Secureworks

DATA SHEET

Secureworks Vulnerability Detection and Prioritization (VDP) In-Depth:

Frequently Asked Questions

How Does Secureworks Account for the Discovery of New Vulnerabilities?

We provide continuous updates to our vulnerability database, releasing new signatures up to multiple times per day when new vulnerabilities are published. Our autoscan model scans on an ongoing basis, meaning that all assets will get scanned for new vulnerabilities, while rescans are autonomously optimized based on emerging threat intel in real-time and on existing knowledge of potentially exposed assets.

We have a database of more than 140k CVEs with over 60k detection rules spanning over 4,000 application versions over 1,400 versions of operating systems. In terms of DAST, we score 95%-96% on WIVET scores, and look for vulns such as XSS, SQLis, XSRFs, XXEs, LFIs, RCIs, Overflows, and the like.

However, we don't believe organizations should be focused on the number of detected vulnerabilities as a leading indicator of a solution's effectiveness; the efficiency of the detection, the reduction in false positives, and the automated meaningful prioritization of all vulnerabilities are what we believe organizations require to significantly reduce vulnerability risk.

"...we don't believe organizations should be focused on the number of detected vulnerabilities as a leading indicator of a solution's effectiveness..."

How Does Secureworks' Scan Technology Help to Reduce Potential Damage to Devices While Providing Scan Depth?

Based on our machine learning technology, Secureworks discovery/scanning functions are intelligent and self-improving at the network and device levels. That having been said, our unique offering - providing a completely autonomous full stack (Discovery + VA + DAST) solution - means we have to take extra precautions with certain problematic payloads, and we have therefore developed automated ways to address such circumstances and adjust accordingly as discussed below.

At the network level, scan initiation can be scheduled by the user, but also includes an autonomous capability. For example, when a new vulnerability is published, scans are automatically triggered on assets relevant to that new vulnerability. As for specific asset scan schedules, those are adjusted automatically based on collected data like device response times or patching schedules. This data is used by the Secureworks engine to determine optimal scan times that are less likely to disrupt the asset's operation.

At the device level, Secureworks adjusts the requests of the asset based on the time-waiting-perrequest. If that metric is long, the rate of requests is slowed, while the opposite is true as well. These adjustments are made in real-time, so scanning times are optimized while the likelihood of crashing a device is nearly eliminated. Additional details of this scanning optimization approach can be found in a Secureworks blog post published in 2019.

We also continuously re-evaluate device status during the scan, and try to actively detect if the device is having issues responding to our scan queries. If so, we immediately abort scanning and clearly inform the user about the situation.

How Does Secureworks' Scanning Engine Respond to Disruptions or New Information like a Power Outage or a Newly Discovered Vulnerability?

Secureworks' scanning function is AI-based, so it adjusts autonomously based on changes in the network, employee behavior, and the external threat environment. When a scan fails, for example as the result of a power outage or machine glitch, the scan is automatically re-scheduled. And, when a new vulnerability is discovered, relevant scans are automatically triggered, all without the need for manual intervention.

How Does Secureworks Handle Web Applications?

Secureworks' VM solution includes machine and connected device scanning, as well as web application discovery and security testing. Not only does this obviate the need to purchase, maintain, and integrate multiple software products, but allows Secureworks to greatly enhance the value of our vulnerability prioritization function. Since the data on which we prioritize vulnerabilities includes knowledge of all machines AND web applications on a network, our risk rankings account for the critical relationship between them. So, for example, if we identify a vulnerability that is only locally exploitable, but it resides on an asset running a vulnerable web application that would combine with the local vulnerability, the risk of the vulnerability increases non-trivially. This is just one example of how Secureworks leverages a comprehensive, holistic view of the network to prioritize vulnerabilities in context.

“This is just one example of how Secureworks leverages a comprehensive, holistic view of the network to prioritize vulnerabilities in context.”

What is the Relationship Between Secureworks' Prioritization Engine and the CVSS Score?

