SecurityScorecard

DETAILED REPORT

Scorecard for SecurityScorecard Demo

Generated **January 9, 2025**
by Jessica Cheng (jessica.cheng@securityscorecard.io), SecurityScorecard, Inc

About this report
This report is a point-in-time capture of this Scorecard as of 6:19:27 AM UTC, January 9, 2025. It should not be confused with a pen test result or a final assessment.

Get the full picture with SecurityScorecard
SecurityScorecard offers ongoing self-monitoring, history reports, CSV data exports, and more to help security teams protect their organizations. For full free access to your organization's Scorecard, create an account today at bit.ly/2P8okyb.

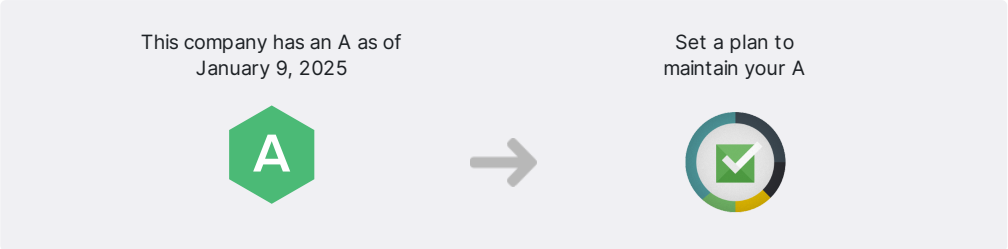
Learn more about SecurityScorecard at bit.ly/2xXNg4N today.

What is SecurityScorecard?

SecurityScorecard is a security ratings service that uses an easy-to-understand A-F grading system to rate companies on their overall security as well as across 10 major risk factors. A company with a C, D, or F rating is 5.4 times more likely to suffer a consequential breach versus A or B-rated companies1. Certain risk factors, such as application security and patching cadence, are even more indicative of the likelihood of breach. An F versus an A in these factors may translate into a tenfold increase in the likelihood of a data breach or successful attack.

Learn more about SecurityScorecard's rating system at bit.ly/2zMLSmW.

Next Steps: Stay at an A



1. Create an account

This file has a lot of detail but remember, it's only for one point in time. Create an account to get full free access to your organizaton's Scorecard along with continuous self-monitoring, history reports, CSV data exports, and more.

2. Validate your Digital Footprint

Once you have an account, review your company's Digital Footprint, the assets SecurityScorecard found as potentially attributable to your company, that affect the ratings in your Scorecard. Request removal or addition of IPs as needed.

3. Review issue findings

Investigate the contents of your Scorecard with your team(s). It's a win for your company's security posture when you identify loose ends of which you weren't aware.

4. Spot new issues, maintain your A

Whether you've deployed a fix, found assets that don't belong to your company, or want to share information about compensating controls, you can let us know by remediating the identified finding(s) and submitting them for resolution approval. Resolutions are handled by our Support team, which will resolve any outstanding item within three business days. Remediate issues within the platform or email support@securityscorecard.com.

We're here to help

The SecurityScorecard platform is based on transparency and collaboration. Our Customer Reliability Support team provides remediation and resolution services at no charge and are happy to work with you and your customers to resolve any issues. If you need assistance at any stage, get in touch by emailing support@securityscorecard.io.

Scorecard Overview

A

SecurityScorecard Demo

97 Security Score

DOMAIN: securityscorecardsales.com

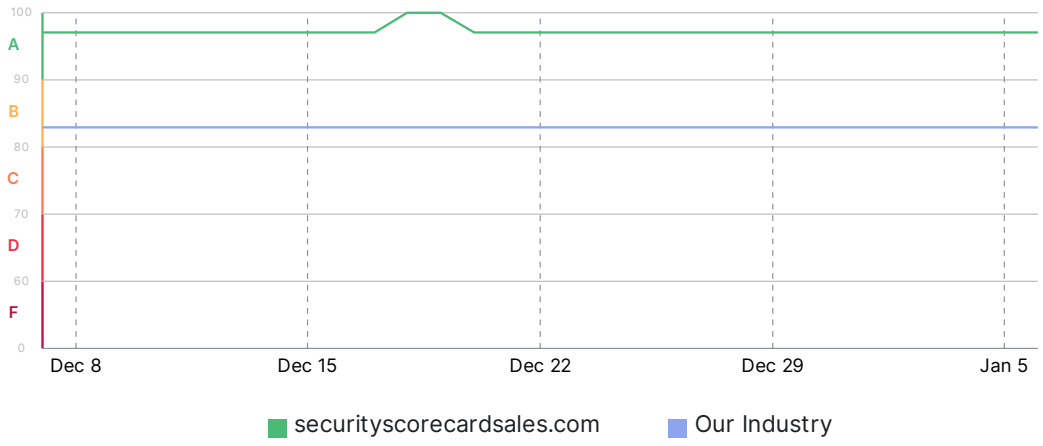
INDUSTRY: Technology

Factors

A	100	APPLICATION SECURITY	0 ISSUES		
A	100	CUBIT SCORE	0 ISSUES		
A	90	DNS HEALTH	1 ISSUE		
A	100	ENDPOINT SECURITY	0 ISSUES		
A	100	HACKER CHATTER	0 ISSUES		
A	100	IP REPUTATION	0 ISSUES		
A	100	INFORMATION LEAK	0 ISSUES		
A	100	NETWORK SECURITY	0 ISSUES		
A	100	PATCHING CADENCE	0 ISSUES		
A	100	SOCIAL ENGINEERING	0 ISSUES		

