Ratings methodology.

How Bitsight Security Ratings are calculated.

December 2, 2024

BITSIGHT

About Bitsight Security Ratings.

Bitsight Security Ratings describe a company's cybersecurity posture, serve as a measure of their risk, and transform how companies manage security risk by using a data-driven, outside-in approach to rate a company's security effectiveness.

We provide daily security ratings through an automated service that leverages 1 year of supporting data. The sophisticated analytics and alerting capabilities provide risk managers the insight they need to proactively identify, quantify, and mitigate the risk of being exposed to a breach, unlike the manual and subjective assessments used to manage risk today.

How Security Ratings are Presented

Bitsight rates companies on a scale of 250 to 900, with 250 being the lowest measure of security performance and 900 being the highest. The upper and lower edges of this range are reserved for future use. Currently, the effective range is 300-820.

A company's security rating is the result of aggregating the information from all weighted risk vectors and normalizing it for that company.

Security ratings are based on a 10-point rating system that's rounded down in 10 point increments. If the current rating is 740, this is a representation of the combined assessments of all risk vectors. The rating may be somewhere between 740 and 749 in actuality.

An actual rating of 735 is represented as a 730.

Rating Categories

Organizations with high ratings historically have a strong security performance and provide the lowest risk. The average rating is 700.

Each organization's rating falls into one of the following categories:

Categories	Security Rating Ranges	Description	Distribution Ratios*
Advanced	740 - 900	Strong security performance and lower risk	50% of Companies
Intermediate	640 – 730	Fair security performance and moderate risk	45% of Companies
Basic	250 – 630	Poor security performance and higher risk	5% of Companies

*The approximate distribution of companies in the entire Bitsight inventory, across the rating categories.

Threshold Considerations

The rationale for the threshold designations are as follows:

- Thresholds are set to allow adjustments for rating algorithm changes.
- The distribution of “advanced” companies is based on the intuition that the overall security posture of the world is in good standing and the number of companies that actually have events is low.
- A majority of the scoring scale is reserved for the bottom half of all companies. This is because there are more ways a company can be considered “basic” than there are ways to be considered “advanced.” It’s more elusive, in that a company will have to succeed in several key aspects to be considered “advanced.”

How Bitsight Security Ratings are calculated.

For each rated organization, we intelligently identify and classify behaviors emanating from that organization's network assets, including communication with Command and Control Server (C&C or C2 Server), participation in a Distributed Denial-of-Service (DDoS) attack, malware distribution, network scanning, and email attacks. The machines participating in these behaviors are generally under the control of external adversaries. While these behaviors may not equate to data loss, each is evidence of a compromise. Evidence from sensors deployed across the globe is collected daily. Each individual security event is analyzed for confidence, severity, and duration, and then mapped to a specific organization.

In addition, we gather externally observable configuration information on rated organizations.

We may include analysis of Sender Policy Framework (SPF) records, Secure Sockets Layer (SSL) implementation, and DomainKeys Identified Mail (DKIM) signatures. Failure to use best practices increases risk and therefore negatively impacts a company's security rating.

- Algorithm
- Risk Category Weights
- Letter Grades
- Finding Grades
- Normalization

We do not engage in any hacking or any intrusive network penetration testing. Our collected data is externally observed from various sources in the public internet. It is available to anyone who chooses to collect it and has the technological capabilities to do so.

Algorithm

Bitsight Security Ratings are calculated daily using a proprietary algorithm that examines two classes of externally observable data – configuration and security events. Security effectiveness is assessed across the following risk categories:

- Compromised Systems
- Diligence
- User Behavior
- Public Disclosures

The ratings algorithm accounts for the following elements:

- **Number and Type(s) of Compromised Systems:** Data is classified into risk vector types and factored into an organization's security rating accordingly.
- **Event Duration:** Calculates the time between when the compromised system was first observed and when it was last seen.
- **Diligence Configurations:** Shows steps an organization has taken to prevent attacks. Similar to Compromised Systems, data is classified into risk vector types and factored into an organization's security rating accordingly.

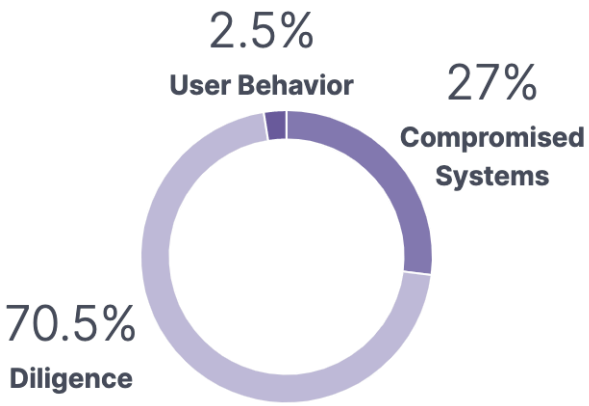
Security ratings are the results of the aggregation of all risk vector letter grades (with different weights) that are normalized for that company.

Learn more about the rationale for rating thresholds and why security ratings may be fluctuating.

Risk Category Weights

Risk categories are weighted as follows:

- Compromised Systems = 27%
- Diligence = 70.5%
- User Behavior = 2.5%
- Public Disclosures = Weighted only if they occur.



Letter Grades

Letter grades provide a quick way to understand how a company is performing in each risk type and also provides a meaningful way to compare risk type performance of one company to another.

Letter grades are directly correlated to how well a company is performing, relative to all companies in the Bitsight inventory. Below is a table that outlines how each grade correlates to their performance, relative to their company size.

Individual Company Reports provide greater precision than letter grades.

Grade	Percentile
A	In the top 10% of companies.
B	In the top 30% of companies.
C	In the top 60% of companies.
D	In the bottom 40% of companies.
F	In the bottom 20% of companies.
N/A	This grade has no correlation with how a company is performing. If a letter grade is "N/A" (Not Available), it may be because: • The risk vector is "informational." • The grade defaults to it, in the absence of findings. • The risk vector is going through an evaluation period before having an impact on the rating.

Finding Grades

Diligence findings are graded as GOOD, FAIR, WARN, BAD, or NEUTRAL based on inherent risk and if best practices can be improved upon. These finding grades contribute towards the letter grade of the risk vector.

Finding Grade	Description
GOOD	Low risk, aligned with best practices. These have a significantly positive impact on the letter grade.
FAIR	Light risk and some opportunity to achieve best practices. These have a minor negative impact or no impact on the letter grade depending on the risk vector.
WARN	Moderate risk and departure from best practices. These have a moderately negative impact on the letter grade.
BAD	Significant risk and departure from best practices. These have a significantly negative impact on the letter grade.
NEUTRAL	Observed data with neither positive nor negative risk. This does not positively or negatively impact the letter grade.
N/A	Finding grades are not applicable (N/A) to Compromised Systems and User Behavior.

Normalization

Large companies will typically have more findings than smaller companies. To ensure ratings are calculated in a way that doesn't unfairly penalize large companies, we normalize ratings based on the size of an organization. We compare organizations using employee count to account for size.

Frequently Asked Questions

Are all findings of a given company displayed?

Findings throughout the past 1 year are shown and a complete list can be obtained through the Bitsight API. Companies with over 10 million findings have a sampled view of their findings, meaning that not all of them are visible in the platform.

What do sharp changes in a rating mean?

Sudden drops in rating can occur due to publicly disclosed Security Incidents, an increase in Compromised Systems events, or poorly configured Diligence findings. Improvements in ratings are due to either many simultaneously resolved events or updates to Diligence findings. Any decreases of 10 points or greater are highlighted in a company's Overview page, next to its 1-year historical trend graph.

When is a security rating impacted?

New findings impact ratings 24-48 hours after they are observed. They continue to impact the rating over a decay period, which varies by risk type.

Please refer to:

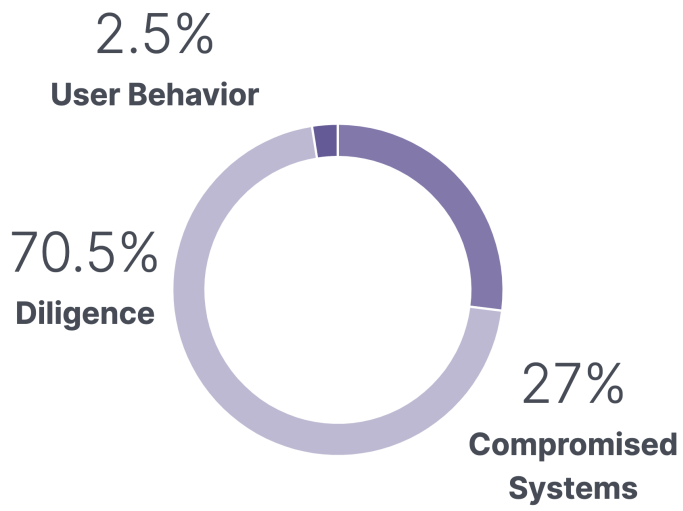
- The duration of Compromised System events
- The impact & lifetime of Diligence findings
- The lifetime of File Sharing events
- The severity & decay of Security Incident events

How the Compromised Systems risk category is calculated.

April 19, 2023: 2023 Ratings Algorithm Update.

Assessment

The Compromised Systems risk category accounts for 27% of a company's Bitsight Security Rating. The total letter grades of all Compromised Systems risk vectors and event duration are factored into the entire Compromised Systems risk category, and then normalized to account for company size:



Each risk vector receives an individual letter grade based on frequency, duration, and severity. The letter grade is relative to all other companies. Individual grades are calculated and refreshed daily:

Frequency

The volume of events that appear in given sets of time.

Unique IP addresses, malware family, number of days, and connection tracking information are taken into consideration when classifying observations as an event:

Consideration	Examples
Number of Days: Determines the duration of an event.	• **One Multi-day Event:** Gamarue was observed in xxx.xxx.12.345 on January 1st, and then for every day until January 4th. All 4 observations are considered as 1 multi-day event. • **Multiple Events:** Gamarue was observed in 7 unique IPs during 7 different days, each observation is counted as an event for a total of 7 events.
Multi-day with Gaps: For multi-day observations with gaps (skips a day or two), there's a 3-day tolerance period that considers these multi-day observations as one multi-day event.	• **One Multi-day Event:** Gamarue was observed in xxx.xxx.12.345 on January 1st. The same infection was observed again on the same IP on January 4th. The 3-day tolerance period considers these observations to be 1 multi-day event. • **Multiple Events:** Gamarue was observed in xxx.xxx.12.345 on January 1st. The same infection was observed again on the same IP address on January 5th. 4 days have passed since the earlier observation. The 3-day tolerance period no longer applies. These observations are considered to be 2 events.
Unique IP: An event must have a unique IP address.	Gamarue was observed 7 times in xxx.xxx.12.345 and 2 times in xxx.xxx.54.321 (different IP), the 9 observations are considered as 2 events.
Malware Family: An event must belong to a unique malware family.	Conficker and Rammit were observed any number of times in xxx.xxx.12.345 on January 1st, each type of malware is considered as a separate event.

Duration

The time between when the system was first observed to be compromised and when it was last observed. Longer lasting events have a larger impact than shorter events.

If a Botnet Infection is first observed in one machine on June 1, is seen again from the same machine on June 2, and then not seen subsequently, the duration is 2 days.

Frequently Asked Questions

When do Security Ratings Improve?

Compromised Systems events are refreshed daily and are based on events that occur over the past 180 days. The letter grade of a particular risk vector will improve over time after the event's end date, assuming no new events occur.

How do Ongoing Infections Impact Bitsight Security Ratings?

All infections have the same raw weight/impact. An infection of a particular family on a given IP only counts against the rating once in a three-day period.

