Cavirin CyberPosture Score 2.0

TECHNICAL WHITEPAPER

July 2019

Bashyam Anant
Vice President Product Management

Naveen Ramachandrappa
Senior Machine Learning Engineer

Cavirin Systems
5201 Great America Parkway Suite 419
Santa Clara, CA 95050

Table of Contents

Overview

Cavirin CyberPosture Scores quantify risk associated with complex, multi-cloud infrastructures on a 0 to 100 scale (0 = HIGH RISK, 100 = LOW RISK) using a proprietary scoring algorithm. Scores are computed for each resource (e.g. an AWS S3 bucket or a virtual machine instance) and aggregated at the organization, environment (AWS, GCP, Azure, Docker, On-Premises), asset group, resource type (e.g. "Object Store") and policy pack levels. Scoring serves several outcomes:

- A CISO can gauge their organization's security posture, assess trends and determine where to direct response plans
- A Chief Compliance Officer can gauge their organization's compliance posture for a compliance requirement such as PCI-DSS, HIPAA or GDPR, assess trends and direct response plans.
- A SecOps user can slice and dice scores from the company level to a resource group to a resource type (e.g. S3 buckets) to an individual resource (an S3 bucket), diagnose problems and prioritize remediation actions
- A DevOps users can create change management plans by prioritizing policies that offer the greatest security / compliance posture improvement

How are CyberPosture Scores computed?

CyberPosture Scoring quantifies the framework in NIST 800-30: Guide for Conducting Risk Assessments (see Appendix for details). Once resources are discovered in your cloud and on-premises accounts, Cavirin assesses each resource based on the technical controls in one or more policy packs assigned by the user. Each technical control that fails represents risk and results in a score reduction. While the exact details are proprietary, Cavirin CyberPosture Scores reflect the following tradeoffs:

- A **weight** (0-10) associated with the technical control assigned by a proprietary machine-learning classifier. 0 is used for INFORMATIONAL controls; 0+ to <4 is assigned for LOW severity controls, 4 to <7 for MEDIUM controls and 7-10 is used for HIGH/CRITICAL controls.
- **Resource Criticality**, 0.8 (LOW criticality) to 5 (HIGH criticality), assigned by users based on Confidential, Integrity and Availability requirements associated with resources.
- Number of resources failing a given control
- Controls that are repeated within multiple policy packs assessed on a resource

In simple terms, high-weighted technical controls that are failing on lots of critical resources and are contained within multiple policy packs will depict a low score (implying high risk) in our scoring algorithm. Such controls will also result in a high improvement potential if remediated – as a result, they will bubble up to the top in the list of Prioritized Issues shown in the Cavirin Dashboard.

CyberPosture Scoring Illustration

Cyberposture Scores are designed to pinpoint "*needles in a haystack*" of resources and findings (failed policies)- scores deteriorate very rapidly with policy failures. Simply put, resources with just a few HIGH/MEDIUM policies failing will show a score of ZERO calling attention. Consider a hypothetical policy pack with 10 HIGH, 20 MEDIUM and 70 LOW severity policies. For just this one policy pack, the CyberPosture Score for a single resource as a function of the number of failed HIGH policies (and zero MEDIUM or LOW policy failures) is plotted in the Figure 1 below. Note that the resource's CyberPosture Score rapidly approaches ZERO with just 5 HIGH fails, calling upon the user to respond immediately. Improvement potential, defined as the impact on scores if one or more findings are addressed, for a

resource are similarly highly non-linear – fixing a small number of HIGH severity issues can improve scores dramatically.

CyberPosture Scores for any collection of resources, such as an Asset Group or all resources in an environment like AWS, are computed as the resource-criticality-weighted average of individual resource scores.

