

COMPANY REPORT

Know who you're working with.



Netflix












netflix.com

19 June 2025





Table of contents

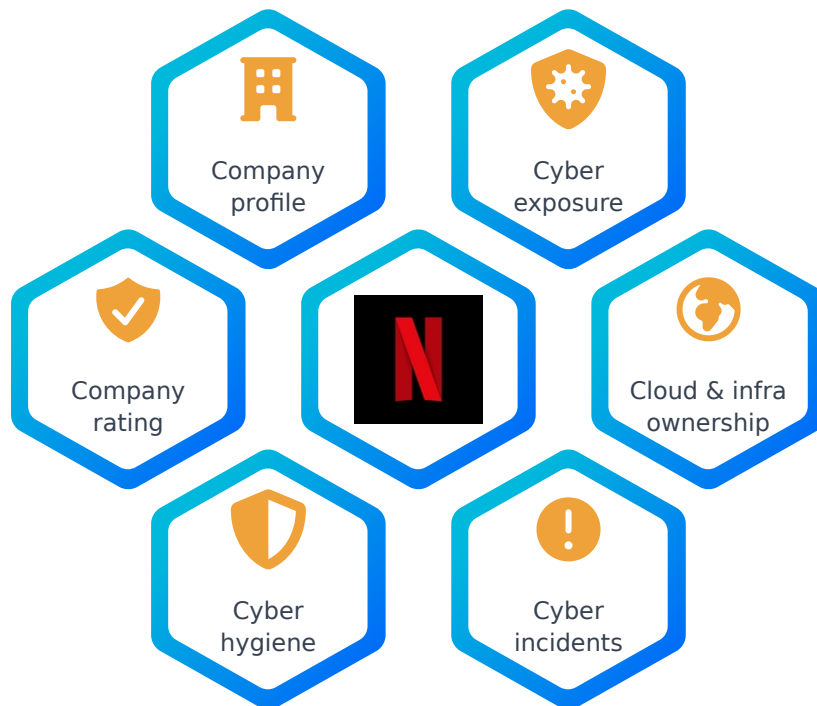
	Introduction	Page 3
	Executive summary	Page 4
	Company profile	Page 5
	Company rating	Page 6
	Cyber hygiene	Page 7
	Cyber exposure	Page 8
	Cloud & infra ownership	Page 9
	Cyber incidents	Page 10
	Recommendations	Page 12
	What's next?	Page 13
	About this assessment	Page 14



Introduction

Overview and purpose of the report

This CompanyReport provides an outside-in perspective, based entirely on publicly available data and external signals. It reveals how the company is perceived by third parties such as customers, regulators, suppliers, and potential attackers.



The report is structured into six key sections:

- **Company profile** – Basic company information such as sector, size, location, and web presence.
- **Company rating** – A company rating is a daily updated assessment that reflects a company's current risk posture.
- **Cyber hygiene** – An assessment of the company's technical security practices, such as certificate management, email security, and configuration issues.
- **Cyber exposure** – Identified vulnerabilities and weaknesses that may be exploited by threat actors.
- **Cloud & infra ownership** – An overview of key infrastructure dependencies and ownership for supply chain resilience and compliance is provided here.
- **Cyber incidents** – A timeline of publicly known data breaches, ransomware attacks, and other cyber events involving the company.

Together, these sections deliver a clear and actionable view of the company's digital presence, risk indicators, and reputation—entirely from an external perspective. This makes the report a powerful resource for third-party risk assessments, vendor onboarding, and continuous monitoring.



Executive summary

Key observations and conclusions

This report provides a comprehensive assessment of Netflix 's cybersecurity posture based on extensive analysis of their digital footprint. Our evaluation reveals both strengths and areas requiring attention to enhance overall security resilience.

Company rating

Netflix qualifies for an F rating based on observable cyber hygiene and exposure posture. This grade indicates significant external risk, with critical issues in configuration and visibility of internet-facing systems, particularly in outdated technologies and hygiene gaps like missing Content Security Policy (CSP). It suggests that Netflix is exposed to potential attacks and should prioritize urgent security improvements.

Key observations

Cyber hygiene: 56

Significant hygiene issues include the absence of key protections such as Content Security Policy (CSP) and incomplete email security configurations like missing DKIM signatures. These gaps could lead to data breaches or spoofing attacks, impacting customer trust.

