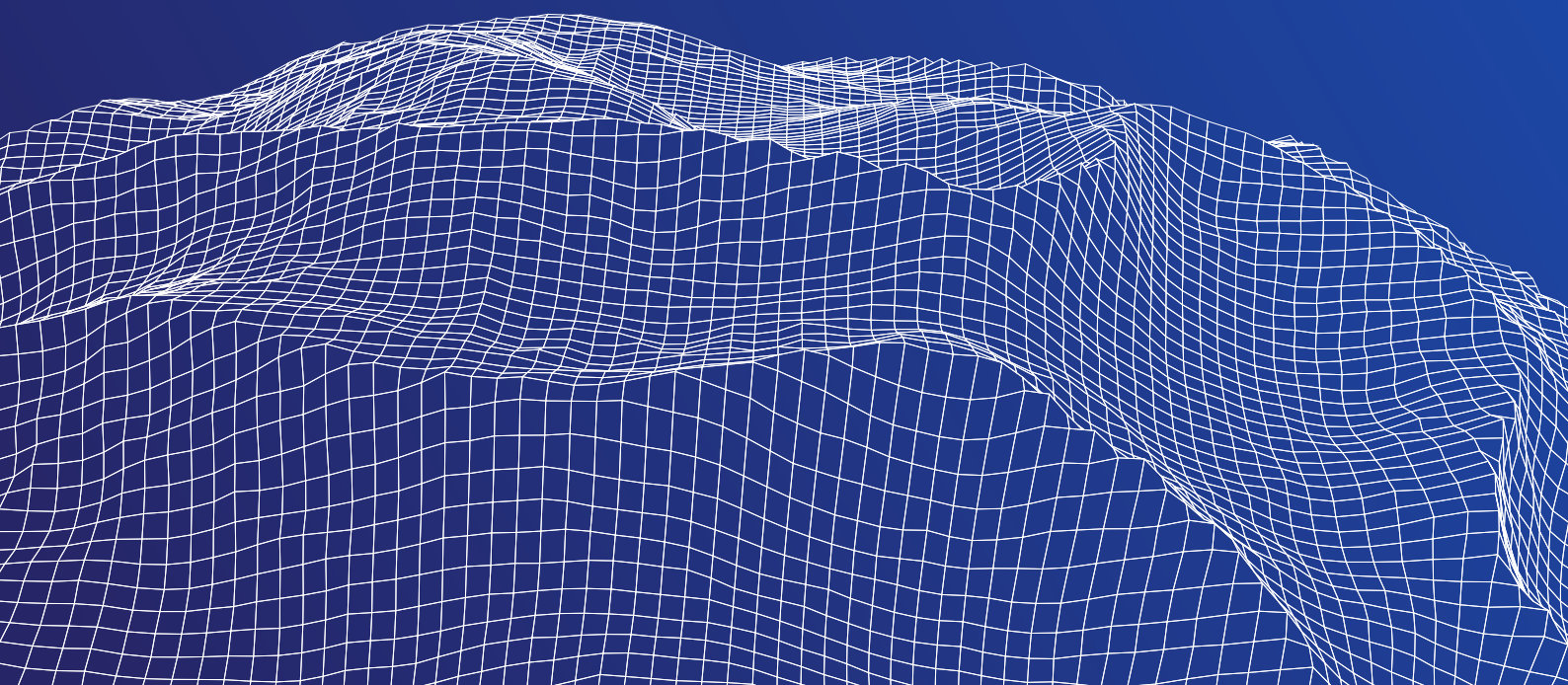
UpGuard

The Buyer's Guide to Third Party Risk Management



Introduction

The extended data center

The data center is no longer confined to a server room or a switch closet. It extends into every vendor that handles data and provides technological services or infrastructure.

Managing the business risk incurred by technology has proven difficult, even when it was confined to a local data center; with the sprawling, interdependent ecosystem of modern digital business, the scope and complexity have increased significantly. The need for efficient management of this risk has created a market for vendor assessment and scoring, in which very different solutions compete for the same function.