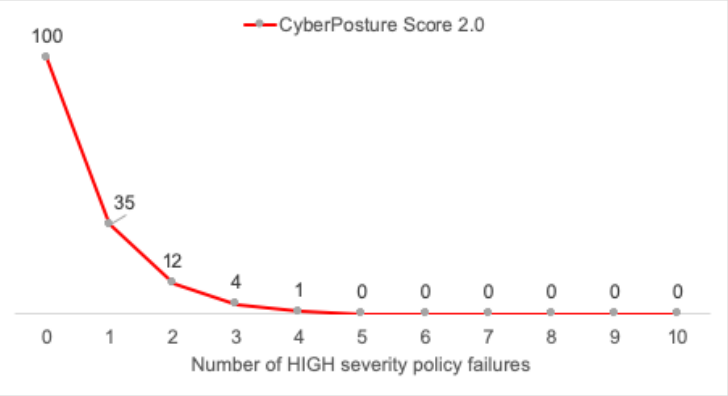

Figure 1: CyberPosture Score for a single resource assessed with a hypothetical policy pack with 10 HIGH, 20 MEDIUM and 70 LOW severity policies; Only HIGH severity policies are failing in this illustration.

How to improve CyberPosture Scores?

The best way to improve CyberPosture Scores is to remediate findings (failed policies) reported by Cavirin and re-run assessments. For failed policies that represent acceptable risk, use Cavirin's policy suppression feature to exclude such failed policies from scoring.

CyberPosture Score Versions

As of the Spring 2019 release, Cavirin has updated the scoring algorithm compared to prior releases, resulting in CyberPosture Score 2.0. Reports generated from prior releases will reflect scores calculated from CyberPosture Score 1.0. New assessments on existing resources using Spring 2019 release will result in CyberPosture Score 2.0. A best practice is to re-run discovery and assessments after upgrading from pre-Spring 2019 to Spring 2019.

APPENDIX: NIST 800-30 Inspired CyberPosture Scores

NIST 800-30: Guide for Conducting Risk Assessments provides the 6 step framework for assessing IT risk as depicted in Figure 2 below. CyberPosture Score 2.0 quantifies some steps as described below and is extensible to other risk signals over time.

Step 1: **Discover and Classify Resources**. Accomplished through Cavirin's agentless resource discovery for AWS, GCP, Azure, On-premises and Docker environments

Step 2: **Assess Threats** through AWS GuardDuty, Exploit DB and other means

Step 3/4: **Identify Weaknesses** & **Evaluate Controls**. Accomplished by evaluating assessing one or more policy packs and the controls included them on the resources discovered in Step 1.

Step 5: **Determine (Breach) Likelihood**. Placeholder for future releases based on signals noted in the figure. The current default for likelihood is 1.0.

Step 6: **Assess Impact**. Accomplished through resource criticality that includes the user's assessment of confidential data, system integrity and system availability requirements.

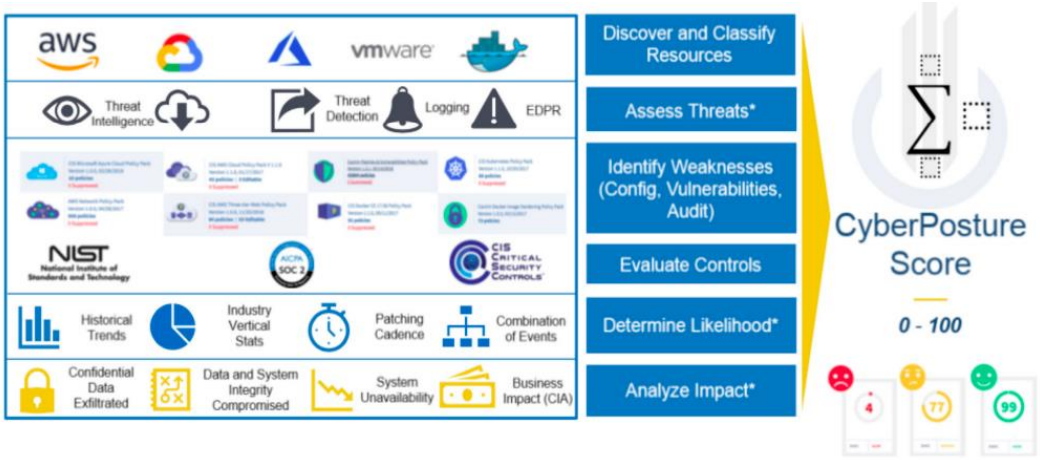

Figure 2: Quantifying NIST 800-30's 6 Step Risk Assessment Framework through CyberPosture Score