Cyber exposure: 73

Netflix faces critical exposure risks due to vulnerable technologies like Bootstrap 3.4.1, which has a known XSS vulnerability (CVE-2024-6484). This increases attacker visibility and the potential for exploits on public-facing websites.

Cloud & infra dependencies: 4

Netflix relies heavily on Amazon.com, Inc. for cloud hosting, with servers in the US and Ireland, which may introduce data residency concerns under GDPR for EU customer data. Certificates are issued by trusted US-based authorities like DigiCert and Google Trust Services, but geographic mismatches warrant review for compliance risks.

Cyber incidents: 2

Netflix has faced two notable incidents: a €4.75 million fine in 2024 for GDPR violations related to privacy policy clarity, and a 2024 data breach involving leaked content via a third-party partner, lyuno, causing reputational damage.

Conclusion

Netflix’s external security posture reveals urgent risks in exposure and hygiene that could compromise customer data and trust. Immediate action is needed to address vulnerable technologies, strengthen email and web protections, and assess cloud data residency risks under GDPR. Prioritizing these improvements will reduce attacker visibility and enhance resilience. The recent incidents underscore the need for robust third-party and privacy controls to prevent further legal and reputational impact.



Company profile

Essential information about the organization

The company profile provides essential information about the analyzed organization. RiskStudio uses this foundational information as the basis for conducting an accurate cybersecurity analysis, ensuring the results and recommendations presented are relevant to the correct entity.

About the company



Watch Netflix movies & TV shows online or stream right to your smart TV, game console, PC, Mac, mobile, tablet and more.

Company details

Company name
Netflix

Primary domain
netflix.com

Industry
Media, Entertainment

Founded
1997

Country
 United States



Company rating

Overall security posture assessment

The Company rating provides a daily, objective snapshot of the organization's cybersecurity posture. It is based on two indicators: the Cyber hygiene score and the Cyber exposure score, which are derived from automated checks on the organization's digital infrastructure.

Company rating overview

The Company rating reflects the current risk level (on a A-F scale), combining the results of internal hygiene and external exposure checks. The accompanying risk level and comparison provide additional context on how the company performs relative to others in the dataset.

Rating
F

Risk level
High

Comparison
16% of the companies are rating worse
84% of the companies are rating better

Breakdown scores

The rating is based on two scores: Cyber hygiene captures internal practices like patching and configuration, while Cyber exposure evaluates public-facing vulnerabilities. Both are based on domain-level checks, with critical issues highlighted separately. The visual overview below shows the number of checks executed and issues identified.

Cyber hygiene score **56**

Measures internal security practices, patch management, and configuration standards

80

Hygiene checks executed

36

Findings found

14

Critical issues found

Cyber exposure score **73**

Evaluates external attack surface and potential vulnerability to threats

40

Exposure checks executed

15

Findings found

1

Critical issues found

Both scores are based on detailed checks and findings, with critical issues highlighted separately. See below for the number of checks executed and findings identified.



Cyber hygiene

Detailed assessment of security implementation



The cyber hygiene analysis provides a deep dive into Netflix security practices based on external observations. This analysis helps indentify potential areas for improvement and highlights security strengths.

Security checks

80

Total number of security-related checks executed.

Findings

36

Number of issues identified during the checks.

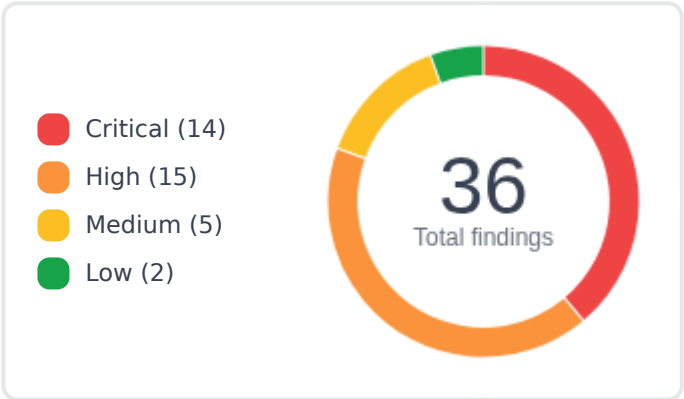
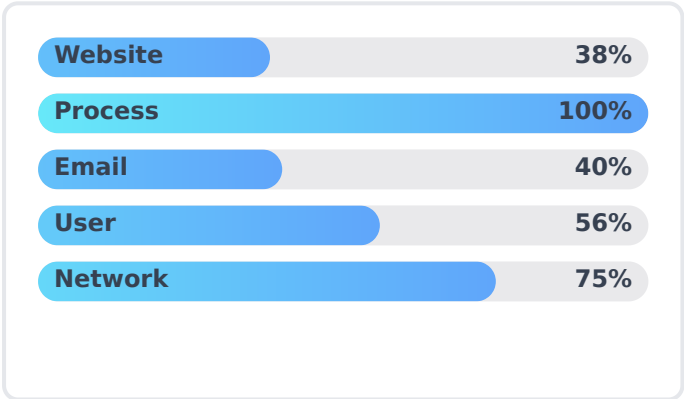
Success rate

