RISKXCHANGE

Understanding Your Security Score

A Comprehensive Guide to Your External and Internal Security Posture Assessment.

riskxchange.co

Table of Contents

1. Introduction

Your security score provides a clear, single view of your organisation's security posture. It is designed to deliver clarity at an executive level, while remaining grounded in detailed technical analysis carried out by the RiskXchange platform.

The score combines two complementary dimensions: a continuous, automated assessment of your external attack surface, and the results of internal shared questionnaires that evaluate your organisation's security policies, controls, and data protection practices from the inside.

The score and accompanying grade are calculated from these combined assessments across multiple security domains. They highlight the areas of greatest risk and help you prioritise remediation efforts so that resources are directed where they will have the most meaningful impact.

This document explains how your score is derived, what each assessment category covers, how the shared questionnaires contribute, how findings are weighted, and how you can use the results to strengthen your security posture over time. It is intended for security leaders, risk managers, board members, and anyone who needs to understand or communicate cyber risk clearly.

2. What the Security Score Represents

Your security score is a numeric representation of your organisation's security posture, calculated on a scale of 0 to 900. It reflects both what an external observer—including potential attackers, regulators, customers, and business partners—can determine about your security from publicly accessible information and internet-facing infrastructure, and the strength of your internal security controls as reported through RiskXchange's shared questionnaires.

The score aggregates findings across eight distinct external security categories and incorporates results from two internal assessment questionnaires: RX Essentials and RX Data Protection. Higher scores indicate a stronger security posture with fewer identified issues, while lower scores signal areas that require attention.

Because the external assessment is continuous and non-intrusive, your score is updated regularly as the platform identifies new findings or confirms that previously identified issues have been resolved. Questionnaire results are incorporated when your organisation completes and shares them through the platform. This means your score is a living metric that reflects your current state, not a point-in-time snapshot.

Score Availability

If your organisation has not yet completed at least one of the RiskXchange shared questionnaires (RX Essentials or RX Data Protection), only the external attack surface score will be available. Once one or both questionnaires have been completed and shared, the score will incorporate those results to provide a more complete picture of your overall security posture.

This means the depth and comprehensiveness of your score improves as you engage more fully with the platform. Organisations that complete both the external assessment and the internal questionnaires benefit from a holistic view that covers both outside-in and inside-out perspectives on security risk.

3. Score Components: External and Internal Assessments

Your overall security score is built from two complementary components, each of which provides a different perspective on your organisation's security posture.

External Attack Surface Assessment

The external attack surface assessment is an automated, continuous evaluation of your organisation's internet-facing infrastructure. It examines your web applications, SSL/TLS configurations, network services, email and DNS settings, malware indicators, breach history, exposed databases, and domain reputation. This assessment requires no action from your organisation—it runs automatically against your registered domains and IP address ranges.

The external assessment forms the foundation of your security score and is always available, regardless of whether internal questionnaires have been completed.

Internal Shared Questionnaires

The internal component of your score is derived from two shared questionnaires that your organisation completes through the RiskXchange platform:

RX Essentials — a comprehensive questionnaire that evaluates your organisation's core security controls, policies, and operational practices. It is designed to assess the fundamentals of your security programme from an inside-out perspective, complementing the external view provided by the attack surface assessment.

RX Data Protection — a focused questionnaire that evaluates how your organisation handles, stores, protects, and governs sensitive data. It covers data protection practices, privacy controls, and compliance with data protection standards and regulations.

Together, these questionnaires provide insights that cannot be observed externally, such as whether your organisation has documented security policies, incident response procedures, employee training programmes, data classification schemes, and appropriate access controls.

How the Components Work Together

When both the external assessment and at least one shared questionnaire have been completed, the platform combines the results to produce a more comprehensive score. The external assessment reveals what the outside world can see; the questionnaires reveal how well your organisation is managing risk internally.

If no shared questionnaires have been completed, only the external attack surface score will be available. As questionnaires are completed and shared, the score is enriched accordingly, providing a progressively more complete picture of your security posture.