Understanding your own goals, and what solutions need to provide to reach those goals, are key to navigating this space.

Vendor risk solutions

The primary risks posed by technology vendors are the breach or exposure of sensitive data, and the unplanned interruption of services by a technical incident in the vendor's environment.

The same concerns an IT department might have about a local environment can be extrapolated to vendor infrastructure, so understanding how a vendor handles their security and operations leads to understanding how likely they are to suffer a breach, leak, or outage. However, equally important, is that this understanding can be achieved with a minimum of overhead.

With dozens or hundreds of vendors, many organizations find themselves unable to keep pace with vendor assessments. A vendor risk solution must eliminate this overhead so that assessment can proceed at scale and with little specialized knowledge and less manual effort.

Businesses simply have too many vendors to assess them all thoroughly.

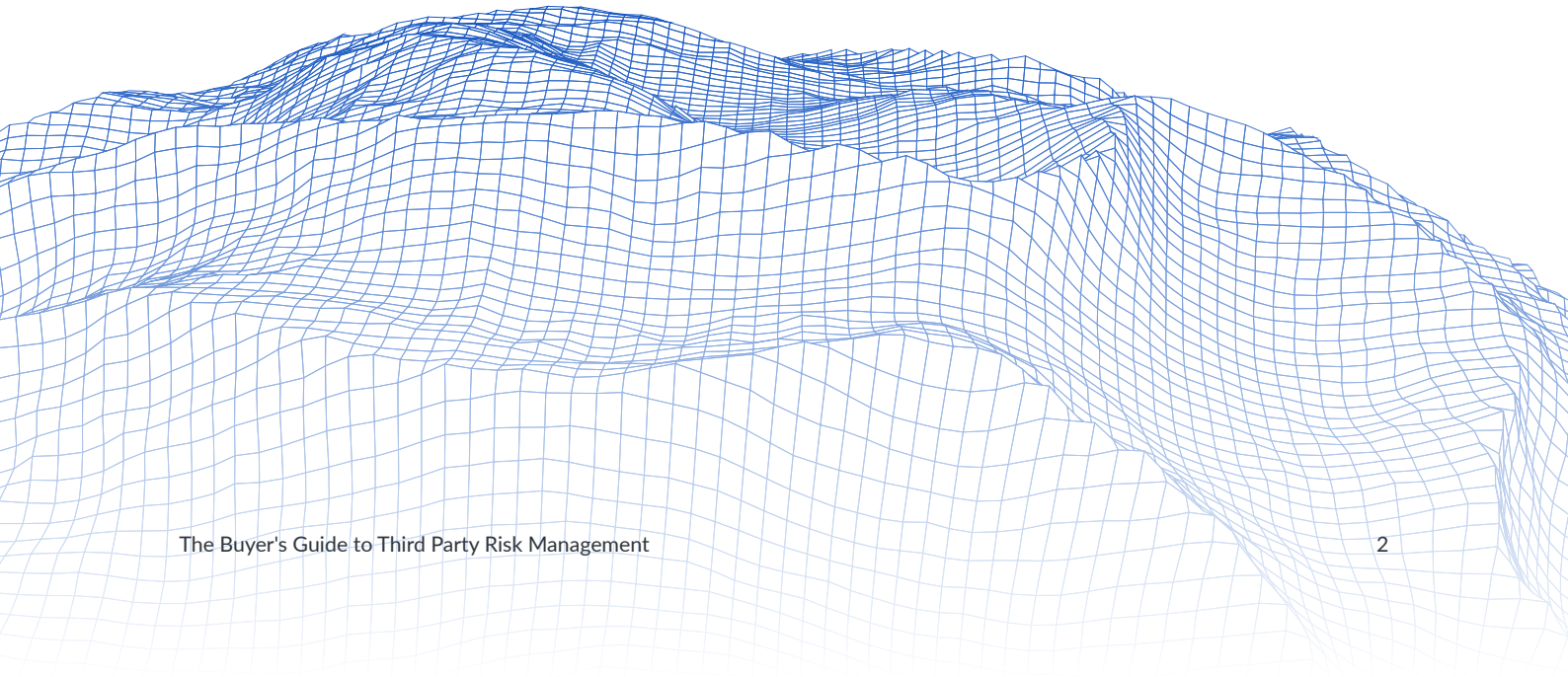
Security Ratings

Why use 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.

