Frontline VM Vulnerabilities Data Feed

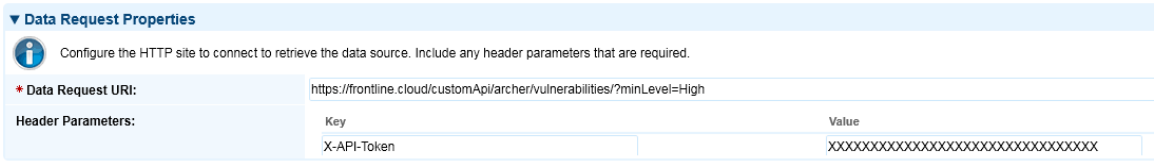
Digital Defense Frontline VM Vulnerability records are created in RSA Archer via a preconfigured Data Feed. It will also create the appropriate cross references to existing device records as needed. This Data Feed loads the vulnerability information from an XML file that is pulled from the Digital Defense 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:**

2. Select **Import** and browse to the Data Feed file (Digital_Defense_Frontline_VM_Vulnerabilities.dfx5).
3. Click on the **Transport** tab.

Internal Use - Confidential

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.

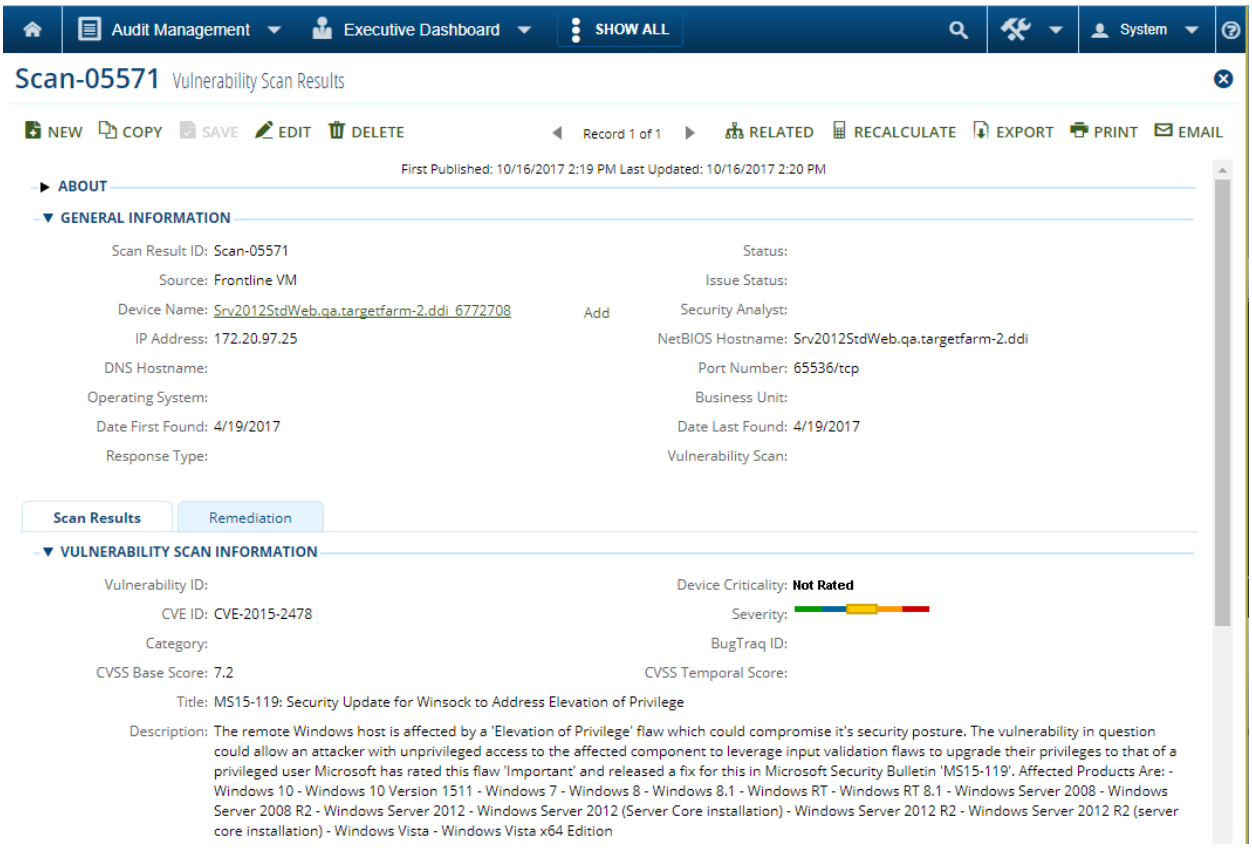


5. Click **Save** above the **General** tab. Review the mappings on the **Data Map** tap if needed.
6. Set a schedule for the feed by clicking the **Schedule** tab. The Frontline VM Vulnerabilities feed should be scheduled to run **after** the Frontline VM Devices feed.

