



BITSIGHT[®]

PvIB  Platform voor
InformatieBeveiliging

Waarde van Security Ratings in 3rd party IT security Risk Management

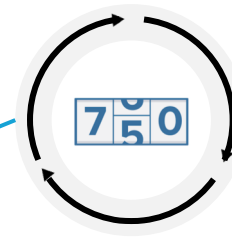
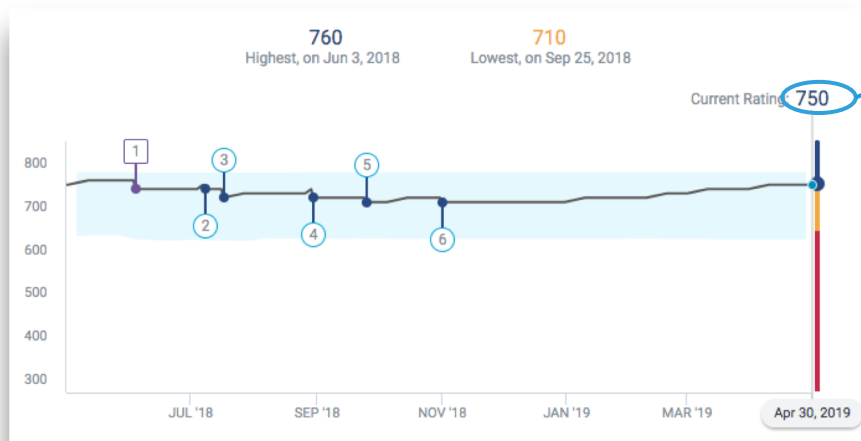
Lennart.Pikaart@bitsight.com

06-51519833

www.bitsight.com

Vertaal Complexe Cybersecurity zaken in eenvoudige business context

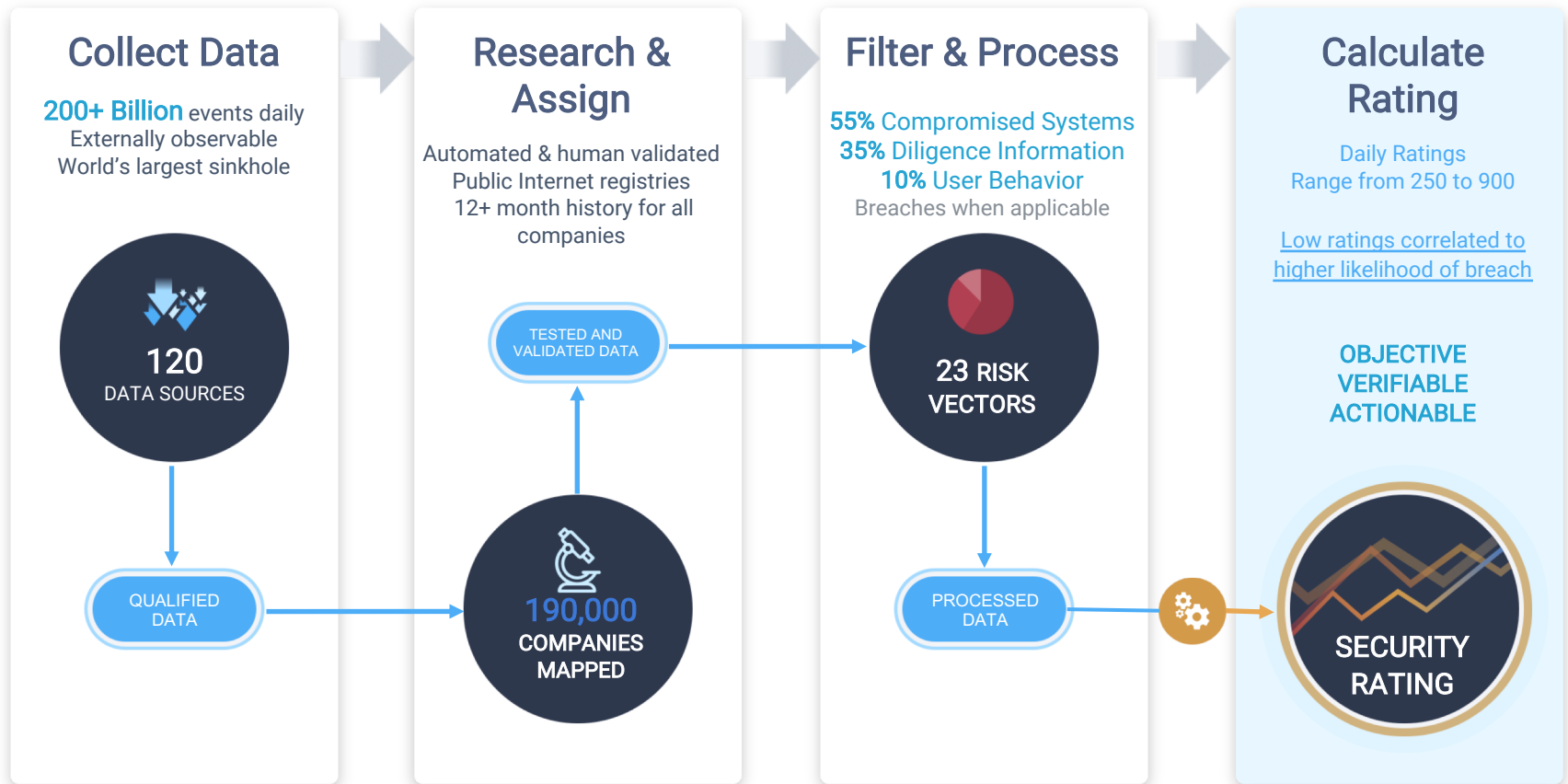
Objective, Verifiable/Actionable, Continuous, Data-Driven Ratings of Organizational Security Performance



