Security Ratings *AND* Assessments

Why Together they Achieve Better Enterprise Health

SECURE HALO

SECURING THE ENTERPRISE

Focus on Security Health, Not Symptoms

Cyber risks continue to escalate and evolve, but resources to address them are often limited. Risk and IT professionals may turn to security ratings as a relatively quick and painless metric to gauge the effectiveness of their organization's security practices, using this information to demonstrate activities for regulatory compliance or executive awareness.

One leading security ratings company likens its approach to assessing a person's health, where coughing, being overweight or other factors of appearance can suggest a reasonable chance that person is not in the best health. Measuring outside indicators of security health, security ratings tools attempt to quantify the likelihood of a breach.

If this is deployed as a key measurement of security health, it leaves the organization focused on symptoms rather than treating the disease. Security ratings measure the effects of a security program, in that they provide a metric that can demonstrate in a relative way how effective a current state security program is in delivering results. But a security rating can't reveal why a security program is delivering unsatisfactory results, nor can it provide insight into how to take the steps necessary to produce a security program that consistently delivers a more secure environment.

For that, a security program must be viewed as an Enterprise effort. An Enterprise assessment examines how security controls are implemented and integrated across the organization, as well as how well these controls address the risks specific to an industry or individual environment. Using security assessments to analyze and address a security program's deficits in conjunction with using security ratings as a metric to measure success or failure in doing so allows an organization to work out root causes of security vulnerabilities and start curing the disease, rather than just treating the symptoms.

SECURE HALO

SECURING THE ENTERPRISE

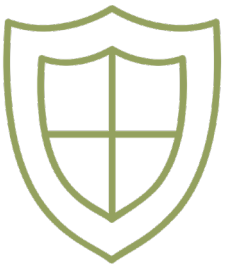
What Do Security Ratings Measure?

Numerous vendors now offer products that rate an information ecosystem's relative security on various scales. In July of 2017, the US Chamber of Commerce attempted to inject some measure of consistency in the Security Rating conversation by publishing its "Principles for Fair and Accurate Security Ratings." It informally defines a Security Rating as a "combination of data points collected or purchased from public and private sources and proprietary algorithms to articulate an organization's security effectiveness into a quantifiable measure or score." A review of existing rating services reveals several data sources used in the construction of existing security ratings.

One ingredient in the generation of ratings is IP reputation lookups. An entity achieves a negative IP reputation when a large volume of spam or virus-laden traffic are observed to be originating from that address, or when open proxies are found, indicating malware infestation. This information can be collected externally from the multiple organizations that track it, without the need for cooperation on the entity's part. IP reputation and the organizations that track and report it have long been a vital part of maintaining internet health.

Ratings services also make use of both external and internal vulnerability scans to search out open ports, unpatched vulnerabilities, and other misconfigurations. The amount, severity, and age of critical vulnerabilities can be used in a proprietary algorithm or formula to derive input for a security rating. Additionally, some security ratings include the discovery of compromised domain credentials and other "chatter" by malicious actors on the Dark Web to provide input into their security score, often in an opaque fashion.

What Security Ratings
Do and Do Not Reveal



Insurance

Security ratings can provide vital information to insurance providers when constructing actuarial models, though they are one of a number of data points. Even security ratings that are correlated with the statistical chance of suffering a material breach cannot by themselves provide enough information to calculate what type of loss is expected.

For example, an organization may contract an external partner to collect and process Personally Identifiable Information (PII) and Payment Card Information (PCI) necessary for their business. If this collection is completely segmented from the original organization's systems, the fact that its network has improperly open ports and unpatched vulnerabilities does not increase the likelihood of a PII or PCI breach. Therefore, additional contextual information is necessary to calculate the true security risk an organization incurs, which a security rating alone does not provide.

Vendor Risk

In a recent survey of security leaders, 56% of respondents said they use security ratings to "identify and manage third-party risk". Even security ratings that are correlated with the statistical chance of suffering a material breach do not provide a complete picture of the risk that a third party injects into an eco-system.

