UpGuard

Whitepaper

Risk Remediation Planning

How to Intelligently Prioritize and Remediate Cyber Risks.

UpGuard

Table of Contents

UpGuard

Introduction

The average global cost of a data breach in 2021 is $US 4.24 million, and the international average cost of cybercrime is expected to peak at US$ 6 trillion annually by the end of 2021.

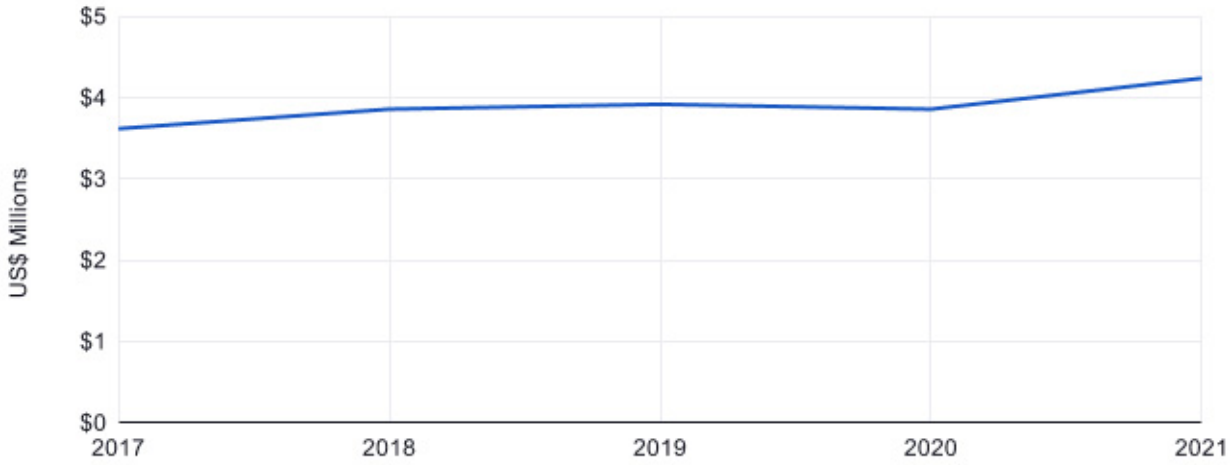
Slow response times significantly inflate remediation costs. According to IBM, victims that respond to data breaches in under 200 days spend an average of $1.1 million less on data breach damages.

This is concerning because the average number of days required to identify and contain a data breach is 287, cementing organizations in the upper pricing range.

This major pricing factor has been poorly addressed in cybersecurity programs across industries causing data breach costs to rise each year.

The current average of $US 4.24 million is a 10% increase since 2020 and the highest it has ever been.

Average Cost of a Data Breach 2015 - 2021



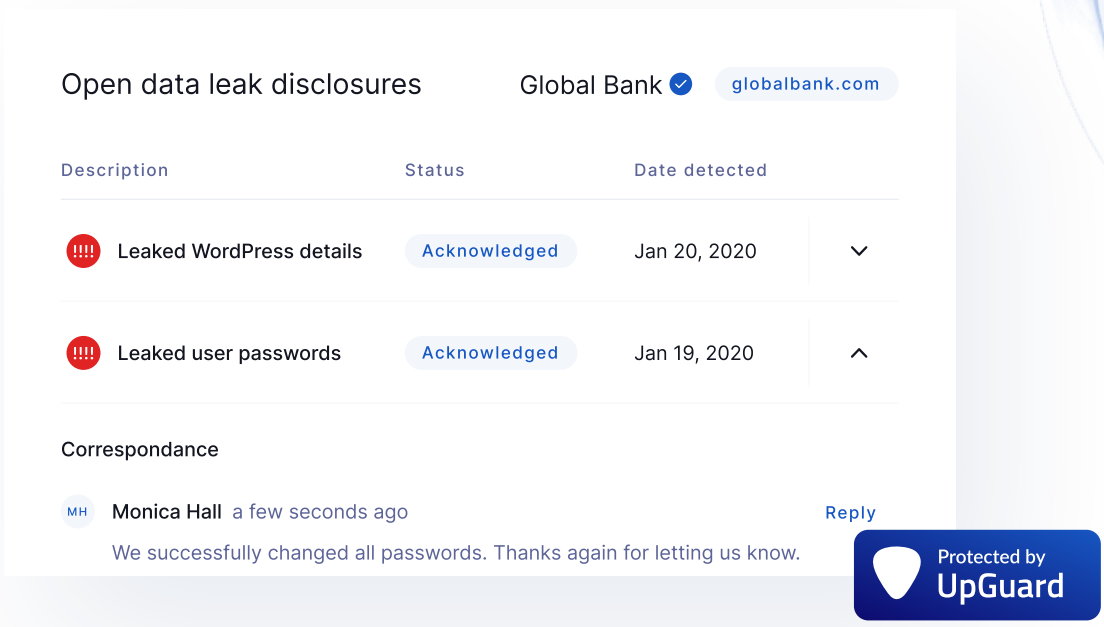
Data source: Cost of a Data Breach Report 2021 (IBM and Ponemon Institute)