250 - 900

- *Unbiased common* metric to measure cybersecurity performance of organizations worldwide
- SaaS solution, ratings updated *daily*

Hoe (BitSight) Security Ratings tot stand komen



Indicatie van Security Performance/Risk

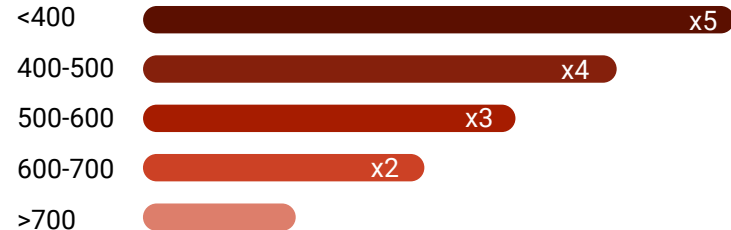


BitSight provides a measurable range of risk and is the only ratings solution with a third party verified correlation to breaches.

Likelihood of suffering a data breach

5x

If the security rating drops below 400 as compared to an organization with a 700 or higher



3x

If 50% of computers run outdated Operating System versions

2x

If the Botnet Grade is **B or lower** or the File Sharing grade is **B or lower** or the Open Ports grade is **F**

*[AIR Worldwide](#) reviewed and approved our data and analyses [Likelihood of a Significant Breach](#)

** [A Growing Risk Ignored: Critical Updates](#)

*** Beware the Botnets: [Botnets correlated to a higher](#)

Toepassingsgebieden IT Risk Ratings

How secure is my organization?



SECURITY PERFORMANCE
MANAGEMENT

- Assess cyber risk and compare to industry and peers
- Efficiently allocate resources to address cyber risks
- Set, track, report on program performance over time

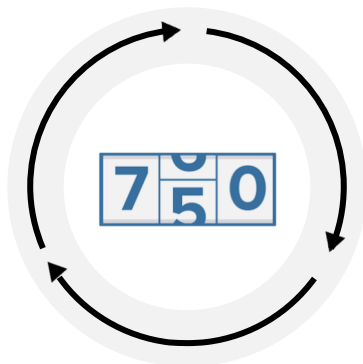
How secure are my third parties?

THIRD PARTY
RISK MANAGEMENT



- Make cyber risk decisions at the speed of the business
- See where the cyber risk is across the supply chain
- Prioritize resources to focus on riskiest vendors
- Team up with vendors to remediate cyber risk

BITSIGHT®



Cyber Insurance

Critical National Infrastructure

Mergers &
Acquisitions

Wie is BitSight

PARTICIPANTS

CUSTOMERS - 2,100 TOTAL

2,100
CUSTOMERS

50+ Gov
orgs

100+
PARTNERS



BITSIGHT
CUSTOMER

ACTIONS



5,500+

EVAs Sent in the
Last 12 Months



2,400+

Self-Published
Ratings



130,000+

Pieces of User
Generated
Content

OUTCOMES

Vendors
familiar with
ratings for
better
collaboration

Gain insights
from your
vendors to
better
prioritize
follow up
action

Add context to
communicate
your security
posture with
customers,
regulators,
insurers

Prioritize
issues with
more **context**

A background image showing a business meeting with people in a white office setting. Overlaid on this is a thick, multi-colored line graph that starts at the bottom left and trends upwards to the top right. The line is composed of several segments in shades of red, orange, yellow, and blue, ending in a solid blue circle.