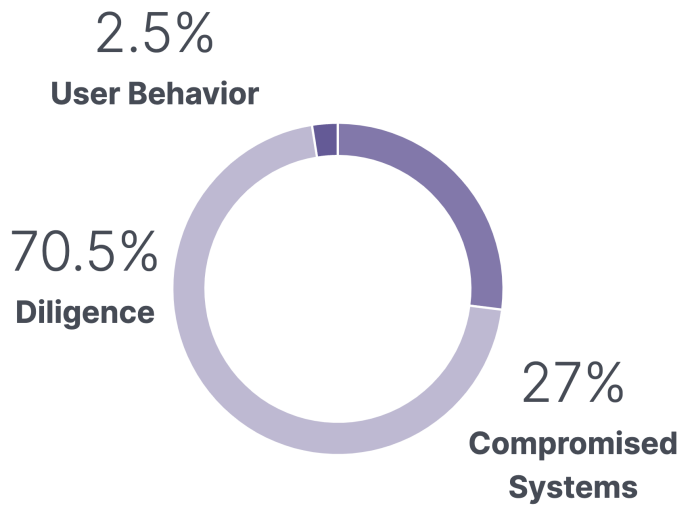
The ratings algorithm is based on relative rankings of companies. This means that the output ratings do not directly match the raw impact.

In practice, what happens is that the first few events have a higher impact because the first few events push the company to a lower rank relative to many other companies - this is because Botnet Infections are rare occurrences. As the number of Botnet Infection findings increases, the ratings impact gets smaller since there are fewer companies with that many findings.

How the Diligence risk category is calculated.

March 26, 2024: Defined “insufficient data.”

The Diligence risk category accounts for 70.5% of a company’s Bitsight Security Rating.



Each risk vector is evaluated based on severity, the impact and lifetime of findings, and then normalized to account for company size.

Severity

The severity of Diligence findings are evaluated as GOOD, FAIR, WARN, BAD, or NEUTRAL based on industry-standard criteria. An overall letter grade is calculated, using the evaluations of individual findings.

If a company has 3 domains and each of them has an effective SPF record, their overall SPF Domains grade would be an “A.” Likewise, if all 3 domains have improperly formatted SPF records, their overall SPF Domains grade would be an “F.”

Finding Refresh

The Bitsight platform regularly checks for new observations. Bitsight findings are updated as these observations change, e.g., newly observed Diligence findings or an existing finding was remediated. There are two types of refresh: automated and requested.

Refer to the "User-Requested Refresh Duration" and "Automated Scan Duration" fields for the refresh duration of particular risk vectors.

To request a refresh:

- Check off any eligible findings in the Findings page [Risks ➔ Findings], and then click the **Refresh** button in the action bar at the bottom.
- Hover over a finding and then click the **Refresh** button at the right of the row.

Impact & Lifetime

Previously captured findings will continue to impact ratings until the finding completes its lifetime (depending on the specific risk vector). It will continue to be listed in the company report, along with the active findings.

The headline security rating will reach a perfect value if all vulnerabilities are fixed and all findings (associated with vulnerabilities) have completed their lifetime.

Learn how each risk vector impacts the Bitsight Security Rating of a company:

- SPF Domains
- DKIM Records
- TLS/SSL Certificates
- TLS/SSL Configurations
- Open Ports
- Web Application Headers
- Patching Cadence
- Insecure Systems
- Server Software
- Desktop Software
- Mobile Software
- DNSSEC
- Mobile Application Security
- Web Application Security
- DMARC
- Domain Squatting

The tables contain the following risk vector information:

- Finding Behavior – How findings behave, depending on the action taken.
- Grace Period – The time before a recognized finding starts to impact ratings.
- Lifetime – The number of days a finding will impact the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.
- Insufficient Data – There could be insufficient data when grading risk vectors. A default risk vector grade is assigned. The threshold varies by risk vector.
- Refresh – The Bitsight platform regularly checks for new observations. Bitsight findings are updated as these observations change, e.g., newly observed Diligence findings or an existing finding was remediated. There are two types of refreshes: automated scans and user-requested refreshes.
- Weight – Each Diligence risk vector is accounted for in the total Diligence weight (70.5%). The percentage is out of the total 100% of the rating.

How the SPF Domains risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

To assess the SPF Domains risk vector, we look for the presence of SPF records in the company's primary domain, subdomains, and any domains that have sent or attempted to send email. These domains typically correspond to mail servers. We also look at subdomains.

Impact

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** F Having SPF records for all domains (including SMTP servers and those that aren’t configured to send email) is best practice. If a company does not intend to send email from a domain, an attacker can still use that domain to spoof email. Only domains that are sending email and don’t have SPF records are affected.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 70.5% in Diligence):** 1%

Evaluation

An assessment is provided based on syntactical correctness and effectiveness of hosts that are authorized to send emails on behalf of a domain:

Syntactical Correctness

A record is syntactically correct if it conforms to the SPF RFC. An effective SPF record identifies a set of hosts that are allowed to send email on behalf of the domain. In addition, that record states that email from all other hosts should either be assigned the state “reject” or “accept but mark.”

Effectiveness

A syntactically correct SPF record may still be ineffective if it contains conflicting elements or assigns the state “accept” or “neutral” to all other hosts. A domain must only have one SPF answer specified in the DNS TXT record and the SPF record of a domain. If both a TXT answer and SPF answer exist, they must match.

Number of Authorized Hosts

The larger the number of hosts authorized to send emails on behalf of a domain, the higher the chances of a mail server getting compromised. All domains should have SPF records, even those that aren't configured to send mail and SMTP servers. Even if a company does not intend to send mail from a domain, an attacker can still use that domain to spoof email. Because of this, companies without SPF records will have an SPF grade of “F.” Domains that aren't being used to send mail should have null SPF records.

Example null record:

```
example.com.        IN  TXT  "v=spf1     a:mail.example.com -all"
mail.example.com.   IN  TXT  "v=spf1     a -all"
www.example.com.    IN  TXT  "v=spf1     -all"
```

Finding Grades

Diligence findings are evaluated as GOOD, BAD, or NEUTRAL. An overall letter grade is calculated, using the evaluations of individual findings.

If there's no message, the SPF record is effectively preventing unauthorized individuals from sending spoofed email from this domain. It is properly configured and only authorizes necessary domains to send email. An effective SPF record is graded as “GOOD.”

How the DKIM Records risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The DKIM Records risk vector is assessed based on if a company has a DomainKeys Identified Mail (DKIM) record for each of their domains and the key length of the public key found in their DNS record. Test records are assessed as if the domain does not have a record.

The following standards are used as a basis for assessing a company's DKIM records:

- RFC-4871
- NIST – Since 2015, this US department of Commerce agency recommends that all RSA keys be at least 2048 bits.
- ECRYPT – This EU initiative, to strengthen European excellence in the area of cryptology, recommends that all RSA asymmetric keys be at least 2048 bits.
- French Network and Information Security Agency (ANSSI) – Recommends that all RSA asymmetric keys be at least 2048 bits since 2014.
- Lenstra – A mathematical algorithm used to estimate when cryptographic attacks against asymmetries are plausible, indicating that 1024 should no longer be used as of 2006.

Impact

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** C Without DKIM records, we cannot verify that a company is effectively preventing email from being spoofed from its domains. This is set in the center of the grading scale for computing into security ratings. If there are no findings and we are temporarily unable to collect data, the most recent grade is assigned for up to 400 days before being assigned the default grade.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new	**Duration:** 60 Days

information. Learn why findings have a decay and lifetime period.	
Weight	**Percentage (out of 70.5% in Diligence):** 1%

Evaluation

DKIM Records findings are evaluated as GOOD, WARN, BAD, or NEUTRAL. An overall letter grade is calculated using the evaluations of individual findings.

If the domain has a DKIM record with a sufficiently long public key, it is graded as GOOD.

How the TLS/SSL Certificates risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

For the TLS/SSL Certificates risk vector, we look at a variety of criteria when determining the effectiveness of TLS/SSL certificates and their implementation. Companies should have up-to-date certificates with any domains interacting with sensitive data.

Impact

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** C This is set in the center of the grading scale for computing into Bitsight Security Ratings. Some findings cannot be traced back to specific companies due to the use of third party systems; such as web filters and Content Delivery Networks (CDN), that are capable of redirecting and encapsulating network traffic. Some firewalls might also be detecting and blocking external data gathering tools from getting any data. If there are no findings and we are temporarily unable to collect data, the most recent grade is assigned for up to 400 days before being assigned the default grade.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 70.5% in Diligence):** 10%

Best Practices

In order to be graded as GOOD, a certificate must adhere to the following industry-standard practices:

- Certificate validity:
  - Today's date must fall within the valid dates for the certificate. If a certificate is expired or if it goes into effect in the future, any data sent to or from the host may be insecure.
  - Apple, Google, and Mozilla no longer trust certificates that were issued on or after September 1, 2020 and have a validity duration greater than 398 days. Certificates issued on or after September 1, 2020 that have a validity period of more than 398 days are graded as WARN.
  - The certificate must be issued by a trusted certificate authority. Certificate authorities must be in at least two of the following stores to be considered as "trusted": Microsoft, MacOS, Google Android, Mozilla NSS.
- The key must be generated using a secure algorithm, such as RSA, DSA or elliptic curve.
- Keys must be the recommended length or longer. For RSA and DSA keys, a length of 2048 bits is recommended; for elliptic curve keys (EC), a length of 224 bits is recommended.
- The certificate must be signed using a secure algorithm. MD2, MD5 and SHA1 are considered insecure.
- Providing a self-signed or untrustworthy certificate for connecting clients, such as not specifying a Server Name Indication (SNI), is a practice that denotes poor security and should be avoided. See recommendations.

Finding Grades

TLS/SSL Certificate findings are evaluated as GOOD, FAIR, WARN, or BAD. Not all attributes are weighted evenly; some messages may be more serious and affect the overall grade more than other, similarly graded messages.

How the TLS/SSL Configurations risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The TLS/SSL Configurations risk vector determines if security protocol libraries support strong encryption standards when making connections to other machines. Companies should have secure configurations on all servers that are hosting TLS/SSL certificates. This includes systems that are hosting the company's website, even if they do not provide any internet-related services or its services are delivered by cloud service providers.

Impact

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** C This is set in the center of the grading scale for computing into Bitsight Security Ratings. Some findings cannot be traced back to specific companies due to the use of third party systems, such as web filters and Content Delivery Networks (CDN) that are capable of redirecting and encapsulating network traffic. Some firewalls might also be detecting and blocking external data gathering tools from getting any data.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 70.5% in Diligence):** 15%

Considerations

TLS/SSL Configurations findings are evaluated as GOOD, FAIR, WARN, or BAD. Not all attributes are weighted evenly; some messages may be more serious and affect the overall finding grade more than other similarly graded messages.

Encryption

Ensure the version of TLS/SSL is not susceptible to any known vulnerabilities.

- A Digital Signature Algorithm (DSA) shorter than 160 bits can be broken with consumer devices. A key length of 2048 bits is recommended.
- An elliptic-curve cryptography (ECC) shorter than 160 bits can be broken with consumer devices. A key length of 224 bits is recommended.
- RSA keys shorter than 2048 bits may be insecure. According to the NIST's Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, keys above 1024 bits and below 2048 bits are acceptable only for legacy use.
- For Simple Mail Transfer Protocol (SMTP) servers:
    - To be graded as GOOD, remove support for TLSv1.0 and TLSv1.1.
    - If TLSv1.2 or greater is supported, the finding is graded as FAIR.
    - If TLSv1.2 or greater is not supported, the finding is graded as BAD.
- Certificates presented on the public internet should be signed by a publicly trusted certificate authority.
- Self-signed certificates and certificates with non-standard roots should either not be exposed to the general Internet or their exposure should be limited by configuring client certificate authentication.

