BITSIGHT® KNOWLEDGE BASE

Portfolio Company Information API Guide

Publication Date – March 7, 2022

Portfolio Company Information

Get information about companies in your portfolio:

Path	Purpose	Description
`/v1/companies/company_guid`	GET: Company Details	Get details about a company, including their rating details, rating history, and risk vector grades.
`/v1/companies/search`	GET: Search for a Company in the BitSight Inventory	Search for a company in the BitSight inventory.
`/v1/portfolio/breaches`	GET: Public Disclosures in Portfolio	Get Public Disclosure details of organizations in your portfolio.

GET: Company Details

https://api.bitsighttech.com/ratings/v1/companies/company_guid

Get details about a company, including their rating details, rating history, and risk vector grades.

Parameters

*Required.

Parameter	Description	Values
company_guid* *Path*	Identify the company to query.	*[String]* Use GET: Portfolio Details [/v2/portfolio] to get the company unique identifier [company_guid].

Example Request

```
curl https://api.bitsighttech.com/ratings/v1/companies/a940bb61-33c4-42c9-9231-c8194c305db3 -u api_token:
```

Example Response

```
{
   "guid":"a940bb61-33c4-42c9-9231-c8194c305db3",
   "custom_id":null,
   "name":"Saperix, Inc.",
   "description":"Saperix Technologies LLC develops risk analysis software
solutions.",
   "ipv4_count":5272,
   "people_count":13000,
   "shortname":"Saperix",
   "industry":"Technology",
   "industry_slug":"technology",
   "sub_industry":"Computer & Network Security",
   "sub_industry_slug":"computer_network_security",
   "homepage":"http://www.saperix.com",
   "primary_domain":"saperix.com",
   "type":"CURATED",

"display_url":"https://service.bitsighttech.com/app/company/a940bb61-33c4-42
c9-9231-c8194c305db3/overview/",
   "rating_details":{
      […]
      "spf":{
         "category":"Diligence",
         "rating":800,
         "beta":false,
         "percentile":94,
         "name":"SPF",

"display_url":"https://service.bitsighttech.com/app/company/a940bb61-33c4-42
c9-9231-c8194c305db3/diligence-details/?filter=spf",
         "grade":"A",
         "category_order":1,
         "order":5,
         "grade_color":"#2c4d7f"
      }
   },
   "ratings":[
      […]
      {
         "rating_date":"2019-06-01",
         "rating":500,
         "range":"Basic",
         "rating_color":"#b24053"
      }
   ],
   "search_count":4227,
   "subscription_type":"Continuous Monitoring",

"sparkline":"https://api.bitsighttech.com/ratings/v1/companies/a940bb61-33c4
-42c9-9231-c8194c305db3/sparkline?size=small",
   "subscription_type_key":"continuous_monitoring",
   "subscription_end_date":null,
   "bulk_email_sender_status":"NONE",
   "service_provider":false,
   "customer_monitoring_count":221,
   "available_upgrade_types":[
   ],
   "has_company_tree":true,
   "is_bundle":false,
   "rating_industry_median":"below",
   "primary_company":{
      "guid":"eed24cfa-c3ea-4467-aefa-89648881e277",
      "name":"Saperix Corporate"
   },
   "permissions":{
      "can_download_company_report":true,
      "can_view_forensics":true,
      "can_view_service_providers":true,
      "can_request_self_published_entity":true,
      "can_view_infrastructure":true,
      "can_annotate":true,
      "can_view_company_reports":true,
      "can_manage_primary_company":true,
      "has_control":true
   },
   "is_primary":false,
   "security_grade":null,
   "in_spm_portfolio":true
}
```

Response Attributes

Field	Description
`guid` *String* [`company_guid`]	The unique identifier of this company.
`custom_id` *String*	The customizable ID assigned to this company.
`name` *String*	The name of this company.
`description` *String*	Details about this company, which typically includes its industry and location.
`ipv4_count` *Integer*	The number of IP addresses attributed to this company.
`people_count` *Integer*	The number of employees in this company.
`shortname` *String*	The abbreviated name of this company.
`industry` *String*	The industry of this company.
`industry_slug` *String*	The industry slug name of this company.
`sub_industry` *String*	The sub-industry of this company.
`sub_industry_slug` *String*	The sub-industry slug name of this company.
`homepage` *String*	The URL of this company's primary external website.
`primary_domain` *String*	The name of this company's primary domain.
`type` *String*	The type of rating. See rating types.
`display_url` *String*	The URL to this company's overview page in the BitSight platform.

