



DETAILED REPORT

Scorecard for Hailongoffshorewind

Generated **April 30, 2025**

by Stanislav Kalynych (stanislav.kalynych@northlandpower.com), Northland Power

About this report

This report is a point-in-time capture of this Scorecard as of 9:00:29 PM UTC, April 30, 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.

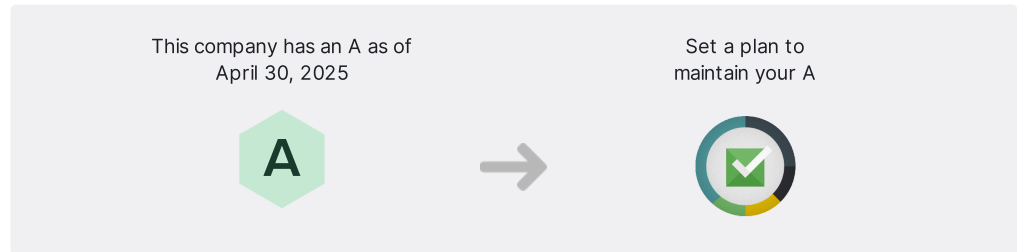
Learn more about SecurityScorecard at bit.ly/2xXNg4N today.

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 organization'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 via the [Support Portal](#).

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 via the [Support Portal](#).