Data breach response times are not protracted because of incompetence. Security teams are too overwhelmed to efficiently manage all of the vulnerabilities that facilitate these events.

UpGuard

Since the proliferation of digital transformation is unavoidable, the only solution for assuming control of cyber threats is to achieve a **more efficient distribution of remediation efforts.**

This whitepaper describes the process of risk remediation planning to help organizations dramatically decrease data breach response times and the cost of these events.



What is Risk Remediation Planning?

Risk remediation planning is the process of strategically prioritizing corrective efforts so that the most critical security risks are addressed first.

The criticality level of each identified risk is proportional to its impact on security posture in the event of exploitation. Because of this, the objective of remediation planning is to distribute response efforts so that the highest possible security posture rating is maintained at all times.

The calculation of such an optimal description is a function of risk identification, risk impact assessment, and risk prioritization analysis.

Common Challenges of Risk Remediation Planning

The rising trend of data breaches demonstrates a lack of adequate risk remediation planning across all industries. This is especially the case for regulated industries like health, finance, and law which suffer the highest rates of cyberattacks each year.

Average Distribution of Data Breach Costs for Highly-Regulated Industries

Data source: Cost of a Data Breach Report 2021 (IBM and Ponemon Institute)

Some of the common challenges fueling this security deficit are discussed below.

Lack of Visibility

Poor visibility of the attack surface prevents security teams from identifying risks early enough to allow sufficient time for remediation.

Time is of the essence especially when data leaks are concerned - involuntary exposures of sensitive data.

When cybercriminals discover data leaks, they get free instant access to vital security intelligence that otherwise could have only been retrieved through laborious reconnaissance campaigns.

By overlooking internal and third-party data leaks, these critical risks cannot be included in remediation strategies. As a result, data breaches events are accelerated and even multiplied, keeping breach response times extended.

Poor Communication

Sluggish communication channels between vendors prevent risk assessments from being managed effectively. Without instant visibility into each vendor's risk assessment status, third-party risk cannot be rapidly identified and addressed in a remediation plan.

No Risk Prioritization Plan

Security risks that are identified are not ordered by level of criticality, and response efforts are not prioritized by risk appetite. As a result, all vulnerabilities are addressed in the order they are received without considering the impact on security posture.

No Vendor Prioritization Plan

Without a risk prioritization mechanism it's challenging to determine which vendors are putting you at a heightened risk of suffering a third-party breach.

This prevents the establishment of a remediation plan where the security risks of each vulnerability are considered to determine the most critical vendors that should be addressed first.

Some vendor relationships are not worth preserving because the security risks they introduce are too extreme. Without a vendor prioritization plan, such dangerous vendor relationships remain overlooked, increasing the chances of your organization being impacted in a supply chain attack.

3 Step Framework for Risk Remediation

An essential prerequisite to the design of a risk remediation plan is a risk management program.