BITSIGHT[®]

Governance: Fair and Accurate Security Ratings

www.bitsighttech.com

Security Ratings Principles

- Transparency
- Dispute, Correction & Appeal
- Accuracy and Validation
- Model Governance
- Independence
- Confidentiality



U.S. Chamber of Commerce

- **Appointed Ombudsman for independent dispute resolution**
 - <https://www.bitsighttech.com/press-releases/bitsight-announces-michael-cusumano-ombudsman>

Transparantie– Mag ik mijn assets verwijderen?

- All ratings are carried out consistently against the BitSight curated entity map associated with **EVIDENCE**.
- In the same manner as credit ratings – **the source record must be rectified** before BitSight can act
- BitSight allows creation of custom entities to facilitate more contextualized understanding of risk, **HOWEVER** such entities are clearly delineated.



SELF PUBLISHED

★ **Saperix Corporate**

Technology saperix.com



Private

Saperix Service Provider

Technology saperix.com

A background image showing a business meeting with several people in professional attire. In the foreground, a stylized line graph rises from the bottom left towards the top right. The graph is composed of three segments: a red segment, an orange segment, and a dark blue segment. The word "BITSIGHT" is overlaid on the graph in a bold, blue, sans-serif font.

BITSIGHT[®]

BitSight for Third-Party Risk Management

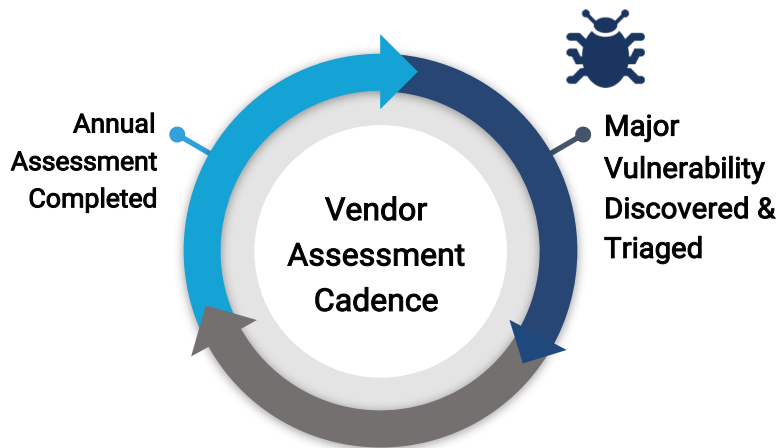
Toegevoegde waarde in contrast met huidige aanpak

Existing Processes

 Questionnaires

 Onsite assessments

 Penetration tests



No visibility on impact or potential risk until next assessment

"I know all the risk based on what my vendors tell me"

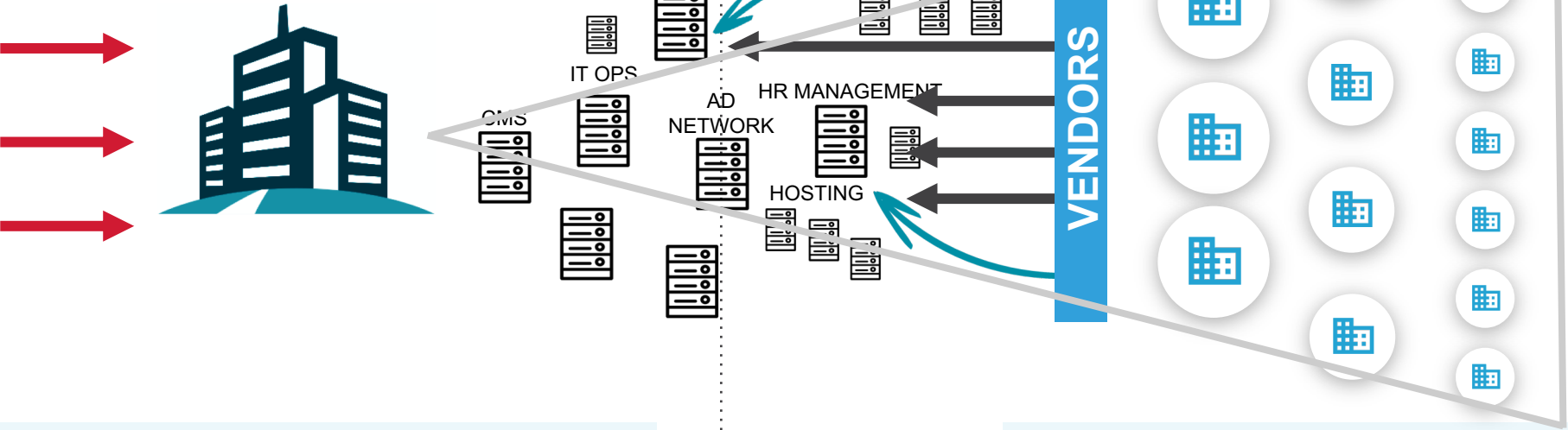
"A single point-in-time view of risk is good enough"