Credit scores make debt risk legible, returning an easily understood aggregation of risk assessment efforts in a standardized, comparable system. Security ratings solve the problem of cyber risk like credit scores: specialists assess each company using a standardized collection of criteria and proprietary tools, and return a rating that can be understood in a business context by nontechnical people.

Risk ratings aren't magic, they're math.



What makes a good rating?

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

Threat focus

There are many factors that can be used to determine a security score. But only those factors that directly relate to the possibility of breach and outage provide actual assistance in reducing the likelihood of those incidents. How the security rating helps address actual threats should be clearly documented.

Business context

You might know that A is better than F, or that a higher number is better than a lower number, but unless the risks causing the lower score are explained in terms of how they could affect business, those comparative scores are arbitrary. Security ratings should explain why a low score is risky, in terms of potential loss and damage.

Transparency

Although the algorithms used to derive the score itself are proprietary, the factors that are considered in the score should be clearly laid out. Security ratings aren't magic, they're math, and the more a client knows about what a security rating really measures, the better they are able to control their vendor risk.

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. Security ratings should continuously audit the vendors they score to always have a current risk analysis and to provide historical trends and timelines.

Internet-wide score database

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 providing ecosystem. Security ratings should be internet-wide, able to report on the risk of any digital business in the world.

Remediation tracking

As vendors address their risks, the security rating should reflect their efforts to do so. If the rating is driven by relevant data, it should immediately reflect changes in vendors' posture, visualize those changes over time, detail what changed, and how each change affects the business risks involved.

Data Collection and Presentation

Scope of coverage

Digital surfaces

Every digital business has an internet footprint. This is the surface area of the domains, devices, and data belonging to the organization that is accessible from the internet. Third party risk solutions analyze this footprint to determine a company's posture. The great advantage of examining this footprint is that it can be assessed independently and remotely, making it an obtainable and objective source of information. Because every organization has a similar footprint, assessments can be compared and contrasted in a standardized system.

The disadvantage of course is that the internet footprint is only a subset of the total digital surface of a business — however, it often telegraphs the state of the internal infrastructure.

Trustworthy attribution

When selecting a third party risk solution, the scale of data collection needs to be balanced against the accuracy and relevance of that data. The internet is vast and dynamic, and just as in any other risk calculation, there are tradeoffs between having more data and having completely trustworthy data. If your organization wishes to perform substantial amounts of work sanitizing and correcting your vendor's data, then solutions that cast a wider net with a higher rate of false positives may be appropriate.

Generally, however, the problem is not getting enough data, but getting the right data: the elements that leads to data breach, that have a strong correlation with internal practices that cannot be observed directly, and which have an auditable provenance you can trust.

Important Threats

Ransomware and malware

Exposed ports and unpatched systems are responsible for nearly all of the major ransomware and malware attacks that occur, including WannaCry and Petya.

Man-in-the-middle

Encryption strategies, including scope, cipher strength, and configuration, determine whether information passed across the internet can be intercepted by a third party.

Phishing and email fraud

Phishing emails trick people into installing malware, exfiltrating sensitive data, and even transferring funds. These, and other fraudulent emails can be prevented from even reaching their human targets by the right defenses.

Vulnerable software

Most exploits target vulnerabilities that have been known for over a year and have available patches. Advertising vulnerable software gives attackers the vectors they need to get inside.

Insider attack

Dissatisfied employees not only increase the risk that sensitive data will be misused, but also increase the risk of operational failure due to oversight or negligence.

Domain hijacking

Redirecting clients to a malicious site allows attackers to capture usernames, passwords, and any other information normally passed to a trusted site. The proper defenses drastically reduce the risk of this possibility.

Prioritized remediation guidance

Technical transparency

We've focused on the risks themselves and how to measure them, but what happens after they are measured?