The following 3 step framework distills the complexity of attack surface management into controllable components that form the foundation of a risk remediation plan.

Step 1

Security Risk and Attack Pathway Identification

All risks that could be potentially detrimental to processes and information security must be identified. But just being aware of vulnerable assets is not enough. It's important to also map their connections so that potential cyberattack pathways can be intercepted.

This can be achieved through digital footprint mapping.

Digital footprint mapping is important because your digital presence is your largest attack vector. This effort considers the third-party threat landscape - an extensive attack landscape that's completely overlooked by antivirus solutions and firewalls.

A digital footprint is a map of your entire attack surface. This could include:

- All shadow IT devices
- All endpoint devices
- Privileged access accounts
- All cloud-based service providers.
- Open Ports
- Misconfigured cloud storage services
- Unpatched vulnerabilities

Digital footprints identify all possible entry points that cyber attackers could exploit. This is done in 2 phases.

Phase 1: Discovery

The first step in mapping your organization's online presence is identifying all assets exposed to the internet.

This includes:

- Cloud solutions
- Domains
- Open Ports
- TLS certificates
- Data APIs

Cloud technology makes this task very difficult since it accelerates the expansion of assets and their connections.

Phase 2: Mapping

With all digital assets and vulnerabilities detected, it's time to map the connections between them.

Both the discovery and mapping phases of digital footprinting should be completed with a cybercriminal mindset. This is because cybercriminals follow the same sequence when planning a cyberattack - first, they discover associated assets, then map their connections to surface potential entry points.

To maintain this unique perspective it helps to use search engines cybercriminals are likely to use. Here are two examples:

- Shodan
- HaveIBeenPwned

These solutions will help you learn how much of your digital footprint is currently exposed to the public, allowing you to fill any gaps in both the discovery and mapping phases of your digital footprint efforts.

All discovered vulnerabilities and their connections can then be represented graphically through network diagrams.

When mapping the third-party network, It's very difficult to estimate the risk profiles of vendors and their digital footprint short of requesting access to their footprinting documentation.

Even if this is provided, there's no way of confirming legitimacy or whether their efforts were thorough enough to identify all critical vulnerabilities.

Because third-party breaches are on a rising trend, statistically speaking, your vendors will not take cybersecurity as seriously as you do.

Next Generation Software Supply Chain Attack

Typosquatting, malicious code injection, and tool tampering

Data source: 2020 State of Software Suppply Chain report (Sonatype)

It's best, therefore, to take ownership of vendor security by using a vendor attack monitoring solution to evaluate the security postures of all third parties.

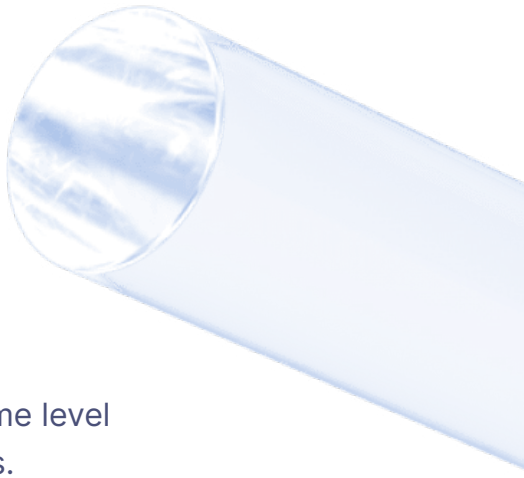
UpGuard

UpGuard Monitors the Entire Threat Landscape to Detect all Internal and Third-Party Security Risks

UpGuard overcomes the challenges of digital transformation by continuously scanning the entire threat landscape to discover vulnerabilities often hidden in cloud technology.

With UpGuard, laborious digital footprint mapping is not required to surface exposures. Security teams can instantly see all of the risks threatening their digital landscape from a single pane of glass view covering both the internal and third-party vendor network.

This uncovers areas with high concentrations of risk - intelligence that can then be used to establish an efficient remediation plan.