Signature

- The server must not use a named Diffie-Hellman prime or use a Diffie-Hellman prime shorter than 2048 bits.
- The server must not support insecure encryption protocols or ciphers (e.g., the EXPORT ciphers).
- Insecure hash algorithms are graded as BAD (e.g., MD2, MD5, and SHA1).

Obsolete Protocols

Though we test for obsolete protocols (SSLv2, SSLv3, TLS 1.0, and TLS 1.1), which are all nominally graded BAD, their penalty is limited; If all four obsolete protocols are used, only a subset is penalized.

Repeated Findings

The presence of wildcards in DNS records can have an unnecessary magnification of the number of TLS/SSL Configurations findings. These repeated findings are handled as a single finding.

How the Open Ports risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The Open Ports risk vector assessment is based on the number of findings an organization has and the security measures in place around those open ports. While very few companies will actually have no ports open, the fewer ports that are exposed to the Internet, the fewer opportunities there are for attack.

When a port is found to be fixed to a certain network protocol or software (such as port 143 for IMAP services), it’s attributed to typical service activity on that port unless the cause can be determined as something else. If a service is detected, this will override the typical service running on that port for grading purposes.

There are different grades for when there is typical service and detected service port activity:

- We assess detected services.
- If no service is detected on the port, we assess typical services.
- Some ports are potentially vulnerable, where the level of risk varies. Potentially vulnerable open ports do not have a set impact on the Open Ports letter grade.

Other grading considerations:

- Only Open Ports findings that were observed in the last 60 days are factored into the Open Ports letter grade. Since the infrastructure of a company is continuously updated, findings are set to expire if no Open Ports findings were observed within the past 60 days.
- If a port is verified to be opened and closed on the same day, it continues to impact the grade into the following day.

  A port is observed to be open on January 1 at 8:00, and then closed shortly after at 11:00. The finding's impact on the grade is removed on January 2, rather than removed on the same day of the observation.

- If the referenced IP of an Open Ports finding has an “end date,” it can no longer be refreshed and will no longer impact the grade when it completes its lifetime.
- Rating drops that are due to only a single Open Port finding are limited to a maximum drop of 80 points.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** A Companies are not required to run open port services. The rating is positively impacted if there are no findings for this risk vector.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 70.5% in Diligence):** 10%

Evaluation

The Open Ports risk vector letter grade is determined by assessing the number of specific findings that are evaluated as GOOD, FAIR, WARN, BAD, or NEUTRAL:

- If the service is secure and used for normal business functions, such as SSH, the port is classified as “GOOD.”

  Port 23 is typically used for Telnet. It’s graded as “BAD.” However, if SSH running on port 23 is detected instead, that port would be marked as “GOOD.”

- Services that are rarely necessary for business functions or that have known vulnerabilities are classified as “WARN” or “BAD,” depending on the security risk of leaving them open.
- If the service is used for normal business functions, but does not use encryption or other security measures, such as HTTP, the port is classified as “NEUTRAL.”

How the Web Application Headers risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

A variety of HTTP headers are assessed to determine if security best practices are being followed. Only the HTTP headers of hosts that return HTTP 200 responses are assessed. Learn why HTTPS is preferred over HTTP:

- National Cyber Security Centre: Serve websites over HTTPS (always)
- Troy Hunt: Here's Why Your Static Website Needs HTTPS

Overview

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** C Some findings cannot be traced back to specific companies due to the use of third party systems; such as web filters and Content Delivery Networks (CDN), that are capable of redirecting and encapsulating network traffic. Some firewalls might also be detecting and blocking external scanning tools from getting any data. This is set in the center of the grading scale for computing into security ratings.

Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 70.5% in Diligence):** 5%

Findings

Remediation Instructions

Web Application Header findings that affect a company's Diligence grades have messages that provide a brief description and remediation instructions (if any). They are specific to a field or value in an application header.

Finding Grading

Since Web Application Header findings are based on the entire header configuration and not on individual errors, finding grades can't be pre-assigned without evaluating the entire finding.

Content Checks

- Websites with mixed HTTP and HTTPS content.
- Intra-site URLs are evaluated for HTTPS protocol use.
- Redirects from HTTPS to HTTP.
- Check if the “WWW-Authenticate” is contained in an HTTP 401 response from non-HTTPS events.

Assessed Headers

- Access-Control-Allow-Origin
- Cache-Control
- Content-Security-Policy
- Expires
- HTTP Strict-Transport-Security
- Set-Cookie
- X-Content-Type-Options
- X-Frame-Options (Frame-Options)
- X-XSS-Protection

Required Headers

These are important for preventing attacks and are checked for usage and correct configurations. If an application header exists and the required header is not found in the findings, the company is penalized on missing headers. The penalties are described below under "Configuration Requirements."

Header	Required For
Cache-Control • Overview • Implementation	HTTP/1.1
Content-Security-Policy • Overview • Implementation	• HTTP/1.1 • HTTP/1.0
Expires • Overview • Implementation	HTTP/1.0
HTTP Strict-Transport-Security (HSTS) • Overview • Implementation	• HTTP/1.1 • HTTP/1.0
X-Content-Type-Options • Overview • Implementation	• HTTP/1.1 • HTTP/1.0

Optional Headers

Optional headers may be present, in addition to required headers.

- If present, optional headers are verified that they are configured correctly and go towards the requirements as a whole for a GOOD or FAIR finding grade.
- If not present, companies are not penalized since they are unnecessary for preventing malicious actions.

Header	Optional For
Access-Control-Allow-Origin • Overview • Implementation	• HTTP/1.0 • HTTP/1.1
Location • Overview • Implementation	• HTTP/1.0 • HTTP/1.1
Set-Cookie • Overview • Implementation	• HTTP/1.0 • HTTP/1.1
WWW-Authenticate • Overview • Implementation	• HTTP/1.0 • HTTP/1.1
X-Frame-Options • Overview • Implementation	• HTTP/1.0 • HTTP/1.1
X-XSS-Protection • Overview • Implementation	• HTTP/1.0 • HTTP/1.1

Configuration Requirements

Requirements for GOOD grade: No misconfigured headers (required or optional) are present.

Requirements for FAIR grade: No more than 50% distinct misconfigured headers can be present (required and optional)

For HTTP connections, no headers are graded unless Set-Cookie is defined. The finding grade will default to NEUTRAL.

Required HTTP 1.1 (HTTPS):

- Content-Security-Policy
- HTTP Strict-Transport-Security
- X-Content-Type-Options
- Cache-Control

Required HTTP 1.1 (non-HTTPS):

- Content-Security-Policy
- X-Content-Type-Options
- Cache-Control
- Set-Cookie

Required HTTP 1.0 (HTTPS):

- Content-Security-Policy
- HTTP Strict-Transport-Security
- X-Content-Type-Options
- Expires
- X-Frame-Options

Required HTTP 1.0 (non-HTTPS):

- Content-Security-Policy
- X-Content-Type-Options
- Expires
- X-Frame-Options
- Set-Cookie

Responses

The following errors downgrade the response from HTTPS to HTTP:

- 200 responses
- 30X responses
- 401 responses

HTTP 1.1 (HTTPS)

Response	Description
200	We validate that no hyperlinks in the HTML for the web page downgrade the user inside the site and the domain of the site. We also validate and ensure the HTML of the webpage does not import resources (such as scripts and images) from outside the site using HTTP instead of HTTPS. The finding is graded BAD if these resources are present.
30x (301, 302, 307)	Any HTTPS finding that immediately downgrades the user to an HTTP connection using a redirect is graded as BAD.

HTTP 1.0 (HTTPS)

Response	Description
200	We validate that no hyperlinks in the HTML for the web page downgrade the user inside the site and the domain of the site. We also validate and ensure the HTML of the webpage does not import resources (such as scripts and images) from outside the site using HTTP instead of HTTPS. The finding is graded BAD if these resources are present.
30x (302, 307)	Any HTTPS finding that immediately downgrades the user to an HTTP connection using a redirect is graded as BAD.

How the Patching Cadence risk vector is assessed.

July 10, 2024: The Patching Cadence lifetime is 90 days.

Patching Cadence is graded based on vulnerability duration, Bitsight severity [of the vulnerability], and the prevalence of vulnerabilities within an organization's infrastructure.

Vulnerability considerations:

- Vulnerability Severity
- Vulnerability Duration - The number of days a vulnerability is present on a given asset before it is remediated.
- Only confirmed vulnerabilities impact the grade.
- A vulnerability that's observed only once has less of an impact than a vulnerability that's observed over the span of several days.

Concept	Description
Duration The number of days a vulnerability is present on a given asset before the vulnerability is remediated.	The number of days a vulnerability is present on a given asset before the vulnerability is remediated. (See Duration for details.)
Insufficient Data A default risk vector grade is assigned.	**Default:** A The rating is positively impacted if there are no findings for this risk vector within its lifetime.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration**: 90 Days Since Patching Cadence is based on an estimate of the mean remediation time of vulnerabilities, this lifetime is set for a longer duration than other Diligence risk vectors to ensure an accurate measure of the mean remediation time. See lifetime for details.
Vulnerability Severity The seriousness of a vulnerability; its innate potential for harm.	See Vulnerability Severity for details.

Weight	**Percentage (out of 70.5% in Diligence):** 20%

Vulnerability Severity

Some vulnerabilities are more critical than others. They carry a greater weight than less critical vulnerabilities that are observed over the same time period. This is summarized by Bitsight severity. It follows the Common Vulnerability Scoring System (CVSS), a scoring system that uses various properties of the vulnerability for determining its level of severity.

Bitsight Severity	CVSS Score
Minor	0.0 - 3.9
Moderate	4.0 - 6.9
Material	7.0 - 8.9
Severe	9.0 - 10.0

Vulnerability Duration

Vulnerability duration is considered to be the time it takes to patch vulnerabilities. It starts from when an asset is first observed to be vulnerable (first seen date) and continues to when the vulnerability is patched (last seen date).

It might take up to 60 days for a vulnerability to be considered to be “remediated.” However, the ratings impact is calculated as if it were remediated on the last vulnerable observation date (last seen date). A vulnerability is considered to be patched if:

- The vulnerability has been remediated (patched) and a subsequent observation confirms that the endpoint is no longer vulnerable.
- The vulnerable asset is fully removed (the service is taken offline) and is no longer reachable.
- An asset can be considered to be patched after a set number of days with no further observations. This is generally after 60 days, depending on the type of vulnerability. In these situations, there is no remediation time. Note, the 60 days is not included as part of the remediation time.

Lifetime & Decay of Patching Cadence Findings

A Patching Cadence finding impacts the risk vector grade for 90 days after it is remediated. The relative weight of the finding decays linearly over this period, and the finding's impact on the average remediation time may be reduced.

After all Patching Cadence findings are remediated, the average remediation time is adjusted so that it decays linearly during the remaining finding lifetime, enabling a corresponding increase in the risk vector score. This linear decay starts 60 days after the Last Seen date of the last vulnerable finding.

Patching Cadence measures average time-to-patch. Lifetime is how long each individual time-to-patch duration continues to be included in the average. This means that the 90-days lifetime period is not inherently negative (or positive) for the risk vector grade. The positive impact of a quickly patched vulnerability lasts throughout the lifetime period, just like the negative impact of a slowly patched vulnerability.