A single number can tell you one organization has a more or less secure environment than another organization, but it does not convey specifically how that affects your organization's risk. A vendor that has a low security rating but does not handle or house any of your sensitive information, or does so only in a securely segmented environment, may still prove to be a suitable candidate for the services they are contracted to provide. Again, contextual information is necessary to make a final decision

What Security Ratings
Do and Do Not Reveal (continued)

Acquistion Targets

In an acquisition, any risk that exists in an acquired entity transfers to the acquirer. This is a driving factor in the Gartner prediction that in the next several years, security ratings will be a consideration in the majority of all M&As.

A security rating alone can provide a useful data point in a more complex model when making the decision about whether or not to proceed with a planned acquisition. In the absence of additional contextual information, however, it can't provide a complete road map about how to reduce that risk in the case of an acquisition that has already occurred, or one that proceeds in spite of a low security rating. Even security ratings products that are transparent about how their ratings are calculated can't prioritize the most urgent and economical fixes to these problems

Self-Assessments

If an organization is making programmatic security changes, a security score can provide useful insight into the impact these changes are having. An increase in rating is a powerful metric to justify ROI for security investments to board members and officers.

Relying only on security scores to identify weaknesses in security programs is more problematic, however. Reliance on IP Reputation, or scans for misconfigurations and unpatched vulnerabilities, will tell you THAT there is a problem but not WHY there is a problem. Delivering a list of common vulnerabilities and exposures (CVEs) gives an IT team a list of tasks to be completed, but those problems exist for a reason, and without an analysis of why, for example, the patch management program is not functioning correctly, the same problem will occur in the future.

Mitigating Risk Through Enterprise Security

At the foundational level, all security programs are attempts to mitigate risk, and risk can be introduced through multiple vectors in an organization, not just technical or network vulnerabilities. Security ratings that are heavily based on IP Reputation and external scans for open proxies or misconfigurations can determine that a high volume of spam or viruses originate from an IP range, or that misconfigurations exist. Security ratings based on internal vulnerability scans can tell you that unpatched vulnerabilities exist and are not being patched. But in both cases, while the rating exposes the vulnerability, it can't tell you why it exists.

Does the organization have policies and procedures that should mitigate the risk? Are the policies and procedures not being followed? Are there other factors involved? A security rating scheme that depends solely on these factors, even if the rating system is transparent and shares that information with the scanned entity, cannot answer those underlying questions. Subsequently, although the target organization may address the acute problems that have resulted in a low rating, whether it be outgoing malware traffic, misconfigurations, or unpatched vulnerabilities, the chronic conditions that caused those acute problems will remain, and those conditions are likely to recur later.

Symptoms Point to Greater Security Health Problems

The only way to address these underlying questions is to assess the health of an organization's security program. An analysis of an organization's strategy for dealing with security risks, as well as the governance functions that ensure that strategy is consistently implemented at the operational level through effective controls, is necessary to discover the deficits that are allowing vulnerabilities to occur and recur.

3 Reasons Security Goes Beyond the Perimeter

Ransomware is the most prevalent variety of malicious software and is now impacting business-critical systems, not only desktops.

We advise: Companies must understand which systems are business-critical and create layered security around them, including the use of encryption and back-ups.

People are a key weakness, with employees falling victim to phishing and social attacks.

We advise: Ongoing education, training, and testing of employees.

Most breaches are financially motivated. Finance employees receive phony wire transfer emails impersonating the C-suite. HR departments are increasingly targeted to obtain W-2 data to file fraudulent tax returns.

We advise: A cross-departmental approach to understand risk and ensure enterprise security, plus stronger governance around policies and procedures.

SOURCE: 2018 Verizon Data Breach Investigations Report

• If a vulnerability is unpatched, a patch management program has failed to patch it.
• If a vendor has not agreed to necessary security controls when dealing with a partner's data, it is likely because those controls were not stipulated in a contract.
• If personnel are handling confidential or sensitive information in inappropriate ways that put that information in danger of compromise, it may be the result of a lack of training on information handling policies, or the absence of information policies entirely.