Step 2

Define Risk Severity

A common misconception amongst security teams is the same level of attention should be applied to all discovered security risks.

This makes risk management burdensome and overwhelming.

A more sustainable approach to vulnerability management is to only focus on the risks that are most detrimental to your security posture and to outsource, or even waive, all other risks.

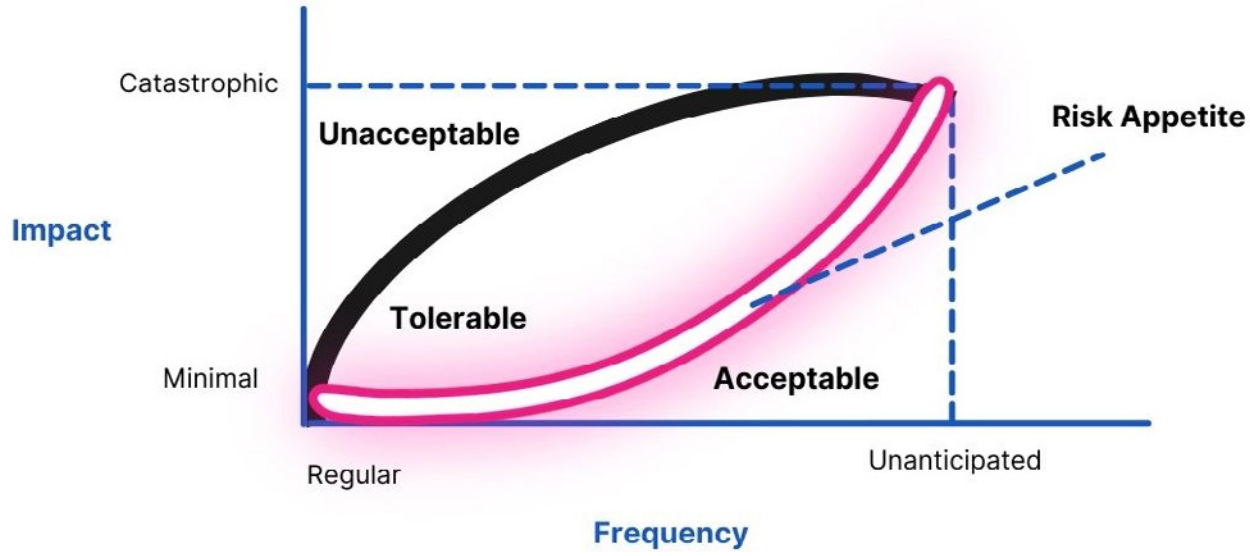
This line in the sand is established by defining a risk severity framework.

Risk severity can be classified into 4 categories:

Avoid	Aim to reduce or eliminate risks by adjusting program requirements.
Accept	Acknowledge risks without implementing controls to address them.
Control	Deploy efforts that minimize the impact and probability of risks.
Monitor	Monitor risks for any changes in severity.

This threshold can be represented graphically on an impact vs frequency graph. Monitoring efforts span across all three segments to detect any changes in the risk distribution.

