SecurityScorecard

Why you can trust SecurityScorecard ratings

Security rating companies use a combination of data points collected organically or purchased from public and private sources and then apply proprietary algorithms to articulate an organization's security effectiveness into a quantifiable score.

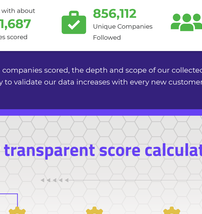
SecurityScorecard provides transparency into our ratings methodology and delivers insights into how it aligns with industry standards. Understand the principles, methodology, and process behind how our cybersecurity ratings work.

It starts with guiding principles

U.S. Chamber of Commerce

In conjunction with the US Chamber of Commerce and other security ratings experts, SecurityScorecard helped shape and then adopted these guiding principles for fair and accurate security ratings.

The Guiding Principles:



Then the data is collected and the score is calculated

More than **255 million** infected IPs over 235 malware families identified daily

Upwards of **100,000,000,000** vulnerabilities and attributions published weekly

SecurityScorecard non-intrusively collects data from publicly available commercial and open source feeds across the internet for a non intrusive, outside-in, hacker perspective of a company's cybersecurity posture.

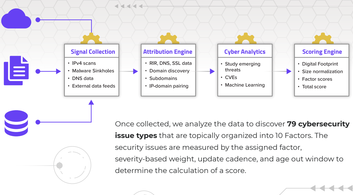
Currently with about **12,101,687** companies scored

856,112 Unique Companies Followed

2,034 Logged Into The Platform Today

With over 12.1 million companies scored, the depth and scope of our collected data is unmatched, and our ability to validate our data increases with every new customer and follower.

Our transparent score calculation



Once collected, we analyze the data to discover **79 cybersecurity issue types** that are topically organized into 10 Factors. The security issues are measured by the assigned factor, severity-based weight, update cadence, and age out window to determine the calculation of a score.

Risk Factors

Application Security · Social Engineering · Patching Cadence · Network Security · IP Reputation

Hacker Chatter · Cubit Score · DNS Health · Endpoint Security · Information Leak

How accurate are our scores?

Companies with an **F rating are 7.7x** more likely **to suffer a data breach** versus those with an A rating.

Improving your score

See something that doesn't look right or you fixed a vulnerability we brought to your attention?

Companies can dispute or remediate any finding associated with their company score.

Dispute
Risk was incorrectly associated & should be removed

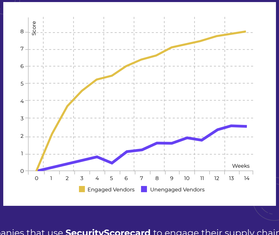
Correction
Provide clarifying data about a compensating control in place

Appeal
The company resolved the risk

SecurityScorecard maintains a response time for resolving customer-submitted refutes that is well within the **48-hour** service level agreement. Scores are then updated within 4 to 7 business days.

SecurityScorecard reports a low False Positive error rate for both IP and domain attribution (less than 2% over 7-day trailing average) based user-submitted refutes.

Improving more than just your score



Companies that use **SecurityScorecard** to engage their supply chain see a quantifiable improvement in their ecosystem security posture.

On average, rated companies that are invited to the platform with low security grades (C, D, or F) typically exhibit an **average a 7 to 8 point score** improvement within 3 months.

See this information and more, in real time by visiting our trust portal.

trust.securityscorecard.com

Gain access to your own score by signing up for a free account.

securityscorecard.com/free-account