UPGUARD CYBERRISK

Understanding and Addressing UpGuard Vendor Risk Scores

UpGuard

Why Use UpGuard Security Ratings?

The technical nature of cyber risk makes it inaccessible to those without advanced skills and knowledge, leaving organizations without visibility into an extremely valuable and critical part of the business.

UpGuard's security ratings solve the problem of understanding cyber risk in the same way credit scores solve understanding debt risk: specialists assess each company using standardized evaluation criteria and proprietary tools, then return a rating that can be understood in a business context by non- technical people.

What Makes a Good Rating?

When comparing security ratings, consider the following qualities and how they relate to your risk management goals:

Transparency

Although security rating providers use proprietary algorithms to derive scores, the risk factors that are considered in the score should be clearly laid out. The more a client knows about what a security rating really measures, the better they are able to control their vendor risk. **UpGuard provides visibility into all the detected risks that produce individual security scores, as well as their criticality levels.**

Internet-Wide & On-Demand

Every digital business has an internet footprint. Monitoring a small subset of these businesses omits a large portion of the companies involved in the data handling and service supply chain. **UpGuard's security ratings are internet-wide and on-demand, currently covering 1.5 million organizations and automatically able to add and report on the risk of any digital business in the world within a few seconds.**

Threat Focus

Many broad factors can be used to determine a security score. However, only risk factors correlated to the possibility of breach and outage provide any assistance in reducing the likelihood of those incidents. **UpGuard's security ratings address actual threats by clearly articulating how and why every listed threat increases information risk.**

Business Context

You might know that a higher score is better than a lower score, but unless the risks affecting scores are explained in terms of business impact, those comparative scores are arbitrary. **UpGuard security scores are mapped to ranges corresponding to potential data loss, financial damage, and business security culture.**

Continuous Audit

Traditional business assessments follow traditional business cadences: annually, quarterly— but cyber risk changes daily, hourly, in real time as someone works on a system. **UpGuard continuously audits vendors to maintain current risk analytics and capture historical trends and timelines.**

Remediation Tracking & Score Weight

As vendors address their risks, UpGuard security ratings reflect their efforts to do so. By focusing on relevant risks, UpGuard immediately captures changes in vendors' posture, visualizes the changes over time, and describes how each change affects overall risks to the business. Scores are weighted by criticality of risk category. Category criticality is calculated based on analysis of the risk that each attack vector presents. This in turn is based on research into the historical breaches that have leveraged this attack vector, as well as the ease with which it can be exploited. Due to the uniqueness of each domain assessed for risk, risk factor weights could vary by no more than (±) 5 percentage points per domain.

Risk Factors by Criticality

Critical Risks - (Score weight: ~50%)

The highest level of risk factors are those sufficient to be the root cause of a breach of information confidentiality with no additional factors, are universally acknowledged to be standard controls, and are easy to exploit.

- SSL not available
- Database ports open
- File sharing ports open
- VOIP ports open
- Mail ports open
- User authentication ports open
- HSTS not enforced
- Application ports open
- User authentication ports open
- Administrative ports open

High Risks - (Score weight: ~30%)

The next tier of risk factors are those that could lead directly to a breach but require a more sophisticated attack or are highly indicative of poor IT processes.

- Domain blacklisted for malware
- Weak SSL algorithm
- SSL expired
- Administrative ports open
- HTTP still accessible
- Suspected phishing pages present
- HSTS does not include sub domains

Medium Risks - (Score weight: ~15%)

Medium risk factors are those that can successfully execute a part of an attack but which require additional action from the human targets or additional specific system configurations that cannot be ascertained externally.

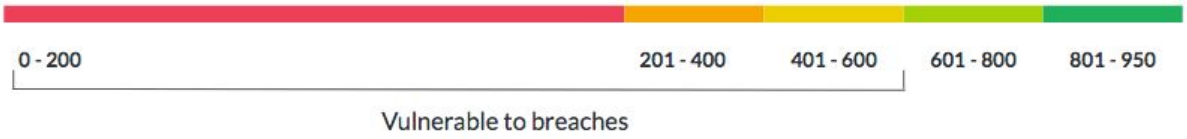
- SPF not enabled
- Domain expiring soon
- Cookies not secured
- Domain registration not secured
- Server headers not obscured
- HttpOnly cookies not used
- Domain expired
- SSL certificate expiring soon

Low Risk - (Score weight: ~5%)

The idea of "low risk" is misleading, in that breaches are typically executed by combining many factors, each of which may be low risk in isolation. These are only rarely seen in actual attacks, or are so widespread that they have a weak correlation with the overall integrity of IT processes.