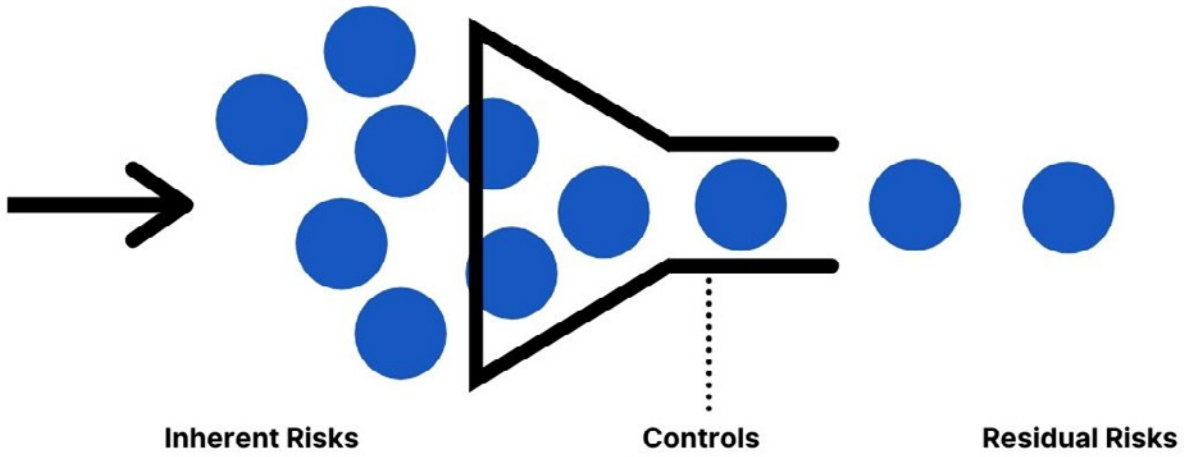
Risk Impact vs. Risk Frequency



Before an acceptable risk severity profile can be applied, it's important to understand the difference between inherent and residual risks.

Inherent risk is the level of risk in the absence of security controls. Residual risk is the level of risk that remains after security controls have been implemented.

Inherent Risks vs. Residual Risks



The level of acceptable risks depends on the risk appetite and regulatory compliance requirements of each organization. At a high level, all acceptable risks should have minimal impact on revenue, business objectives, service delivery, and attack surface management.

Acceptable risks need to be defined for each individual asset. The following risk threshold calculation analysis framework will distribute this effort and speed up the process.

- Identify all assets with digital footprint mapping.
- Assign each asset, or group of assets, to an owner.
- Identify each asset's current and potential vulnerabilities.
- Quantify the likelihood of these vulnerabilities being exploited
- Quantify each asset's risk using the following formula:

  Risk = Likelihood x Impact

  Where:

  Likelihood is a function of vulnerabilities, exposure, and threats.

  Impact is a function of business criticality.

The acceptable levels of risk should be defined as a percentage where:

- If the inherent risk factor is less than 3 = 20% acceptable risk (low severity).
- If the inherent risk factor is between 3 and 3.9 = 15% acceptable risk (medium severity).
- An inherent risk factor between 4 and 5 = 10% (high/critical severity).

The lower the percentage, the more severe the cybersecurity risk control requirements are. And the better the risk controls, the higher the chances of recovery after a cyber attack.

The maximum risk tolerance can be calculated with the following formula:

Maximum risk tolerance = Inherent risk tolerance percentage x Inherent risk factor

And the final risk tolerance threshold is calculated as follows:

Risk tolerance threshold = Inherent risk factor - maximum risk tolerance.

For example:

With an inherent risk factor of 3, the corresponding inherent risk tolerance is 15%. The maximum risk tolerance is:

3 × 15% = 0.45.

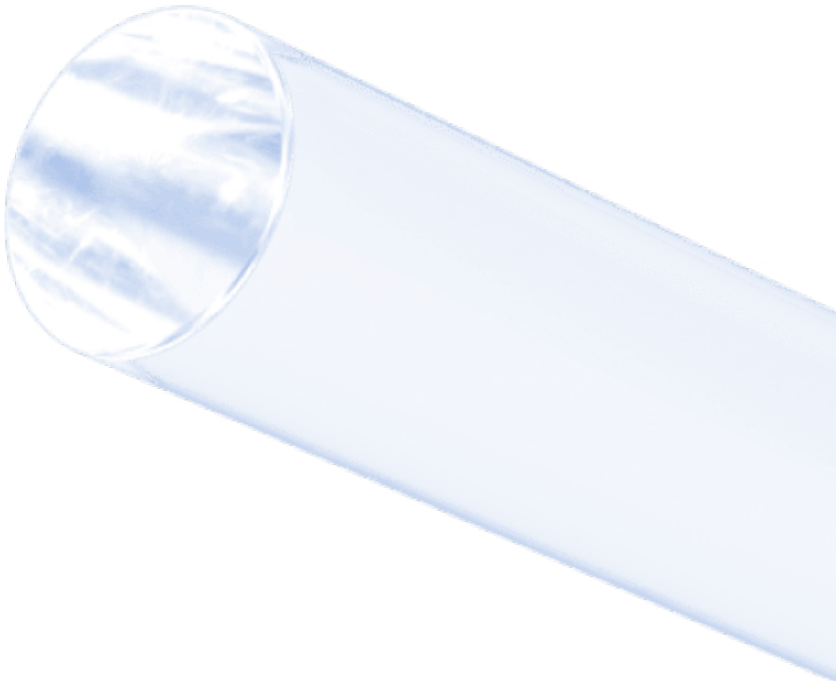
The risk tolerance threshold then becomes:

3 - 0.45 = 2.55.

This means, for mitigating controls to be within tolerance, their capabilities must add up to 2.55 or higher.

Even with solutions in place, new residual risks will keep popping above the threshold, such as the risk of new data leaks.

The mitigation of these risks requires a dynamic “whack-a-mole” style of management - rapidly identifying new risks breaching the threshold and pushing them back down with appropriate remediation responses. The goal is to keep all residual risks beneath the acceptable risk threshold for as long as possible.



Step 3

Risk Prioritization

After identifying all assets and mapping their connections, the vulnerabilities in your entire threat landscape should be evident. Each of these vulnerabilities should then be assigned a severity score to separate the critical exposures that must be prioritized in your remediation plan.

This strategy will minimize the impact of any cyberattacks that might occur before remediations are complete.

Your risk appetite established in step 2 should then be used to create a risk matrix.

A risk matrix determines the severity of each assessed risk (x-axis) and the likelihood of exploitation (y-axis) relative to the set risk threshold.

Risk Matrix Example

Severity →

Likelihood ↓	! Low Little impact	!! Medium Impact is notable but not critical to remediate	!!! High Serious impact and should be remediated immediately	!!!! Critical Could lead to a disaster
Impossible Risk unlikely to occur				
Possible Risk might occur				
Probably Risk will occur				

This risk matrix is then used to evaluate the resilience of specific security policies in a vendor's security program. This information is most efficiently obtained through vendor risk assessments.

Each vendor questionnaire response is reviewed with the risk matrix and assigned a risk rating.

The average number of responses of each risk type provides a very loose estimation of a vendor's security posture

This arduous manual process can be replaced with a vendor risk monitoring solution capable of instantly calculating vendor security ratings. This is especially useful for organizations with a comprehensive vendor network.

All risks in the ‘extreme’ category should be prioritized in a remediation plan. This framework can also be used to rank vendors by criticality through the assessment of extreme risk distribution across each vendor’s security posture.

UpGuard

UpGuard Evaluates the Criticality of all Third-Party Vendors

UpGuard assigns a security rating to each vendor based on the types of vulnerabilities detected on their attack surface.

Security ratings range from 0 to 950 and are comprised of a weighted average of the risk rating across all externally facing assets, such as web applications, IP addresses, and marketing sites.

UpGuard's security ratings are based on an analysis of 70+ vectors including:

- Susceptibility to man-in-the-middle attacks
- Insecure SSL/TLS certificates
- SPF, DKIM and DMARC settings
- HTTP Strict Transport Security (HSTS)
- Email spoofing and phishing risk
- Vulnerabilities
- Malware susceptibility
- Network security
- Unnecessarily open administration, database, app, email, and file sharing ports
- Exposure to known data breaches and data leaks
- Vulnerable software
- HTTP accessibility
- Secure cookie configuration
- Results of intelligent security questionnaires

This rating system allows vendors to be instantly ranked by level of criticality to support proficient remediation planning.