4. External Attack Surface — Security Assessment Categories

The external component of your security score is derived from findings across eight defined categories. Each category focuses on a different aspect of your external attack surface and is composed of several underlying checks to ensure a balanced and comprehensive evaluation.

Category	What Is Assessed
Application Security	Web application controls such as HTTPS enforcement, cookie security, Content Security Policy, clickjacking protection, HTTP Strict Transport Security (HSTS), and known application-level vulnerabilities.
SSL / TLS	Certificate validity and trust chain, encryption strength, protocol security, cipher suite configuration, and known cryptographic weaknesses or vulnerabilities.
Network Security	Externally exposed ports and services, identification of unnecessary or risky open services, and known vulnerabilities affecting network-facing systems.
Mail & DNS	Email authentication mechanisms (SPF, DKIM, DMARC), DNS security controls, domain registration and configuration status, protection against unauthorised zone transfers, and domain or IP blacklist exposure.
Malware	Indicators of malicious activity associated with your IP addresses, including connections to known command-and-control infrastructure.
Data Breaches	Evidence of historical data breaches linked to your organisation, including credential exposure and ransomware incidents.
Database Servers	Detection of database services that are accessible from the public internet, which can significantly increase the risk of unauthorised access or data loss.
Business Reputation	Domain reputation across major safe-browsing and trust services, which can affect customer confidence, email deliverability, and brand perception.

Together, these categories provide a broad and realistic view of your organisation’s external security risk, covering the most common vectors that attackers exploit and that regulators and business partners evaluate.

5. Category Weighting and Score Calculation

The overall security score is calculated out of a maximum of 900 points. The external attack surface assessment categories each contribute a fixed allocation of points, reflecting their relative impact on business risk. This weighting ensures that the categories with the most significant potential consequences carry the greatest influence on your final score.

When shared questionnaire results are available, these are factored into the overall score alongside the external findings to provide a more complete assessment.

Category	Maximum Points	Contribution to Score
Data Breaches	300	33%
Application Security	190	21%
Network Security	190	21%
SSL / TLS	190	21%
Other Categories	30	4%
Total	**900**	**100%**

Why Data Breaches Carry the Highest Weighting

Data Breaches are assigned the greatest weighting (33%) due to their direct and often severe operational, financial, and reputational impact. A confirmed breach can result in regulatory fines, loss of customer trust, litigation costs, and significant operational disruption. Breach history is also one of the first things that prospective customers, partners, and insurers evaluate when assessing third-party risk.

The “Other Categories” Grouping

The remaining categories—Mail & DNS, Malware, Database Servers, and Business Reputation—share a combined allocation of 30 points (4%). While these categories carry a smaller point contribution, they remain important indicators of security hygiene and can highlight issues that, if left unresolved, may escalate into more significant risks.

How the Final Score Is Produced

Within each category, multiple subcategories are assessed. Each identified issue is assigned a severity level, and subcategory results are combined to form a category score. Category scores are then normalised according to their fixed weighting and summed to produce the external component of your score out of 900. When shared questionnaire results are available, these are incorporated into the overall scoring model to produce a combined score that reflects both your external posture and internal controls. The specifics of the normalisation and combination formulae are proprietary, but the principle is straightforward: higher-severity findings in higher-weighted categories will have the greatest impact on your overall score.

6. Detailed Category Evaluations

This section provides a deeper look at what is assessed within each of the eight external security categories. Rather than relying on a single control or finding, the platform evaluates a range of related indicators within each category to produce a balanced and representative score.

6.1 Application Security

Application Security focuses on how well your web-facing applications protect users and data. Modern web applications are a primary target for attackers, making this one of the most heavily weighted categories in the scoring model.

Assessments within this category include: the use of encrypted connections (HTTPS) across all web-facing services; secure cookie handling, including the use of Secure, HttpOnly, and SameSite attributes; implementation of Content Security Policy (CSP) headers to mitigate cross-site scripting and data injection attacks; protection against clickjacking through X-Frame-Options or CSP frame-ancestors directives; enforcement of HTTPS through HTTP Strict Transport Security (HSTS), including preload eligibility; and identification of known application-level vulnerabilities through version detection and advisory matching.

