How Does Scoring Work?

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

Tower 49 12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

To level the playing field, SecurityScorecard developed a statistically robust method to adjust and compare scores for large and small organizations.

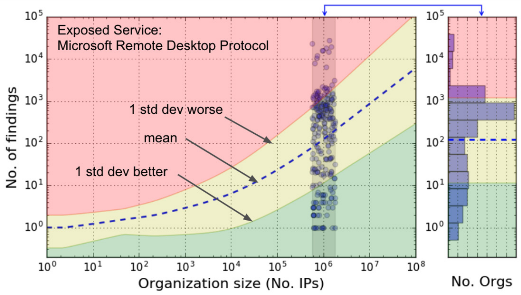
It starts with attribution and continuous monitoring

SecurityScorecard non-intrusively scans the entire IPv4 webspace at a regular cadence. Cloud-based assets are scanned every two hours. Other assets are scanned at a slower pace. In addition, we use domain name system (DNS) records, domain registration information, transport layer security (TLS) certificates, and other data sources to find related domains and subdomains belonging to an organization. Notably, the attribution process identifies and removes from the scoring pipeline shared and low-risk assets, such as content delivery networks (CDNs) and parked domains.

The scans reveal the possible presence of more than 40,000 different common vulnerabilities and exposures (CVEs), exposed ports, weak ciphers, and more than 100 other types of cybersecurity flaws of varying severity. In addition, SecurityScorecard operates one of the largest networks of sinkholes worldwide to capture malware signals emanating from an organization's servers or end-user computers.

Leveling the playing field - size matters!

The organizations we scan have an enormous range in size, from a handful of web pages to a network of millions of IPs. A company with a large digital footprint (DF) has more ways of being attacked than a company with a small one. Therefore, if left alone, large organizations would have poorer scores than small ones. Meaningful comparisons would be difficult.



The solution is that high school staple: the standard deviation from the mean. For each issue type that we measure, we group organizations by similar DF size (e.g. the number of IPs) and determine an average number of vulnerabilities using a logarithmic scale. After scanning and measuring a single organization's vulnerabilities, we calculate - in terms of standard deviations - the distance above or below the average for that size. This is known as a z-score, and gives us a valid number for comparisons between organizations of different sizes.

Calculating the score

Total and Factor Scores are reported on a scale of 0 to 100 with an associated letter grade. The Total Score indicates an overall grade for cybersecurity posture. The Factor Score is a score given for each different sub-category.

These scores are calculated from:

- the severity level of the findings, and
- their associated z-scores.

To get there, we start at the level of the issue type. Every issue type has a severity level (high, medium, low), assigned by external authorities, such as the industry's Common Vulnerability Scoring System (CVSS), or subject matter experts.

Issue types are topically grouped into factors, e.g. Network Security, Application Security, etc. (See Appendix for all 10 factors.). We calculate a score for each factor. The Factor Scores are calculated by:

1. multiplying the z-score for each observed issue type in the factor by its associated severity-based issue weight,
2. summing these, scaling the result, and
3. subtracting the weighted sum from 100, which is the maximum score.

Showing the Math

The Factor Score is given by:

$$FS = 100 - k\sum_i w_i \times z_i$$

where FS is the Factor Score; w_i is the severity-based weight for issue i; z_i is the organization's z-score for issue type i; and k is a scaling constant.

Once we have scores for each factor, we can calculate the Total Score. The Total Score is calculated as the weighted average of the Factor Scores:

$$TS = \sum_f w_f \times FS_f$$

where TS is the Total Score; FS_f is the Factor Score for factor f; and w_f is the factor weight. Factor weights have been derived using a data-driven approach described in the Validation section below.

Score	Grade
≥ 90	A
80 to 90	B
70 to 80	C
60 to 70	D
< 60	F

Once we have scores for each factor, we can calculate the Total Score. The Total Score is calculated as the weighted average of the Factor Scores. Factor weights have been derived using a data-driven approach described in the Validation section below.