How the Insecure Systems risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The Insecure Systems risk vector assessment is based on the supported/unsupported status and the level of risk that has been introduced to an organization.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** A The rating is positively impacted if there are no findings for this risk vector.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 70.5% in Diligence):** 2.5%

Evaluation

Insecure Systems findings are evaluated as WARN, BAD, or NEUTRAL. An overall letter grade is calculated, using the evaluations of individual findings.

Software versions that cannot be determined or are unsupported, but still receive security fixes are evaluated as “NEUTRAL.” These items do not affect the Insecure Systems grade, but should be resolved.

How the Server Software risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

Server Software findings are evaluated based on the supported/unsupported status of an organization’s server software.

We cannot make any special exemptions with regards to the impact of this risk vector if an organization's business requirements depend on outdated or insecure server software applications. Please contact Bitsight Support if you would like to discuss your Server Software findings.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** A The use of server software is not required to improve an organization’s cyber security posture. Therefore, there’s no penalty or negative impact to the rating in the absence of Server Software findings.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days There is a grace period of 28 days to allow for validating and updating software packages.
Weight	**Percentage (out of 70.5% in Diligence):** 2%

Finding Grading

Grade	Considerations
GOOD	The installed software is up-to-date or it has the latest OS distribution-specific patches applied.

FAIR	The version has been unsupported for less than 4 weeks.
WARN	The version has been unsupported for less than 52 weeks. Software that are no longer supported are evaluated as WARN for a grace period of 28 days. After 28 days, WARN becomes BAD.
BAD	The version has been unsupported for over 52 weeks. The software is either unsupported or it does not have the latest OS-specific patches applied. These impact an organization's Server Software risk vector grade and Bitsight Security Rating.
NEUTRAL	The software status could not be determined or it is unsupported but still receives security fixes. There's either not enough information to determine if the software version is supported, not enough information to determine if the latest OS-specific patches are installed, or the software is unsupported, but still receives security fixes. These do not impact the Server Software risk vector grade and remediation is unnecessary.

Backported Security Fixes

If server software that normally appears out-of-date receives backported security fixes, the software is graded as "GOOD."

This occurs when software vendors still distribute updates (patches) for old software versions that are technically unsupported or when operating system distribution developers create patches for third-party software (Ubuntu developers update the Ubuntu version of OpenSSH) as a courtesy. They essentially duplicate security fixes from supported software versions and port them to the unsupported software.

Learn more about backports.

Extended Security Updates

The general support life cycle of some software products are split into two periods – the first half with “mainstream support,” followed by the second half with “extended support.” After the extended support period, “extended security updates (ESU)” might be offered. Extended support and ESU are taken into consideration when determining if software is supported.

This currently applies within the Bitsight platform to Microsoft products. These ESU programs do not include all security fixes and upgrades.

Software with ESU are evaluated in the following manner:

- **Good:** From the date of release to the end date of extended support.
- **Fair:** The first and second years of ESU.
- **Warn:** The third year of ESU.
- **Bad:** The end date of ESU.

How the Desktop Software risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The Desktop Software risk vector assesses the supported or unsupported status of the software version. The use of desktop software is not required to improve an organization's cyber security posture.

Assessed Desktop Browsers

- Chrome
- Edge
- Firefox
- Internet Explorer (IE)
- Safari

All other browsers are graded as NEUTRAL.

Graded Desktop Operating Systems

- Chrome OS
- Mac OS X
- Windows: ME, NT, NT 4.0, Vista, XP, 95, 98, 7, 8, 8.1, 10, 2000

All other operating systems are graded as NEUTRAL, including the following:

- Debian
- Fedora
- FreeBSD
- Linux
- NetBSD
- OpenBSD
- Slackware
- Ubuntu

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** ⊘ This default grade does not have a negative impact on the rating. It is equivalent to a perfect grade. Either: • There are no findings. • The estimated number of users falls below a minimum threshold. To avoid sudden fluctuations, the risk vector is reassigned an A to F grade when the estimated number of users has stayed above the threshold for 65 days.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 65 Days There's a grace period of 28 days for validating and updating software packages. See finding behavior.
Weight	**Percentage (out of 70.5% in Diligence):** 3%

Evaluation

Desktop Software findings are a combination of the evaluated operating system (OS) and browser, which are graded independently from one another, and the Desktop Software finding grade represents the calculated combination of the OS and browser. The OS and browsers are evaluated based on their supported status:

- **Good:** The version is supported.
- **Fair:** The version has been unsupported for less than 4 weeks.
- **Warn:** The version has been unsupported for less than 52 weeks.
- **Bad:** The version has been unsupported for over 52 weeks.

The general support life cycle of some software products are split into two periods – the first half with "mainstream support," followed by the second half with "extended support." After the extended

support period, “extended security updates (ESU)” might be offered. Extended support and ESU are taken into consideration when determining if software is supported.

This currently applies within the Bitsight platform to Microsoft products. These ESU programs do not include all security fixes and upgrades.

Software with ESU are evaluated in the following manner:

- **Good:** From the date of release to the end date of extended support.
- **Fair:** The first and second years of ESU.
- **Warn:** The third year of ESU.
- **Bad:** The end date of ESU.

Versions that are undetermined or unknown default to the following evaluations:

❗**Undetermined:** If there’s no version available, if the finding cannot be identified, or if both the OS and browser are unknown; the finding is evaluated as NEUTRAL.

❓**Unknown:** If either the OS or browser has been graded and the other is unknown, the finding is evaluated as the given grade.

OS & Browser Status	Supported Browser (GOOD)	Unsupported Browser (FAIR, WARN, BAD)	❗ Undetermined/ ❓ Unknown Browser
Supported OS (GOOD)	Supported OS (GOOD) + Supported Browser (GOOD) = GOOD	Supported OS (GOOD) + Unsupported Browser (FAIR) = FAIR Supported OS (GOOD) + Unsupported Browser (WARN) = WARN Supported OS (GOOD) + Unsupported Browser (BAD) = BAD	Supported OS (GOOD) + ❓ Browser (NEUTRAL) = GOOD
Unsupported OS (FAIR, WARN, BAD)	Unsupported OS (FAIR) + Supported Browser (GOOD) = FAIR	Unsupported OS (FAIR) + Unsupported Browser (WARN) = WARN Unsupported OS (FAIR) + Unsupported Browser (BAD) = BAD	Unsupported OS (FAIR) + ❓ Browser (NEUTRAL) = FAIR
	Unsupported OS (WARN) + Supported Browser (GOOD) = WARN	Unsupported OS (WARN) + Unsupported Browser (FAIR) = WARN Unsupported OS (WARN) + Unsupported Browser (BAD) = BAD	Unsupported OS (WARN) + ❓ Browser (NEUTRAL) = WARN
	Unsupported OS (BAD) + Supported Browser (GOOD) = BAD	Unsupported OS (BAD) + Unsupported Browser (FAIR) = BAD Unsupported OS (BAD) + Unsupported Browser (WARN) = BAD	Unsupported OS (BAD) + ❓ Browser (NEUTRAL) = BAD
❗ Undetermined/ ❓ Unknown OS	❓ OS + Supported Browser (GOOD) = GOOD	❓ OS + Unsupported Browser (FAIR) = FAIR ❓ OS + Unsupported Browser (WARN) = WARN ❓ OS + Unsupported Browser (BAD) = BAD	❗ OS (NEUTRAL) + ❗ Browser (NEUTRAL) = NEUTRAL
	❗ OS (NEUTRAL) + Supported Browser (GOOD) = GOOD	❗ OS (NEUTRAL) + Unsupported Browser (FAIR) = FAIR ❗ OS (NEUTRAL) + Unsupported Browser (WARN) = WARN ❗ OS (NEUTRAL) + Unsupported Browser (BAD) = BAD	❓ OS + ❓ Browser = NEUTRAL

Message	Description	Remediation Instructions	Finding Grade (OS + Browser Support Status)
Neutral Operating System and Supported Browser	The operating system version could not be determined and the browser is supported.	If obfuscation of the operating system version is intentional, there is no penalty. Ensure an operating system update strategy is in place.	❗ OS (NEUTRAL) + Supported Browser (GOOD) = GOOD
Neutral Operating System and Unknown Browser	The operating system version and browser could not be determined.	If obfuscation of the browser and operating system version is intentional, ensure an update strategy for browsers and operating systems is in place.	❗ OS (NEUTRAL) + ❗ Browser (NEUTRAL) = NEUTRAL
Neutral Operating System and Unsupported Browser	The operating system version could not be determined and the browser is not supported.	Ensure the latest version of the browser for that operating system is installed.	❗ OS (NEUTRAL) + Unsupported Browser (FAIR) = FAIR
			❗ OS (NEUTRAL) + Unsupported Browser (WARN) = WARN
			❗ OS (NEUTRAL) + Unsupported Browser (BAD) = BAD
Supported Operating System and Browser	The operating system and browser are both supported.		Supported OS (GOOD) + Supported Browser (GOOD) = GOOD
Supported Operating System and Unknown Browser	The operating system is supported and the browser could not be recognized.	If obfuscation of the browser version is unintentional, ensure end-users are using approved mobile applications in order to be able to analyze the supported (or unsupported) status of those applications.	Supported OS (GOOD) + ❓ Browser (NEUTRAL) = GOOD
Supported Operating System and Unsupported Browser	The operating system is supported and the browser is not supported.	Ensure the latest version of the browser for that operating system is installed.	Supported OS (GOOD) + Unsupported Browser (FAIR) = FAIR
			Supported OS (GOOD) + Unsupported Browser (WARN) = WARN
			Supported OS (GOOD) + Unsupported Browser (BAD) = BAD

Unknown Browser and Operating System	The operating system and browser could not be recognized.	If obfuscation of the browser and operating system version is intentional, ensure an update strategy for browsers and operating systems is in place.	? OS + ? Browser = NEUTRAL
Unknown Operating System and Browser	The browser and operating system could not be recognized.	If obfuscation of the browser and operating system version is intentional, ensure an update strategy for browsers and operating systems is in place.	? OS + ? Browser = NEUTRAL
Unknown Operating System and Supported Browser	The operating system details could not be recognized and the browser is supported.	If obfuscation of the operating system version is intentional, for which there is no penalty, ensure an operating system update strategy is in place.	? OS + Supported Browser (GOOD) = GOOD
Unknown Operating System and Unsupported Browser	The operating system is unknown and the browser is unsupported.	Ensure the latest version of the operating system is installed. After that, install the latest supported version of the desired browser.	? OS + Unsupported Browser (FAIR) = FAIR ? OS + Unsupported Browser (WARN) = WARN ? OS + Unsupported Browser (BAD) = BAD
Unsupported Operating System and Browser	The operating system and the browser are both unsupported.	Ensure the latest version of the operating system is installed. After that, install the latest supported version of the desired browser.	Unsupported OS (FAIR) + Unsupported Browser (WARN) = WARN Unsupported OS (FAIR) + Unsupported Browser (BAD) = BAD Unsupported OS (WARN) + Unsupported Browser (FAIR) = WARN Unsupported OS (WARN) + Unsupported Browser (BAD) = BAD Unsupported OS (BAD) + Unsupported Browser (FAIR) = BAD

			Unsupported OS (BAD) + Unsupported Browser (WARN) = BAD
Unsupported Operating System and Supported Browser	The operating system is not supported and the browser is the latest supported version for that OS.	Ensure the latest version of the operating system is installed. After that, install the latest supported version of the desired browser.	Unsupported OS (FAIR) + Supported Browser (GOOD) = FAIR
			Unsupported OS (WARN) + Supported Browser (GOOD) = WARN
			Unsupported OS (BAD) + Supported Browser (GOOD) = BAD
Unsupported Operating System and Unknown Browser	The operating system is not supported and browser information could not be determined.	Update the operating system to the latest version.	Unsupported OS (FAIR) + ❓Browser (NEUTRAL) = FAIR
			Unsupported OS (WARN) + ❓Browser (NEUTRAL) = WARN
			Unsupported OS (BAD) + ❓Browser (NEUTRAL) = BAD

How the Mobile Software risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The Mobile Software risk vector assesses the supported or unsupported status of the software version. The use of mobile software is not required to improve an organization's cyber security posture.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** ⊘ This default grade does not have a negative impact on the rating. It is equivalent to a perfect grade. Either: • There are no findings. • The estimated number of users falls below a minimum threshold. To avoid sudden fluctuations, the risk vector is reassigned an A to F grade when the estimated number of users has stayed above the threshold for 65 days.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 65 Days There’s a grace period of 28 days for validating and updating software packages.
Weight	**Percentage (out of 70.5% in Diligence):** 1%

Finding Grading

Mobile Software findings are a combination of the evaluated operating system (OS) and browser, which are graded independently from one another, and the Mobile Software finding grade represents the calculated combination of the OS and browser. The OS and browsers are evaluated based on their supported status:

- **Good:** The version is supported.
- **Fair:** The version has been unsupported for less than 4 weeks.
- **Warn:** The version has been unsupported for less than 52 weeks.
- **Bad:** The version has been unsupported for over 52 weeks.