`rating_details` *Object*	Information about this company's security management performance by risk vector and details for use in HTML applications.
Risk Vector Slug Name *Object*	Information about this company's security performance for this risk vector.
`category` *String*	The risk category of this risk vector. ● `Compromised Systems` ● `Diligence` ● `User Behavior` ● `Public Disclosures`
`rating` *Integer*	For internal BitSight use.
`beta` *Boolean*	A `true` value indicates this risk vector is in beta and does not affect this company's security rating.
`percentile` *Integer*	This company's performance on this risk vector against their peers.
`name` *String*	The name of this risk vector.
`display_url` *String*	The URL in the BitSight platform that contains the details of this risk vector.
`grade` *String*	The letter grade of this risk vector.
`category_order` *Integer*	For internal BitSight use to visually sort this risk category in the BitSight platform.
`order` *Integer*	For internal BitSight use to visually sort this risk vector in the BitSight platform.
`grade_color` *String*	The hex code to display letter grade colors in HTML applications.
`ratings` *Array*	Daily security ratings. Each entry is one day, starting with the most recent entry and goes back to one year.
`rating_date` *String* [`YYYY-MM-DD`]	The date when this BitSight Security Rating Report was generated.
`rating` *Integer*	The BitSight Security Rating of this company on this day.

<table>
<tr><td></td><td><code>range</code>
<em>String</em></td><td>The rating category of this company on this day:
<table>
<tr><th>Categories</th><th>Security Rating Ranges</th><th>Distribution*</th></tr>
<tr><td>Advanced</td><td>740 – 900</td><td>½ of Companies</td></tr>
<tr><td>Intermediate</td><td>640 – 730</td><td>⅓ of Companies</td></tr>
<tr><td>Basic</td><td>250 – 630</td><td>⅙ of Companies</td></tr>
</table>
*The approximate distribution of companies in the entire BitSight inventory, across the rating categories.</td></tr>
<tr><td></td><td><code>rating_color</code>
<em>String</em></td><td>The hex code to display rating category colors in HTML applications.</td></tr>
<tr><td colspan="2"><code>search_count</code>
<em>Integer</em></td><td>The number of times this company has been listed in search results.</td></tr>
<tr><td colspan="2"><code>subscription_type</code>
<em>String</em></td><td>The type of subscription used to monitor this company.</td></tr>
<tr><td colspan="2"><code>sparkline</code>
<em>String</em></td><td>The URL path to the security rating trend line of this company during the past one year.</td></tr>
<tr><td colspan="2"><code>subscription_type_key</code>
<em>String</em></td><td>The slug name of the subscription used to monitor this company.</td></tr>
<tr><td colspan="2"><code>subscription_end_date</code>
<em>String</em> [<code>YYYY-MM-DD</code>]</td><td>The date when the subscription to this company expires.</td></tr>
<tr><td colspan="2"><code>bulk_email_sender_status</code>
<em>String</em></td><td>A <code>FULL</code> value indicates this company provides bulk email sending services, which excludes this company from the Spam Propagation risk vector.</td></tr>
<tr><td colspan="2"><code>service_provider</code>
<em>Boolean</em></td><td>A true value indicates this company is a service provider.</td></tr>
<tr><td colspan="2"><code>customer_monitoring_count</code>
<em>Integer</em></td><td>The number of companies that are monitoring this company.</td></tr>
<tr><td colspan="2"><code>available_upgrade_types</code>
<em>Array</em></td><td>For internal BitSight use.</td></tr>
<tr><td colspan="2"><code>has_company_tree</code>
<em>Boolean</em></td><td>A <code>true</code> value indicates this company has a Ratings Tree.</td></tr>
<tr><td colspan="2"><code>is_bundle</code>
<em>Boolean</em></td><td>A <code>true</code> value indicates this company is part of a ratings bundle.</td></tr>
</table>