55%

Percentage of checks passed without findings.

Technical checks summary

A total of 80 technical checks were conducted across all domains, spanning the categories listed below. Findings were identified in 36 of these checks, with their severity reflected in the scoring distribution graph.



Finding details

Below is a summary of key critical findings and recommendations

Most critical findings

Missing Content Security Policy (CSP), leaving websites open to XSS and data injection attacks.

Incomplete email security with absent DKIM signatures, enabling email spoofing risks.

Lack of HSTS preload listing, reducing protection against man-in-the-middle attacks on web traffic.

Recommended actions

Implement a strict CSP to control resource loading and block malicious scripts on websites.

Configure DKIM signatures alongside existing SPF and DMARC to secure email authenticity.

Enroll in HSTS preload lists and ensure proper max-age settings for robust HTTPS enforcement.



Cyber exposure

Assessment of vulnerability to external threats



The cyber exposure evaluates Netflix external cyber footprint through a series of technical checks across multiple categories. Some checks will result in findings with severity levels (critical, high, medium or low) based on potential impact and exploration risk.

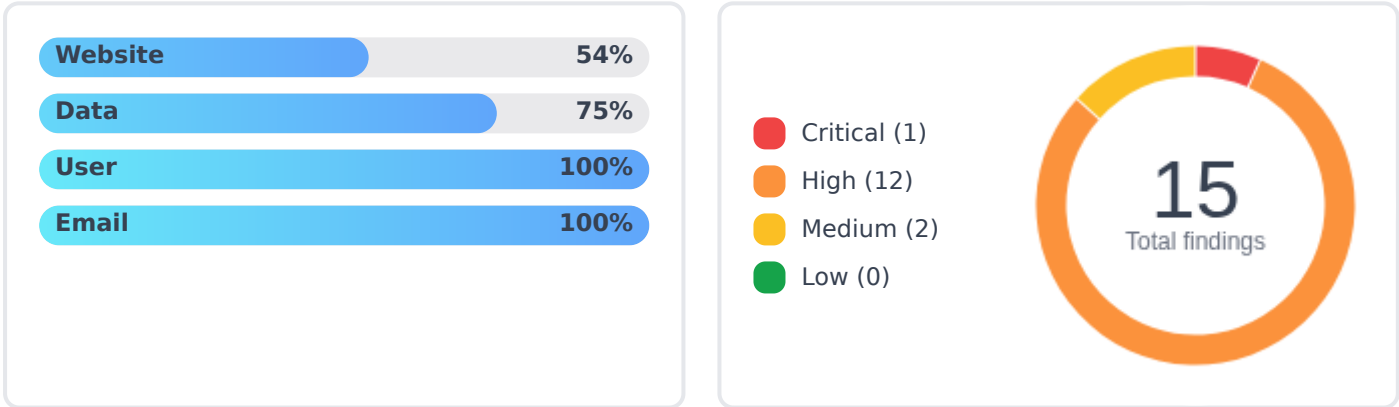
Security checks
40
Total number of security-related checks executed.

Findings
15
Number of issues identified during the checks.

Success rate
63%
Percentage of checks passed without findings.

Technical checks summary

A total of 40 technical checks were conducted across all domains, spanning the categories listed below. Findings were identified in 15 of these checks, with their severity reflected in the scoring distribution graph.



Finding details

Below is a summary of key critical findings and recommendations

Most critical findings

- Vulnerable technology exposure with Bootstrap 3.4.1, susceptible to XSS attacks via CVE-2024-6484.
- Exposure of development configurations like Git directories, risking sensitive data leaks.
- Listing on phishing blacklists like PhishTank, indicating potential malicious use of domains.