With the exception of specific software which have their own end-of-life policies, software that becomes unsupported are given an additional grace period of up to 7 days and will be considered as "supported" during that time; the previous version reaches its end-of-life within 7 days after the release of a newest version. This is because as the software reaches its end-of-life (EOL), an entire week of data on those versions is aggregated on a weekly basis (currently every Friday).

The general support life cycle of some software products are split into two periods – the first half with "mainstream support," followed by the second half with "extended support." After the extended support period, "extended security updates (ESU)" might be offered. Extended support and ESU are taken into consideration when determining if software is supported.

This currently applies within the Bitsight platform to Microsoft products. These ESU programs do not include all security fixes and upgrades.

Software with ESU are evaluated in the following manner:

- **Good:** From the date of release to the end date of extended support.
- **Fair:** The first and second years of ESU.
- **Warn:** The third year ESU.
- **Bad:** The end date of ESU.

Graded Mobile Browsers

- Android Browser
- BlackBerry WebKit
- Chrome Mobile iOS
- Chrome Mobile
- Firefox Mobile

All other browsers are evaluated as NEUTRAL.

Graded Mobile Operating Systems

- Android
- iOS
- BlackBerry OS

All other operating systems are evaluated as “NEUTRAL.”

Versions that are undetermined or unknown default to the following evaluations:

❗ **Undetermined:** If there’s no version available, if the finding cannot be identified, or if both the OS and browser are unknown; the finding is graded as NEUTRAL.

❓ **Unknown:** If either the OS or browser has been evaluated and the other is unknown, the finding is graded as the given grade.

OS & Browser Status	Supported Browser (GOOD)	Unsupported Browser (FAIR, WARN, BAD)	❗ Undetermined/ ❓ Unknown Browser
Supported OS (GOOD)	Supported OS (GOOD) + Supported Browser (GOOD) = GOOD	Supported OS (GOOD) + Unsupported Browser (FAIR) = FAIR Supported OS (GOOD) + Unsupported Browser (WARN) = WARN Supported OS (GOOD) + Unsupported Browser (BAD) = BAD	Supported OS (GOOD) + ❓ Browser (NEUTRAL) = GOOD
Unsupported OS (FAIR, WARN, BAD)	Unsupported OS (FAIR) + Supported Browser (GOOD) = FAIR	Unsupported OS (FAIR) + Unsupported Browser (WARN) = WARN Unsupported OS (FAIR) + Unsupported Browser (BAD) = BAD	Unsupported OS (FAIR) + ❓ Browser (NEUTRAL) = FAIR
	Unsupported OS (WARN) + Supported Browser (GOOD) = WARN	Unsupported OS (WARN) + Unsupported Browser (FAIR) = WARN Unsupported OS (WARN) + Unsupported Browser (BAD) = BAD	Unsupported OS (WARN) + ❓ Browser (NEUTRAL) = WARN
	Unsupported OS (BAD) + Supported Browser (GOOD) = BAD	Unsupported OS (BAD) + Unsupported Browser (FAIR) = BAD Unsupported OS (BAD) + Unsupported Browser (WARN) = BAD	Unsupported OS (BAD) + ❓ Browser (NEUTRAL) = BAD
❗ Undetermined/ ❓ Unknown OS	❓ OS + Supported Browser (GOOD) = GOOD	❓ OS + Unsupported Browser (FAIR) = FAIR ❓ OS + Unsupported Browser (WARN) = WARN ❓ OS + Unsupported Browser (BAD) = BAD	❗ OS (NEUTRAL) + ❗ Browser (NEUTRAL) = NEUTRAL
	❗ OS (NEUTRAL) + Supported Browser (GOOD) = GOOD	❗ OS (NEUTRAL) + Unsupported Browser (FAIR) = FAIR ❗ OS (NEUTRAL) + Unsupported Browser (WARN) = WARN ❗ OS (NEUTRAL) + Unsupported Browser (BAD) = BAD	❓ OS + ❓ Browser = NEUTRAL

Messages

Message	Description	Remediation Instructions	Finding Grade (OS + Browser Support Status)
Neutral Operating System and Unknown Browser	The operating system and browser versions could not be determined.	If obfuscation of the browser and operating system version is intentional, ensure an update strategy for browsers and operating systems is in place.	❗ OS (NEUTRAL) + ❗ Browser (NEUTRAL) = NEUTRAL
Neutral Operating System and Unsupported Browser	The operating system version could not be determined and the browser is not supported.	Ensure the latest version of the browser for that operating system is installed.	❗ OS (NEUTRAL) + Unsupported Browser (FAIR) = FAIR
			❗ OS (NEUTRAL) + Unsupported Browser (WARN) = WARN
			❗ OS (NEUTRAL) + Unsupported Browser (BAD) = BAD
Supported Operating System and Browser	The operating system and browser are both supported.		Supported OS (GOOD) + Supported Browser (GOOD) = GOOD
Supported Operating System and Unknown Browser	The operating system is supported and the browser could not be recognized.	If obfuscation of the browser version is unintentional, ensure end-users are using approved mobile applications in order to be able to analyze the supported (or unsupported) status of those applications.	Supported OS (GOOD) + ❓ Browser (NEUTRAL) = GOOD
Supported Operating System and Unsupported Browser	The operating system is supported and the browser is not supported.	Ensure the latest version of the browser for that operating system is installed.	Supported OS (GOOD) + Unsupported Browser (FAIR) = FAIR
			Supported OS (GOOD) + Unsupported Browser (WARN) = WARN
			Supported OS (GOOD) + Unsupported Browser (BAD) = BAD

Unknown Browser and Operating System	The browser and operating system could not be recognized.	If obfuscation of the browser and operating system version is intentional, ensure an update strategy for browsers and operating systems is in place.	❓OS + ❓Browser = NEUTRAL
Unknown Operating System and Browser	The browser and operating system could not be recognized.	If obfuscation of the browser and operating system is intentional, ensure an update strategy for browsers and operating systems is in place.	❓OS + ❓Browser = NEUTRAL
Unknown Operating System and Supported Browser	The operating system details could not be recognized and the browser is supported.	If obfuscation of the operating system version is intentional, for which there is no penalty, ensure an operating system update strategy is in place.	❓OS + Supported Browser (GOOD) = GOOD
Unknown Operating System and Unsupported Browser	The operating system is unknown and the browser is unsupported.	Ensure the latest version of the operating system is installed. After that, install the latest supported version of the desired browser.	❓OS + Unsupported Browser (FAIR) = FAIR
Unsupported Operating System and Browser	The operating system and browser are both not supported.	Ensure the latest version of the operating system is installed. After that, install the latest supported version of the desired browser.	Unsupported OS (FAIR) + Unsupported Browser (WARN) = WARN
			Unsupported OS (FAIR) + Unsupported Browser (BAD) = BAD
			Unsupported OS (WARN) + Unsupported Browser (FAIR) = WARN
			Unsupported OS (WARN) + Unsupported Browser (BAD) = BAD
			Unsupported OS (BAD) + Unsupported Browser (FAIR) = BAD
			Unsupported OS (BAD) + Unsupported Browser (WARN) = BAD

Unsupported Operating System and Supported Browser	The operating system is not supported and the browser is the latest supported version for that OS.	Ensure the latest version of the operating system is installed. After that, install the latest supported version of the desired browser.	Unsupported OS (FAIR) + Supported Browser (GOOD) = FAIR Unsupported OS (WARN) + Supported Browser (GOOD) = WARN Unsupported OS (BAD) + Supported Browser (GOOD) = BAD
Unsupported Operating System and Unknown Browser	The operating system is not supported and the browser information could not be determined.	Update the operating system to the latest version.	Unsupported OS (FAIR) + ❓Browser (NEUTRAL) = FAIR Unsupported OS (WARN) + ❓Browser (NEUTRAL) = WARN Unsupported OS (BAD) + ❓Browser (NEUTRAL) = BAD

User Count Thresholds for Grading Endpoint Risk Vectors

March 26, 2024: Published.

When there's insufficient data, the Desktop Software and Mobile Software risk vectors are assigned a default grade. Either:

- There are no findings.
- The estimated number of users falls below a minimum threshold. To avoid sudden fluctuations, the risk vector is reassigned an A to F grade when the estimated number of users has stayed above the threshold for 65 days.

The threshold is determined as follows:

- The estimated number of users is less than 5, or
- The estimated number of users is less than 100 and less than the number of employees divided by 1,000.

Examples

Number of Employees	Threshold (Estimated Users)
1,000	Less than 5
5,000	Less than 5
20,000	Less than 20
100,000	Less than 100
200,000	Less than 200

How the DNSSEC risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

For the DNSSEC risk vector, we look at a variety of criteria when determining the effectiveness of a Domain Name System Security Extensions (DNSSEC) record. Without DNSSEC configured, some data from the DNS server may not be secure.

Though DNSSEC is not standard in the industry, this risk vector is evaluated since DNSSEC protects DNS resolvers from receiving bad data by using public key encryption to sign domains or other zones to ensure authenticity of records. In short, this technology helps to protect everyday users from malicious redirects when looking up domain names. Refer to the list of registrars that support end-user DNSSEC management.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** C No ratings impact. This risk vector does not currently affect security ratings. It is being evaluated for a period before being factored into Bitsight Security Ratings.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 70.5% in Diligence):** Not Applicable

Finding Grading

DNSSEC findings are evaluated and then graded as GOOD, WARN, BAD, or NEUTRAL.

- GOOD
- WARN
- BAD
- NEUTRAL

Messages

Each issue has a message shown in the platform as an individual entry, along with the associated IP address. For instance, “DSA public key is less than 2048 bits.” The text in the remediation column is also available in the platform. Remediation is guidance on how to resolve the issue so that it no longer adversely impacts the organization's Bitsight Security Rating.

GOOD

In order to be graded as GOOD, the domain should have DNSSEC enabled and should be properly configured. The certificate must adhere to the following rules:

- It must be encrypted using a secure hash algorithm with a sufficiently long key.
- It must have a validated chain of trust.

WARN

The presence of these issues affects an organization's Bitsight Security Rating. They should be remediated as soon as possible.

BAD

The presence of these issues affects an organization's Bitsight Security Rating. They should be remediated as soon as possible.

