TAG CYBER

Using the Digital Defense Platform to Support Comprehensive Vulnerability Management

An Independent Criteria-Based Assessment

A recent criteria-based study by independent industry analysts at TAG Cyber concluded that the advanced, risk-based capabilities offered in the Digital Defense platform are well suited to address the comprehensive vulnerability management needs of the modern organization.

Prepared by Edward Amoroso, Katie Teitler, Stan Quintana, and Adam LeWinter

www.tag-cyber.com

Version 1.0

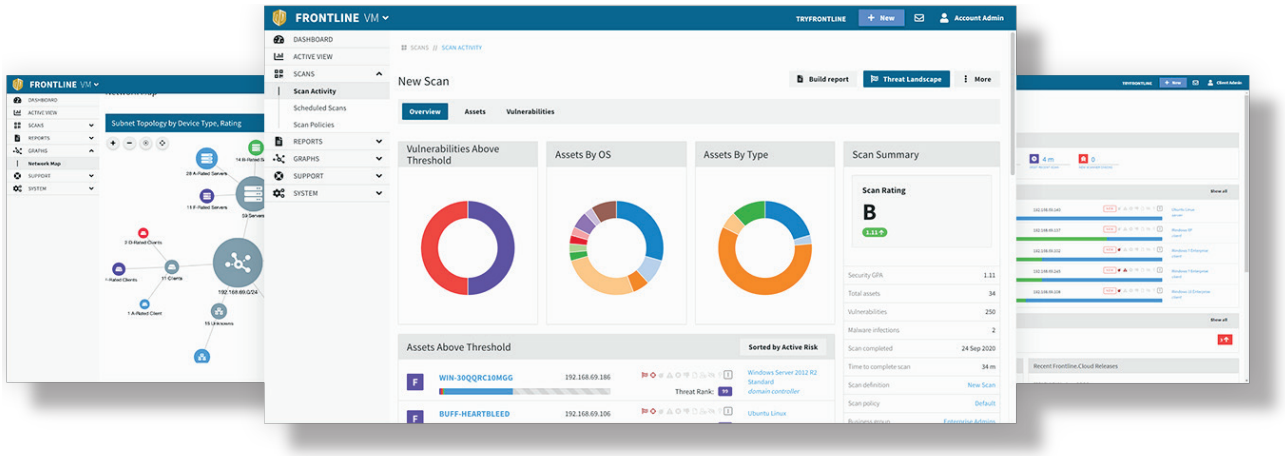
January 25, 2021

Introduction

TAG Cyber[1] was recently engaged to independently assess the effectiveness of the Digital Defense Vulnerability Management platform. The assessment, completed in 4Q20, focused on Digital Defense's capabilities for modern IT security teams. TAG Cyber analysts reviewed the platform, assessed practical use cases, and performed an overall evaluation with respect to TAG Cyber's criteria for modern vulnerability management platforms.

The set of evaluation criteria was developed by the TAG Cyber analyst team to support the needs of IT security teams in their selection of suitable vulnerability management platforms from commercial vendors. Since no meaningful set of evaluation criteria exists for vulnerability management, the TAG Cyber team focused not only on the Digital Defense assessment, but also on creating a framework that might be more generally useful to the community.

Based on the criteria-based assessment, TAG Cyber offers the independent view here that Digital Defense compares favorably to the criteria set. Specifically, the platform was shown to support the highest level of requirements, dubbed Comprehensive Vulnerability Management Support in the criteria set. The sections below introduce the set of criteria and outline the decisions made in making the Digital Defense assessment.



1 Founded in 2016 by Dr. Edward Amoroso, TAG Cyber is a professional research and analyst firm that focuses on closing the trust gap between practitioners and commercial cyber security vendors.

Evaluation Criteria for Risk-based Vulnerability Management

For this exercise, TAG Cyber developed a set of functional evaluation criteria to gauge the completeness, efficacy, and quality of commercial vulnerability management platforms. The set of criteria is organized into three successive classes of vulnerability management platform functional and security requirements. The three classes are designed to reflect basic coverage, enhanced coverage, and comprehensive coverage (see Figure 1).

Figure 1. Evaluation Criteria for Vulnerability Management Platforms

Basic Vulnerability Management Support	**1-1 Inventory**—Create inventory physical devices, software platforms, and applications
	1-2 Scanning—Perform vulnerability scans to identify vulnerabilities
	1-3 Configuration—Identify security configurations including versions and patch status
	1-4 Automation—Automate inventory, vulnerability scanning, and security testing
	1-5 Reporting—Provide accurate reporting of vulnerabilities with drill-down capability
Enhanced Vulnerability Management Support	**2-1 Patching**—Protect against data leakage and malicious code through patch management
	2-2 Threats—Identify cyber threats both internal and external
	2-3 Likelihood—Determine threat and vulnerability likelihoods to determine risk impacts
	2-4 Impact—Support determination of impact of vulnerabilities detected
	2-5 Priority—Support prioritization of assets based on classification, criticality, and value
Comprehensive Vulnerability Management Support	**3-1 Events**—Collect event data and correlate from multiple sources and sensors
	3-2 Methods—Support identification and analysis of attack targets and methods
	3-3 Multi-Hop—Determine presence of vulnerabilities on multi-hop attack vectors
	3-4 Audit—Integrate analysis of audit records with vulnerability scanning information
	3-5 Policy—Support creation of vulnerability management policy and procedures

