

DATASHEET

Applying AI-Driven Methodologies to Generate More Meaningful Cybersecurity Ratings

SecurityScorecard leads the industry in breach predictability with its new scoring algorithm

Across the globe, organizations are working to avoid the financial, operational, and reputational damage that can follow a data breach. Many of these events are caused by third-party suppliers, which highlights the need for companies to not only monitor their own security posture, but that of their vendors as well. Companies are now relying on security ratings to understand how a company's cybersecurity posture correlates with the likelihood of sustaining a data breach.

SecurityScorecard continuously rates **more than 12 million companies** across a range of sizes, industry sectors, and geographical locations. Analyzing a growing collection of cybersecurity data allows us to quickly understand and monitor the cyber health of organizations to provide SecurityScorecard users with valuable and unique insights.

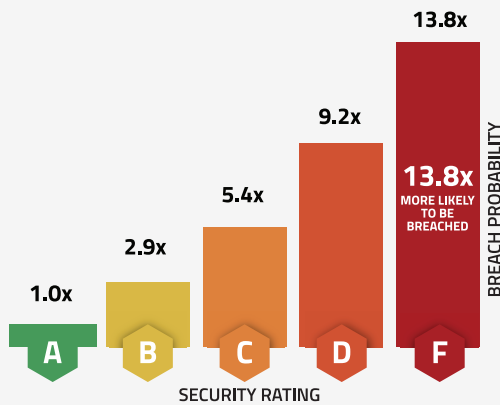
Scoring 3.0 has applied fine-tuned machine learning (ML) to ensure that our letter grades are maximally correlated with the relative probability of sustaining a data breach. This allows organizations to make more informed, risk-based business decisions based on the most accurate data available.

DATA BREACH REACHED AN ALL-TIME HIGH COST OF USD

4.45M

"The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million, according to the 2023 "Cost of a Data Breach Report" by IBM and the Ponemon Institute.

<https://www.ibm.com/downloads/cas/E3G5JMBP>



Companies with a higher SecurityScorecard Rating are less likely to sustain a breach

By applying machine learning-tuned issue type weights, we found that **organizations with an F rating are 13.8x more likely to sustain a breach than those with an A rating**. With our innovative scoring the correlation of SecurityScorecard Ratings and relative breach likelihood has improved by 79%. Generating a rating based on issue types rather than factor weights makes the overall score easier to interpret and more indicative of score impacts.

Unparalleled Precision and Insight with Enhanced Scoring Methodology



Over **15,000 publicly disclosed data breaches** analyzed from companies of different sizes & industries



The organizations studied are geographically diverse and span **18 different industrial sectors**

To create the industry's most sophisticated and data driven algorithm, SecurityScorecard leveraged the power of Data Science and Machine Learning. Through analysis of over 15,000 breaches, we pinpointed issue types with predictive capabilities for breaches, systematically assigning risk-based weights to optimize performance. This analytical process sets a new standard for precision in security ratings.


Setting the Bar: Elevating Precision in Security Ratings


SecurityScorecard ratings have always been a reflection of everything we scan **on a daily basis**. Our scanning infrastructure operates at scale, detecting IPs and domains to attribute to a digital footprint while also discovering vulnerabilities on an organization's attack surface. The detected findings are displayed on an issues types page, which are categorized in different risk factor groups.

Our overall A-F scores are a direct representation of a weighted average of all detected issues. The overall score is not influenced by factor weights, making our ratings easier to understand and monitor. Read more about our scoring methodology in our [Trust Portal](#).

More Meaningful Scores

By utilizing a data-driven model to optimize the weighting of our 200+ issue types, SecurityScorecard provides users with a better understanding of relative breach likelihood, enabling more informed business and security decisions.

 With over 10 years of crowdsourcing historical data, one of the world's largest malware DNS sinkhole with 2B+ malware requests per day, and analysis of 100B+ daily signals and crowd-sourced intel, SecurityScorecard uses a greater sample of significant data to better train our scoring algorithms, leading to increased accuracy and breach predictability.

 With Ratings that are highly correlated with breach likelihood, SecurityScorecard helps cybersecurity practitioners and risk managers more accurately assess both enterprise and third-party risk. Only rely on the most meaningful ratings when it comes to protecting your company from cyber risk.



SECURITYSCORECARD'S 10 RISK FACTOR GROUPS

- 1 Application Security
- 2 Cubit Score
- 3 DNS Health
- 4 Endpoint Security
- 5 Hacker Chatter
- 6 Informational Leak
- 7 IP Reputation
- 8 Network Security
- 9 Patching Cadence
- 10 Social Engineering



Best predictor of breach in the industry

Fine-tuned machine learning models and more balanced score distribution.



Easy to interpret A-F ratings

Remove factor level weights, allowing the overall score to be a direct representation of issue types.



Assess a company's risk at a glance

An organization with an 'F' grade will be 13.8x more likely to be impacted by a breach compared to an organization with an 'A' rating.

VIEW AND IMPROVE YOUR ORGANIZATION'S SECURITY RATING FOR FREE

Please visit securityscorecard.com/free-account-trial



SecurityScorecard.com
info@securityscorecard.com

©2024 SecurityScorecard Inc. All Rights Reserved.