`rating_industry_median` *String*	Indicates this company's position in the peer group distribution chart.
`primary_company` *Object*	Identifies the primary company of this organization.
`guid` *String* [`company_guid`]	The unique identifier of this organization's primary company.
`name` *String*	The name of this organization's primary company.
`permissions` *Object*	Your BitSight account capabilities.
`can_download_company_report` *Boolean*	A `true` value indicates you can view and download BitSight Security Rating Reports (PDF).
`can_view_forensics` *Boolean*	A `true` value indicates you have the Event Forensics add-on package.
`can_view_service_providers` *Boolean*	A `true` value indicates you can access BitSight for Fourth Party Risk Management.
`can_request_self_published_entity` *Boolean*	A `true` value indicates you can request the creation of a self-published rating.
`can_view_infrastructure` *Boolean*	A `true` value indicates you can view your infrastructure attribution.
`can_annotate` *Boolean*	A `true` value indicates you can identify assets and segment your network with infrastructure tags.
`can_view_company_reports` *Boolean*	A `true` value indicates you can view BitSight Security Rating Reports.
`can_manage_primary_company` *Boolean*	A `true` value indicates you can highlight a primary for your organization.
`has_control` *Boolean*	For internal BitSight use.
`is_primary` *Boolean*	A `true` value indicates your company is the primary for your organization.
`in_spm_portfolio` *Boolean*	A `true` value indicates this company is in your Security Performance Management portfolio (My Company, SPM Subsidiary, etc.).

GET: Search for a Company in the BitSight Inventory

`https://api.bitsighttech.com/ratings/v1/companies/search`

Search for a company in the BitSight inventory.

Parameters

❖ Either the `domain` or `name` parameter is required.

Parameter	Description	Values
`domain`❖ *Query*	Search by domain name.	*[String]* The domain of a company. **Example:** `saperix.com`
`expand` *Query*	Include additional company information. Using this parameter could slow the performance of the endpoint and will limit results to 10 companies.	*[String]* `details` = Return additional company information.
`limit`	Set the maximum number of results. The results might include fewer records (even zero), but not more.	*[Integer]* If not set, the default number of results can vary depending on the endpoint.
`name`❖ *Query*	Search by company name.	*[String]* The name of a company. **Example:** `Saperix, Inc.`
`offset`	Set the starting point of the return.	*[Integer]* A `0` (zero) value starts the results from the first record in the result set. **Default:** `100`

Example Request

```
curl -u 'api_token:'
'https://api.bitsighttech.com/ratings/v1/companies/search?domain=saperix.com
&expand=details'
```

Example Response

```
{
   "links":{
      "next":null,
      "previous":null
   },
   "count":10,
   "results":[
      […]
      {
         "guid":"819b6a11-d1c6-4518-9566-0611c34d5d8e",
         "name":"Saperix Hosting Service",
         "industry":"Technology",
         "industry_slug":"technology",
         "primary_domain":"saperix.com",
         "description":"Saperix Technologies LLC develops risk analysis
software solutions.",
         "website":"http://saperix.com/hosting",
         "details":{
            "is_bundled":false,
            "is_primary":false,
            "is_service_provider":false,
            "has_company_tree":true,
            "search_history_count":5143,
            "customer_monitoring_count":84,
            "self_published":"public",
            "confidence":"High",

"logo":"https://api.bitsighttech.com/ratings/v1/companies/819b6a11-d1c6-4518
-9566-0611c34d5d8e/logo-image",
            "in_portfolio":true,

"search_token":"540H3GPGtrT-_T2WZ3m8vkn5TEzXumFwQCoYZGhLunUCCWo77BHf19Ik9XeW
h0TbONQAI-9uJaVC7fdQee_vlRK28r_RDQM0MuSNHpHbUpV3btbfS3vkReJ7jirHGKud3t3J1Cfx
BMiyUp_N21Fv0Xh03itXMWXOQkCNjlvXFqghJbeXgIv5xgFhm8Ght2nn",
            "primary_company":null
         }
      }
   ]
}
```

Response Attributes

Field	Description
`links` *Object*	Navigation for multiple pages of results. See pagination.
`next` *String*	The URL to navigate to the next page of results.
`previous` *String*	The URL to navigate to the previous page of results.
`count` *Integer*	The amount of search results.
`results` *Array*	Company search results.
Object	A company in the search results.
`guid` *String* [`company_guid`]	The unique identifier of this company.
`name` *String*	The name of this company.
`industry` *String*	This company's industry.
`industry_slug` *String*	The slug name of this company's industry.
`primary_domain` *String*	The main domain that belongs to this company.
`description` *String*	A description of this company and its purpose.
`website` *String*	The web address (URL) to this company's primary domain.
`details` *Object*	If the `expand` parameter is set to `details` (`&expand=details`), these company details are included.
`is_bundled` *Boolean*	A `true` value indicates this company is part of a ratings bundle.
`is_primary` *Boolean*	A `true` value indicates this company is designated as the primary, which the publisher believes is the most accurate indication of their security posture.