Scorecard Overview



Hailongoffshorewind
93 Security Score

DOMAIN: hailongoffshorewind.com

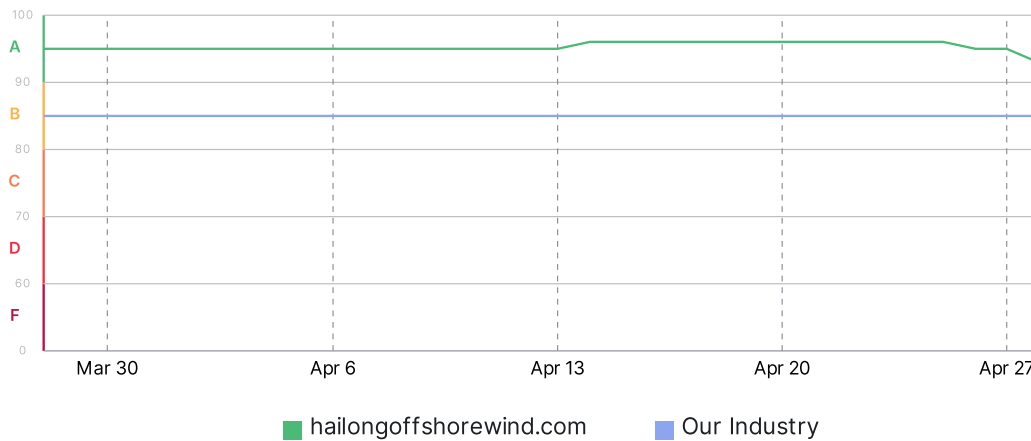
INDUSTRY: Technology

Factors

B 80	APPLICATION SECURITY	6 ISSUES	A 100	IP REPUTATION	0 ISSUES
A 100	CUBIT SCORE	0 ISSUES	A 100	INFORMATION LEAK	0 ISSUES
A 100	DNS HEALTH	0 ISSUES	A 100	NETWORK SECURITY	0 ISSUES
A 100	ENDPOINT SECURITY	0 ISSUES	A 100	PATCHING CADENCE	0 ISSUES
A 100	HACKER CHATTER	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 issues, 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
Application Security		-2.4	Unsafe Implementation Of Subresource Integrity. Without SRI, externally loaded resources, like scripts and stylesheets, lack integrity verification. This makes them susceptible to tampering. This creates a potential avenue for attackers to inject malicious scripts, which leads to Cross-Site Scripting (XSS) vulnerabilities, unauthorized data access, and other security threats.
		-0.3	Website Does Not Implement HSTS Best Practices. Not implementing HTTP Strict Transport Security (HSTS) means potentially exposing websites to man-in-the-middle attacks and potential security breaches. Without HSTS, malicious actors could exploit vulnerabilities such as protocol downgrades or cookie hijacking, compromising the confidentiality and integrity of sensitive user data. The absence of a strict policy directing browsers to enforce secure connections over HTTPS increases the likelihood of attackers intercepting and manipulating communication between users and the website. HSTS serves as a crucial defense mechanism. Its absence leaves web applications more vulnerable to various forms of unauthorized access and data interception.
		-0.2	Content Security Policy Contains 'unsafe-*' Directive. The use of "unsafe" directives in a Content Security Policy (CSP) introduces significant security risks. The 'unsafe-inline' and 'unsafe-eval' pose a heightened risk of Cross-Site Scripting (XSS) attacks and code injection. These directives compromise the application's security by expanding the attack surface and potentially allowing malicious code to execute within the trusted domain. Additionally, they undermine the intended security of a CSP and reduce the effectiveness of the policy protecting against web-based threats.
		-2.1	Site does not enforce HTTPS. Not enforcing HTTPS poses significant dangers to the security and integrity of online communication. Without it, sensitive data exchanged between users and websites is susceptible to the following: - Interception by malicious actors. This could lead to breaches and unauthorized access. - Identity spoofing. Attackers impersonate legitimate sites to trick users into providing confidential information. - Data tampering. This enables attackers to change data or add malicious content. It can also result in trust issues. Modern browsers warn users about unsecure connections that can undermine the credibility of the website. Additionally, search engines penalize non-HTTPS sites, affecting their rankings and visibility, and reducing their ability to compete in online searches.
		-1.2	Website does not implement X-Content-Type-Options Best Practices. Not using the "X-Content-Type-Options" header poses several risks, including the potential for MIME type sniffing vulnerabilities. Without this header set to "nosniff," browsers may attempt to interpret content based on heuristics, leading to security vulnerabilities and the risk of executing malicious scripts. This could expose websites to cross-site scripting (XSS) attacks where attackers inject harmful code into the content. Additionally, the absence of the header may result in inconsistencies across different browsers, impacting the reliable interpretation of content types and potentially compromising the security and integrity of web applications.
		-0.3	Site emits visible browser logs. The risk of emitting browser logs lies in the potential exposure of sensitive information to unauthorized parties. These logs may inadvertently disclose user credentials, personally identifiable information, or other confidential data, which can be exploited by malicious actors for identity theft, fraud, or other nefarious purposes. Additionally, exposing internal system details or error messages may provide attackers with insights into potential vulnerabilities or weaknesses within the website's infrastructure.

B⁸⁰ 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	<div>Unsafe Implementation Of Subresource Integrity 1</div> <div>Website Does Not Implement HSTS Best Practices 1</div> <div>Content Security Policy Contains 'unsafe-*' Directive 1</div> <div>Site does not enforce HTTPS 1</div> <div>Website does not implement X-Content-Type-Options Best Practices 1</div> <div>Site emits visible browser logs 1</div>

Unsafe Implementation Of Subresource Integrity

-2.4 SCORE IMPACT

Without SRI, externally loaded resources, like scripts and stylesheets, lack integrity verification. This makes them susceptible to tampering. This creates a potential avenue for attackers to inject malicious scripts, which leads to Cross-Site Scripting (XSS) vulnerabilities, unauthorized data access, and other security threats.

Description

Subresource Integrity (SRI) is a security feature in web development designed to ensure the integrity of externally loaded resources on a webpage. These include scripts, stylesheets, and fonts. With SRI, developers include a cryptographic hash of the expected resource content in the HTML. When a user visits the webpage, the browser checks this hash against the actual content fetched from the external source. If the hashes match, that means the resource hasn't been tampered with or compromised.

Recommendation

- Ensure accurate cryptographic hashes are specified for all externally loaded resources using SRI attributes in the HTML.
- Routinely review and update cryptographic hashes to align with changes in resource content.
- Implement robust input validation and sanitization practices to prevent injection attacks.
- Use CSP to restrict resource sources. This adds an extra layer of control over content execution.
- Conduct regular security audits and penetration testing to promptly identify and address vulnerabilities.

0 findings

DOMAIN	SCHEME	OBSERVATIONS	LAST OBSERVED
--------	--------	--------------	---------------

Website Does Not Implement HSTS Best Practices

-0.3 SCORE IMPACT

Not implementing HTTP Strict Transport Security (HSTS) means potentially exposing websites to man-in-the-middle attacks and potential security breaches. Without HSTS, malicious actors could exploit vulnerabilities such as protocol downgrades or cookie hijacking, compromising the confidentiality and integrity of sensitive user data. The absence of a strict policy directing browsers to enforce secure connections over HTTPS increases the likelihood of attackers intercepting and manipulating communication between users and the website. HSTS serves as a crucial defense mechanism. Its absence leaves web applications more vulnerable to various forms of unauthorized access and data interception.