These deficits, and therefore the fixes, are not limited to the technical. They are also reliant on personnel, policies, and procedures, which no scan or network monitoring tool can rectify. Without a discovery method to reveal these shortfalls, analyze them, and develop a strategy to mitigate them, they are likely to remain uncorrected and continue to result in technical and non-technical vulnerabilities.

Enterprise Security Assessments
Support Holistic Security

The Secure Halo Enterprise Security Assessment (ESA) and the Secure Halo online assessment produce a security rating - the Customer Risk Profile (CRP) score - which can be tracked over time or compared within and across industries. The Secure Halo methodology provides granular data that delivers context and insight, and which can be used to strategically address the root cause of shortcomings and build from strengths.

The assessment process examines information security from the perspective of six Domains: Data Security, Physical Security, Internal Business Operations, External Business Operations, Mobile Security, and Insider Threat. These domains are divided into control families and control objectives. The report produced for the ESA or Secure Halo online assessment customer contains detail about every control that is evaluated, as well as recommendations to address weaknesses.

During an ESA, controls are evaluated by certified proctors who assess not only the completeness and maturity of the control's implementation, but also provide context by examining the business risk that the control is designed to mitigate. During a review period, clients can request information on elements used in the calculation of the final scores or discuss the cause of any negative findings. The algorithm for the calculation of the CRP and other scores is explained to the client upon request. All results are confidential and delivered only to the client.

Assessment Enables Governance Critical to Security

The Secure Halo assessment is a more in-depth process than other security rating tools, and doesn't rely upon automated scans, whether external or internal. Through the focus on multiple Domains, it examines settings and configurations for adherence to standards and best practices, but it also examines the programs, governance, and management that either enforce conformity or allow non-conformity with the preferred state.

Most importantly, the assessment provides actionable information to address why the problems that exist are occurring. For example, rather than simply telling you that you have unpatched vulnerabilities, it tells you where the weak points are in your Patch Management, Change Control, and Change Management programs so you can begin curing the disease, rather than just chasing the symptoms.

With this approach, the Secure Halo Enterprise Security Assessment and Secure Halo online assessment provide the programmatic information that puts any security rating in context. This is particularly important for identifying what the weaknesses in your current security program are, rather than just identifying that weaknesses exist. And since Secure Halo puts this programmatic information in context, we are able to provide recommendations on how to address these weaknesses.

> "Business leaders who need to align security with business objectives demand stronger insights into the impact of their security investments on their corporate ecosystem. An assessment provides comprehensive measurement of security maturity across physical, technical, and procedural controls."

This is particularly useful whether you need to demonstrate security program improvements for compliance or insurance, weed out high-risk vendors and partners, or conduct M&A due diligence.

Secure Halo supports the use of security ratings generated by IP Reputation monitoring, or internal or external scans as one part of a security assessment strategy. Proper use cases for these types of ratings should be analyzed, and their shortcomings recognized. In cases where a simple metric for comparison is all that is needed, any security rating that is sufficiently widely used to provide a basis for comparison is suitable.

The Enterprise Security Assessment and Secure Halo online assessment are more suitable to identify and fix specific weaknesses in security programs. Since they provide specific and programmatic recommendations to address shortcomings, they can also offer a roadmap to make these improvements. A security rating that provides a reliable metric (including the Secure Halo CRP score) can then be used to measure the effects of this effort.

SECURE HALO

About Secure Halo

Companies need meaningful insight into how vulnerable they are to expanding and evolving digital risks. Secure Halo provides enterprise cyber risk assessments, managed services, and cybersecurity consulting to Fortune 500 companies and federal agencies. Our Secure Halo™ platform provides a holistic view of cyber risk to empower market-driven and threat-based decisions, while also meeting regulatory requirements.

Learn more at www.securehalo.com