			`is_service_provider` *Boolean*	A `true` value indicates this company is a service provider.
			`has_company_tree` *Boolean*	A `true` value indicates this company has a Ratings Tree.
			`search_history_count` *Integer*	The number of times this company has appeared in searches.
			`customer_monitoring_count` *Integer*	The number of companies that are currently monitoring this company.
			`self_published` *String*	Indicates if this self-published report is public or private.
			`confidence` *String*	The level of confidence in the quality of the company data. ● `High` = The data is accurate. ● `Low` = The data is limited.
			`logo` *String*	The URL path of this company's logo image.
			`in_portfolio` *Boolean*	A `true` value indicates this company is in your portfolio.
			`search_token` *String*	An auto-generated unique identifier for this search.
			`primary_company` *String*	The name of the primary designated for this company's organization.

Pagination

The BitSight API might return a large number of results for a given query and will be paginated. Paginated results include the next, previous, and count fields.

Field	Description
count *Integer*	The number of results.
next *String* [URL]	The link to navigate to the next page of the results.
previous *String* [URL]	The link to navigate to the previous page of the results.

Recommendations

We recommend using the following query parameters, if available, to modify the response and improve the performance of the API:

- Define a start_date and end_date.
- The maximum number of results per query is controlled by the limit parameter; a request might return fewer results than this (even zero), but not more.

GET: Public Disclosures in Portfolio

https://api.bitsighttech.com/ratings/v1/portfolio/breaches

Get Public Disclosure details of organizations in your portfolio.

- Parameters
- Example Request
- Example Response
- Response Attributes

Parameters

Parameter	Description	Values
company *Query*	Filter by a specific company.	*[String]* Use GET: Portfolio Details [/v2/portfolio] to get the company unique identifier [company_guid].
Dates	Date filters.	
start *Query*	Filter from the specified date.	*[String]* YYYYMMDD
end *Query*	Filter before the specified date.	*[String]* YYYYMMDD
folder *Query*	Filter companies in the specified folder.	[String] Use GET: Folder Details [/v1/folders] to get the folder unique identifier [folder_guid].
Severity	Filter by Security Incidents severity.	
severity *Query*	Filter events that are equal to a specified severity level.	*[Integer]* ● 0 = Informational ● 1 = Minor ● 2 = Moderate ● 3 = Severe
severity_gte *Query*	Filter events that are greater than or equal to a specified severity level.	
severity_gt *Query*	Filter events that are greater than a specified severity level.	
severity_lte *Query*	Filter events that are less than or equal to a specified severity level.	

	`severity_lt` *Query*	Filter events that are less than a specified severity level.	
`tier` *Query*		Filter companies in the specified tier.	*[String]* Use GET: Tiers [`/v1/tiers`] to get the tier unique identifier [`tier_guid`].

Example Request

```
curl 'https://api.bitsighttech.com/ratings/v1/portfolio/breaches' -u
api_token:
```

Example Response

```
[
   {
      "event_type":"Web Apps",
      "category_slug":"breach",
      "text":"Hackers gained access to the Pollinate, Inc. customer
database. This action compromised the financial information of 1234
individuals.",
      "is_direct":true,
      "date":"2019-09-29",
      "breached_company":{
         "guid":"19d16bf5-11a6-467b-b7b1-f5563daece69",
         "name":"Pollinate, Inc."
      },
      "category_name":"Breach Security Incident",
      "severity":2,

"preview_url":"http://s3.amazonaws.com/com.bitsighttech.breachpdf/fakery/Fak
e%20Breach%20Form.pdf",
      "event_type_description":"An incident in which a web application was
the attack vector, including code level vulnerabilities in the application
and thwarted authentication mechanisms",
      "date_created":"2020-02-20",
      "affected_portfolio_company":{
         "guid":"19d16bf5-11a6-467b-b7b1-f5563daece69",
         "name":"Pollinate, Inc."
      }
   }
]
```

