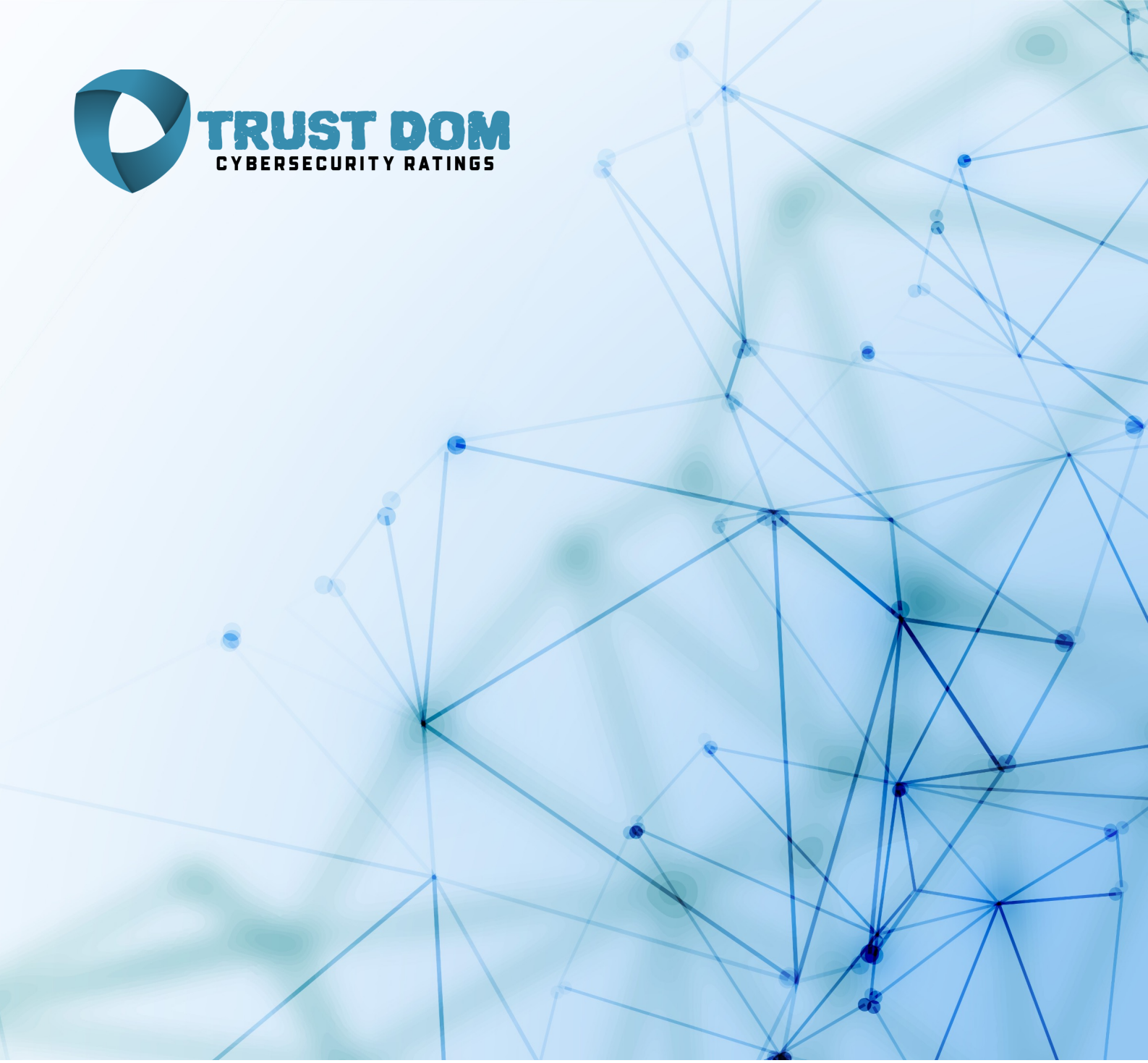


Domain
Cybersecurity Ratings

Table of Contents

01. Report Introduction 03

02. Overview of Cybersecurity Ratings 04

03. Trust Dom Cyber Ratings 05

04. Risk Zone Cyber Ratings 06

05. Probe Cyber Ratings 07

06. How accurate are Trust Dom Ratings 08

07. Your Domain Result

1. Executive Summary

2. Email Zone Rating

3. Website Zone Rating

4. Compromised Zone Rating

5. Vulnerability Zone Rating

6. Data Privacy compliance Rating

> **"By 2022, security ratings will become as important as credit ratings when assessing the risk of existing and new business relationships"**

Innovation Insight for Security Rating Services, Gartner, July 2019

Report
Introduction

This is an executive report which provides an insight into an organisation's commitment to cyber privacy, accountability and trustworthiness. This report offers a comprehensive analysis of a domain's cyber security posture, a domain's attack surface and an overview of domain data and communication security.

In addition to results, this report also provides additional information, which allow the reader to understand the nature of rating calculation within the broader risk zones and at the scanning level.