The primary limitation in the CVSS score is lack of available updated context. The CVSS Base score is constant for a given vulnerability, independent of the network it’s on, or more importantly, the specific location on the network, the specific asset, etc. While there are allowances in CVSS v3.x for additional metrics, these factors must be known, maintained, and applied to the system and vulnerability combination. Without this information, for example, a locally-exploitable vulnerability with a CVSS score of 3 or 4 on the same machine as three web applications is probably not, in context, a low risk. Secureworks' Contextual Prioritization actually starts with the CVSS Base score, and then applies an additional three dozen factors to rank the risk of every vulnerability on a network in context, and in comparison to one another. Secureworks does this every 5 minutes, recognizing that a

“The primary flaw in the CVSS score is lack of available updated context.”

vulnerability's risk changes as its environment does. The hyper-fluid nature of enterprise networks and the external threat environment makes a static score for any vulnerability largely meaningless.

"Philosophically, we prefer to approach vulnerability management from a risk perspective in favor of a compliance based approach."

Does Secureworks Offer Compliance-Specific Product Features?

Philosophically, we prefer to approach vulnerability management from a risk perspective in favor of a compliance based approach. With this in mind, our machine learning driven prioritization is the ultimate form of a tailored configuration, not just for specific vertical markets, but for each specific organization. Secureworks autonomously scans and discovers assets and vulnerabilities across the network in a holistic manner. Therefore, we are always working within the risk prioritization framework. However, we recognize for compliance and regulatory reasons that compliance-specific views or reports are needed; as such, our tagging and filtering capabilities allow organizations to easily view, research, and export compliance related information. Further, we believe that, as many compliance requirements are report-driven, an "after the fact" approach is most sound. That is, extract data from existing scan results as opposed to limiting the scans beforehand to only gather information needed for compliance. In short, our approach is to design vulnerability management efforts for risk reduction first, then extract what is needed for compliance afterward.

How is the Secureworks Solution Delivered and Priced?

Secureworks is a SaaS solution, and external scans can be run with no downloads or configurations. Users simply input an external IP range. For scanning "inside the network", Secureworks provides an Edge Service, which is a dynamically-scaled, small-footprint virtual machine supporting almost every virtualization technology or cloud platform. Organizations will install one or more virtual Edge Services depending on topology and needs. The Edge Service generation, download, and configuration process takes 30 minutes to an hour for most customers. What limited configuration is required is completed via a web browser, and all reports are accessed from Secureworks' multi-tenant customer cloud, where all data resides as well. The cloud architecture not only enhances customer ease-of-use, but also enables Secureworks' machine learning engine to leverage user behavior data across all customer tenants to benefit all others over time.

How is ML/AI used in your platform to reduce false negatives and false positives?

False positive detection is one of the many ways AI is employed by Secureworks to optimize and automate vulnerability operations. Factors such as services running on the asset and the detection mechanism that flagged the vulnerability are used to assess the probability that the identified vulnerability is, in fact, a legitimate one. And, as the collected data analyzed by the Secureworks VDP engine increases over time, its ability to accurately predict false positives versus legitimate vulnerabilities improves.

To improve the reliability of vulnerability detections, Secureworks uses an AI technique called Bayesian networks. The technique allows other observations to be included as evidence in

the assessment, for example, how frequently the detection mechanism being used generates false positives, or whether the specific vulnerability has often been identified manually as a false positive in the past. Like all machine learning-based analyses, false positive identification improves with use in the Secureworks VM solution.

What we end up with, all done behind the scenes, is a supervised classification of every vulnerability as either being confirmed or false positive. This classification is done using a blend of methods that blindly takes user labels and features (Random Forest Classifier) and prior expert knowledge (Bayesian Networks) in a statistically-sound ensemble machine learning model, just like a democratic process.

One additional note on false positives and Secureworks' solution approach: minimizing false positives is step 0 in any thoughtful prioritization process; those are the first “vulnerabilities” to eliminate. As a company committed to providing an automated, meaningful prioritization solution, leveraging Secureworks VDP to minimize false positives is essential to our mission.

“...minimizing false positives is step 0 in any thoughtful prioritization process; those are the first ‘vulnerabilities’ to eliminate.”

What Other Scanning Techniques Does Secureworks Employ to Discover Devices in the Network that are not Subject to a Conventional Device VM Scan?

