Secureworks®

BUYER'S GUIDE

Secureworks® Taegis™ VDR Buyers Guide

BUYER'S GUIDE INTRODUCTION

The Current State of Affairs

The sheer number of vulnerabilities continues to increase, both the existing number residing on business networks and the endless, and accelerating, flow of ones newly discovered and published. Existing vulnerability assessment tools are difficult to use, cumbersome to set up, require significant human intervention at multiple points in the workflow, and demand a high level of expertise and sustained effort from company staff to operate and realize full value. Many organizations rapidly shifted to a remote-work model in 2020, increasing the attack surface threat actors target and adding to the challenge of securing corporate assets.

Consider the following that illustrates the current state of vulnerability management:

4	The number of consecutive years the U.S. CERT Vulnerability Database has recorded a record number of vulnerabilities[1]
167.3%	The percentage increase in the number of vulnerabilities classified as High or Medium from 2016-2020[1]

[1] U.S. CERT Vulnerability Database, CVSS Severity Distribution Over Time, April 2021

Customers historically have tried to combat vulnerabilities by purchasing point solutions, but many of those don't provide the holistic coverage needed as critical data increasingly resides outside the network. Those solutions also don't prioritize vulnerabilities by the context of a company's environment. That's a challenge considering many organizations struggle to hire, train and retain security staff, and the combination of gaps in visibility and missing context only increases the burden on security resources.

Why the Old Way of Doing Vulnerability Management Does Not Solve the Problem

The traditional approach to vulnerability management focuses on generating an all-encompassing list of discovered vulnerabilities in an organization's environment. Given the ever-increasing rate of identifying new vulnerabilities, just producing a list with no context and no guidance on what presents the highest risk for a particular organization does not provide the actionable, impactful solution that organizations need. The vulnerability management marketplace is full of tools designed to provide some aspects of effective vulnerability management, but lack the completeness that organizations need.

A New Approach to Vulnerability Management

Organizations need a different approach to vulnerability management. Traditional solutions simply do not provide actionable information needed to meet the requirements of handling the onslaught of new vulnerabilities and getting true value from vulnerability management. Nobody is able to patch every single vulnerability discovered, so the ability to automatically identify and prioritize vulnerabilities is critical to achieving secure vulnerability management.

Holistic vulnerability management security is not just an all-encompassing list of vulnerabilities discovered in a company's environment that require remediation. That list must be prioritized based on the risk a vulnerability presents within the context of an organization's specific environment. Another important consideration comes at the beginning: how to implement a solution and get the most value from it without overwhelming the security resources an organization may have. Automating manual tasks that security resources normally would have to perform frees up those security resources to focus on other things, and not get bogged down with configuration or technology management.

Today's vulnerability management also must leverage artificial intelligence and machine learning, using technology to improve the solution's effectiveness over time. Self-learning capabilities pick up on priorities based on continuous use of the solution through activities such as scanning, remediation, and reporting. Put these elements together, and the result is a vulnerability management solution that includes the essential aspects of a complete program, including endpoint and website discovery and scanning.

Required Capabilities Needed to Solve the Problem

What comprises the right vulnerability management solution? Here are 5 must haves:

- A solution that is self-learning and driven by artificial intelligence
- Automated, configuration-free approach
- Fully integrated and comprehensive cloud-based solution
- Contextualized prioritization that provides meaningful guidance on what to remediate first
- Automated integration with threat intelligence for inclusion in comprehensive, risk-based prioritization

Questions to Ask a Vendor When Evaluating a Vulnerability Management Solution

- What is the process for discovering vulnerabilities?
- What do you do when a vulnerability is discovered?
- How does your organization handle the publication of vulnerabilities?
- What is your remediation planning process?
- Does your staff possess experience around set up and maintenance of vulnerability tools?
- Is your vulnerability technology easy to learn / use?
- How would you describe your organization's ability to react to a new vulnerability?
- What is the process for determining which vulnerabilities could have the most impact on your organization? How long does that process take?
- Is your vulnerability technology able to learn based on scanning, patching and reporting activities?
- Is compliance a significant factor in your vulnerability management strategy?
- How many different tools and vendors make up your vulnerability management solution? Are they integrated?
- Can your vulnerability management technology discover vulnerabilities throughout your environment (endpoint, network, and cloud)?

- Do your vulnerability management tools include threat intelligence feeds? If so, are they from the same vendor, and are they known in the industry for threat research and frontline security operations experience?
- What is the licensing model for asset discovery, vulnerability scanning, threat intelligence, and risk-based prioritization?
- How many and what types of factors are used in prioritization, and do they include the local context?