Response Attributes

Field	Description
`event_type` *String*	The Public Disclosures incident type. Breach Security Incidents: ● `Crimeware` = An instance of malware installed for the purpose of acquiring unauthorized data or assets. ● `Espionage` = An incident of unauthorized network or system access exhibiting the motive of state-sponsored or industrial espionage, where trade secrets or IP are frequently targeted. ● `Intrusion` = Unauthorized access which does not involve exfiltration of records or other resources. ● `Phishing` = An attack in which fraudulent email is used to mimic the access of an authorized employee or legitimate contact. ● `Ransomware` = An attack designed to block access to a computer system until a sum of money is paid. ● `Social Engineering` = An attack which uses deception to trick individuals into divulging unauthorized information or access. ● `Web Apps` = An incident in which a web application was the attack vector, including code level vulnerabilities in the application and thwarted authentication mechanisms. General Security Incidents: ● `Account Takeover (Employee)` = An attacker gains unauthorized access into a service through the use of employee's account credentials. ● `Account Takeover (User)` = An attacker gains unauthorized access into a service through the use of a user's account credentials. ● `DNS Incident`[1] = An organization lost control or never had control of one of the associated assets, as defined by the DNS record[2]. ● `Error` = An incident involving unintentional actions that directly compromise a sensitive asset. ● Internal Incident = An incident discovered by the company in question and remediated with no apparent compromise. ● `Lost/Stolen Asset` = An incident where an information asset went missing, whether through misplacement or malice. ● `Lost/Stolen Asset (Encrypted)` = An incident where an encrypted asset went missing, whether through misplacement or malice, with no evidence of encryption compromise. ● `Other Incident` = A security incident that does not fall into one of the other categories.

	• `Point of Sale (PoS)` = Remote attacks against the environments where retail transactions are conducted, specifically where purchases are made. • `Privilege Abuse` = An unapproved or malicious use of organizational resources beyond what is authorized. • `Unknown` = A security incident where certain classification details pertaining to the event are unknown. • Unsecured Database = A database is left unsecured due to error and the data is accessible by third parties. Other Security Incidents: • ATM/Skimmer = A physical attack involving unauthorized access to an ATM, or the use of a skimming device to gather data from payment cards. • DoS = An attack intended to compromise the availability of networks and systems. • Fraud = An incident where a company was tricked into releasing information, funds, or other resources to an unauthorized party, not necessarily involving systems intrusion. • Other Disclosure = A disclosure that does not fall into one of the other categories.
`category_slug` *String*	The slug name of the Public Disclosures incident category.
`text` *String*	A summary of the Public Disclosures event.
`is_direct` *Boolean*	A true value indicates this company was the original target within a multiparty event.
`date` *String* [`YYYY-MM-DD`]	The date when this event will start to impact the rating. This is either the date of disclosure or the publication date of the source (whichever is earlier).
`breached_company` *Object*	The company where the event occurred.
`guid` *String* [`company_guid`]	The unique identifier of the company where the event occurred.
`name` *String*	The name of the company where the event occurred.
`category_name` *String*	The name of the Public Disclosures incident category.

`severity` *Integer*	The severity of the Public Disclosures event. **Values:** ● `0` = Informational ● `1` = Minor ● `2` = Moderate ● `3` = Severe
`preview_url` *String*	The URL path for the news source and documentation.
`event_type_description` *String*	A description of the incident type.
`date_created` *String* [`YYYY-MM-DD`]	The date when this Public Disclosures event was added to the BitSight Security Ratings Platform.
`affected_portfolio_company` *Object*	This company in your portfolio was affected by this Public Disclosures event.
`guid` *String* [`company_guid`]	The unique identifier of this company in your portfolio.
`name` *String*	The name of this company in your portfolio.

API Fields: Rating Types

To best manage risk, using the BitSight-curated version in your portfolio rather than the self-published rating is suggested. However, your approach may vary depending on your relationships with the companies in your portfolio.

Type	Description	Slug Name
BitSight-Curated	The default designation.	`CURATED`
Self-Published	A standalone BitSight Security Rating report. It consists of CIDR blocks, IP addresses, and domains that are specifically selected by the company itself, rather than curated by BitSight.	`SELF-PUBLISHED`
Privately Published	Created by an organization for internal use and are not available for other organizations to monitor and do not appear in searches by other organizations.	`PRIVATE`