"I only need to focus on my top tier vendors - the others don't matter"

Current processes are valuable efforts to understand third party cyber risk but are not continuous, scalable, and staying ahead of this dynamic risk

Your Organization and Your Data

Your Extended Ecosystem



39% of breaches are caused by direct*

61% of breaches are caused by third parties*

95%

Resources
People
Budget

Limited

Resources
People
Budget

Manage Third-Party Risk with Confidence

IT Ratings give you the confidence to make faster, more strategic cyber risk management decisions.

VISIBILITY

See the cyber risk across your supply chain to avoid “blind spots”



PRIORITIZATION

Target your resources towards achieving significant, measurable cyber risk reduction



COLLABORATION

Team up with your vendors and BitSight to quickly and collectively reduce cyber risk



With BitSight you can quickly launch, grow, or optimize your TPRM program with the resources you have today.

BitSight for TPRM



Inzicht


Prioriteren

Samenwerken

DRILL DOWN ON CRITICAL RISKS

Compromised Systems	Diligence
Botnet Infections	SPF Domains
Spam Propagation	DKIM Records
Malware Servers	TLS/Ssl, Certificates
Unscheduled Communications	TLS/Ssl, Configurations
Potentially Exploited	Open Ports
	Web Application Headers
User Behavior	
File Sharing	Insecure Systems
Exposed Credentials*	Server Software
	Desktop Software
Public Disclosures	
Breaches	Mobile Application Security*
Other Disclosures*	Domain Squatting**

CUSTOMIZE ALERTS

 790 → 640 (-18%)

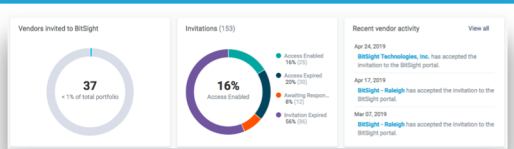
FOCUS ON THE RISKIEST ISSUES



TARGET RESOURCES



COMMUNICATE PROACTIVELY



TAKE ACTION BASED ON CONTEXT



A background image showing a business meeting with several people in professional attire. In the foreground, a stylized line graph is overlaid, starting from the bottom left and trending upwards to the top right. The graph is composed of several segments in different colors: red, orange, yellow, and dark blue. The word "BITSIGHT" is written in a bold, blue, sans-serif font across the middle of the image, partially overlapping the graph and the background scene.

BITSIGHT[®]

Geef vendoren inzicht in hun eigen performance

www.bitsighttech.com

Risk rating: 12 maanden performance

BitSight Security Rating

490 BASIC

[About](#)

[View Ratings Tree](#)

Company Info

[Set Custom ID](#)

Industry: **Food Production**

Homepage:

Monitored by **3 companies**

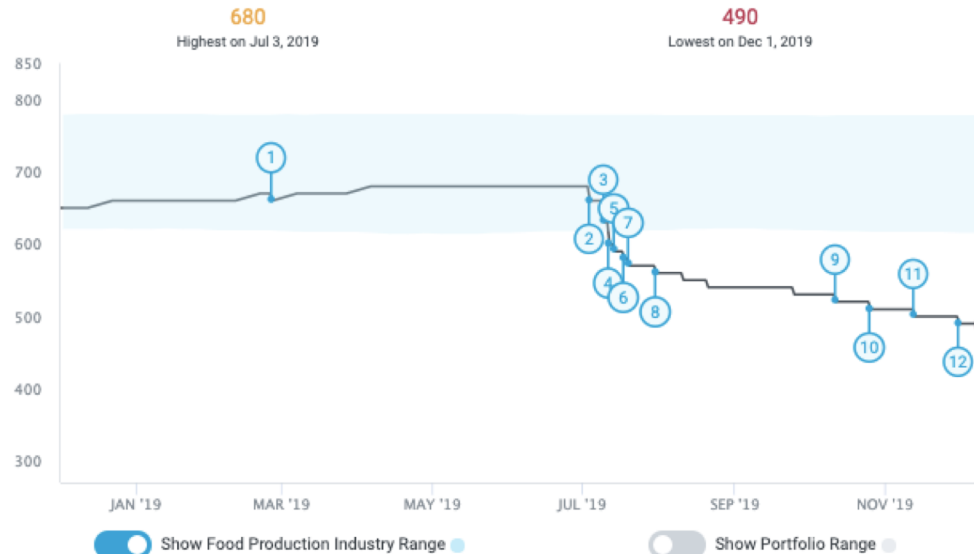
Subscription: **Continuous Monitoring**

Switch

Tier:

[Show Details](#)

Security Ratings



Highlights

[Export](#)

- 12** Dec 1, 2019
10 point drop (500 ↘ 490)
Desktop Software: grade change from C to D.
Mobile Software: minor change, grade remains F.
- 11** Nov 13, 2019
10 point drop (510 ↘ 500)
File Sharing: minor change, grade remains C.
Open Ports: minor change, grade remains F.
- 10** Oct 26, 2019
10 point drop (520 ↘ 510)
Desktop Software: grade change from C to D.
- 9** Oct 12, 2019
10 point drop (530 ↘ 520)

Brede dekking met risico indicatoren

Rating Overview

Rating Overview Panel shows how well this company is managing each risk vector. Click on a risk vector to see more details about the risk.

Compromised Systems

Botnet Infections	F
Spam Propagation	C
Malware Servers	C
Unsolicited Communications	F
Potentially Exploited	D

User Behavior

File Sharing	A
Exposed Credentials**	N/A

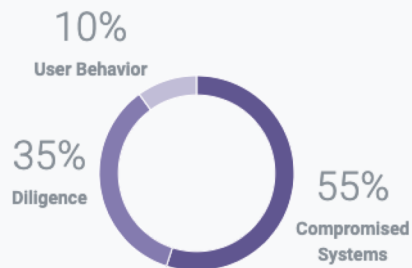
Public Disclosures

Breaches	A
Other Disclosures*	N/A

Diligence

SPF Domains	A
DKIM Records	C
TLS/SSL Certificates	D
TLS/SSL Configurations	F
Open Ports	F
Web Application Headers	C
Patching Cadence	D
Insecure Systems	F
Server Software	D
Desktop Software	F
Mobile Software	F
DNSSEC*	C
Mobile Application Security*	N/A
Domain Squatting**	N/A

What Makes A Security Rating?



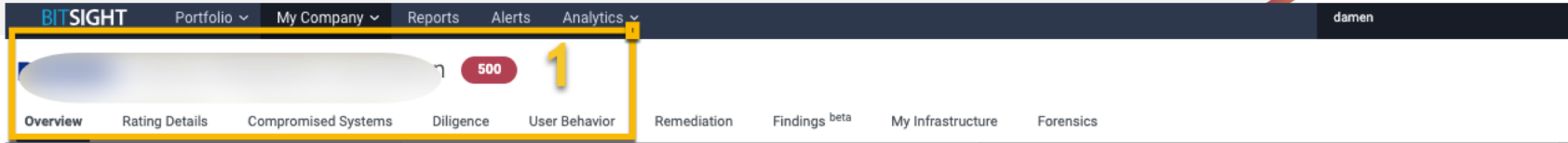
The grades show how well this company is managing each risk vector. These grades do not contribute evenly to a company's overall BitSight Security Rating.

Breaches have a negative impact on Security Ratings **only if they occur**.

[Learn more about how ratings are calculated.](#)

[Learn more about every risk vector.](#)

Maakt thema security inzichtelijk en begrijpelijk



Verbindt

Board/Stakeholders (1)

intuïtieve rating, trend & benchmark, met

Risk/Ciso (2), 23 indicators of security performance/risk met:

SecOps (3), objective & actionable data inzetbaar voor remediation

2

The 'Rating Overview' panel provides a summary of the company's security posture. It includes a 'Rating Overview Panel' description and a table of risk indicators. The indicators are categorized into 'Compromised Systems', 'Diligence', 'User Behavior', and 'Public Disclosures'. Each indicator has a corresponding grade (A, B, C, D, F, N/A) and a brief description.

Category	Indicator	Grade
Compromised Systems	Botnet Infections	F
	Spam Propagation	F
	Malware Servers	A
	Unsolicited Communications	A
	Potentially Exploited	D
Diligence	SPF Domains	A
	DKIM Records	C
	TLS/SSL Certificates	C
	TLS/SSL Configurations	F
	Open Ports	C
User Behavior	File Sharing	D
	Exposed Credentials**	N/A
	Breaches	A
	Other Disclosures*	N/A
Public Disclosures	Server Software	
	Desktop Software	
	Mobile Software	
	DNSSEC*	
	Domain Squatting	