Simple remediation strategies are provided at the end of each report, allowing users to take steps to mitigate their identified cyber risks. These can be passed on to in-house teams or external vendors who can help an organisation improve their risk ratings over time.

TRUST DOM
CYBERSECURITY RATINGS

Gain insight into an organisation's commitment to cyber privacy, accountability and trust worthiness.

Overview
Of Cybersecurity Ratings

Cybersecurity Ratings provide a quick and cost-effective way to review a company's cyber security posture. We do this by pointing cyber probes at domain security entry points and open source data to collect real-time information on an organisation's online presence and associated security risks.

Cybersecurity Ratings guide the user in making risk-related decisions based on the security of a domain's data and communication posture. By providing the user with critical cyber security information, a user can ascertain the level of risk associated with the domain. (For example, has it been compromised? How well is the website secured? What are its vulnerabilities?)

Using Trust Dom Scanners, users can passively probe any internet domain for a non-intrusive cybersecurity profile assessment. By dispatching a collection of finely tuned probes, we can retrieve and dissect important data signals to reveal a domain's trustworthiness.

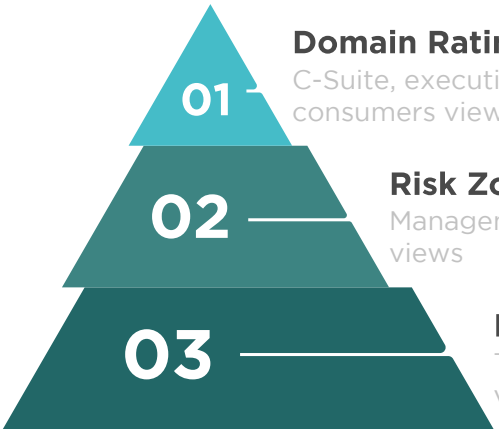
Trust Dom
Cyber Ratings

Trust Dom Cyber Ratings are categorised into three broad cyber rating areas; Domain Rating, Risk Zone Rating and Probe Rating. Each area has been designed to target the needs of a specific audience. For example, the C-Suite executives are more likely to be interested in the domains overall rating, whilst the IT department maybe more likely to focus on the lower level probes and remediation reports.

Domain Rating indicates the average result of the Risk Zone and Probes

Risk Zones review probe results and package them by risk areas

Probes record technical details and remediation plans



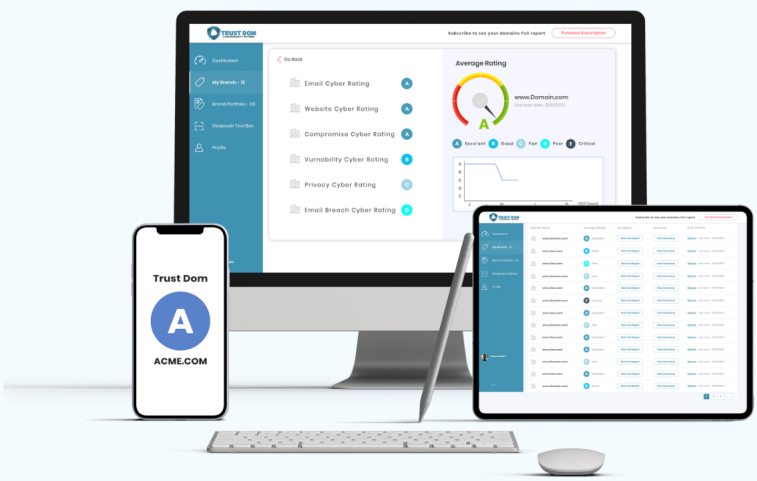
Domain Rating
C-Suite, executives & consumers view

Risk Zone
Management levels views

Probes
Technical support views

Domain Rating

A Domain Rating indicates an overarching cybersecurity profile for the domain's website and email services. All Domain Ratings are available in real-time, providing the user with an immediate grade at their fingertips. Domain ratings provide the user with confidence that an 'A' grade domain exhibits an excellent level of cyber security and trustworthiness and is therefore safe to use.



Risk zone
Cyber Ratings

Risk Zones are assessed across four sub zones i.e. Email, Website, Compromised, Vulnerability. Each Risk Zone consists of several probes that are designed to assess the level of cybersecurity exposure and vulnerability. These four Risk Zones comprise a composite of over 50 probes which when scanned and scored, produce each Risk Zone Rating. A Grade is then assigned to the website for its compliance with Data Privacy regulations e.g. GDPR and Local Privacy Laws.

As example, an 'E' grade for the Email Zone reflects very poor communication security. This may potentially lead to emails being susceptible to malware, ransomware and spam.

EMAIL ZONE EVALUATION

Can we trust that the email communications has protected our privacy? Is it susceptible to email fraud and malware ? Does it protect, encrypt, and secure communications?

WEBSITE ZONE EVALUATION

Can we trust the website to protect our privacy, data and access? Does the website protect us from malware and attempted data breaches?

COMPROMISED ZONE EVALUATION

Can we trust that the domain has not been compromised by hackers? Is it safe to join the website or communicate with this domain?