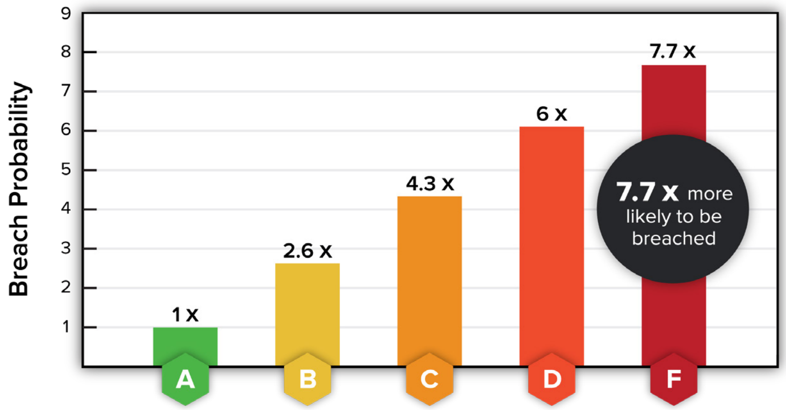
Improving your score through remediation

The scores given by our system are not permanent. Correcting issue findings (remediation) improves the score. Notably, remediating a given percentage of findings with a given severity (rather than the absolute number) will increase the score by a set number of points. For example, if there are 200 findings of a particular type, fixing, say, 10 percent of them (20 findings) would elevate the score by X points. If 10 percent of the remaining 180 issues were resolved (18 findings), the score would again be lifted by another X points. It's the relative, rather than the absolute, reduction in the number of findings that increases the score by a given amount.

Validating the score

Cybersecurity ratings should correlate with cybersecurity risk. SecurityScorecard uses machine learning to tune the factor weights w_f so that total scores would be optimally correlated with the relative risk of breach. Analyzing scores of 100,000 organizations over a three-year period, including 2,200 breaches, we found that organizations with a low score (F) were 7.7x more likely to incur a breach than ones with a high score (A). We believe this performance to be best-in-class.

Companies with a better SecurityScorecard rating are more resilient



7.7 x more likely to be breached

Appendix

These are the 10 factors that we score.

Factor	Description	Factor	Description
Network Security	open ports (such as SMB and RDP), insecure or misconfigured SSL certificates, database & IoT vulnerabilities.	**DNS Health**	misconfigurations like Open Resolvers, & recommended configurations for DNSSEC, SPF, DKIM, & DMARC.
Application Security	vulnerabilities, misconfigurations, & best practices on publicly detected web apps.	**Hacker Chatter**	underground & dark web discussions about targeted orgs & IP addresses.
IP Reputation	Sinkhole system ingests millions of malware signals and maps infected IP addresses back to impacted organizations.	**Information Leak**	credentials exposed by a data breach or leak, keylogger, pastebin, & database dumps, & other information repositories.
Endpoint Security	exploitability of laptops, desktops, mobile devices, & BYOD devices on the network.	**Social Engineering**	corporate accounts in social networks, financial accounts, & marketing lists.
Patching Cadence	frequency of updates for an organization's identified services, software, & hardware.	**Cubit Scores**	critical security & configuration issues, like exposed administrative control panels

Looking for more insights into how our scoring process works? Click here to learn more!

ABOUT SECURITYSCORECARD

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base. SecurityScorecard continues to make the world a safer place by transforming the way organizations understand, improve and communicate cybersecurity risk to their boards, employees, and vendors. Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating.

FOR MORE INFORMATION, VISIT OUR TRUST PORTAL FOR A DEEPER DIVE INTO OUR SCORING METHODOLOGY TRUST.SECURITYSCORECARD.COM OR CONNECT WITH US ON LINKEDIN.

SecurityScorecard.com

info@securityscorecard.com

Tower 49 12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

SecurityScorecard