30-Day Score History

The chart below shows the evolution of the company's relative security ranking over time. Peaks in score performance represent improvements to overall security, remediation of open isues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.



Action Items

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
DNS Health		-7.4	SPF Record Missing. Not having an SPF (Sender Policy Framework) record poses several risks for domain owners. Malicious actors can easily spoof email addresses associated with the domain, leading to phishing attacks, spam distribution, and other forms of email fraud. This can damage the domain's reputation and cause legitimate emails to be marked as spam or rejected by recipient servers. Additionally, without SPF protection, domain owners have limited control over who can send emails on behalf of their domain. This makes it harder to maintain the integrity and security of their email communications.

A 100 APPLICATION SECURITY

The Web Application Vulnerability module uses incoming threat intelligence from known exploitable conditions identified via: whitehat CVE databases, blackhat exploit databases, and sensitive findings indexed by major search engines. The module ingests data from multiple public data sets, third party feeds, and an internal proprietary indexing and aggregation engine.
The score determines the likelihood of an upcoming web application breach, and checks for any existing defacement code. Presence of vulnerable applications, outdated versions, and active defacements are used to calculate the overall grade.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Application Security	There are no Medium Severity Issues for Application Security	There are no Low Severity Issues for Application Security

No issues found

A 100 CUBIT SCORE

This proprietary module measures a variety of security issues that a company might have. For example, we check public threat intelligence databases for IP addresses that have been flagged. These misconfigurations may have high exploitability and could cause significant harm to the privacy of your data and infrastructure

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Cubit Score	There are no Medium Severity Issues for Cubit Score	There are no Low Severity Issues for Cubit Score

No issues found

A 90 DNS HEALTH

This module measures the health and configuration of a company's DNS settings. It validates that no malicious events occurred in the passive DNS history of the company's network. It also helps validate that mail servers have proper protection in place to avoid spoofing. It also helps verify that DNS servers are configured correctly.

HIGH SEVERITY		MEDIUM SEVERITY		LOW SEVERITY
There are no High Severity Issues for DNS Health		SPF Record Missing	1	There are no Low Severity Issues for DNS Health

SPF Record Missing

-7.4 SCORE IMPACT

Not having an SPF (Sender Policy Framework) record poses several risks for domain owners. Malicious actors can easily spoof email addresses associated with the domain, leading to phishing attacks, spam distribution, and other forms of email fraud. This can damage the domain's reputation and cause legitimate emails to be marked as spam or rejected by recipient servers. Additionally, without SPF protection, domain owners have limited control over who can send emails on behalf of their domain. This makes it harder to maintain the integrity and security of their email communications.

Description

An SPF (Sender Policy Framework) record is a DNS (Domain Name System) record used to prevent email spoofing and unauthorized use of a domain. It specifies which mail servers are allowed to send emails on behalf of a domain by listing authorized sending IP addresses or domain names. When an email is received, the recipient's mail server can check the SPF record of the sender's domain to verify the authenticity of the sender's identity. If the sending server is not listed in the SPF record, the recipient's server may mark the email as potentially fraudulent or reject it altogether.

Recommendation

- Create an SPF record for your domain that specifies authorized sending servers.
- Implement strict DMARC (Domain-based Message Authentication, Reporting, and Conformance) policies to enforce email authentication and protect against spoofing.
- Consider implementing additional email security measures such as DKIM (DomainKeys Identified Mail) and DMARC to enhance email authentication and protection.
- Educate users about phishing threats and encourage vigilance when handling suspicious emails.
- Regularly review and update the SPF record to reflect changes in your email infrastructure.