Basic Vulnerability Management Support – The five requirements included in this lowest criteria class include basic support for inventory, scanning, configuration, automation, and reporting. These are considered the minimum capabilities for a platform to be effective in a typical business. The decision was made that four of the five requirements, each offering foundational support, would be necessary for a commercial platform to meet this class.

Enhanced Vulnerability Management Support – The five requirements included in this criteria class include support for patching, threats, likelihood, impact, and priority. These add to the basic set to form an enhanced vulnerability management approach. Since these requirements build on the lowest class, the decision was made that four of the five requirements would be required to meet this interim class.

Comprehensive Vulnerability Management Support – The five requirements included in this criteria class include support for events, methods, multi-hop, audit, and policy. If added to the enhanced list, the result is a comprehensive approach to vulnerability management. Since these requirements build on the interim class, the decision was made that four of the five requirements would be required to meet this highest class.

Assessment – Determining support coverage for a given requirement was simplified to three possible cases. First, the requirement might be fully met by the platform, which means that deployment of the platform would fully satisfy the desired functionality. Second, the requirement might support the requirement, which means that separate, complementary capability is needed. Finally, the requirement might simply not be met in the platform.

Digital Defense Platform

The Digital Defense Frontline Vulnerability Manager™ (VM) platform was evaluated in the context of this assessment. The broader Digital Defense Frontline.Cloud™ platform, which includes web application scanning (Frontline WAS™), active threat sweeping (Frontline ATS™), and penetration testing (Frontline Pen Test™), was included in this assessment wherever these features contributed to the vulnerability management evaluation.

The Frontline VM™ capability is thus assumed in the context of this evaluation, to be delivered as part of the Frontline.Cloud platform. The combined deployment is thus designed to provide a wide range of vulnerability management support using proprietary scanning technology, security assessments, prioritization and tracking features, and guidance on efficient and timely remediation. Frontline VM includes five specific components:

- ***Frontline Threat Landscape***™ – This capability ranks threats and vulnerabilities using a proprietary Threat Analysis Pipeline (TAP) model that aggregates threat intelligence feeds to correlate reported incidents with vulnerability exploitation.
- ***Frontline Security GPA®*** – This capability offers a letter and number security rating metric to measure progress as vulnerabilities are identified and managed.
- ***Frontline Insight Peer Comparison***™ – This capability offers enhanced peer comparison of vulnerability and threat-related metrics.
- ***Frontline Network Map***™ – This capability provides support for scanning and host correlation to visualize security posture.
- ***Frontline Connect Security Automation***™ – This capability supports integration of discovery, scoring, and prioritization of vulnerabilities into workflow tools and security information and event management (SIEM) tools.

Criteria Assessment of Digital Defense

The assessment of the Digital Defense platform with respect to the set of vulnerability management evaluation criteria established by TAG Cyber is summarized in the figure below. As can be seen from the analysis summary, the Digital Defense platform is shown to meet the highest class in the criteria set – namely, the class designated Comprehensive Vulnerability Management Support.

Figure 2. Criteria-Based Assessment of Digital Defense for Vulnerability Management

		Meets	Supports	N/A
Basic Vulnerability Management Support	**1-1 Inventory**—Create inventory physical devices, software platforms, and applications		✓	
	1-2 Scanning—Perform vulnerability scans to identify vulnerabilities	✓		
	1-3 Configuration—Identify security configurations including versions and patch status	✓		
	1-4 Automation—Automate inventory, vulnerability scanning, and security testing	✓		
	1-5 Reporting—Provide accurate reporting of vulnerabilities with drill-down capability	✓		
Enhanced Vulnerability Management Support	**2-1 Patching**—Protect against data leakage and malicious code through patch management	✓		
	2-2 Threats—Identify cyber threats both internal and external	✓		
	2-3 Likelihood—Determine threat and vulnerability likelihoods to determine risk impacts	✓		
	2-4 Impact—Support determination of impact of vulnerabilities detected	✓		
	2-5 Priority—Support prioritization of assets based on classification, criticality, and value	✓		
Comprehensive Vulnerability Management Support	**3-1 Events**—Collect event data and correlate from multiple sources and sensors	✓		
	3-2 Methods—Support identification and analysis of attack targets and methods	✓		
	3-3 Multi-Hop—Determine presence of vulnerabilities on multi-hop attack vectors	✓		
	3-4 Audit—Integrate analysis of audit records with vulnerability scanning information	✓		
	3-5 Policy—Support creation of vulnerability management policy and procedures		✓	

Potential customers of any vulnerability management platform are welcome to use the set of criteria as basis for their own independent assessment – perhaps using additional commercial platforms for comparison. During this analysis, TAG Cyber did not use other platforms for comparison, but the analysts are certain, based on experience and judgment, that not all commercial offerings will meet the highest class – but this is for buyers to determine locally.