Secureworks uses many continuous and dynamic active network detection techniques to find not only machines but also potential Web applications on machines, whatever port they may be present at. We use a number of methods to do so, but what’s most different from the typical discovery process is that it’s entirely dynamic and evolves over time as we learn more about the characteristics of the network we’re looking at. For instance, ports that we look for to discover machines will be dynamically modified at almost every run depending on patterns we find during scans of existing machines, allowing us to find potentially “left over” machines that a more traditional discovery process would miss. The same logic exists for Web applications, where we construct a knowledge map through indicators extracted from Web scans and existing hosts on the network, such as domain names, links, keywords, comments, etc. in order to continuously look for exposed Websites, or even hidden virtual hosts on existing web Servers that are then autonomously scanned by the platform.

What is Secureworks' Philosophy on the Use Agents?

All Secureworks scanning is agentless. We found that issues with reliability of scan data could be improved without the need for agents by using our false-positive-detection algorithms. Furthermore, any form of new agent potentially increases the attack surface on an endpoint as has been prominently reported with vulnerabilities in leading endpoint detection products.

How Does Secureworks Leverage User Behavior in its Solution?

Secureworks incorporates user behavior into our VM solution in several areas. One example is the identification of business-critical assets. Legacy VM products require the tedious manual identification of business-critical assets, while Secureworks does so automatically by collecting and analyzing user behavior data. We observe which assets are most frequently

scanned, most quickly patched, and are otherwise receiving the most attention from IT teams. Secureworks uses that data to confidently identify which assets are considered most important to the business.

Another example is crowd-sourced behavior. As a multi-tenant SaaS solution, Secureworks leverages behavioral data across our entire customer ecosystem to benefit all customers. For example, if a particular vulnerability is being addressed quickly by many organizations, we can reasonably deduce that its priority is high.

"As a multi-tenant SaaS solution, Secureworks leverages behavioral data across our entire customer ecosystem to benefit all customers."

Therefore, our use of user behavior data is based on the explicit behavior of users in the Secureworks interface as well as observed behavior of changes in an asset, patching attention, and other remediation. As an example, through the constant discovery of vulnerabilities on a given set of assets, Secureworks monitors the remediation patterns of assets on the network. We use this behavior to determine patching cadence, regularity, and which assets are routinely remediated and which ones are ignored. This is a very dynamic factor in our risk prioritization because we can correlate the occurrence of a vulnerability, the expectation of if and when it will be remediated (user behavior), the availability of an exploit, and the likelihood of exploitation.

Does Secureworks Have Any Way to Look at the Security of Virtual Machines?

Yes, the Secureworks platform will not only autodiscover but can also scan anything that is exposed on the network, including virtual machines or their hosts, and any Web application that they expose on these subnets. Additionally, we have specific provisions to detect vulnerabilities in virtualization environments (ESXi, Virtualbox, etc.).

At a High Level, What Elements Does Secureworks' Contextual Prioritization Take into Account?

Secureworks' solution collects data on, and analyzes, over 35 factors to generate a meaningful priority list from 1 to n of all vulnerabilities on an enterprise network. Those 35+ factors fall into 5 categories:

- The characteristics of the vulnerability itself
- The asset on which the vulnerability resides
- The network environment in which the asset is located
- How the asset relates to the organization and its priorities
- The ever-changing external threat environment

Secureworks' autonomous and comprehensive solution requires no connectors to other software tools or data sources to deliver this prioritized list.

"Secureworks' solution collects data on, and analyzes, over 35 factors to generate a meaningful priority list from 1 to n of all vulnerabilities on an enterprise network."

How Does Secureworks Use the CVSS Score to Identify Vulnerabilities that Present the Most Risk?

Secureworks' exclusive Contextual Vulnerability Prioritization begins with the vulnerability's CVSS score, but then processes over 35 factors using our Secureworks VDP engine to rank every vulnerability on the network from 1 to n, without human intervention, every 5 minutes. Moreover, ranked items are actually groups of vulnerabilities on individual assets, so applying

a single patch to, for example, the top-ranked vulnerability, might efficiently address 5, 10, or more individual CVEs on that prioritized asset. This emphasis on prioritization and prescriptive remediation flows from Secureworks' core philosophy: identifying vulnerabilities alone is unhelpful. Security improves, and risk is reduced, only when remediation efforts are judiciously undertaken.

"Secureworks customers can build multiple remediation plans and assess how effective each will be before committing resources."

How Does Secureworks Help its Customers Build Effective Remediation Plans?