A strong Application Security score indicates that your web applications implement defence-in-depth controls and follow current best practices for protecting user sessions and sensitive data in transit.

6.2 SSL / TLS

The SSL / TLS category evaluates the security of encrypted communications between your servers and their clients. Weak or misconfigured encryption can expose sensitive data to interception, even when connections appear to be secured.

Assessments cover: certificate validity, including expiry dates, trust chain integrity, and correct hostname matching; the strength of supported cipher suites, with a focus on identifying weak or deprecated algorithms; the use of modern and secure protocol versions (TLS 1.2 and TLS 1.3) and deprecation of older, vulnerable protocols such as SSLv3, TLS 1.0, and TLS 1.1; and exposure to known SSL or TLS vulnerabilities such as Heartbleed, POODLE, BEAST, and others.

Maintaining strong SSL / TLS configurations is essential not only for security but also for regulatory compliance and customer trust.

6.3 Network Security

Network Security examines your externally visible network footprint. Every open port and exposed service represents a potential entry point for an attacker, and this category is designed to identify unnecessary exposure.

Assessments include: identification of all externally exposed ports and services across your IP address ranges; evaluation of whether exposed services are necessary and appropriately configured; detection of known vulnerabilities in network-facing systems, based on service version identification and advisory correlation; and identification of services that are commonly targeted by attackers, such as RDP, Telnet, FTP, and database ports exposed to the public internet.

A strong Network Security score reflects a well-managed external perimeter where only necessary services are exposed and known vulnerabilities are promptly addressed.

6.4 Mail & DNS

Mail & DNS assessments focus on the security and reliability of your domain and email infrastructure. Email remains one of the most exploited attack vectors, and misconfigured DNS can undermine other security controls.

Checks include: email authentication mechanisms, specifically SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance), which together help prevent email spoofing and phishing; DNS security extensions and configuration hygiene; domain registration status, including expiry monitoring; protection against unauthorised DNS zone transfers that could reveal internal infrastructure details; and monitoring for domain or IP address presence on email and security blacklists, which can affect deliverability and reputation.

Properly configured email authentication is increasingly expected by customers, partners, and email providers, and is now a requirement under several regulatory frameworks.

6.5 Malware

The Malware category identifies whether any of your IP addresses have been associated with known malware command-and-control (C2) infrastructure or other malicious activity. This is a critical indicator because active malware associations suggest that systems within your environment may have been compromised.

The platform cross-references your IP address ranges against continuously updated threat intelligence feeds to detect associations with botnets, C2 servers, malware distribution points, and other indicators of compromise. Even a single confirmed association can significantly affect your score and warrants immediate investigation.

6.6 Data Breaches

Data Breaches carry the highest weighting in the scoring model because of their direct and measurable impact on an organisation. This category identifies evidence of historical data breaches linked to your organisation, including credential exposure, customer data leaks, and ransomware incidents.

The platform monitors a wide range of sources for breach data, including public breach notification databases, dark web monitoring feeds, and ransomware disclosure sites. Findings in this category are assessed based on the severity and recency of the breach, the type and volume of data exposed, and whether the breach has been publicly disclosed and remediated.

Organisations with no identified breach history will receive a full score in this category, which significantly boosts their overall rating.

6.7 Database Servers

This category detects database services that are accessible from the public internet. Exposed databases represent one of the highest-risk findings because they can provide direct access to sensitive data if not properly secured.

The platform scans for publicly reachable instances of common database systems, including but not limited to MySQL, PostgreSQL, MongoDB, Microsoft SQL Server, Redis, and Elasticsearch. Any database service that is accessible from the internet without appropriate access controls is flagged, as best practice dictates that database services should only be accessible from trusted internal networks or through secure, authenticated intermediaries.

6.8 Business Reputation

Business Reputation monitoring checks whether your domain has been flagged by major reputation and safe-browsing services. Being listed on such services can have immediate and tangible consequences, including blocked access to your website for users of major browsers, email deliverability failures, and erosion of customer and partner trust.