1 finding

DOMAIN	LAST OBSERVED
securityscorecardsales.com	1/5/2025, 10:28:35 PM

A 100 ENDPOINT SECURITY

The Endpoint Security Module tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins. The information gathered allows companies to identify outdated versions of these data points which can lead to client-side exploitation attacks.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Endpoint Security	There are no Medium Severity Issues for Endpoint Security	There are no Low Severity Issues for Endpoint Security

No issues found

A 100 HACKER CHATTER

The SecurityScorecard Hacker Chatter module is an automated collection and aggregation system for the analysis of multiple streams of underground hacker chatter. Forums, IRC, social networks, and other public repositories of hacker community discussions are continuously monitored, collected and aggregated in order to locate mentions of business names and websites. The Hacker Chatter score is an informational indicator ranking that is ranked based on the quantity of indicators that appear within the collection sensors.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Hacker Chatter	There are no Medium Severity Issues for Hacker Chatter	There are no Low Severity Issues for Hacker Chatter

No issues found

A 100 IP REPUTATION

The IP Reputation and Malware Exposure module makes use of the SecurityScorecard sinkhole infrastructure as well as a blend of OSINT malware feeds, and third party threat intelligence data sharing partnerships. The SecurityScorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures globally from all over the world. The incoming data is processed and attributed to corporate enterprises. The quantity and duration of malware infections are used as the determining factor for calculating is module the Malware Exposure Key Threat Indicator.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for IP Reputation	There are no Medium Severity Issues for IP Reputation	There are no Low Severity Issues for IP Reputation

No issues found

A 100 INFORMATION LEAK

This Information Leak module makes use of chatter monitoring and deep web monitoring capabilities to identify compromised credentials being circulated by hackers. These come in the form of bulk data breaches announced publicly as well as smaller breaches, and smaller exchanges between hackers

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Information Leak	There are no Medium Severity Issues for Information Leak	There are no Low Severity Issues for Information Leak

No issues found

A 100 NETWORK SECURITY

The Network Security module checks public datasets for evidence of high risk or insecure open ports within the company network. Insecure ports can often be exploited to allow an attacker to circumvent the login process or obtain elevated access to the system. If misconfigured, the open port can act as the entry point between a hacker's workstation and your internal network

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Network Security	There are no Medium Severity Issues for Network Security	There are no Low Severity Issues for Network Security

No issues found

A 100 PATCHING CADENCE

The Patching Cadence module analyzes how quickly a company reacts to vulnerabilities to measure patching practices. We look at the rate at which it takes a company to remediate and apply patches compared to peers.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Patching Cadence	There are no Medium Severity Issues for Patching Cadence	There are no Low Severity Issues for Patching Cadence

No issues found

A 100 SOCIAL ENGINEERING

The SecurityScorecard Social Engineering Module is used to determine the potential susceptibility of an organization to a targeted social engineering attack. The Social Engineering module ingests data from social networks and public data breaches, and blends proprietary analysis methods. The Social Engineering Score is an informational indicator calculated based on the quantity of indicators that appear in SecurityScorecard collection sensors.

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
There are no High Severity Issues for Social Engineering	There are no Medium Severity Issues for Social Engineering	There are no Low Severity Issues for Social Engineering

No issues found

No content (including ratings, data, reports, software or other application or output therefrom) or any part thereof (collectively, Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system without the prior written permission of SecurityScorecard, Inc. (SSC) The Content shall not be used for any unlawful or unauthorized purposes.

SSC and any third-parties, and their directors, officers, shareholders, employees, customers and agents (collectively SSC Parties) do not guarantee or warrant the accuracy, completeness, timeliness or availability of the Content. SSC Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of the Content. The Content is provided on an "as is" basis. SSC PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS,(3) FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall SSC Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

USERS OF THE CONTENT MUST USE ALL REASONABLE ENDEAVORS TO MITIGATE ANY LOSS OR DAMAGE WHATSOEVER (AND HOWSOEVER ARISING) AND NOTHING HEREIN SHALL BE DEEMED TO RELIEVE OR ABROGATE USERS OF ANY SUCH DUTY TO MITIGATE ANY LOSS OR DAMAGE.

IN ANY EVENT, TO THE EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF THE SSC PARTIES FOR ANY REASON WHATSOEVER RELATED TO ACCESS TO OR USE OF CONTENT SHALL NOT EXCEED THE GREATER OF (A) THE TOTAL AMOUNT PAID TO SSC BY THE USER FOR SERVICES PROVIDED DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY, AND (B) U.S. $100.

Security-related analyses, including ratings and statements in the Content, are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SSC's opinions, analyses and ratings should not be relied on as a substitute for the skill, judgment and experience of the user and its management, employees, advisors and clients when making business decisions. SSC assumes no obligation to update the Content following publication in any form or format. While SSC has obtained information from sources it believes to be reliable, SSC does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Users expressly agree that (a) the security ratings and other security opinions provided via the Content do not reflect, identify or detect every vulnerability or security issue or address any other risk; (b) the security ratings and other opinions provided do not take into account users' particular objectives, situations or needs; (c) each rating or other opinion will be weighed, if at all, solely as one factor in any decision made by or on behalf of any user; and (d) users will accordingly, with due care, make their own study and evaluation of the risks of doing business with any entity. If a user identifies any in the Content, we invite you to share that information with us by emailing us at support@securityscorecard.io.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements ofcurrent or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts toindependently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS ANDDEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.The views and opinions expressed in any comment in this Company's Scorecard are those of the authors of such comments, and do not reflect the official policy, position or views of SecurityScorecard or any other entity.