NEUTRAL

These issues don't affect an organization's Bitsight Security Rating.

How the Mobile Application Security risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

Mobile Application Security evaluates an organization's mobile application offerings in Android and iOS app stores (assets) to find security risks that can compromise end-users' devices and networks (findings).

This risk vector does not currently affect security ratings. It is being evaluated for a period before being factored into security ratings.

Concept	Behavior
Application Assessment Assessment results depending on the action taken during testing.	**Result:** Pass/Fail Assessment is immediate. If a new app version is available, the new version replaces all assessments related to the previous one. If an assessment for a specific version is improved, it also replaces the associated finding.
Insufficient Data A default risk vector grade is assigned.	**Default:** Not all organizations have mobile application offerings. This default grade is assigned if the organization has not published any mobile applications (no assets).

Concept	Behavior
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 1 year, with no decay period. Unless updated, all findings have the same impact throughout their lifetime. Their impact is fully removed when updated or after 1 year. If an app is removed from all app stores or updated to a software version that is not supported (and therefore cannot be scanned), its impact is fully removed. The following software versions are supported: • Android: 12 and 14 • iOS: between 7 and 17.1.1
Weight	**Percentage (out of 70.5% in Diligence):** Not applicable

Criteria

If a third party developer is involved, please contact Bitsight Support to learn more about Total Risk Monitoring with the Bitsight Security Ratings Platform.

Methodology

Mobile apps are no longer assigned finding grades (GOOD, FAIR, WARN, BAD, etc.). The new, numerical app grade is intended to be a more intuitive replacement that's indicative of the app's overall vulnerability to security issues. Although it's derived directly from the CVSS values of vulnerabilities, found in an app, and evaluated on a scale from 0.0 to 10.0, the app grade is not a CVSS value. Learn more about this ratings methodology update...

Assets are subjected to static and dynamic analysis to evaluate specific types of problems, like how the application handles sensitive data, interaction vulnerabilities, and API security and determine the severity of security vulnerabilities (presented as the findings).

Finding Severity

The evaluation method for tested security vulnerabilities is based on the Common Vulnerability Scoring System (CVSS). The assigned value (of 0.1 to 10.0) is indicative of the severity of each vulnerability.

A number of informational vulnerabilities are also tested. However, these informational vulnerabilities do not negatively impact the rating.

CVSS	Passed Test Finding Severity	Failed Test Finding Severity
0.0	Informational	Informational
0.1 - 3.9	Minor	Minor
4.0 - 6.9	Minor	Moderate
7.0 - 8.9	Minor	Material
9.0 - 10.0	Minor	Severe

App Grade Calculation Based on Security Tests

Each individual finding in a mobile app is quantified using the Common Vulnerability Scoring System (CVSS). CVSS is a ten-point scale, spanning 0.0 to 10.0 in increments of 0.1. A CVSS value of 0.0 indicates findings that are informational in nature.

The active sum contribution of individual apps is calculated as an app score (α) based on the failure of security tests (τ):

$$\alpha = \sum_{\tau, CVSS(\tau) > 0} 2^{CVSS(\tau)}$$

The app grade (γ) is calculated as:

$$\gamma = \begin{cases} min\{10, log_2(\alpha);\} \; \alpha > 0, \\ 0; \; \alpha = 0 \end{cases}$$

Risk Vector Grade Calculation Based on the Individual App Grade

To calculate the risk vector grade, first, calculate the mean AppGrade (alpha) based on the individual AppGrades.

The second step is to calculate a pre risk vector score X based on (alpha) using the following formula:

$$x = \begin{cases} min\{10, \, max\{0.1, \, log_2(\bar{\alpha});\}\} \; \bar{\alpha} > 0, \\ 0; \; \bar{\alpha} = 0 \end{cases}$$

Lastly, the risk vector grade is determined mapping X to the grade using the following table:

Range of App Grades Average	Risk Vector Grade
$0 \leq \chi < 2.4$	A
$2.4 \leq \chi < 4.0$	B
$4.0 \leq \chi < 5.7$	C
$5.7 \leq \chi < 7.0$	D
$7.0 \leq \chi < 10$	F
No applications.	N/A

How the Web Application Security risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The Web Application Security risk vector performs multiple assessments related to web application security. It provides information about components with known vulnerabilities, broken authentication and access control, sensitive data exposure, cross-site scripting prevention mechanisms, and security misconfigurations.

- Criteria
- Methodology

This risk vector does not currently affect security ratings. It is being evaluated for a period before being factored into security ratings.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** Some findings cannot be traced back to specific companies due to the use of third party systems; such as web filters and Content Delivery Networks (CDN), that are capable of redirecting and encapsulating network traffic. Some firewalls might also be detecting and blocking external scanning tools from getting any data. This is set in the center of the grading scale for computing into security ratings. If there are no findings and we are temporarily unable to collect data, the most recent grade is assigned for up to 400 days before being assigned the default grade.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days

Weight	**Percentage (out of 70.5% in Diligence):** This risk vector does not currently affect security ratings.

Criteria

Only domains that provide an HTTP or HTTPS service are included in these assessments.

Methodology

Domains that are included are loaded using a standard web browser connection. Bitsight then captures the entire response of the page load, including redirects and all dynamic page content, and performs a set of assessments on that response. Bitsight does not send out specific requests to trigger or identify vulnerabilities that may be present on the web application. We also do not crawl the loaded page for additional responses.

Assessment Categories

Web Application Security findings are subjected to different assessments to determine the presence and severity of vulnerabilities. The assessments are defined to target a specific Common Weakness Enumeration (CWE) or a category within the Open Web Application Security Project (OWASP) Top 10.

The Assessments can be generalized as follows.

Field	Description
Cross-Site Scripting	Validation of security measures such as SRI and CSP to ensure no malicious remote resource is included on a web application.
Components with Known Vulnerabilities	Using a library with missing security patches can make your web application exceptionally easy to abuse, making it crucial to ensure that any available security updates are to be applied immediately.
Broken Authentication and Access Control	Access control policies ensure that users cannot act outside their intended permissions.
Sensitive Data Exposure	Ensuring application design includes controls to reduce the exposure of critical and sensitive information.
Security Misconfiguration	Assessment of web application implementations regarding security hardening or unnecessary features and privileges.

How the DMARC risk vector is assessed.

April 30, 2024: Released.

The DMARC risk vector determines whether domains have a Domain-based Message Authentication, Reporting and Conformance (DMARC) policy or not and evaluates how effective it is at ensuring only verified senders are able to use this domain for email.

Note: This is a temporarily non-graded risk vector and is assigned with an ⊘ N/A grade.

See the criteria for classifying findings as DMARC.

- Finding Details
- Finding Grading
- Finding Messages

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** ⊘
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	Duration: 60 Days
Weight	Percentage (out of 70.5% in Diligence): This risk vector does not currently affect security ratings.

Finding Grading

Refer to the DMARC finding messages to see all possible grades.

Common Issues

DMARC findings are evaluated by validating the following common issues:

- The presence of findings – No DMARC record present. It should be present to authenticate that the sender of an email is legitimately authorized to send emails on a company's behalf.

- Invalid DMARC record – A record has syntax errors or is otherwise misspecified and is ineffective.
- Ineffective passthrough policy – The passthrough policy is ineffective in protecting recipients from spoofed emails.
- Missing reporting configuration – The records do not receive reporting emails and their implementation cannot be monitored. This is consequential for records using the passthrough policy.
- Use of unauthorized third-party reporting – The mailto links lack corresponding authorization records for their domains and do not receive reporting emails.
- Low percentage filtering – Less than 100% filtering means that some spoofed emails can be delivered. This is acceptable only in early stages of adoption.

Policy Enforcement

Finding grades by how the policy is enforced:

- No Enforcement – This is ineffective and does not protect against spoofing, it is graded BAD.
- Limited Enforcement – While not discarded, such emails are forwarded to a spam or junk folder or are otherwise marked to indicate the authentication failure to the recipient. However, some confirmed fraudulent emails can end up being delivered since the pct tag specifies a value less than 100.
    - The best grade when using a non-maximum pct value is FAIR.
    - The best grade when using pct≤50 is WARN.
- Full Enforcement – For DMARC records to be grade GOOD:
    - An active policy must be used (p=reject or p=quarantine) and the policy must act on all authentication failures (pct=100).
    - Any existing third-party reporting domains must be associated with a valid authorization record.

How the Domain Squatting risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The Domain Squatting risk vector reveals if a company has registration coverage for domains that resemble their own primary/secondary domains, which render them most susceptible to these types of attacks.

See domain registration statuses.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** ⊘ This is an informational risk vector. It does not currently affect security ratings.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** Not Applicable
Weight	**Percentage (out of 70.5% in Diligence):** Not Applicable

Domain Registration Statuses

We determine if domains are registered based on the information provided by DNS queries.

If new primary or secondary domains are added to a company, the data will be available the following week. If newly mapped companies are added to the Bitsight inventory during the nightly data collection process, findings will be available for those companies the following day.

Each domain variation is evaluated and grouped into one of the following states:

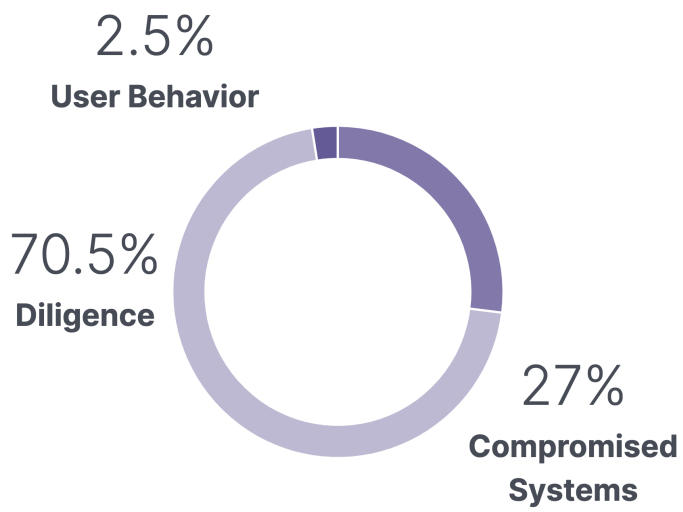
Ownership Status	Description
Own Company	Indicates if the company who owns the target domain (appears in its domain map) registered the variation.
Another Company	Indicates if another company registered the variation. This assumes that organizations are not maliciously squatting. This helps resolve issues where Cosco legitimately has “cosco.com,” a domain variation of “cisco.com,” registered. This also captures cases where we have mapped Identity/Brand Protection companies and various companies in our inventory use these third-parties for brand protection. Example: SBC.com and ABC.com
Third Party	This domain is registered, but not by a known organization.
Not Registered	The domain is unregistered.

How the User Behavior risk category is calculated.

April 19, 2023: 2023 RAU weight adjustment.

Assessment

The User Behavior risk category accounts for 2.5% of a company's Bitsight Security Rating.



Overview

User Behavior findings that are older than 60 days no longer affect a company’s grade. User Behavior findings are updated daily.

Risk Vectors

User Behavior is comprised of the following risk vectors:

Risk Vector	Description
File Sharing	Based on a 60-day rolling average.
Exposed Credentials	Data verification is an important part of ensuring high-quality ratings and grades.  This is an informational risk vector and does not affect security ratings.

How the File Sharing risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

File Sharing activity is assessed based on the unique file appearances across unique IP addresses and vice versa.

Evaluation

File Sharing is based on the following elements:

- The number of unique torrents in the company’s infrastructure.
- The number of unique IP addresses that are associated with File Sharing events.
- The duration of the event, measured in days.
- The File Sharing category, which considers application events to be more high-risk than all other File Sharing categories (non-application events).