The platform monitors your domain against services such as Google Safe Browsing, PhishTank, and other widely used reputation databases. A clean reputation score indicates that your domain has not been associated with phishing, malware distribution, or other malicious activity.

7. Internal Assessments — Shared Questionnaires

While the external attack surface assessment reveals what the outside world can see, your organisation's internal security controls, policies, and data protection practices are equally important to your overall risk posture. RiskXchange's shared questionnaires provide this inside-out perspective, capturing information that cannot be determined from external scanning alone.

Completing and sharing these questionnaires through the RiskXchange platform enables a more comprehensive and accurate security score. If your organisation has not yet completed at least one shared questionnaire, only the external attack surface score will be available.

7.1 RX Essentials

The RX Essentials questionnaire evaluates your organisation's core security controls and operational practices. It is designed to assess the fundamentals of your security programme, covering the policies, procedures, and technical controls that form the backbone of a mature security posture.

The questionnaire is structured across twelve assessment categories, each of which examines a specific domain of internal security.

Category	What Is Assessed
Employees	Security awareness training, acceptable use policies, background checks, onboarding and offboarding procedures, and the overall security culture within the workforce.
Network Assessment	Internal network architecture, segmentation controls, firewall configuration, intrusion detection and prevention capabilities, and network monitoring practices.
Physical Security	Physical access controls to offices, data centres, and sensitive areas, including visitor management, surveillance, and environmental protections.
System Security	Operating system hardening, patch management processes, endpoint protection, configuration management, and system lifecycle practices.
Critical Data	Identification, classification, and protection of critical and sensitive data assets, including data storage controls, backup procedures, and encryption practices.
Remote Access	Secure remote access controls including VPN usage, multi-factor authentication for remote connections, remote device management, and policies governing remote and hybrid working.
Portable Data	Controls around portable storage devices and media, including encryption of portable devices, USB policies, and procedures for the secure transport of data.
Risk Management Procedures	Formal risk assessment and management processes, risk registers, risk appetite definitions, and the integration of risk management into business decision-making.

3rd Party Risk Management	Processes for assessing and managing the security posture of third-party vendors and suppliers, including due diligence procedures, contractual security requirements, and ongoing monitoring.
Legal / Regulatory	Compliance with applicable legal and regulatory requirements, including data protection legislation, industry-specific regulations, and contractual obligations related to security.
Security Incident Management	Incident response planning, detection and escalation procedures, communication protocols, post-incident review processes, and readiness for security events.
Certification	Security certifications and accreditations held by the organisation, such as ISO 27001, SOC 2, Cyber Essentials, and other recognised standards that demonstrate commitment to formal security frameworks.

By completing RX Essentials, your organisation provides evidence of the internal controls that support and reinforce the security posture observed externally. This allows the platform to recognise organisations that invest in comprehensive security programmes, even where their external footprint may show minor findings.

7.2 RX Data Protection

The RX Data Protection questionnaire focuses specifically on how your organisation handles, stores, protects, and governs sensitive data. Structured around GDPR vendor assessment principles, it evaluates data protection practices across eight categories that align with key regulatory expectations and data governance best practices.

Category	What Is Assessed
Data Collection and Processing	How personal and sensitive data is collected, the legal bases for processing, purpose limitation, data minimisation practices, and the transparency of processing activities.
Third-Party Data Sharing	Controls and agreements governing the sharing of data with third parties, including data sharing agreements, due diligence on recipients, and safeguards for cross-border data transfers.
Security Measures	Technical and organisational security measures in place to protect personal data, including encryption, access controls, monitoring, and security testing practices.
Data Subject Rights	Processes for handling data subject requests, including access, rectification, erasure, portability, and restriction of processing, in compliance with applicable data protection regulations.
Data Retention and Disposal	Data retention policies, schedules, and procedures for the secure disposal or anonymisation of data that is no longer required, ensuring compliance with retention obligations.
Vendor Accountability	Accountability measures for vendors and data processors, including data processing agreements, audit rights, compliance monitoring, and evidence of ongoing oversight.
Sub Processor Management	Controls governing the use of sub-processors, including approval processes, contractual flow-down of data protection obligations, and visibility into the sub-processor chain.
Breach and Incident Reporting	Data breach detection, notification, and reporting procedures, including timeliness of notification to supervisory authorities and affected individuals, root cause analysis, and remediation tracking.

