digitaldefense
by HelpSystems

TECHNOLOGY RSA READY PARTNER

SOLUTION BRIEF *(Cybersecurity)*

Digital Defense Frontline Vulnerability Manager™ and RSA Archer® Suite deliver Vulnerability data that is Accurate and Complete for Risk Management

The integrated solution combines the power of Frontline Vulnerability Manager (Frontline VM™) device discovery and vulnerability detection with RSA Archer Risk Management features to view devices and vulnerability in the context of the business risk they pose.

What is Digital Defense Frontline VM Platform?

Built entirely as a SaaS platform, a fully functional GUI can be accessed whenever or wherever you happen to be.

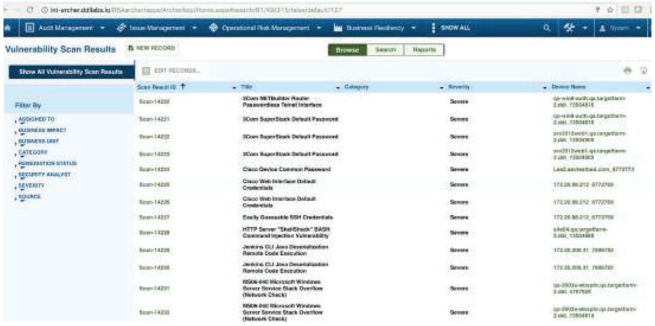
Access the platform seamlessly with browsers, on tablets and mobile devices. Streamline your workflow with granular filtering and categorizing capabilities to quickly identify areas of high risk and focus eforts on defending your enterprise, driving risk out.

Why RSA Archer?

RSA Archer is the leading enterprise governance, risk and compliance (GRC) solution.

Organizations benefit from Digital Defense's patented scan-to-scan host correlation combined with the RSA Archer IT Security Vulnerabilities Program use case.

The scan-to-scan host correlation ensures RSA Archer receives highly 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 within RSA Archer.



Scan Result ID	Title	Category	Severity	Device Name
Scan-14220	3Com NETBuilder Router Passwordless Telnet Interface		Severe	[illegible]
Scan-14221	3Com SuperStack Default Password		Severe	[illegible]
Scan-14222	3Com SuperStack Default Password		Severe	[illegible]
Scan-14223	3Com SuperStack Default Password		Severe	[illegible]
Scan-14224	Cisco Device Common Password		Severe	[illegible]
Scan-14225	Cisco Web Interface Default Credentials		Severe	[illegible]
Scan-14226	Cisco Web Interface Default Credentials		Severe	[illegible]
Scan-14227	Easily Guessable SSH Credentials		Severe	[illegible]
Scan-14228	HTTP Server "ShellShock" BASH Command Injection Vulnerability		Severe	[illegible]
Scan-14229	Jenkins CLI Java Deserialization Remote Code Execution		Severe	[illegible]
Scan-14230	Jenkins CLI Java Deserialization Remote Code Execution		Severe	[illegible]
Scan-14231	MS06-040 Microsoft Windows Server Service Stack Overflow (Network Check)		Severe	[illegible]
Scan-14232	MS06-040 Microsoft Windows Server Service Stack Overflow (Network Check)		Severe	[illegible]

Supported Platform Version: This ofering has been developed for and validated on RSA Archer Platform release 6.3 and Digital Defense Frontline Vulnerability Manager v6.0.

Solution Overview

Digital Defense's Frontline SaaS Platform is the only vulnerability management solution that digitally audits hosts, reconciles assets (helping to minimize duplicates or unknown), prioritizes vulnerabilities, and automates workflow across the hybrid network to make better risk management decisions, faster. Frontline VM streamlines remediation eforts, ofering a way to automate your workflow process of identifying hosts, and scanning for known vulnerabilities and risk of hosts.

SCAN
Quickly, comprehensively and accurately assess your network for vulnerabilities.

ANALYZE
Identify which assets are at risk and receive actionable intelligence.

SCORE
Benefit from a clear, easy-to-understand metric to determine your organization's security posture.