A good vendor risk solution should transparently detail how each vendor incurs risk, and offer technical remediation advice, so that vendors and their clients can directly relate the security rating to real world IT practices, and understand the steps necessary to improve their posture.

A solution should also prioritize these risks so that work can focus on remediating the most dangerous aspects first.

Risk transparency

Additionally, the consequences of failed technical checks should be explained to both parties in terms of potential loss and damage. Not many people care about whether port 1433 is open to the internet; a great many more people care about corporate databases leaking onto it.

A vendor risk solution that translates one to the other will expedite remediation efforts and help resource and budget planning.

The need for attestations

The limitations of security ratings

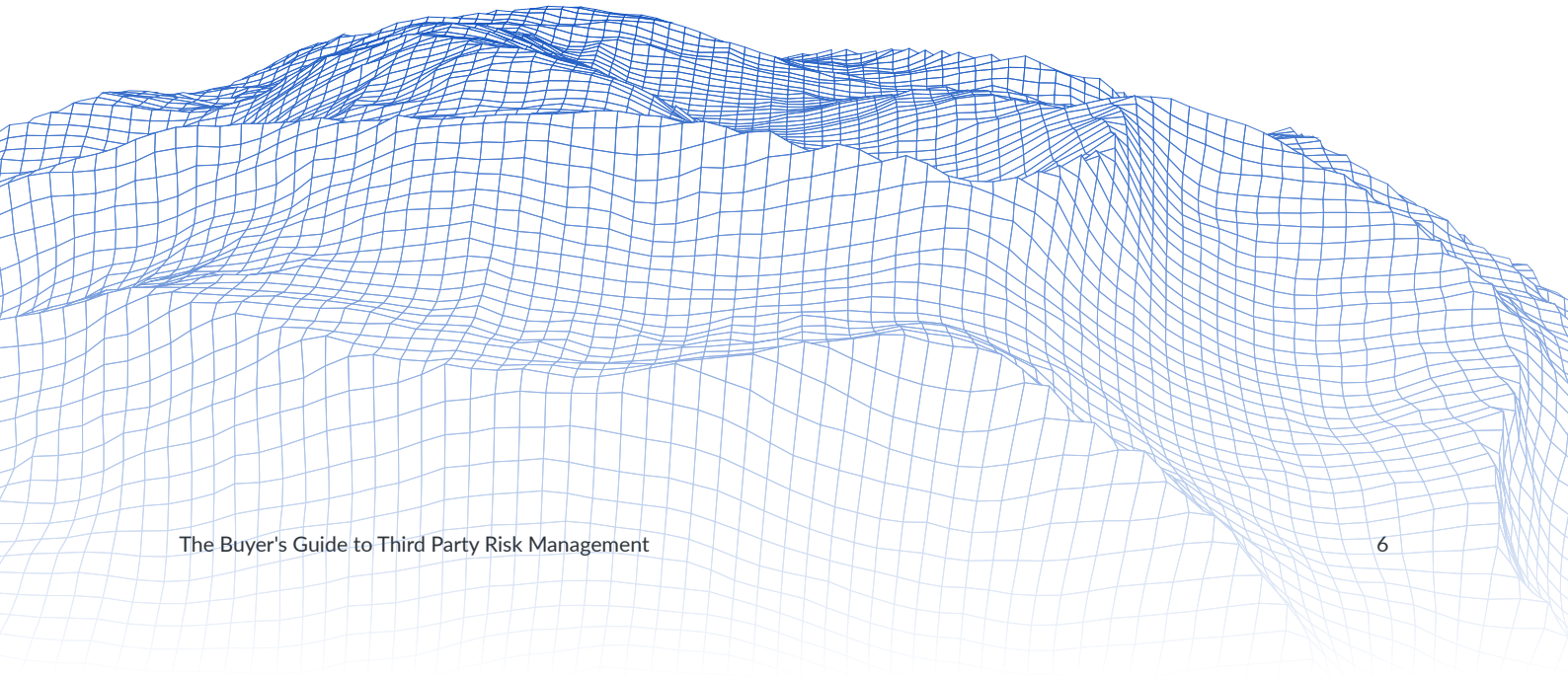
The technical assessments provided by vendor risk solutions are based on the internet footprint. However, the internal technology and processes used by the vendor also determine their risk to a great degree.