Chapter 3: Using the Digital Defense Integration

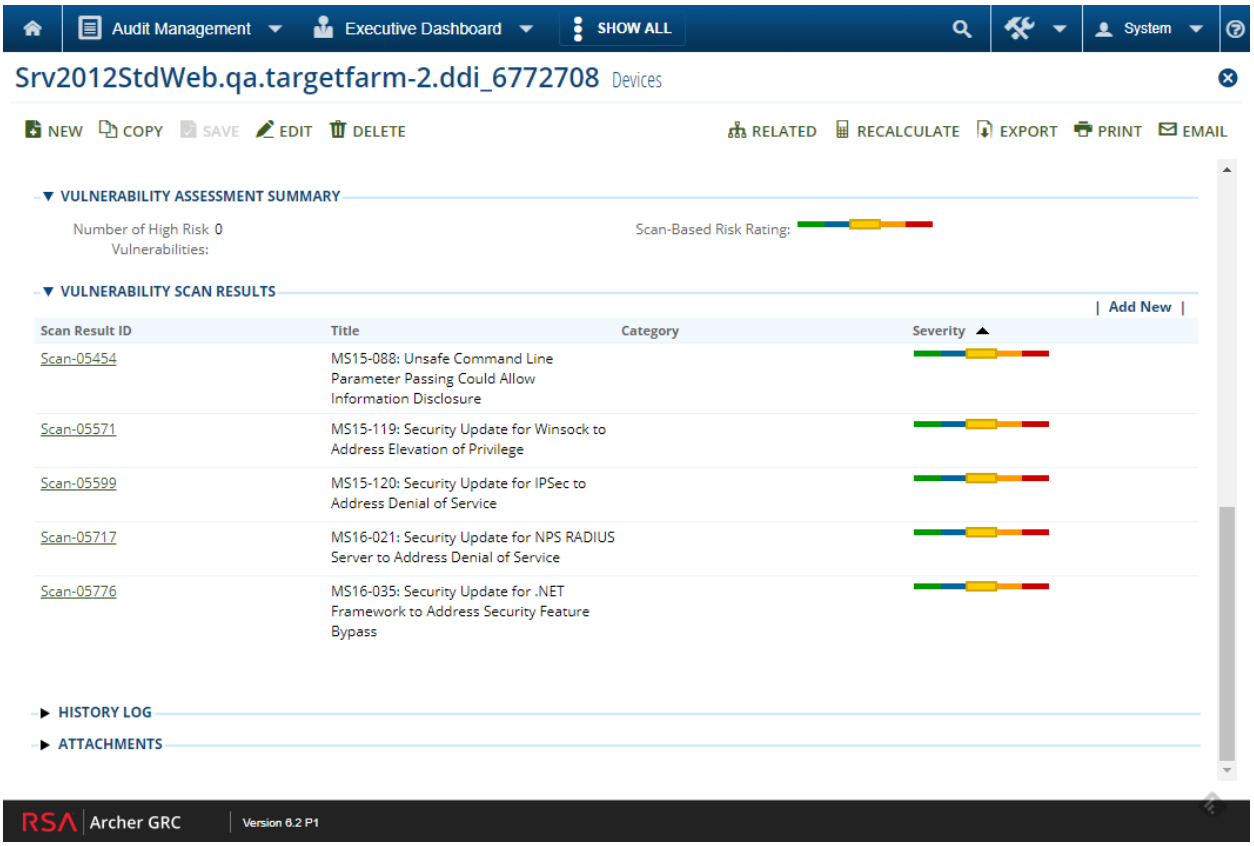
Task 1: Using Frontline VM with RSA Archer

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.



Internal Use - Confidential

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 host.



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

Internal Use - Confidential

Appendix A: Certification Environment

Date Tested: September 23, 2019

Product Name	Version Information	Operating System
RSA Archer	6.6	Windows
[Partner Product]	6.0	SaaS

Internal Use - Confidential