Description

HTTP Strict Transport Security (HSTS) is a web security mechanism that helps protect websites against man-in-the-middle attacks. When a website is configured with HSTS, it instructs the user's browser to only connect to the server over HTTPS (encrypted connections) and to ignore any attempts to establish unencrypted HTTP connections. This ensures that sensitive information, such as login credentials and session cookies, is transmitted securely. HSTS headers are sent by the server to the browser, indicating the website should only be accessed through secure channels.

Recommendation

- Implement HTTP Strict Transport Security (HSTS) on your web server.
- Configure the HSTS header to instruct browsers to only connect to your website over HTTPS.
- Set an appropriate max-age directive to specify the duration (in seconds) for which the HSTS policy should be enforced.
- Include the 'includeSubDomains' directive, if applicable, extending HSTS protection to subdomains.
- Ensure all resources on your website, including third-party content, are available over HTTPS to avoid mixed content issues.
- Regularly review and update the HSTS policy to adapt to changes in your website and security best practices.
- Test the effectiveness of HSTS implementation to verify that browsers properly enforce secure connections.
- An acceptable HSTS header would declare: "Strict-Transport-Security: max-age=31536000; includeSubDomains;"

1 finding

ANALYSIS	DOMAIN	SCHEME	OBSERVATIONS	FINAL URL	LAST OBSERVED
hsts_missing_subdomain	hailongoffshorewind.com	https	1	https://hailongoffshorewind.com/	4/9/2025, 8:35:30 PM

Content Security Policy Contains 'unsafe-*' Directive

-0.2 SCORE IMPACT

The use of "unsafe" directives in a Content Security Policy (CSP) introduces significant security risks. The 'unsafe-inline' and 'unsafe-eval' pose a heightened risk of Cross-Site Scripting (XSS) attacks and code injection. These directives compromise the application's security by expanding the attack surface and potentially allowing malicious code to execute within the trusted domain. Additionally, they undermine the intended security of a CSP and reduce the effectiveness of the policy protecting against web-based threats.

Description

A Content Security Policy (CSP) is a security standard implemented by web browsers to defend against Cross-Site Scripting (XSS) attacks. It defines rules through HTTP headers that tell the browser which sources are permitted for loading scripts, styles, and other resources on a web page. "Unsafe" directives, such as 'unsafe-inline' and 'unsafe-eval,' offer flexibility, but include security implications. 'Unsafe-inline' allows the execution of inline scripts and styles, while 'unsafe-eval' permits the evaluation of dynamic code.

Recommendation

- Specify trusted sources for scripts and styles using appropriate directives like 'script-src' and 'style-src' instead of relying on 'unsafe-inline.'
- Minimize or eliminate the use of 'unsafe-eval' and refactor code to avoid dynamic code generation, opting for safer alternatives.
- Implement nonce or hash values for inline scripts and styles to allow specific exceptions while maintaining security.
- Strive for a strict and minimalistic CSP configuration, avoiding unnecessary permissions and using secure constructs.

- Periodically review and update the CSP configuration to adapt to changes in the application, dependencies, and emerging security threats.

1 finding

DOMAIN	SCHEME	OBSERVATIONS	FINAL URL	LAST OBSERVED
hailongoffshorewind.com	https	1	https://hailongoffshorewind.co	4/9/2025, 8:35:30 PM
Evidence : "base-uri 'self';default-src 'self' 'strict-dynamic' 'unsafe-inline' https://www.google-analytics.co...				

Site does not enforce HTTPS

-2.1 SCORE IMPACT

Not enforcing HTTPS poses significant dangers to the security and integrity of online communication. Without it, sensitive data exchanged between users and websites is susceptible to the following:

- Interception by malicious actors. This could lead to breaches and unauthorized access.
- Identity spoofing. Attackers impersonate legitimate sites to trick users into providing confidential information.
- Data tampering. This enables attackers to change data or add malicious content.

It can also result in trust issues. Modern browsers warn users about unsecure connections that can undermine the credibility of the website. Additionally, search engines penalize non-HTTPS sites, affecting their rankings and visibility, and reducing their ability to compete in online searches.

Description

HTTPS (Hypertext Transfer Protocol Secure) is a secure version of HTTP, the protocol used for transmitting data between a user's web browser and a website's server. It uses encryption and authentication mechanisms to improve the security of data exchanged.

Recommendation

It's highly recommended to implement HTTPS across all web communications.