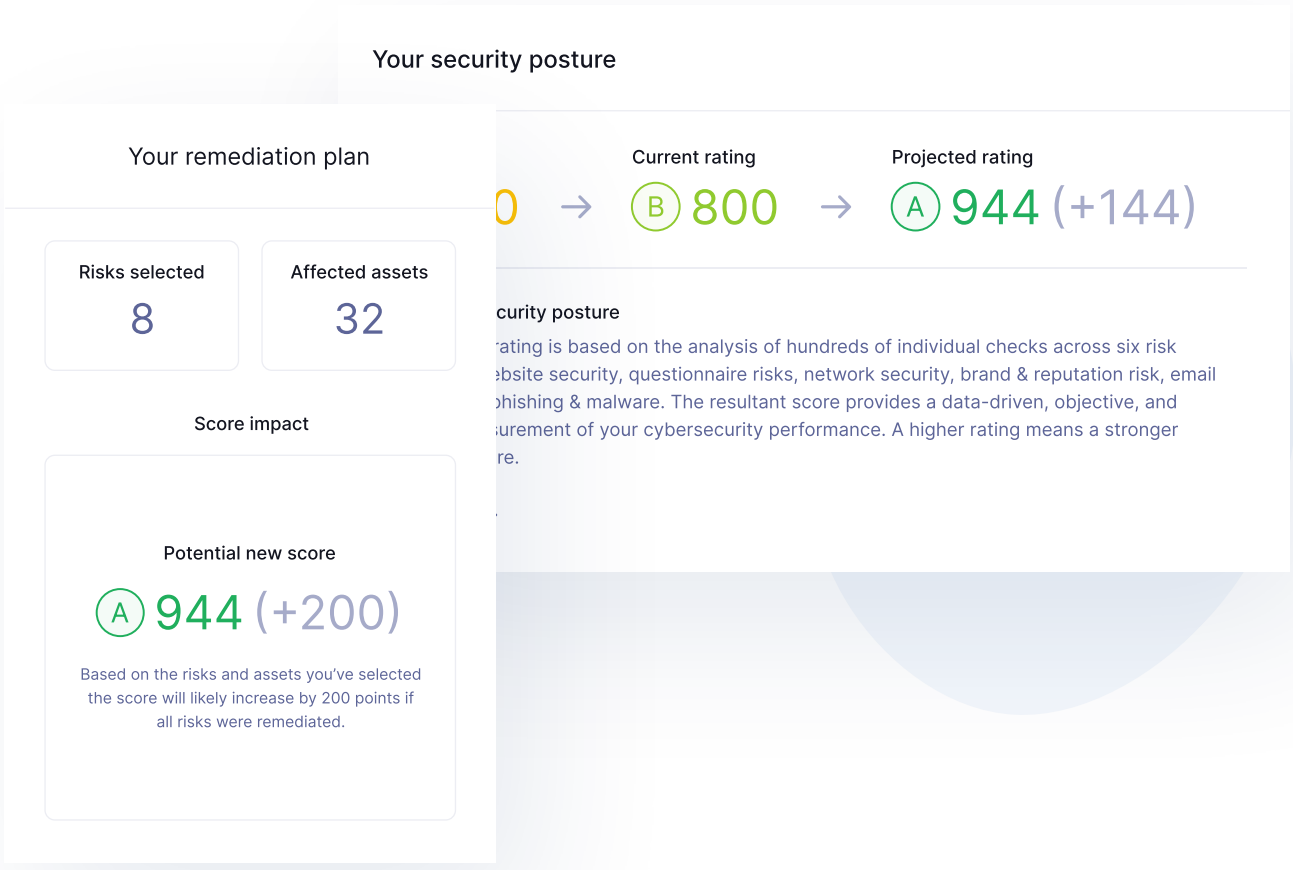
UpGuard

Remediation Planner by UpGuard

Remediation planner by UpGuard further enhances the valuable insights provided by security ratings.