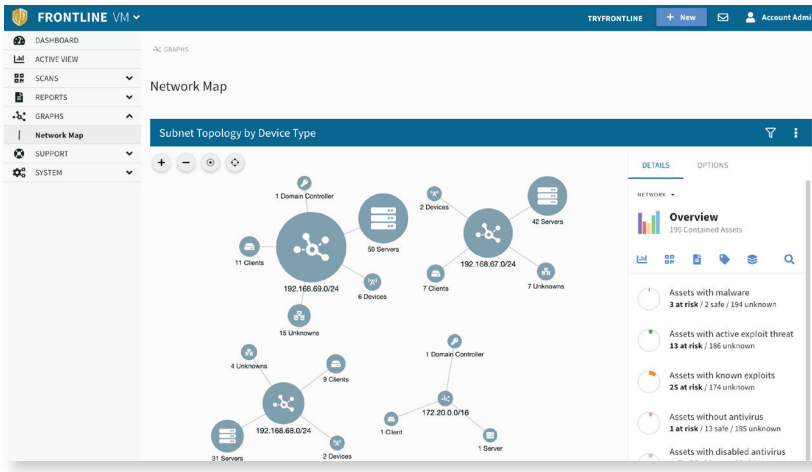
THE DIGITAL DEFENSE PLATFORM IS SHOWN TO MEET THE HIGHEST CLASS IN THE CRITERIA SET – NAMELY, THE CLASS DESIGNATED COMPREHENSIVE VULNERABILITY MANAGEMENT SUPPORT.

Additional Notes on the Platform

Frontline Threat Landscape – This tool is powered by Frontline Threat Analysis Pipeline (TIP) which is a proprietary machine learning model that aggregates external threat intelligence feeds which are then used to identify the risk of exploitation of internal vulnerabilities in the network. Threat intelligence such as threat trends and CVSS, CWE, and CPE metrics are integrated with the vulnerability data from Frontline Network Map to provide the likelihood of exploitability for each vulnerability in the environment. With the machine learning algorithms Frontline TAP can detect and analyze events, understand attack targets and methods, determine the presence of multi-vulnerabilities on multi-hop attack vectors, and ranks possible avenues of exploitation found in the environment that have not yet been exploited.

Frontline Security GPA – This tool supports vulnerability impact and security posture scoring metrics using letter and numerical grades to help determine risk impacts to the environment. The metrics also identify trends in security posture as vulnerabilities are continually assessed and remediated over time. Incremental improvements can be observed as even the smallest remediation efforts are accounted for in the perceived criticality of individual systems. Metrics can then be compared internally or from an industry perspective with Frontline Insight Peer Comparison. Metrics such as highest risk vulnerabilities and time to remediation can be compared and provide a measure against performance benchmarks.

Frontline Network Map – This tool utilizes Digital Defense's patented scanning and host correlation technologies to provide a map of the network and presents the information in an interactive graphic visual. Users are then able to act against single assets or a cluster of assets to scan for changes, assign prioritization based on criticality and business value, and identify hotspots on the network. Users can choose from a variety of clustering algorithms to view asset relationships and interconnectivity to identify and document vulnerabilities and active threats.



Frontline Connect Security Automation – This tool is used to integrate discovered, analyzed, and prioritized vulnerabilities into other security operations tools which supports the creation of vulnerability management policy and procedures. Integrations are more than passive data uploads and include remediation recommendations with associated CVE and vendor patch links. Through the bidirectional REST API with JSON data users can utilize Digital Defense to automate inventory discovery, vulnerability scanning, and security testing in ways that make sense for their environment.

Summary of Findings

In comparing with the criteria presented above, the Digital Defense offering scores as a comprehensive solution. The advanced analytic and metric gathering feature set allow users of the solution to automatically identify vulnerabilities, receive remediation recommendations, and determine risk impact based on criticality and business value all while integrating into the existing security toolset in the environment.

About TAG Cyber

Founded in 2016 by Dr. Edward Amoroso, TAG Cyber provides world class research and advisory services, with advanced market reporting for cyber security teams. TAG Cyber's goal is to bridge the communication gap between commercial security vendors and business practitioners. TAG Cyber's insights are delivered through an innovative on-line portal with support for expert on-demand research.

Digital Defense
by HelpSystems

Contact us for more information:

Toll Free: 888.273.1412

Email: sales@digitaldefense.com

Visit us at: www.DigitalDefense.com