Each event represents activity for a unique torrent shared through a unique IP address during 1 day.

Description	File Sharing Activity Types (On a given day)	Events
1 file is counted as 1 event, regardless of how many times it was observed from an IP address on a given day.	1 File	1 Event
1 file across 4 IP addresses are counted as 4 events; 1 event per IP address.	1 File, 4 IP Addresses	4 Events
4 files in 1 IP address counts as 4 events: 1 event per unique file.	4 Files, 1 IP Address	4 Events

Whitelisting of torrents is available upon request. Please send the torrent hash you wish to whitelist to Bitsight Support.

The overall letter grade is based on the number of times illegitimate files are shared within a company’s infrastructure, compared to all companies in the Bitsight inventory. The higher the volume of file sharing activity, the lower the grade. The score is then normalized to account for company size.

Impact

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** A The rating is positively impacted if there are no File Sharing findings.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	**Duration:** 60 Days
Weight	**Percentage (out of 2.5% in User Behavior):** 2.5%

How the Public Disclosures risk category is calculated.

The Public Disclosures risk category provides information related to possible incidents of undesirable access to a company's data, including breaches, general security incidents, and other disclosures.

Risk Vectors

The risk vectors within the Public Disclosures risk category affect Bitsight Security Ratings in the following manner:

Risk Vector	Description
Security Incidents	Only certain events impact a company's rating and only if they occur, as opposed to having a percentage of the rating dedicated to them. Unlike other risk vectors, the absence of these events do not positively affect ratings, but its presence can have a negative impact. The impact of events starts on the effective date. A – "A" Letter Grade in the Absence of Events This is designed to neutralize any positive or negative impact to the risk vector.
Other Disclosures	This does not currently impact the rating. It's considered to be the least severe among the Public Disclosures risk vectors. Its impact to business continuity is minimal if they were to occur. N/A – "N/A" Letter Grade in the Absence of Events

How the Security Incidents risk vector is assessed.

March 26, 2024: “No findings/low findings” changed to “insufficient data.”

The Security Incidents risk vector involves a broad range of events related to the undesirable access of a company’s data. They’re grouped into Breach Security Incidents and General Security Incidents.

This risk vector only impacts Bitsight Security Ratings if an incident occurs. When an incident is recorded, its base impact may be adjusted based on the number of lost or exposed records, the company size, and any delay in Bitsight’s recording.

Any event that’s under investigation can possibly have an initial impact value of 0, depending on the amount of available information. The impact might change in the future if further information becomes available that changes our understanding of the incident.

Base Impact

Each incident type within each incident category (breach and general) has a base impact.

Ratings-impact is subject to change from informational to ratings-impacting and vice versa based on changes in public recommendations.

Concept	Behavior
Insufficient Data A default risk vector grade is assigned.	**Default:** A The absence of Security Incidents results in an A grade. Unlike other risk vectors, an A in Security Incidents has a neutral effect on security ratings.
Lifetime The number of days a finding impacts the risk vector grade, assuming nothing changes in the future and the finding is not updated with new information. Learn why findings have a decay and lifetime period.	Ratings-impacting Security Incident events have a 120-day half life starting from the effective date. The impact reduces smoothly and continuously by half every 120 days (e.g., 40, then 20, then 10 and so on.). Individual events completely stop impacting the rating after 2 years.

Breach Security Incident Impact

Breach Security Incidents are ratings-impacting.

Incident Type	Ratings Impact
Crimeware	80
Espionage	60
Intrusion (No Records)	60
Phishing	70
Ransomware	100
Social Engineering	70
Web Apps	80

General Security Incident Impact

General Security Incidents are considered more severe than the Other Disclosures risk vector. Some general security incident types are ratings-impacting, while others are informational only and do not impact the rating.

❖ Does not impact ratings, regardless of record count.
⚠ Does not impact ratings if the record count is less than 10 or is unknown.

Incident Type	Ratings Impact
Account Takeover (Employee)	20
Account Takeover (User)	❖
DNS Incident	❖
Error	50⚠
Internal Incident	❖
Lost / Stolen Asset	30⚠

Lost / Stolen Asset (Encrypted)	❖
Other Incident	20
Point of Sale (POS)	20
Privilege Abuse	50
Unknown	30
Unsecured Database	30

Adjustments

Record Count

The base impact may be increased based on the number of records of personal information involved, as follows:

- 0-10 records = +0 points
- 11-100 records = +10 points
- 101-1000 records = +20 points
- 1001-10,000 records = +30 points
- 10,001-100,000 records = +40 points
- 100,001+ records = +50 points

A ransomware incident involving 9,000 records has an impact of 130 (100 for incident type + 30 for record count).

Company Size

The impact may be reduced based on the size of the company to reflect the higher baseline risks of larger companies. This reduction is as follows:

- 0-100 employees = No adjustments
- 101-1000 employees = Reduced up to 20%
- 1001-10,000 employees = Reduced up to 40%
- 10,001-100,000 employees = Reduced up to 60%
- >100,000 employees = Reduced by 60%

The reduction varies smoothly between the values. For example, the adjustment for 5000 employees is between 20% and 40%.

- In the ransomware example above, 130 would be the actual impact for a company with 0–100 employees.
- For a large company with over 100,000 employees, the actual impact for the same incident would be around 52 points, reflecting the 60% reduction for such companies (130 × 40%).

Recording Delay

Finally, the impact may be reduced to reflect any delay between the public disclosure date and Bitsight's recording of the incident. This is calculated using the same 120-day half life with which the rating recovers from security incidents.

Examples:

- If the ransomware incident on the larger company were made public today and immediately recorded, its impact today would be 52 points.
- If the incident had been made public four months ago and promptly recorded, its impact today would be approximately 26 points (52 × 0.5), reflecting the natural recovery from the original impact.
- If the incident had been made public four months ago but not recorded until today, its impact would be 26 points–Bitsight's failure to record the incident in a timely manner does not change what its impact is today.

How ratings are normalized.

Large organizations typically have more domains, more machines, and a greater network presence than smaller ones. As a result, they generally have more Compromised Systems, User Behavior, and Diligence findings. Risk vector grades are normalized based on an organization's size to ensure ratings are fairly calculated for large companies.

Each risk vector is normalized using a specific method dependent on the associated risk and assigned a letter grade. Then, each risk vector is assigned a weight as outlined in the risk categories and risk vectors overview. These methods ensure the security rating of a large company is comparable to that of a small company and vice versa.

Normalization by Risk Type

Different methods are used to normalize the final result depending on the risk type. The selection of these methods is determined by the associated risk we are evaluating. For example, user behavior-related risk vectors take into consideration the count of employees, while risk vectors that evaluate the configuration of systems take into consideration the total number of findings we are able to generate.

Risk Category	Risk Vector	Method Used for Normalization
Compromised Systems	Botnet Infections	Employee Count
	Spam Propagation	Employee Count
	Malware Servers	Employee Count
	Unsolicited Communications	Employee Count
	Potentially Exploited	Employee Count
Diligence	SPF Domains	Findings Count
	DKIM Records	Findings Count
	TLS/SSL Certificates	Findings Count
	TLS/SSL Configurations	Findings Count
	Open Ports	Findings Count
	Web Application Headers	Findings Count
	Patching Cadence	Findings Count

Risk Category	Risk Vector	Method Used for Normalization
	Insecure Systems	Employee Count
	Server Software	Active IP Count
	Desktop Software	Estimated User Count
	Mobile Software	Estimated User Count
	DNSSEC	Findings Count
	Mobile Application Security	Findings Count
	Web Application Security	Findings Count
	Domain Squatting	Not applicable
User Behavior	File Sharing	Employee Count
	Exposed Credentials	Not applicable
Public Disclosures	Security Incidents	Employee Count
	Other Disclosures	Not applicable

Diligence Risk Vectors

Most Diligence risk vector findings are graded GOOD, FAIR, NEUTRAL, WARN, or BAD, with the exception of Patching Cadence and Domain Squatting. Insecure Systems findings are only graded NEUTRAL, WARN, or BAD; because of the nature of this risk vector, findings are never GOOD or FAIR. With those exceptions in mind, Diligence grades can be considered the ratio of FAIR, WARN, and BAD records to the total number of records associated with an organization. A larger organization will usually have more findings, and any given finding will have less impact than it would for a smaller organization.

Findings in a given grade may have different scoring impacts due to their estimated severity. To build a risk vector grade, we add the scoring impacts of all findings and divide them by the normalization factor to produce a raw score. To determine the risk vector's letter grade (A-F), we convert the raw score to a percentile by ranking all the organizations we rate across all industries and locations.

Some organizations are excluded from the ranking process. These include cloud service providers and telecommunications companies, whose ratings are typically low because of customer-hosted assets that are not controlled by the organizations that own the IP address space.

Special cases are noted below.

Desktop Software and Mobile Software

Since these risk vectors track the operating systems and browser versions of outbound web traffic, normalization is based on the estimate of the number of users we can observe within a company's infrastructure. This value takes into account the different traffic that is generated from each IP and is grouped by user agent, target domains, and a session identifier that allows us to calculate the approximate number of different users within that infrastructure.

Server Software

Normalization is based on the number of unique IP addresses with exposed services, such as HTTP[S], SMTP, or SSH. This is derived from the data available on the Open Ports risk vector.

Compromised Systems Risk Vectors, File Sharing, and Insecure Systems

The Compromised Systems risk category tracks malware infections on internal endpoints by intercepting traffic to the malware's command and control (C2) infrastructure; the File Sharing risk vector tracks BitTorrent activity from a company; the Insecure Systems risk vector assesses endpoints that are communicating with an unintended destination. All inform Bitsight about the abuse of endpoints and are, therefore, based on company size (employee count). Each risk vector uses this metric to normalize the final result assigned to them.

If the employee count for an organization is unknown, the employee count defaults to 100.

Security Incidents

The size of an organization (measured by the number of employees) factors into the impact calculation on a logarithmic basis. Employee count is restricted to 100 employees at the lower end and 100,000 at the upper end to account for the sparsity of data. Refer to How is the Security Incidents Risk Vector Assessed? for additional details.

Adjusted Peer Analytics Data Counts

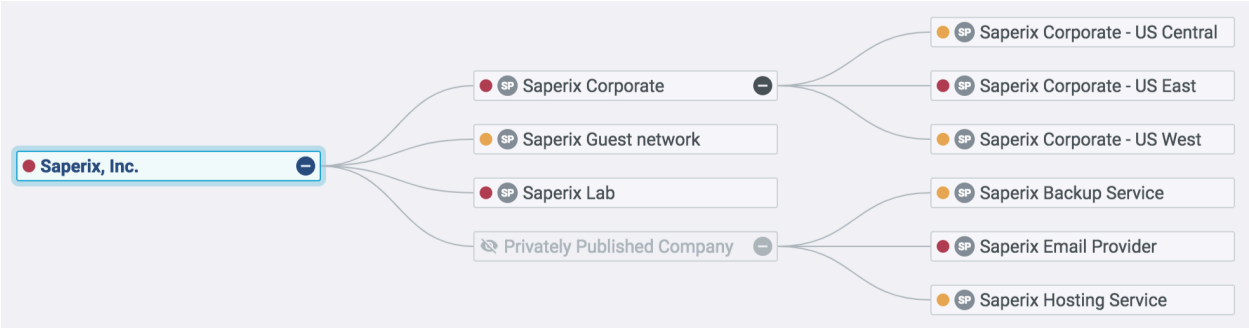
For the Risk Vector Details data in Peer Analytics, the displayed finding counts are adjusted to match the size of your organization. This adjustment results in more meaningful comparisons and ensures the displayed reference values are useful for guidance in defining your security performance goals.