- Get an SSL/TLS certificate for the website to enable secure connections.
- Make sure it's properly configured and up-to-date.
- Update all internal and external references to use the "https://" protocol and set up automatic redirects from HTTP to HTTPS to ensure a seamless transition for users.
- Regularly monitor and audit the security configuration to promptly detect and address any vulnerabilities.
- Employ security best practices such as HTTP Strict Transport Security (HSTS).

1 finding

DOMAIN	SCHEME	OBSERVATIONS	FINAL URL	LAST OBSERVED
hailongoffshorewind.com	http	1	http://hailongoffshorewind.co	4/14/2025, 4:19:02 PM
m/				

Website does not implement X-Content-Type-Options Best Practices

-1.2 SCORE IMPACT

Not using the "X-Content-Type-Options" header poses several risks, including the potential for MIME type sniffing vulnerabilities. Without this header set to "nosniff," browsers may attempt to interpret content based on heuristics, leading to security vulnerabilities and the risk of executing malicious scripts. This could expose websites to cross-site scripting (XSS) attacks where attackers inject harmful code into the content. Additionally, the absence of the header may result in inconsistencies across different browsers, impacting the reliable interpretation of content types and potentially compromising the security and integrity of web applications.

Description

The "X-Content-Type-Options" is an HTTP header that enhances web security by influencing how a browser interprets the type of content used in an HTTP response. When set to "nosniff," this header instructs the browser to strictly adhere to the declared content type and refrain from sniffing or interpreting the content in alternative ways. This measure helps prevent potential security issues related to MIME type confusion and promotes a more secure browsing environment by ensuring that the browser accurately processes content as intended by the server.

Recommendation

- Configure your web server to include the "X-Content-Type-Options" header in HTTP responses.
- Set the "X-Content-Type-Options" header in HTTP responses and configure it with the value "nosniff" to instruct browsers not to perform MIME type sniffing.
- Consider implementing a Content Security Policy (CSP) that complements X-Content-Type-Options.

1 finding

ANALYSIS	DOMAIN	SCHEME	OBSERVATIONS	FINAL URL	LAST OBSERVED
x_content_type_options_multiple	hailongoffshorewind.com	https	1	https://hailongoffshorewind.com/	4/21/2025, 3:50:16 PM

Site emits visible browser logs

-0.3 SCORE IMPACT

The risk of emitting browser logs lies in the potential exposure of sensitive information to unauthorized parties. These logs may inadvertently disclose user credentials, personally identifiable information, or other confidential data, which can be exploited by malicious actors for identity theft, fraud, or other nefarious purposes. Additionally, exposing internal system details or error messages may provide attackers with insights into potential vulnerabilities or weaknesses within the website's infrastructure.

Description

Browser logs refer to messages or information generated by a website's scripts or back-end processes that are sent directly to the browser's console. These logs typically include debugging information, error messages, warnings, or other diagnostic output that developers and users use for troubleshooting.

Recommendation

- Limit browser logs to essential diagnostic information.
- Avoid logging sensitive data like user credentials or personally identifiable information.
- Implement controls to restrict access to browser logs to authorized personnel only.
- Use encryption or obfuscation techniques to protect sensitive information within logs.
- Regularly review and monitor browser logs for any unusual or suspicious activity.

1 finding

URL	LAST OBSERVED
https://hailongoffshorewind.com/	4/26/2025, 7:21:59 PM
Evidence : "[{"content":"source: javascript; message: https://hailongoffshorewind.com/ 791:38 Uncaught Synta..."}]	

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

No issues found

A

100

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

There are no Medium Severity Issues for DNS Health

There are no Low Severity Issues for DNS Health

No issues found



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

A¹⁰⁰ 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

There are no High Severity Issues for IP Reputation

MEDIUM SEVERITY

There are no Medium Severity Issues for IP Reputation

LOW SEVERITY

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

There are no High Severity Issues for Information Leak

MEDIUM SEVERITY

There are no Medium Severity Issues for Information Leak

LOW SEVERITY

There are no Low Severity Issues for Information Leak

No issues found



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

There are no High Severity Issues for Network Security



MEDIUM SEVERITY

There are no Medium Severity Issues for Network Security



LOW SEVERITY

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

There are no High Severity Issues for Social Engineering

MEDIUM SEVERITY

There are no Medium Severity Issues for Social Engineering

LOW SEVERITY

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. ©2025 SecurityScorecard, Inc. All rights reserved.