- DMARC not enabled
- DNSSEC not enabled
- Lenient SPF filtering
- Low employee satisfaction
- Low CEO approval rating

How our scoring works



801 - 950 Excellent hygiene

- Absolute low risk for data breach in the immediate future; organizations possess strong competencies in creating, adopting, and implementing strong security policies. About 85% or more of all domains and information assets exhibit consistent security state with scores above 800. Internal security practices are consistent in strength to external state. Excellent at gathering insights into their attackers. Understand their vulnerabilities and conduct realistic simulations against them on a monthly to quarterly basis. Organizations in highly targeted industries like finance, government, health, energy, or education are highly resilient against any persistent threats. Very few remediation activities, if any will need to be produced for these suppliers as conditions of business. Organization fosters a culture that keeps personnel motivated to proactively look for potential risks and have efficient processes for these to be flagged. Financial loss due to data exposure is unlikely.

800 - 601 Inconsistent security practices

- Low to medium risk of data breach in the immediate future; organizations refer to best practice frameworks for security policies and dedicate financial and human resources to implement them, but they may be inconsistently applied across digital surfaces. Some domains and information assets may be scored notably less secure than others, but overall about 75% - 85% score higher than 650. Organizations being considered for critical supply functions at total scores of 650 or below may require special care in the SLA process or may require demonstrated remediations as conditions of business. Internal security practices refer to commonly adopted frameworks or more stringent custom policies, but a shortage of financial, human, or talent resources may cause inconsistent application; security questionnaires are highly recommended, and these organizations are likely to respond in accordance with reality. These organizations often train employees about two times a year on what cyber risks may lead to leaks, but often lack the effective processes for personnel to flag them. If organizations in this score range are in highly targeted industries like finance, government, health, energy, or education, then persistent attacks may lead to successful breach and financial impacts.

400 - 600 Identified risk

- Medium to high risk of data breach in the immediate future; may have already been breached in the last year or are continuously being breached and are unaware. Organizations in the range of 500-600 may know that they need to adopt best practice security frameworks but the implementation of known frameworks, or the development of stronger custom standards may not be placed on the organizational roadmap until a well publicized breach occurs, until regulators levy fines, or until their public trust is endangered. Domains and information assets are inconsistently

managed, with unknown owners in the organization and less than 20% of domains scoring above the 650 range and less than 10% scoring above 750 - 800. Potential vendors in this range being considered for fulfilling critical functions will require extreme care and verification of remediations as part of the SLA process. Internal practices are poorly managed with lack of visibility into systems and processes that deliver services to customers. High risk of major outage in the future. The organization may conduct a yearly training on cyber risk or neglects to distribute this knowledge to employees. Organizations in critical sectors like finance, government, health, energy, or education are in critical need to divert resources to security as it is highly likely that attackers targeting these organizations today will succeed in breach.

201 - 400 Risk concurrent with breach states

- High risk of being breached in the immediate future or that this organization has already been breached. For smaller organizations with 500 - 1,000 or fewer employees in non-technology or service sectors such as manufacturing, industry, materials, agriculture, etc., security is very much often not considered in the roadmap of their business and may even be seen as an unnecessary expense. For organizations at the enterprise level or in service and technology sectors, scores in this range are high cause for concern. Organizations do not consider or implement security frameworks for external or internal security practices. Smaller organizations in non service or technology sectors will only manage a small number of domains and information assets, and do not dedicate many resources to their monitoring. Larger organizations will have fewer than 60% to 70% of their domains or digital assets scoring above the 350-500 range, with only about 15% to 20% scoring above 450. At the organization level, security may not be owned by one person and may be handed to a systems administrator, generalized IT employee, or non-reputable contractor to fulfill. Very little to any communication of cyber risk in the organization. Organizations in critical sectors like finance, government, health, energy, or education are in dire state and pose an immediate threat to the public with high likelihood of regulatory fines or litigation in the future. Potential vendors in the 300 to 400 range will need a very large partnership investment and transfer of knowledge in order for remediation to occur that would make them viable suppliers. Potential suppliers in the 200 - 300 range or below should be avoided.

0 - 201 Compromise, compliance violation, financial loss

- Organizations in this range will have multiple points of entry for breach. Any organization in any sector of business in this range does not dedicate close to the appropriate amount of resources to security. Understanding and assessing cyber risk is not on the roadmap of the organization. Fewer than 80% of individual domains or information assets score above 400, with fewer than 50% scoring above 350. It is likely that these organizations do not have a large external digital footprint or internal network. Ownership of IT operations and security is not defined or handled by a non-professional. Organizations in this score range should not be considered for any business function. These organizations do not adhere to any security policies of frameworks. These organizations may be too small to be in the scope of regulation or have their business irrevocably harmed by regulatory fines.

Businesses depend on trust, but breaches and outages erode that trust. UpGuard is the world's first cyber resilience platform, designed to proactively assess and manage the business risks posed by technology.

UpGuard gathers complete information across every digital surface, stores it in a single, searchable repository, and provides continuous validation and insightful visualizations so companies can make informed decisions.

723 N. Shoreline Blvd.
Mountain View, CA 94043
+1 888 882 3223
www.UpGuard.com