Recommended actions

- Update or replace Bootstrap to a secure version to prevent XSS exploits.
- Secure development assets by restricting access to Git directories and other sensitive files.
- Investigate and remediate blacklist listings to restore domain reputation and prevent user harm.



Ownership of the digital infrastructure & cloud usage

Insight into key cloud and infrastructure dependencies.

As part of supply chain and resilience assessments, this section identifies key infrastructure dependencies. It highlights cloud providers and certificate authorities to support compliance with evolving cybersecurity and digital supply chain requirements.



Footprint domains

2

Domains the footprint is based on



Cloud providers

2

Cloud service providers used for delivering



Certificate authorities

2

CA responsible for issuing certificates

Cloud infrastructure dependencies and ownership

This overview highlights the key third-party (cloud)providers and jurisdictions involved in delivering the organization's digital services. Visibility into these dependencies supports risk management, compliance with data residency requirements, and supplier governance.



Cloud providers



Amazon.com, Inc.

50%



Source2Cloud B.V.

50%



Certificate authorities



Google Trust Services

50%



netflix.ca

3 July 2025



DigiCert Inc

50%



account.netflix.com

24 September 2025



Cyber incidents

Security events and incident response metrics

This section tracks and analyzes security incidents detected across Netflix's digital infrastructure. It provides insights into the frequency, severity, and resolution status of cybersecurity events that may impact business operations and data security.



Total incidents

2

All reported cyber incidents



Severe incidents

2

Incidents with the highest impact



Recent incidents

2

Recent incidents still under investigation

Found cyber incidents

This section details the cyber incidents that have been identified and confirmed, offering insights into their severity, incident type and status. It helps assess the organization's exposure to known threats and vulnerabilities.

Netflix Fined €4.75 Million for Privacy Violations

High



Incident type: Other



Incident date: 18 December 2024



Updated at: 2 May 2025

The Autoriteit Persoonsgegevens fined Netflix €4.75 million for multiple AVG violations, including unclear privacy policies and non-compliance with data access requests. Netflix improved its privacy practices in 2022 following the breaches.

Key points

- Netflix fined €4.75 million
- Violations occurred between 2018 and 2020
- Netflix improved privacy policy in 2022
- Cooperation during investigation led to reduced fine
- Large number of EU customers affected




Involved companies

- Netflix • Role: Victim • Impact: High
- Autoriteit Persoonsgegevens • Role: Regulator • Impact: High



Netflix Cyber Incident Investigation Report

High

 Incident type: **Data Breach**  Incident date: 1 August 2024  Updated at: 22 April 2025

In August 2024, a security breach at Iyuno led to the unauthorized release of Netflix episodes. The incident highlighted vulnerabilities in content security protocols, prompting Netflix to enhance security measures and take legal action.

Key points

- Unauthorized episodes leaked
- No direct financial impact reported
- Significant reputational damage
- Stricter security measures implemented

Involved companies

- Netflix, Inc. • Role: **Primary Organization** • Impact: **High**
- Iyuno • Role: **Partner Company** • Impact: **Medium**
- Potential Regulatory Authorities • Role: **Regulator** • Impact: **Low**



Recommendations

Strategic actions for security improvement

Based on external analysis and observable security indicators, the following risk management actions are recommended to strengthen the security posture and address identified vulnerabilities:



Strengths

- Strong certificate management with valid, non-expired TLS certificates from trusted issuers like DigiCert.
- Effective email authentication with properly configured SPF and DMARC policies, reducing spoofing risks.
- No exposure of sensitive data like API keys or database credentials in public-facing systems.



Areas of concern

- Critical exposure risks from outdated technologies like Bootstrap 3.4.1, increasing attack surface for XSS exploits.
- Hygiene gaps such as missing CSP and incomplete email security, risking data breaches and customer trust.
- Cloud dependency on Amazon with servers in the US and Ireland, potentially conflicting with GDPR data residency rules for EU users.

1 Update Vulnerable Technologies

Prioritize updating or replacing outdated software like Bootstrap 3.4.1 to patched versions to eliminate known vulnerabilities such as CVE-2024-6484. This reduces the risk of XSS attacks on public-facing websites, protecting user data and maintaining service integrity.