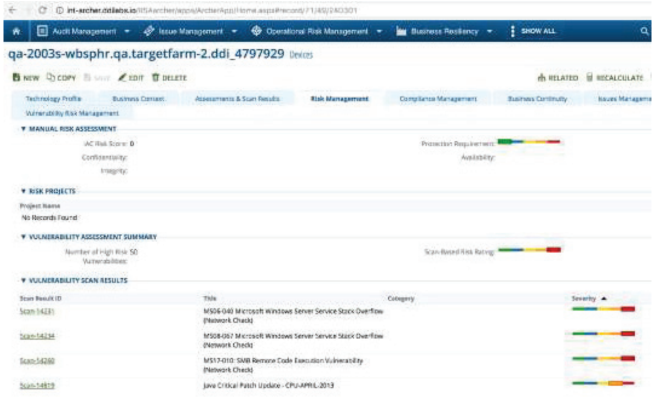
AUTOMATE
Seamlessly integrate Frontline vulnerability findings into your security workflow.

Complete and Accurate Analysis of Devices on Netwrok Via Integration

Digital Node Attribution (DDI DNA™) is the core technology within Frontline VM that eliminates network drift.

As a point in time network vulnerability scanner that feeds data into Frontline VM, DNA is able to match host identification artifacts associated with a specific endpoint over time – including dynamic identifiers like IP address, DNS hostname and NetBIOS hostname – and reconcile them back to a common entity.

Regardless of how identification artifacts may change over time, otherwise known as network drit, DNA can accurately and consistently pin vulnerability scans to each discrete endpoint over time. This forms the basis of DNA's accuracy superiority in addition to maintaining historical vulnerability data of the host. The reconciliation helps to automate the process to correct inaccuracies of your CMBD or asset tracking platform.



qa-2003s-wbsphr.qa.targetfarm-2.ddi_4797929 Devices

▼ MANUAL RISK ASSESSMENT

IAC Risk Score: 0
Confidentiality:
Integrity:
Protection Requirement:
Availability:

▼ RISK PROJECTS

Project Name
No Records Found

▼ VULNERABILITY ASSESSMENT SUMMARY

Number of High Risk Vulnerabilities: 50
Scan-Based Risk Rating:

▼ VULNERABILITY SCAN RESULTS

Scan Result ID	Title	Category	Severity ▲
Scan-14231	MS06-040 Microsoft Windows Server Service Stack Overflow (Network Check)		
Scan-14234	MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check)		
Scan-14260	MS17-010: SMB Remote Code Execution Vulnerability (Network Check)		
Scan-14919	Java Critical Patch Update - CPU-APRIL-2013		

Using Frontline VM empowers users to correlate, analyze and prioritize vulnerabilities within a constantly changing environment and be proactive against new breaches that are introduced every day. The integrated solution automatically operationalizes the information to evaluate the security posture of the organization on a continuous basis.

Communicate, Collaborate and Transform

Through Frontline VM's RSA Ready certified integration, organizations gain valuable insight to streamline the vulnerability and risk management process. The assimilation of data through the two platforms provides a level of depth and context to efectively reduce risk.

Users benefit from:

- Complete and accurate detailed analysis of devices on a network
- The correlation of scan information over time through patented technology that ensures "network drit" is eliminated
- Delivery of a prioritized, efective path to remediation

Deliver An Effective Path to Remediation

To efectively execute against risk to improve the organizational risk posture, remediation eforts must be identified and prioritized. Combining Digital Defense's remediation plan recommendations, integration with RSA Archer helps prioritize and reduce time to accurately identify vulnerable assets and yield a complete inventory of vulnerabilities, helping to produce a concise and actionable remediation plan.

Learn More

To learn more about the advantages of the Digital Defense Frontline Vulnerability Manager RSA Ready certified integration:

- Review the Implementation Guide; and Download the Integration Package.
- Technical support questions, can be directed to: integrations@digitaldefense.com

digitaldefense
by HelpSystems

www.digitaldefense.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.