Completing RX Data Protection demonstrates your organisation's commitment to safeguarding the data entrusted to it by customers, partners, and employees. The results contribute to your overall score by providing visibility into practices that are invisible to external scanning but critical to risk assessment.

How Questionnaire Results Are Incorporated

When one or both shared questionnaires have been completed and shared through the platform, the results are incorporated into your overall security score alongside the external attack surface findings. This combined view provides a significantly more complete and accurate representation of your organisation's true security posture.

Organisations that complete both questionnaires benefit from the most comprehensive assessment available, as the platform can evaluate security from both external and internal perspectives. If only one questionnaire has been completed, that questionnaire's results will be incorporated while the other dimension remains unassessed.

8. How Issues Affect Your Score

Each identified issue—whether from the external attack surface assessment or from the shared questionnaire results—is assigned a severity level. The platform uses a tiered severity model to ensure that the most dangerous findings have a proportionally greater negative impact on your score.

Severity Level	Description
Critical	Issues that pose an immediate and severe risk to the organisation, such as known exploited vulnerabilities or exposed sensitive services. These have the greatest negative impact on your score.
High	Significant issues that should be addressed promptly, such as weak encryption configurations or missing critical security headers.
Medium	Issues that represent a moderate risk and should be included in planned remediation cycles, such as use of deprecated but not yet critically vulnerable protocols.
Low	Minor issues that represent limited immediate risk but should be addressed as part of good security hygiene.
Informational	Observations that do not directly impact your score but may be useful for improving your overall security posture.

Higher-severity issues reduce points within the relevant subcategory by a greater amount than lower-severity issues. Subcategory results are combined to form a category score, and category scores are then normalised and weighted according to the allocations described in Section 5. Where shared questionnaire results are available, these are also factored into the overall score to produce the final result.

Resolving critical and high-severity issues will have the most significant positive effect on your score. However, addressing lower-severity issues is also important, as a pattern of unresolved minor findings can indicate systemic weaknesses in security governance.

9. Security Grades

For ease of interpretation and communication, the numeric score is converted into a letter grade. This makes it straightforward to understand your overall security posture at a glance and to communicate it to non-technical stakeholders, board members, customers, and partners.

Grade	Score Range	Interpretation
A	100% (900 / 900)	Excellent
B	80–99% (720–899)	Good
C	60–79% (540–719)	Fair
D	40–59% (360–539)	Poor
E	20–39% (180–359)	Weak
F	Below 20% (0–179)	Critical

The grade provides a useful benchmark for tracking progress over time and for comparing your security posture against industry peers or third-party requirements. Many organisations and regulatory frameworks now require that third-party vendors maintain a minimum grade as a condition of doing business.

10. Using Your Score Effectively

Your security score is most valuable when used as an ongoing management tool rather than a one-time assessment. The following guidance can help you get the most from your score.

Complete Both Shared Questionnaires

To receive the most comprehensive and accurate score possible, ensure that your organisation completes both the RX Essentials and RX Data Protection questionnaires. Without these, your score reflects only your external attack surface and may not capture the full strength of your internal security programme.

Prioritise by Severity and Weighting

Focus remediation efforts on critical and high-severity issues first, particularly in the highest-weighted categories (Data Breaches, Application Security, Network Security, and SSL / TLS). Addressing these will produce the greatest improvement in your score.

Monitor Trends Over Time

Track your score and grade over successive assessment periods. A consistently improving score demonstrates the effectiveness of your security programme, while a declining score may indicate emerging risks or gaps in your remediation processes.