Secureworks actually prioritizes remediation recommendations by first automatically grouping CVE's in a remediation-centric display of information. Secureworks provides a numbered list of remediation activities - from 1 to n - that will optimize risk reduction, all based on our 35+ factor prioritization engine. Moreover, Secureworks' VM solution includes a remediation scenario function that allows users to build remediation plans, and then understand how each plan would improve the organization's vulnerability Health Score if implemented. Secureworks customers can therefore build multiple remediation plans and assess how effective each will be before committing resources. As would be expected, detailed remediation information is included with the prioritized recommendations so that the risks and remediation actions can be easily understood and implemented by the teams responsible for remediation.

What are Some of the Unique Ways Secureworks Employes AI/ML in its Solution?

Building a vulnerability management solution from the ground up with a mandate to automate a previously-manual process has yielded a number of elements that are not only unique to Secureworks' VM solution, but add significant value to our users. One example is our built-in outlier detection function. Experienced pen testers are skilled at a hacking technique that attempts to identify assets on a target network that are unique in some way. Such "outlier" assets are attractive to pen testers - and bad actors as well - as they are often soft targets. Knowing which assets on your network are particularly appealing to intruders is an important factor in prioritizing vulnerabilities on those assets. Thus, Secureworks has developed a machine-learning based approach to automating the identification of these unique assets, a previously manual effort reserved for the most experienced and capable pen testers. Part of our prioritization engine, this outlier asset detection insight is included in the Secureworks solution and one of the many factors used to prioritize remediation efforts. Further, Secureworks has made this capability available to the security community as an open-source tool so any organization with an Nmap scan can have access to the results of our outlier identification function. Secureworks customers can quickly filter all assets by their outlier score as well, so they can see their outlier assets within the product without requiring an Nmap scan.

"Secureworks has developed a machine-learning based approach to automating the identification of unique assets, a previously manual effort reserved for the most experienced and capable pen testers."

Other unique elements of our solution enabled by our Secureworks VDP engine include:

- **Remediation Time Prediction**
  Machine Learning is used to predict how long it should take to remediate a specific vulnerability based on a number of factors that are continuously

computed. These include the characteristics of the organization itself (each client) but are also influenced by peer-data (what the best teams are doing). The remediation time prediction not only contributes to the CPS (Contextual Prioritization Score), but also provides Secureworks customers a remediation team benchmarking opportunity.

- **Predictive Attention Prediction**
  By passively collecting signals from analysts using the platform in a continuous way, we have built ML models that are able to infer what the typical priorities are for specific users in the same organization. We then use this model to infer which assets & vulnerabilities are more important for the organization globally. This not only is taken as a factor during our prioritization, but coupled with knowledge of the global customer landscape, we can drive comparative analysis and help influence users to remediate more valuable vulnerabilities.
- **Attack Path Simulation**
  By looking at vulnerabilities present on assets and how they relate to each other in the same network, we can simulate probable paths of attacks from asset to asset over thousands of these statistical simulations, giving us a very good data science approach to understanding which assets are the most likely to be targeted during a real attack scenario. This probabilistic ranking that continuously evolves over time allows for more precision during the evaluation of network-centric factors of prioritization.
- **Vulnerability Trends Analysis**
  Secureworks consumes data from specialized infosec public sources, dark web feeds and other semi-private sources in order to draw trend insights that can be mapped to not only current customer-specific vulnerabilities, but also emerging findings that haven't been catalogued by the industry quite yet.
- **EPP - Exploit Publication Prediction**
  This is Secureworks' AI-based analysis of newly-discovered vulnerabilities that don't yet have exploits that have been published. The goal is to predict whether or not there's a good chance that an exploit will be published in the next few days for these theoretically unexploitable vulnerabilities. This is one step beyond some competitive approaches that look at what vulnerabilities already have exploits and which are more easily weaponizable based on past activity. Note that some competitors in the market rely on this kind of predictive analysis exclusively to prioritize vulnerabilities, while EPP represents just one of the 35+ factors in Secureworks' exclusive Contextual Prioritization offering.

If your organization needs immediate assistance call our **Global Incident Response Hotline (24x7x365).**
+1-770-870-6343

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

About Secureworks
Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs. With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.
www.secureworks.com