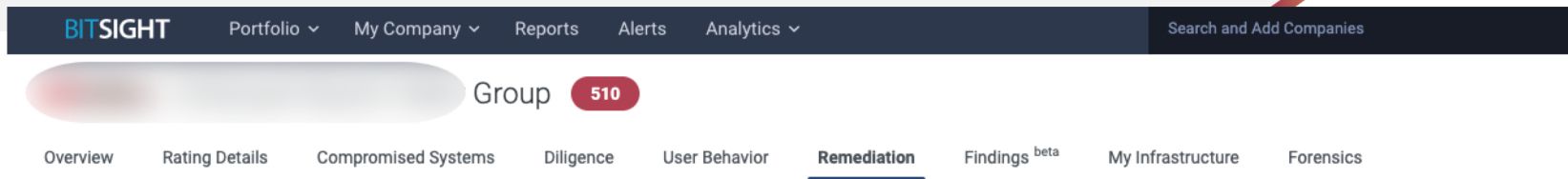
The 'Open Ports' panel displays the current grade (C) and the number of records (165). It also indicates that the company is in the top 50% of all companies. Below this, there is a breakdown of records by grade: 101 Good, 0 Fair, 52 Neutral, 8 Warn, and 4 Bad. A description explains that open ports are necessary for business functions but can be exploited by attackers.

3

The remediation table lists specific security issues, their risk vectors, and grades. It includes columns for 'Risk Vector', 'Grade', and 'Details'. The table is filtered to show only items that impact the grade.

Risk Vector	Grade	Details
SSL Certificates	BAD	Expired certificate, Self-signed certificate
SPF	BAD	SPF record is ineffective
Web Application Headers	BAD	HTTPS redirect to HTTP
SSL Certificates	BAD	Expired certificate
SSL Configurations	BAD	Allows insecure protocol: TLSv1.0, Allows insecure protocol: TLSv1.1, Diffie-Hellman prime is less than 2048 bits, Short Diffie-Hellman prime is very commonly used

Als een organisatie in de Rating-Spiegel kijkt?



Veel waardevolle usecases:

Prioritiseren remediation & resources

root cause **analysis** for trends & process verbetering

Schept **transparantie** daar waar de organisatie die normaliter niet heeft

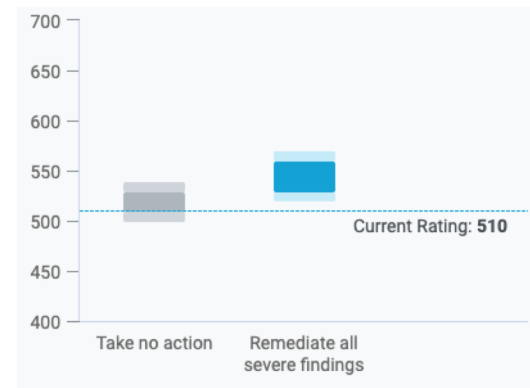
Remediation Overview

[Download Remediation Data](#)

