API Impact Report

Risk Type Rename

Patching Cadence → **Critical Vulnerability Management**

Old display name	Patching Cadence
New display name	Critical Vulnerability Management
Internal slug	patching_cadence (stable — never changes)
Breaking changes	**1 endpoint**
Informational changes	**17 endpoints**
No action needed	**4 endpoints/params**

1. Overview

Bitsight is renaming the risk type previously displayed as "Patching Cadence" to "Critical Vulnerability Management". This document covers every Customer API v1 endpoint affected by this change, categorised by the severity of impact on existing integrations.

The rename affects display names only. The internal slug (patching_cadence) used for filtering and object keys is permanently stable and never changes.

⚠ Breaking	i Informational	✓ No Action
1 endpoint Must update code before release or integration will break.	17 endpoints Display name in response changes. Update string comparisons if you have them.	4 endpoints / params Slug-based — completely unaffected.

2. Breaking Change ⚠

What you need to know

Only one endpoint requires a code change. If your integration reads the details_by_name dictionary from GET /defaults/ using the key "Patching Cadence", that key will no longer exist after this release and your code will receive undefined / null.

All other changes are informational — your integration will continue to work, but returned display names will change.

2.1 GET /defaults/ — details_by_name Dictionary Key

The GET /defaults/ response includes a details_by_name object keyed by the display name of each risk type. After the rename, the key changes:

```
// Before — breaks after release:
const entry = response.details_by_name["Patching Cadence"];

// After — required:
const entry = response.details_by_name["Critical Vulnerability Management"];
```

Endpoint	Required Action
GET /defaults/	Update dict key lookup from "Patching Cadence" to "Critical Vulnerability Management".

3. Informational Changes — rating_details Response Field i

What this means

All endpoints in this section return a rating_details object or array containing a "name" field.
The name field will change from "Patching Cadence" to "Critical Vulnerability Management".
The object key (the slug patching_cadence) does NOT change — you can still use rating_details.patching_cadence to access the entry.

Action needed only if your code does a hardcoded string comparison against "Patching Cadence".

3.1 rating_details Object (keyed by slug)

These endpoints return rating_details as an object. Access the Patching Cadence entry via the stable slug key rating_details.patching_cadence. Only the .name field inside it changes.

Endpoint	Field that changes	Impact
GET /companies/{guid}/	rating_details.patching_cadence.name	Informational
GET /companies/{guid}/preview/	rating_details.patching_cadence.name	Informational
GET /fast-ratings/	rating_details.patching_cadence.name	Informational
GET /fast-ratings/requests/{guid}/response/	rating_details.patching_cadence.name	Informational
GET /portfolio/ratings/?expand=rating_details	results[].rating_details.patching_cadence.name	Informational

3.2 rating_details Array (industry endpoints)

These endpoints return rating_details as an array. Each element has a "name" field (changes) and a "slug" field (remains patching_cadence).

Endpoint	Field that changes	Impact
GET /industries/?expand=rating_details	results[].rating_details[n].name(where slug = patching_cadence)	Informational
GET /industries/{slug}/?expand=rating_details	rating_details[n].name(where slug = patching_cadence)	Informational

4. Informational Changes — risk_vectors[].name Response Field i

What this means

These endpoints return an array of risk vector objects. Each object contains a "name" field (changes) and a "slug" field (remains patching_cadence).

Action needed only if your code compares or hardcodes the string "Patching Cadence" from this array.

Endpoint	Field that changes	Impact
GET /companies/{guid}/quick-view/ai-summary/	risk_vectors[n].name(where slug = patching_cadence)	Informational
GET /portfolio/diligence-summary/	results[].risk_vectors[n].name	Informational
GET /subsidiaries/statistics/	risk_vectors[n].name(patching_cadence entry)	Informational
GET /companies/{guid}/assessments/	risk_vector_grades[n].name	Informational

5. Informational Changes — risk_type_label and Name Fields i

What this means

These endpoints return the risk type display name as a single field value in the response body.
The value changes from "Patching Cadence" to "Critical Vulnerability Management".
No structural schema change — the field name itself stays the same.

Endpoint	Field that changes	Impact
GET /companies/{guid}/summary-risk-vector-report/	Risk type label in report structure	Informational
GET /companies/{guid}/findings/	risk_type_label (on each finding object)	Informational
GET /companies/{guid}/findings/statistics/	risk_type_label (in statistics response)	Informational

6. Informational Changes — CSV Downloads and NIST Report Text

6.1 CSV Column Header Changes

If your pipeline downloads CSV reports and parses column headers by name string, update the column names.

Endpoint	Column header change	Impact
GET /companies/{guid}/reports/diligence/ (CSV)	"Patching Cadence" → "Critical Vulnerability Management"	Informational
GET /companies/{guid}/rating-release-previews/ (CSV)	"Patching Cadence Grade" → "Critical Vulnerability Management Grade"	Informational

6.2 NIST Report Summary Text

Six NIST CSF category summaries in the regulatory report reference the risk type name in their text. This is a display-only change — no structural schema change.

Endpoint	NIST CSF Categories	Impact
GET /companies/{guid}/regulatory/nist/	ID.RA-1, ID.RA-5, PR.IP-12PR.MA-1, DE.CM-8, RS.MI-3	Informational — display text only

7. No Action Required ✓

Why these are safe

The following endpoints and parameters use the internal slug name (patching_cadence or patching-cadence), which is permanently stable and never changes with display name updates. No code changes are needed for any of the items in this section.