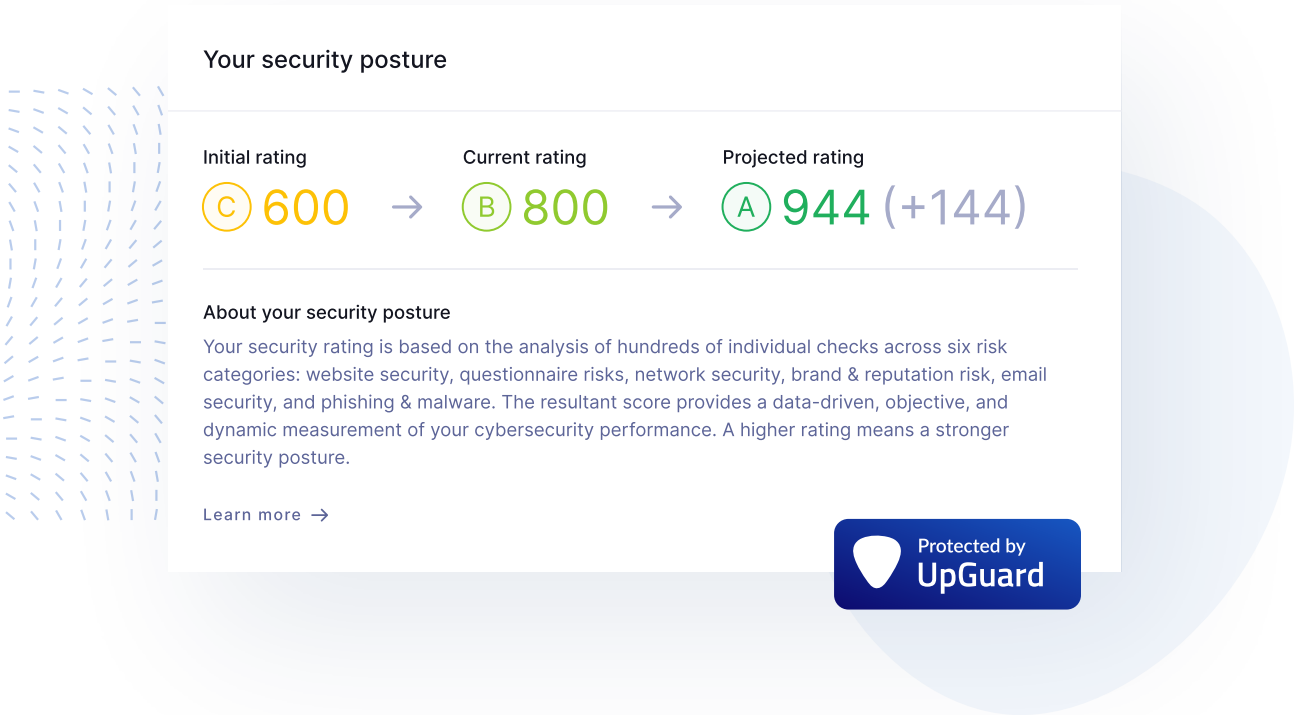
UpGuard's Remediation Planner shows you the projected improvements to security ratings for internal and third-party risks if they are remediated. This allows remediation efforts to be prioritized so that the tasks that have the greatest positive impact on security ratings can be addressed first.

This inverts the inefficient sequence of conventional remediation programs which require security teams to address risks in order to understand the impact of response efforts.



Remediation Planner removes the uncertainty currently stalling response efforts. Because the projected impact of response efforts is instantly known, the lengthy waiting period currently required to evaluate the success of each task is removed.

This significantly reduces incident response times, mitigating the risk of cyberattacks and the impact of data breaches.



Security rating improvements also serve as a guiding metric for security teams, helping them efficiently distribute their efforts while giving stakeholders advanced visibility into the effectiveness of a security program.

Spend less time planning and prioritizing, and more time remediating security risks. Click below to book a free demo of Remediation Planner by UpGuard.

UpGuard

Questions? We have answers

We're here to help, shoot us an email at sales@upguard.com

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.

Contact sales | Free demo →

Trusted by hundreds of companies worldwide

www.upguard.com

+1 888-882-3223

650 Castro Street, Suite 120-387, Mountain View CA 94041 United States