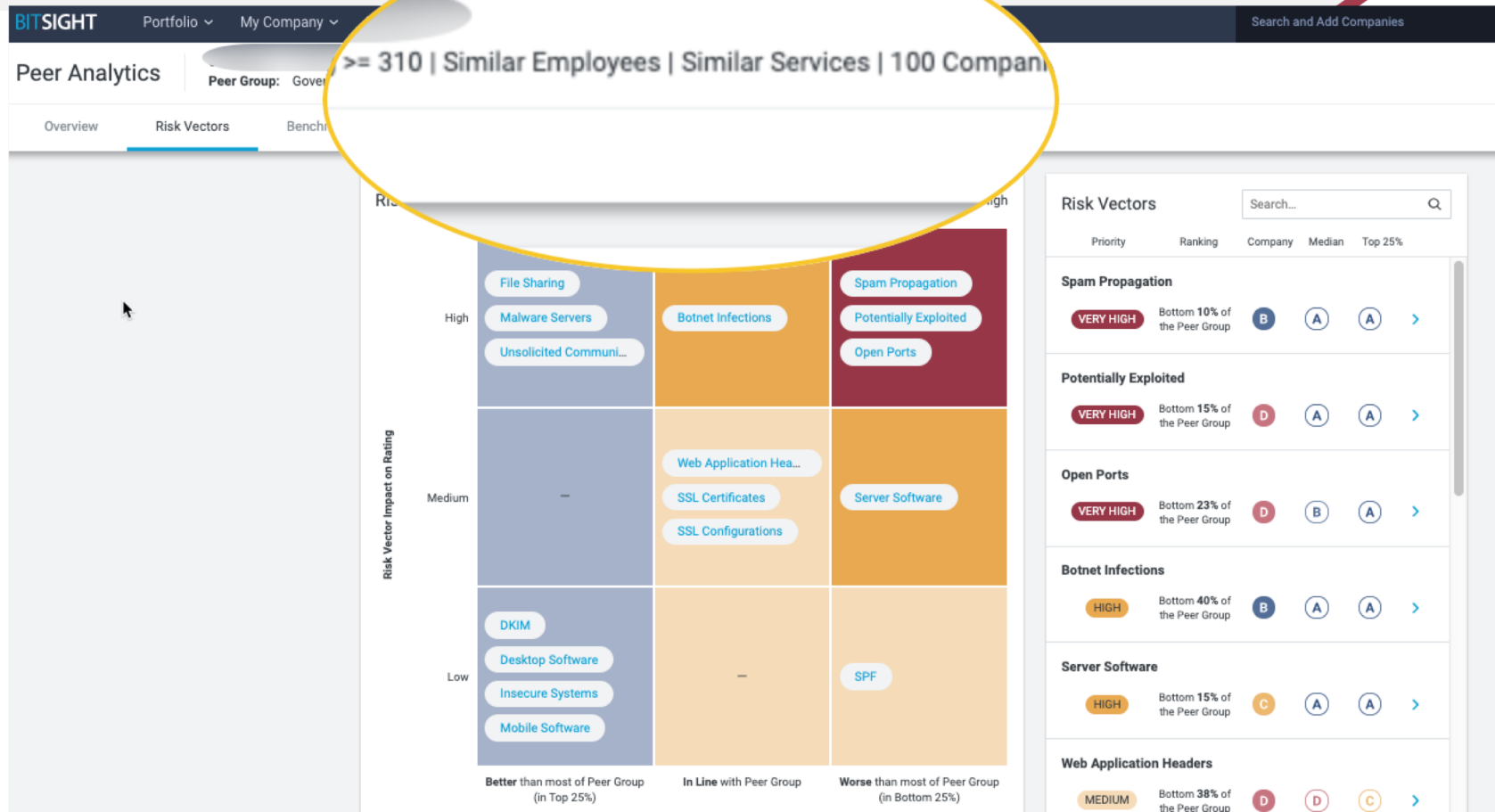


Remediation Forecasts

View how remediation efforts will impact your rating in the future using **Forecasts**. This shows your rating forecast range in three months, based on taking action today. [Generate this forecast](#).



Benchmark met 100 organisaties zoals u



Schept **transparentie** in prestaties van onderdelen van de organisatie



BITSIGHT Portfolio ▾ My Company ▾ Reports Alerts Analytics ▾ Search and Add Companies 🔍 939 ? ⚙️

Enterprise Performance

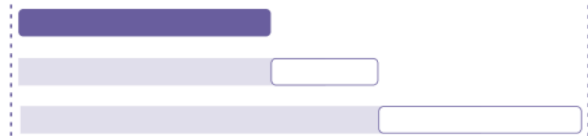
As of Jan 14, 2020

Lens BitSight Rating ▾ Time Period 6 Months ▾ Sort by Performance - Worst to Best ▾

	Current	Jan 2020	Dec 2019	Nov 2019	Oct 2019	Sep 2019	Aug 2019
	500	500	500	510	510	510	520
	400	410	410	420	430	430	430
	680	680	680	680	680	680	680
	740	740	740	740	740	740	740
	760	760	760	730	720	720	720

Basic < 410 420 - 520 530 - 630 Intermediate 640 - 670 680 - 700 710 - 730 Advanced 740 - 760 770 - 790 > 800

[View Ratings Tree](#)



View Your Impact Analysis →

Improve your company rating faster by analyzing which subsidiary issues are having the biggest impact.