While the external posture does reflect overall priorities and efforts, it is only a subset of the risk picture. For this reason, it is necessary for organizations to get a better picture of a vendor's internal infrastructure and IT methodology, to complement the independent external assessment.

The questionnaire process

Vendor questionnaires address the need for more visibility into internal operations by prompting the vendor to disclose their security practices, employed technology, and vendors in their supply chain that will affect data handling and services.

The questionnaire aspect should be fully addressed in a vendor risk solution so as not to rely solely on the external examination. A questionnaire automation solution should be sufficiently extensible and automated to save time and enable human analysts to spend more time examining the most problematic or complicated responses.



Automating assessments

Integrated questionnaires

The core questions asked to determine security and operations are the same for nearly every vendor. These questions should be easily available within the vendor risk solution for general use.

Customization options

Core concerns aren't the only concerns, and a good vendor risk solution should allow the customization of questionnaires to include any additional important information and omit anything unnecessary.

Automated delivery and renewal

Keeping up with vendor questionnaires on a regular schedule is extremely difficult at scale— a good solution for managing third party risk should eliminate the manual steps of the delivery and renewal process so questionnaires get processed in a timely manner.

Questionnaire storage and history

Storing the questionnaires and organizing them for easy access is important for a vendor risk solution if it is to be a system of record for vendor due diligence. Likewise, questionnaires should be kept in perpetuity and available in a chronological context.

Risk Transparency and Remediation

Both the vendor and the client should have context and guidance provided to them by the questionnaire, based on the answers given. This helps vendors understand areas to improve, and helps clients understand why a vendor's practice introduces risk.

Final Considerations

Pricing and feasibility

Finally, for whatever functionality a vendor risk solution offers, an obstructive price renders it moot. If high prices don't remove the solution completely, they greatly reduce the scope of coverage. A good vendor risk management solution should be feasible at scale, with a clear pricing model.

Some questions to consider about pricing include:

- Is the solution priced per vendor? How much per vendor?
- Does the price per vendor allow coverage for all vendors?
- Will you have to compromise on the frequency of assessment due to a solution's price?
- Does the solution offer value in terms of risk mitigation and administration reduction?
- Does the solution provide enough information for your technical staff to know how to improve your risk score?
- How much effort is required to remove false positives from the risks attributed to your business' digital footprint?
- What parts of the data center are outsourced, if any?

Conclusion

Finding the right solution for third party risk management is different for every company. Different concerns, priorities, and resources demand flexibility, while the primary threat vectors introducing cyber risk into a vendor should be covered comprehensively. The process of assessment should be as automated as possible, and legible without special training or expertise. The solution should cover both an independent technical assessment and questionnaires about internal infrastructure and processes.

Holding vendors to the same standard a company would hold their own IT department is how we build a resilient digital ecosystem. The threats to data and services in a vendor's hands are the same as if they are running on company servers— and the consequences are the same as well.

With the right solution, proactive vendor risk management is possible to both perform due diligence when selecting or renewing vendors, and to help remediate vendor risk, so that business can be done safely, in private, and without interruption.

About UpGuard

UpGuard's products provide a better, smarter way to automate cybersecurity risk assessments and prevent breaches

UpGuard is a cybersecurity company that helps businesses manage IT security risks, both internally and in the supply chain. UpGuard's integrated risk platform combines third party security ratings, security assessment questionnaires, and proactive threat intelligence capabilities to give businesses a full and comprehensive view of their risk surface.

UpGuard VendorRisk

Explore >

Monitor your third-party vendors

UpGuard VendorRisk monitors, rates and sends targeted security questionnaires to your vendors. We also automate security questionnaires so you don't have to.