7.1 URL Path Segments

Endpoint	Status	Impact
GET /companies/{guid}/findings/patching-cadence/critical/	Both patching-cadence and critical-vulnerability-management path segments are accepted	No Action
GET /companies/{guid}/peer-analytics/statistics/patching-cadence/	URL is unchanged in this release. A future release may add an alias with the updated slug.	No Action

7.2 Slug-Based Query Parameters

Endpoint	Parameter	Value	Impact
GET /companies/{guid}/observations/statistics/	include_patching_cadence	unchanged	No Action
GET /companies/{guid}/peer-analytics/statistics/diligence/	exclude_patching_cadence	unchanged	No Action

8. Migration Checklist

Use this checklist to audit your integration before the release date.

Required — will break without this change ⚠

□ GET /defaults/ — Update any code reading details_by_name["Patching Cadence"]. Change the key to "Critical Vulnerability Management".

Best practice: switch to looking up by slug in the risk_types array to avoid being affected by future renames.

Recommended — not required, but update string comparisons i

□ Search your codebase for the string "Patching Cadence" in any response-parsing or comparison logic.

□ rating_details[].name — Value changes. If you compare or display this, it will read "Critical Vulnerability Management".

□ risk_vectors[].name — Value changes. If you compare or display this, it will read "Critical Vulnerability Management".

□ risk_type_label — Display field on findings and statistics responses changes.

□ CSV column names — Update parsers that match on "Patching Cadence" or "Patching Cadence Grade".

No changes needed ✓

✓ ?risk_vector=patching_cadence — Slug filter; stable and unaffected.

✓ include_patching_cadence / exclude_patching_cadence — Query params; slug-based, unaffected.

✓ URL paths containing patching-cadence — Still accepted; unaffected.

✓ rating_details.patching_cadence (object key) — Slug key; stable and unaffected.

9. Full Endpoint Reference (22 Endpoints)

Complete list of all endpoints in scope, ordered by impact severity. Colour coding: red = breaking, amber = informational, green = no action.

#	§	Endpoint	What Changes	Impact
1	§2.1	GET https://api.bitsighttech.com/v1/defaults/	details_by_name key "Patching Cadence" → "Critical Vulnerability Management"	⚠ BREAKING
2	§3.1	GET https://api.bitsighttech.com/v1/companies/{company_guid}/	rating_details.patching_cadence.name	i Info
3	§3.1	GET https://api.bitsighttech.com/v1/companies/{company_guid}/preview/	rating_details.patching_cadence.name	i Info
4	§3.1	GET https://api.bitsighttech.com/v1/fast-ratings/	rating_details.patching_cadence.name	i Info
5	§3.1	GET https://api.bitsighttech.com/v1/fast-ratings/requests/{request_guid}/response/	rating_details.patching_cadence.name	i Info
6	§3.1	GET https://api.bitsighttech.com/v1/portfolio/ratings/?expand=rating_details	results[].rating_details.patching_cadence.name	i Info
7	§3.2	GET https://api.bitsighttech.com/v1/industries/?expand=rating_details	results[].rating_details[n].name (slug=patching_cadence)	i Info
8	§3.2	GET https://api.bitsighttech.com/v1/industries/{industry_slug}/?expand=rating_details	rating_details[n].name (slug=patching_cadence)	i Info
9	§4	GET https://api.bitsighttech.com/v1/companies/{company_guid}/quick-view/ai-summary/	risk_vectors[n].name (slug=patching_cadence)	i Info
10	§4	GET https://api.bitsighttech.com/v1/portfolio/diligence-summary/	results[].risk_vectors[n].name	i Info
11	§4	GET https://api.bitsighttech.com/v1/subsidiaries/statistics/	risk_vectors[n].name (patching_cadence entry)	i Info

12	§4	GET https://api.bitsighttech.com/v1/companies/{company_guid}/assessments/	risk_vector_grades[n].name	i Info
13	§5	GET https://api.bitsighttech.com/v1/companies/{company_guid}/summary-risk-vector-report/	Risk type label in report structure	i Info
14	§5	GET https://api.bitsighttech.com/v1/companies/{company_guid}/findings/	risk_type_label (per finding)	i Info
15	§5	GET https://api.bitsighttech.com/v1/companies/{company_guid}/findings/statistics/	risk_type_label (in stats response)	i Info
16	§6.1	GET https://api.bitsighttech.com/v1/companies/{company_guid}/reports/diligence/ (CSV; often ?format=csv)	Column header "Patching Cadence" → "Critical Vulnerability Management"	i Info
17	§6.1	GET https://api.bitsighttech.com/v1/companies/{company_guid}/rating-release-previews/ (CSV)	Column header "Patching Cadence Grade" → "Critical Vulnerability Management Grade"	i Info
18	§6.2	GET https://api.bitsighttech.com/v1/companies/{company_guid}/regulatory/nist/	Summary text for 6 NIST CSF categories (display only)	i Info
19	§7.1	GET https://api.bitsighttech.com/v1/companies/{company_guid}/findings/patching-cadence/critical/ https://api.bitsighttech.com/v1/companies/{company_guid}/findings/critical-vulnerability-management/critical/	Both slugs accepted — no change	✓ No Action
20	§7.1	GET https://api.bitsighttech.com/v1/companies/{company_guid}/peer-analytics/statistics/patching-cadence/	URL unchanged	✓ No Action
21	§7.2	GEThttps://api.bitsighttech.com/v1/companies/{company_guid}/observations/statistics/?include_patching_cadence=true	Slug param — no change	✓ No Action
22	§7.2	GET https://api.bitsighttech.com/v1/companies/{company_guid}/peer-analytics/statistics/diligence/?exclude_patching_cadence=true	Slug param — no change	✓ No Action