VULNERABILITY ZONE EVALUATION

Can we trust that the domain is not vulnerable to a cyber attack? Has the domain been regularly patched and fixed with the latest security service advisories?

DATA PRIVACY COMPLIANCE RATING

Can we trust that the website follows global privacy standards? Is the website secure in protecting personal information?

Probe
Cyber Ratings

There are over 50 Probes dispatched across four sub Risk Zones. Each probe has been carefully designed to passively interrogate a domain's cybersecurity posture and return the results back to the user.

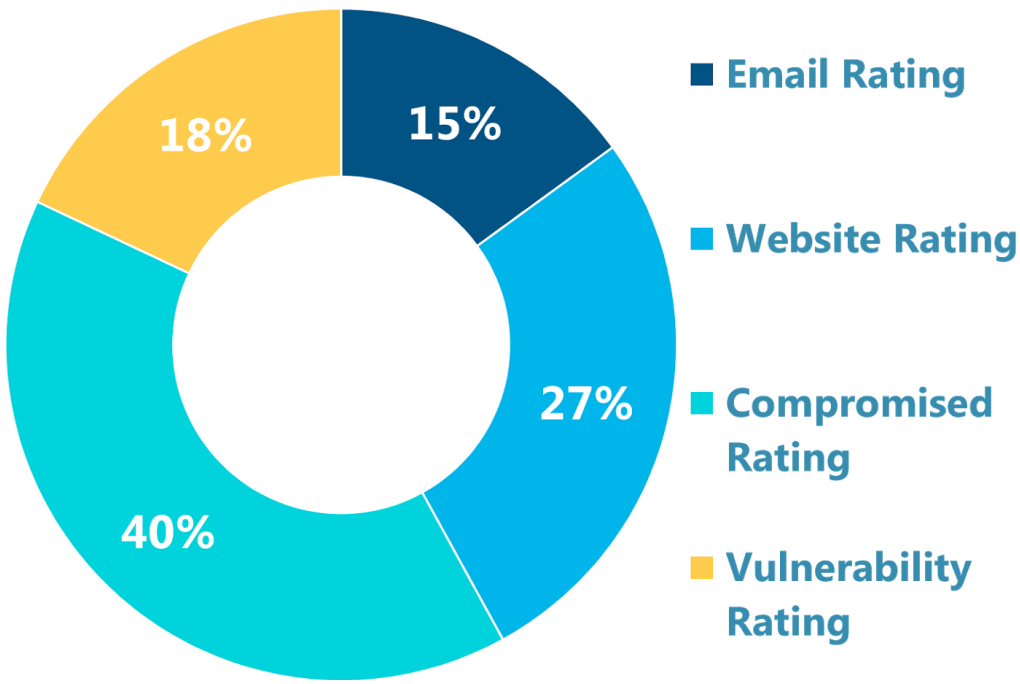
Each probe is assigned an impact and severity value; which in total, calculates the results for the Domain Rating and its associated sub Risk Zones.

Probe Ratings are demarcated as either a pass or fail grade. For example, a 'Failed' Botnet probe would indicate the domain is hosting malware and other hacker services.

Risk Weighting & Algorithm

The risk weighting is managed by an algorithm that calculates each Risk Zone against a probe's impact value and severity before assigning a Rating. For example, the Email Zone is weighted 15% of the overall Domain Rating.

Note: The algorithm may change from time to time as our experts adjust it to reflect new cyber risks. Please also note that we do not share details of our Probes values or our algorithms.



How accurate are **Trust Dom ratings?**

We have taken every effort to ensure that our ratings are accurate and transparent. We have focused on assessing data points that are tangible and clearly quantifiable.

Our ratings explicitly indicate whether an organisation has sufficiently implemented security standards that allow us to trust their public security and trust profile and our email and web-based interactions with them.

Whilst these ratings can correlate to the internal security profile of an organisation, we should NOT assume that an “A” rating definitively means that an organisation is fully secure.

Trust Dom Global Cyber Security Standards

Trust Dom is aligned to the following industry standards:

01. National Institute of Standards and Technology (NIST)

02. ISO27001, PCI, IETF, CVE, NIST CVSS

03. UK Cyber Essentials

Executive **Summary**

RISK ZONE RATINGS

A Excellent B Good C Fair D Poor E Critical

Risk Zones
& Probes

Cyber Stats

Cyber-attacks are on the rise

Let’s work together to stop your company becoming yet another cyber-attack statistic. As the world becomes increasingly connected and more businesses move online, cyber security will become everyones shared responsibility.

More Cyber Security Stats...

01. The global cybercrime economy generates approx USD 1.5 trillion yearly

02. The average cost of a data breach for a company in 2020 was US$3.86m

03. The average cost per stolen record is US$120

"SRM (security and risk management) leaders should leverage security ratings services as an additional data point to provide continuous independent scoring for their overall digital ecosystem- public-facing assets and otherwise"

Top 10 Security Projects for 2019, Gartner, July 2019

THANK **YOU**