2 Enhance Web and Email Security Controls

Implement a Content Security Policy (CSP) to prevent malicious script execution and complete email security by adding DKIM signatures. These steps block common attack vectors like XSS and spoofing, safeguarding customer interactions and trust.

3 Assess Cloud Data Residency Compliance

Conduct a Data Protection Impact Assessment (DPIA) to evaluate data residency risks from using Amazon servers in the US and Ireland, ensuring compliance with GDPR for EU customer data. Review Standard Contractual Clauses (SCCs) and consider European hosting alternatives to mitigate legal and operational risks.

Conclusion

Netflix’s external cyber posture shows significant vulnerabilities that could lead to data breaches and compliance issues. Addressing outdated technologies, implementing missing web protections, and reviewing cloud data residency are critical next steps. These actions will reduce attacker visibility, strengthen customer trust, and ensure alignment with legal obligations like GDPR. Ongoing vigilance over third-party risks is also essential given recent incidents.





What's next?

Turn insights into action

A CompanyReport gives you a clear, data-driven snapshot of an organization's cybersecurity posture — ideal for informed decisions around vendor onboarding, due diligence, or internal reviews. But cyber risks don't stand still. New vulnerabilities, misconfigurations, or third-party breaches can emerge at any time.

To stay ahead, we recommend requesting updated CompanyReports for your most critical suppliers and partners on a regular basis. This ensures you always have an up-to-date view of potential risks in your ecosystem — especially before audits, renewals, or key procurement decisions.

In the coming months, CompanyReports will be expanded with even more insights, including in-depth findings on data handling practices, third-party technology ownership, and stolen credentials — helping you make even more informed decisions with greater detail.

Looking for 24/7 insights?

If you want to move beyond point-in-time assessments, CompanyMonitor offers continuous monitoring of the cybersecurity posture of all your suppliers, partners, or acquisition targets. It gives you near real-time alerts on changes in exposure, hygiene, cyber incidents or known vulnerabilities — without needing supplier input.

CompanyMonitor goes further by enabling you to organize your third-party landscape using smart labels, critical process mapping, and role-based accountability. You can benchmark security performance, detect trends early, and act on incidents before they escalate.

For organizations that rely on complex supply chains, CompanyMonitor helps you respond faster, reduce hidden risks, and strengthen resilience — continuously.



Know who you're working with

In today's digital landscape, trust is everything. CompanyMonitor by RiskStudio gives you continuous insights into the cyber posture of your business partners — so you always know how secure your relationships really are.

[Learn more](#)



About this assessment

How the assessment was performed

This CompanyReport provides an outside-in assessment of the organization's cybersecurity posture. It is fully based on externally observable signals—such as public services, domain configurations, and exposed digital infrastructure. No internal access, questionnaires, or company-provided information is used.

Scope of assessment

The analysis uses two scopes. The Company rating scope includes domains with active services where technical checks could be performed. These domains directly influence the final Company rating. The Cyber footprint scope shows the top five public-facing domains that represent the organization's online presence. Some domains may appear in both scopes. These are automatically selected and offer a representative, though partial, view of the company's digital surface.



Company rating scope

2

Domains used for performing the checks

● netflix.com

● netflix.ca



Cyber footprint scope

2

Top 5 domains reflecting external visibility

● netflix.ca

● netflix.com

The domains shown above were automatically selected based on external visibility and technical relevance at the time of assessment.

Data collection and profiling

The assessment begins with a single entry domain—usually the organization's main website. RiskStudio then performs targeted scans and collects data from trusted public sources. This includes indicators of cyber exposure (e.g. vulnerabilities), hygiene (e.g. missing protections), and infrastructure footprint (e.g. cloud use, third-party services). Where relevant, connections to other companies are also identified.

These findings are structured into a cybersecurity profile and benchmarked. The resulting Company rating helps assess the relative risk posture of the organization—for use in supplier evaluations, investment due diligence, or internal monitoring.

Limitations and Disclaimer

This report reflects a snapshot in time and focuses solely on public internet-facing systems. It does not include internal networks, employee behavior, or non-public policies. Risk signals may evolve and the absence of findings does not guarantee security. Likewise, identified risks do not confirm incidents.

The CompanyReport is an informational product, not a certified audit. Use of the report is subject to RiskStudio's terms and conditions. No legal rights can be derived from its content.

This CompanyReport incorporates by reference the legal notices available on the RiskStudio [website](#).