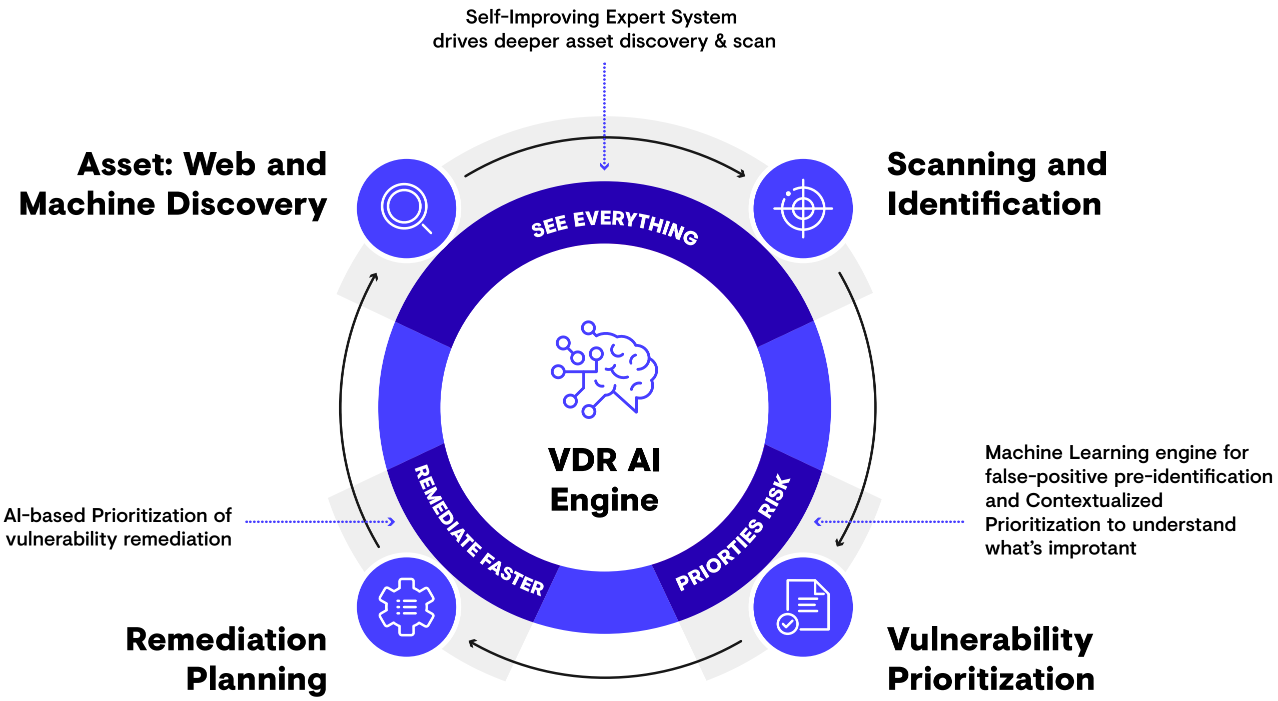
Why Secureworks?

Overview of Secureworks History

Secureworks has spent the past two decades providing industry-leading information security services, with a focus on managed security services, incident response, threat intelligence, and security consulting. Founded in 1999, our sole focus has been on cybersecurity. The Secureworks Taegis platform – formerly known as Red Cloak™ – marks our shift to delivering software services, leveraging the years of threat findings and security expertise to combine human intellect with security analytics.

Introduction to Secureworks solution

Secureworks Taegis VDR delivers a fully integrated, comprehensive vulnerability management solution via an automated and configuration-free approach with machine learning and self-learning, and built-


Self-Improving Expert System
drives deeper asset discovery & scan
Asset: Web and Machine Discovery
Scanning and Identification
SEE EVERYTHING
VDR AI Engine
REMEDIATE FASTER
PRIORTIES RISK
AI-based Prioritization of vulnerability remediation
Machine Learning engine for false-positive pre-identification and Contextualized Prioritization to understand what's improtant
Remediation Planning
Vulnerability Prioritization

in contextual prioritization. VDR automatically performs asset and service discovery, dynamically adjusting its discovery process based on learnings from past discovery results and in-depth scanning activity. VDR's contextual prioritization provides a prioritized list of every vulnerability, allowing organizations to address the most critical ones, plus build remediation plans that are measurable and visible to give customer the most impact and value from their VM investment.

How Secureworks Solves the Problem

For organizations seeking an effective solution to the risk posed by vulnerabilities, Secureworks Taegis VDR provides a SaaS-based managed service based on automation, artificial intelligence and machine learning. VDR automates previously manual vulnerability management tasks, and the machine learning-based system improves autonomously with use. Unlike traditional vulnerability management solutions, VDR provides contextual prioritization based on the unique attributes of your environment. VDR is the evolution of traditional vulnerability management solutions, following a risk-based approach that prioritizes remediation based on the specific context of your environment. The automation of manual tasks removes the burden of initial configuration and constant maintenance many traditional solutions require, resulting in more time for your staff to focus on other business critical objectives.

Next Steps

Want to see how VDR works?

Request a demo to see how VDR delivers impact throughout the vulnerability management process.

Learn more about VDR.

Explore a risk-based approach to vulnerability management.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist **secureworks.com**

About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Secureworks®