Communicate with Stakeholders

Use the grade and score to communicate your security posture clearly to board members, executive leadership, customers, and partners. The letter grade system is designed to be understood by non-technical audiences without losing the rigour of the underlying technical assessment.

Benchmark Against Third-Party Requirements

Many organisations now set minimum security score thresholds for their vendors and partners. Understanding your score helps you anticipate and meet these requirements proactively, rather than reacting to third-party assessments after the fact.

Integrate with Your Risk Management Framework

Your security score should be considered alongside other risk indicators such as internal vulnerability assessments, penetration testing results, and compliance audit findings. Together, these provide a comprehensive picture of your organisation’s overall cyber risk posture.

11. Frequently Asked Questions

How often is my score updated?

Your score is updated continuously as the platform completes new assessments and identifies changes in your external security posture. The frequency of updates depends on the assessment schedule configured for your organisation. Questionnaire results are updated when you submit or revise a shared questionnaire.

Why is only the external score available for my organisation?

If your organisation has not yet completed at least one of the RiskXchange shared questionnaires (RX Essentials or RX Data Protection), only the external attack surface score will be displayed. Once you complete and share at least one questionnaire, the internal assessment results will be incorporated into your overall score.

Why is my score different from what I expected?

The score reflects your externally observable security posture and, where available, your internal assessment results from shared questionnaires. Internal controls, policies, and security investments that are not captured by the external assessment or by the questionnaires may not be reflected in your score. Additionally, the weighting model means that a single critical finding in a heavily weighted category (such as Data Breaches) can have a disproportionate impact on your overall score.

Can I improve my score without resolving every issue?

Yes. Because the scoring model is severity-weighted, resolving the highest-severity issues in the most heavily weighted categories will produce the largest score improvements. You do not need to achieve a perfect score in every category to earn a strong overall grade. Additionally, completing the shared questionnaires can improve your score by demonstrating strong internal controls.

What does the “Other Categories” grouping include?

The “Other Categories” grouping includes Mail & DNS, Malware, Database Servers, and Business Reputation. These share a combined allocation of 30 points (4% of the total score).

Does the score include internal security assessments?

Yes, when shared questionnaires have been completed. The RX Essentials and RX Data Protection questionnaires capture your internal security controls, policies, and data protection practices. These results are incorporated into your overall score alongside the external attack surface findings. If no questionnaires have been completed, the score reflects only the external assessment.

What is the difference between RX Essentials and RX Data Protection?

RX Essentials evaluates your organisation’s core security controls and operational practices across a broad range of security domains. RX Data Protection focuses specifically on how your organisation

handles, stores, protects, and governs sensitive data. Both questionnaires contribute to your overall score and together provide a comprehensive internal assessment.

How should I share this score with customers or partners?

Your letter grade and numeric score are designed to be shared directly. The grade provides an accessible summary for non-technical audiences, while the numeric score and category breakdown offer the detail that security-focused stakeholders may require. Organisations that have completed the shared questionnaires can demonstrate a more comprehensive assessment.

12. Summary

Your security score is a concise, risk-weighted representation of your security posture, combining the results of continuous external attack surface monitoring with the findings from internal shared questionnaires. By bringing together multiple assessment domains with severity-based weighting, the score ensures that the most material risks have the greatest influence on the final result, while still providing a complete view of your overall security hygiene.

The external assessment evaluates your internet-facing infrastructure across eight categories, from application security and encryption to breach history and domain reputation. The internal assessment, through the RX Essentials and RX Data Protection questionnaires, captures the policies, controls, and data protection practices that cannot be observed from outside your network.

Together, these components produce a score that reflects both what the world can see and how well your organisation is managing risk from within. The 0–900 scale and accompanying letter grade make it straightforward to understand, communicate, and act on your results. Whether you are reporting to your board, responding to a customer questionnaire, or planning your next quarter's security roadmap, your RiskXchange security score provides the clarity and evidence needed to make informed decisions.

For further information on how to interpret specific findings, plan remediation activities, complete the shared questionnaires, or use your score in third-party risk management workflows, please contact your RiskXchange account team or visit riskxchange.co.