- Automated vendor reports and scoring
- Intelligent questionnaire engine
- 3rd and 4th party supply chain analysis
- Industry benchmarking and classification

UpGuard BreachSight

Explore >

Monitor your external security posture

UpGuard BreachSight continuously monitors your business for data exposures, enabling you to prevent breaches, protect your reputation and avoid regulatory fines.

- Continuous monitoring of your digital posture
- Modular plugins for new security vectors
- Billions of signals being discovered daily
- Remediation workflow automation

UpGuard Core

Explore >

Monitor your internal IT infrastructure

UpGuard Core automates internal security and compliance for enterprises with hybrid on-premise/cloud IT, giving you instant visibility into your entire infrastructure.

- Automated security configuration monitoring
- Agent and agentless data collection
- Smart infrastructure policy and scoring
- Change detection and compliance

About UpGuard cybersecurity ratings

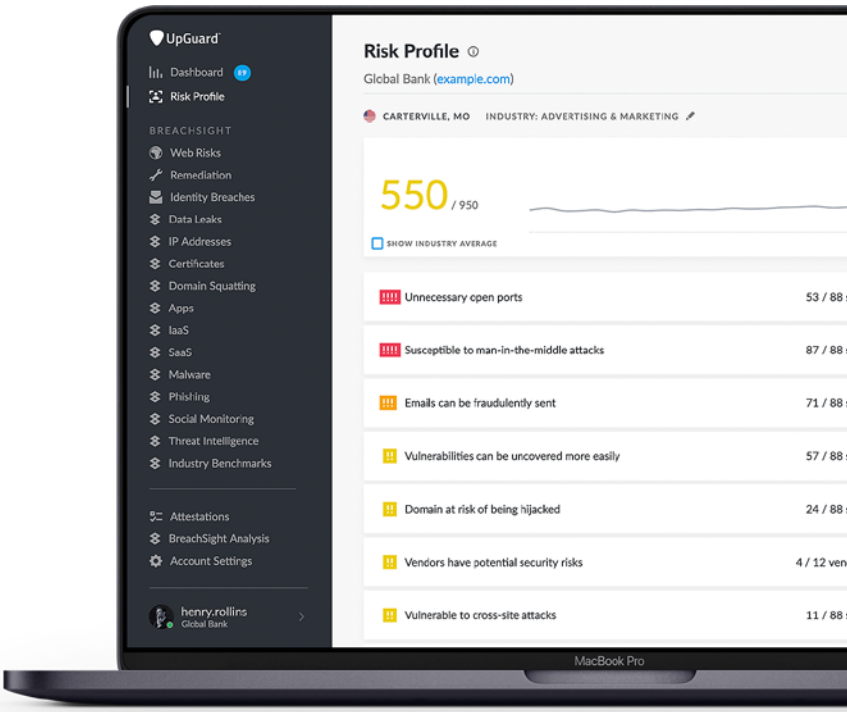
UpGuard Cyber Security Ratings (CSR)

Historically, cyber risk been measured through a combination of manual processes such as employee surveys and rudimentary automated scanning. However, without reliable, comparable risk assessments, organizations cannot benchmark their cybersecurity performance and improve it over time.

UpGuard Cyber Security Ratings (CSR) are a single, easy-to-understand score from 0-950 that represent an organization's cybersecurity performance. Similar to a consumer credit score for cybersecurity. A higher rating represents better performance. UpGuard CSR also takes into account historical security performance and performance over time.

Based on millions of data points, we calculate an instant snapshot of each company that covers the following basic elements of security:

- Security misconfigurations
- Indicators of malware, phishing, and similar attacks
- Susceptibility to web vulnerabilities
- Weaknesses in security practices and hygiene
- What parts of the data center are outsourced, if any?



UpGuard

Know your vendors. Secure yourself.

Looking for a better, smarter way to protect your data and prevent breaches?

UpGuard offers a full suite of products for security, risk and vendor management teams.

Book a demo | Learn more

Trusted by hundreds of companies worldwide

Bill.com MORNINGSTAR NASA NYSE iag ICE Akamai ADP

www.upguard.com

+1 888-882-3223

723 N Shoreline Boulevard, Mountain View CA 94043, United States