- **Compromised Systems:** We adjust for company size (employee count).
- **Diligence:** We adjust for either the IP count for the Server Software risk vector or finding count for all other Diligence risk vectors.
- **File Sharing:** We adjust for company size (employee count).

If your company has 10 findings in total with 2 BAD findings, a peer with 100 findings in total with 20 BAD findings is similar. The peer's BAD finding count is adjusted to “2,” i.e. there are 2 BAD findings per 10 total findings.

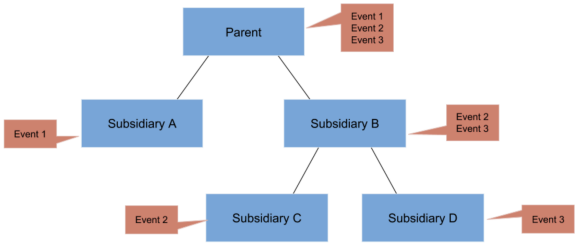
How Bitsight Security Ratings are calculated within parent-subsidiary relationships.

Subsidiaries that are within the hierarchy of an organization are depicted in the organization's Ratings Tree. Ratings Tree relationships are structured as a parent company and subsidiary company. If you are the parent company, your subsidiary is a company in your Ratings Tree that is below your company. A subsidiary company can be a parent of another subsidiary, which means some organizations may have multiple levels in their Ratings Tree.



Relationship Impact on Security Ratings

Relationships are only used to percolate assets up the tree. The rating algorithm has no information about subsidiary relationships. The rating algorithm is applied independently to each company in the Ratings Tree and the company hierarchy is ignored.

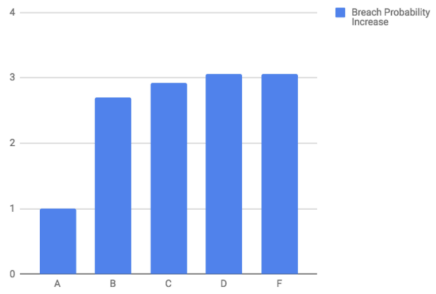


The root parent owns all assets (IP ranges and domains) and all employees of its subsidiaries. Assets flow up from the bottom towards the top (parent) of the Ratings Tree. This means BAD findings or Compromised Systems findings of a subsidiary also affects the parent.

As an additional benefit, the outside-in approach to Security Ratings is impervious to company reorganization and restructuring.

Probability of a Breach Security Incident

A study on our breach database shows that companies with an A have an average of little to no Botnet Infections events per month and that a letter grade of B results in almost 3x of an increase in the probability of a breach.



This means that a small number of events from a single subsidiary will substantially reduce the rating of that subsidiary and all its ancestors. It only takes 1 Botnet Infection to be vulnerable to a Breach Security Incident. Most subsidiaries are likely to be clean of events due to sparseness. Therefore, parents will have a rating close to their worst subsidiary.

Correlation

The Security Rating of a parent is most correlated to the weakest subsidiary. In the same way that a vendor with weak cyber security practices introduces vulnerabilities, a weak subsidiary also makes the parent vulnerable.

Access to the parent is easier from a subsidiary or vendor. All companies within the Ratings Tree are affected when a subsidiary is impacted by a Ratings-impacting Security Incidents event, which will result in reputation damage, data exposure, and network exposure through the entire organization.

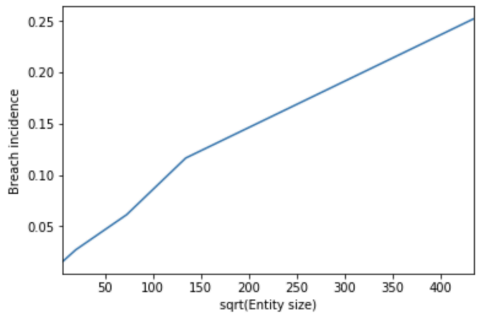
This is similar to supply chain risk assessment. If a crucial link is weak (regardless of network size), the entire supply chain is at risk.

Normalization Factor

Grade by Employee Rate

The grade on a Compromised Systems risk vector is based on a per employee rate, as opposed to a raw count. The employee rate allows a comparison of the security posture for companies of varying sizes.

3 Botnet Infections for a company of 100 employees is worse than 3 Botnet Infections for a company of 1000 employees. However, it only takes 1 Botnet Infection to be vulnerable to a breach. The probability of breach based only on size is near linear to the square root of employee count, as seen in the graph below.



Employee Count Normalization

The normalization factor for Compromised Systems can be interpreted as the square root of the employee count.

Using the square root of employee count to normalize means fewer Compromised Systems events are required per employee, in order for large companies to have the same rating as small companies.

Raw Count vs Normalization Factor Example:

- Dogs has 9 employees and 3 Botnet Infections events.
- Cats has 16 employees and 2 Botnet Infections events.
- Dogs and Cats are subsidiaries of Pets, Inc. The parent company is treated as a shell company. It includes the 25 employees and 5 events from its subsidiaries and employees from itself.

If the rate of events per employee (events/employee count) is used, Dogs has the worst rating (0.3333), Cats has the best rating, and Pets, Inc. is in the middle:

Companies	Events	Employee Counts	Calculated Ratings (events/employee count)
Dogs	3 Botnet Infections	9 employees	0.3333
Cats	2 Botnet Infections	16 employees	0.125
Pets, Inc.	5 Botnet Infections	25 employees	0.2

However, the normalization factor is the square root of the parent company rather than the raw count (events/√employee count). Therefore, Pets, Inc. is the same as the worst of the subsidiaries, which is Dogs. The parent is penalized in this situation.

Companies	Events	Normalized Employee Counts	Calculated Ratings (events/√employee count)
Dogs	3 Botnet Infections	√9 (normalized to 3 employees)	1
Cats	2 Botnet Infections	√16 (normalized to 4 employees)	0.5
Pets, Inc.	5 Botnet Infections	√25 (normalized to 5 employees)	1

The lifetime of findings.

July 10, 2024: The Patching Cadence lifetime is 90 days.

Every finding has a lifetime that indicates how long it impacts the risk vector grade, depending on the particular risk vector. This is defined by the number of days a finding will impact the risk vector grade.

Remaining Lifetime shows the projected number of days that a finding will continue to impact risk vector grading. This is a projection that assumes nothing changes in the future and a finding is not updated with new information. It may change if a finding is updated.

Learn why findings have a lifetime and decay period.

Risk Type	Lifetime
Compromised Systems	180 Days
Diligence (except Patching Cadence)	60 days on average, depending on the risk vector.
Patching Cadence	90 Days
User Behavior	60 Days
Security Incidents	2 Years

Frequently Asked Questions

Why do findings with a GOOD grade have a remaining lifetime?

All findings that impact a risk vector grade have a lifetime, including positive (GOOD) and neutral grades. The lifetime simply indicates how long any impact will last.

Why would a GOOD finding stop impacting ratings?

While the remaining lifetime is likely to be more useful when working on remediating findings, this is still a function of how risk vectors – and ultimately rating – are graded.

Why do findings of risk vectors that are in beta have a remaining lifetime?

Because the lifetime of a finding is the number of days the finding will impact the risk vector grade and is not directly impacting the rating, beta risk vectors have a lifetime.

Beta risk vectors function exactly like regular risk vectors, which evaluates the underlying data and is given an overall assessment. However, the data is undergoing testing. Any grade does not ultimately impact the rating during the beta period.

Risk Vector Grading with Insufficient Data

October 29, 2024: Updated.

There could be insufficient data when grading risk vectors. A default risk vector grade is assigned. The threshold varies by risk vector.

Insufficient data could be due to any of the following reasons:

- There are no findings or the findings have no impact on the score. Neutral findings do not impact the score. If only Neutral findings are detected, a default letter grade is assigned.
- For Desktop Software and Mobile Software, the estimated number of users falls below a minimum threshold.
- For Mobile Application Security, the organization has not published any mobile applications (no assets).
- We are temporarily unable to collect data.
  For select risk vectors, the most recent grade is assigned for up to 400 days before being assigned the default grade.

Why Bitsight Security Ratings fluctuate.

Bitsight Security Ratings are the results of the aggregation of all risk vector letter grades (with different weights) that are normalized for that company.

Security ratings are based on a 10-point rating system that's rounded down in 10 point increments. If the current rating is 740, this is a representation of the combined assessments of all risk vectors. The actual rating may be somewhere between 740 and 749.

An actual rating of 735 is represented as a 730.

The fluctuations in security ratings coincides with the daily shifts in:

- The number of new observations.
- Adjustments when events fully decay or when findings complete their lifetime and no longer impact the rating.

When the combined risk vectors are given an assessment, the subtle differences may increase or decrease the overall Security Rating with no visible changes to the individual risk vector letter grades (the risk vectors did not change to the next A-to-F letter grades).

A slight increase in observations for a few combined risk vectors may have been sufficient enough to decrease the overall rating of 741 (represented as 740) to a 739 (represented as 730).

The opposite is also true. If there are minor improvements to the individual risk vectors and the overall score is 749 (represented as 740), the significant improvement to an actual rating of 755 (represented as a 750).

Why findings have a decay and lifetime period.

July 10, 2024: The Patching Cadence lifetime is 90 days.

When a piece of malware or a vulnerable open port is sensed on a company's network, something new has been discovered about the cybersecurity posture of the company. For example, it is possible to install a piece of software on the network without permission. In other ratings contexts, this event is analogous to

- missing a credit card payment,
- finding a cockroach at a restaurant,
- getting a speeding ticket, or
- failed smoke-alarm inspection for a commercial building.

The knowledge is immediate and shows that an entity that was previously thought to have a certain level of security, in fact, was not at that level. A ratings company or insurance company uses such indicators as a way to estimate the risk of bad things happening such as a major security breach or, following the analogies above, a

- loan default,
- major foodborne disease outbreak,
- car accident, or
- major fire.

Thus, events in the first list lower ratings and raise premiums, interest rates etc. The events in the first list often have clear causal links to those in the second. However, it should be noted that often the root causes are difficult to sense but have correlates that can be sensed. Such correlates are often used by ratings agencies and insurance companies. The correlations are established via a set of historical data over a set of representative companies and show that the correlates raise the likelihood of the bad outcomes.

The above discussion is indicative of a crucial difference between ratings companies and other service companies such as vulnerability identification services, for example. One of the elements of newly discovered information (first list above), say a vulnerable open port, is that it’s an indicator of a security posture problem for ratings companies. Simply closing it upon being informed of its existence does little to remove the crucial fact that it was opened in the first place. Ratings companies and insurance companies require a period of time to be convinced that the underlying problem has been fixed. Thus, the impact of the original event stays in place for a period of time. Again, this lifetime is supported by studies of historical data exemplified by questions of the form “if a company had malware infection in the last year, what is their likelihood of having a Ratings-impacting Security Incidents event in the near future?” Or analogously, “if a person had a speeding ticket in the last year, what is the likelihood that they will get in an accident in the near future” or “if a person missed a credit card payment, what is their likelihood of defaulting on a home improvement loan?”

Depending on the results of these studies, ratings and insurance companies, set the length and decay of the impact of an event type. When nothing new happens, then it can be assumed that whatever general problem was fixed. The table below presents the outcomes of these experiments.

The following table summarizes the different time scales:

Risk Type	Impact Timespan
Compromised Systems	180 Days
Diligence (except Patching Cadence)	Approximately 60 Days
Patching Cadence	90 Days
User Behavior	60 Days
Security Incidents	2 Years