Verbeter meetbaar de organisatie op basis van data en transparantie



BITSIGHT

Portfolio

My Company

Reports

Alerts

Analytics

Working: Paulo Gonias

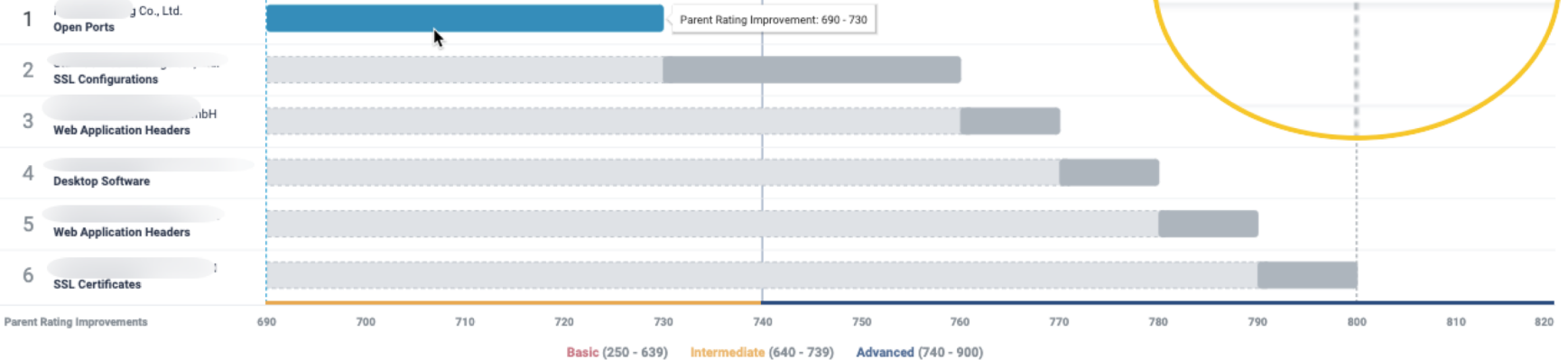


Impact Analysis

maximize parent company rating impact.

Projected Parent Rating: 800

Step Current Parent Rating: 690



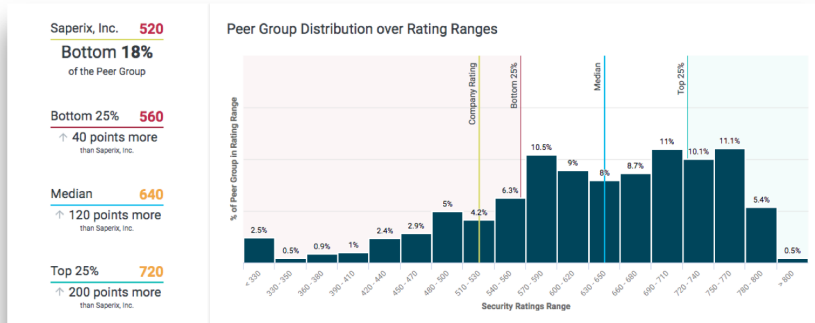
Veracode Highlights Their Own Security Posture as a Competitive Differentiator

THE CHALLENGE

Communicating complex cybersecurity topics to the company's board of directors, partners, prospective customers, and trusted advisors.

THE SOLUTION

BitSight Security Ratings for SPM



VERACODE



Being able to show our board, leaders, and even customers and partners how Veracode is performing over time and relative to others in our space is a powerful tool for communicating our commitment to security excellence, and has also become a terrific competitive differentiator.

— **Bill Brown**
(Former) CIO & CISO

Measurable Results from Security Performance Management

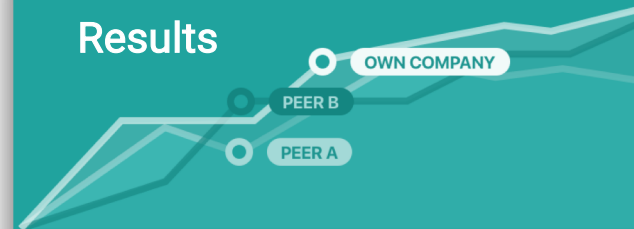
13

Clear, concise communication to Board on performance against 13 competitors/industry peers

31

Continuous monitoring of 31 subsidiaries

Results



Customer is better able to differentiate against competition

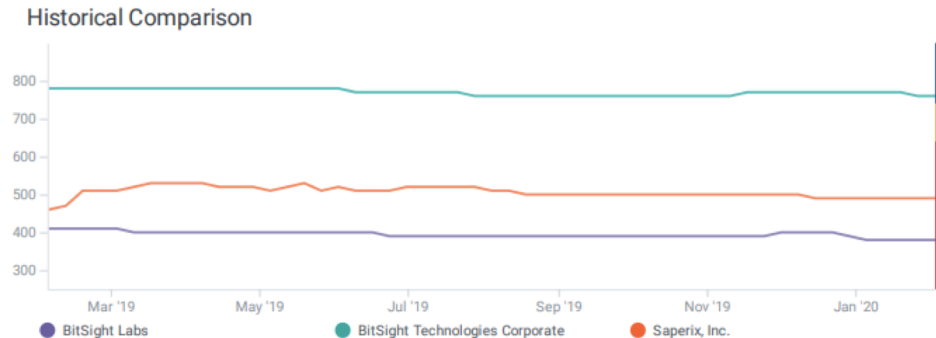
Standard metric is used to report to audit committee, Board and other key executives

Subsidiaries now compete amongst themselves

Onboarden van nieuwe vendoren

Compare **new vendors** on security
risk,

use in depth data to **enhance** and
speed up current **vendor**
onboarding risk assesment



Current Comparison

BITSIGHT

BitSight Labs

BITSIGHT

BitSight Technologies Corporate



Saperix, Inc.

Security Rating
February 03, 2020

380

Basic

760

Advanced

490

Basic

Compromised Systems

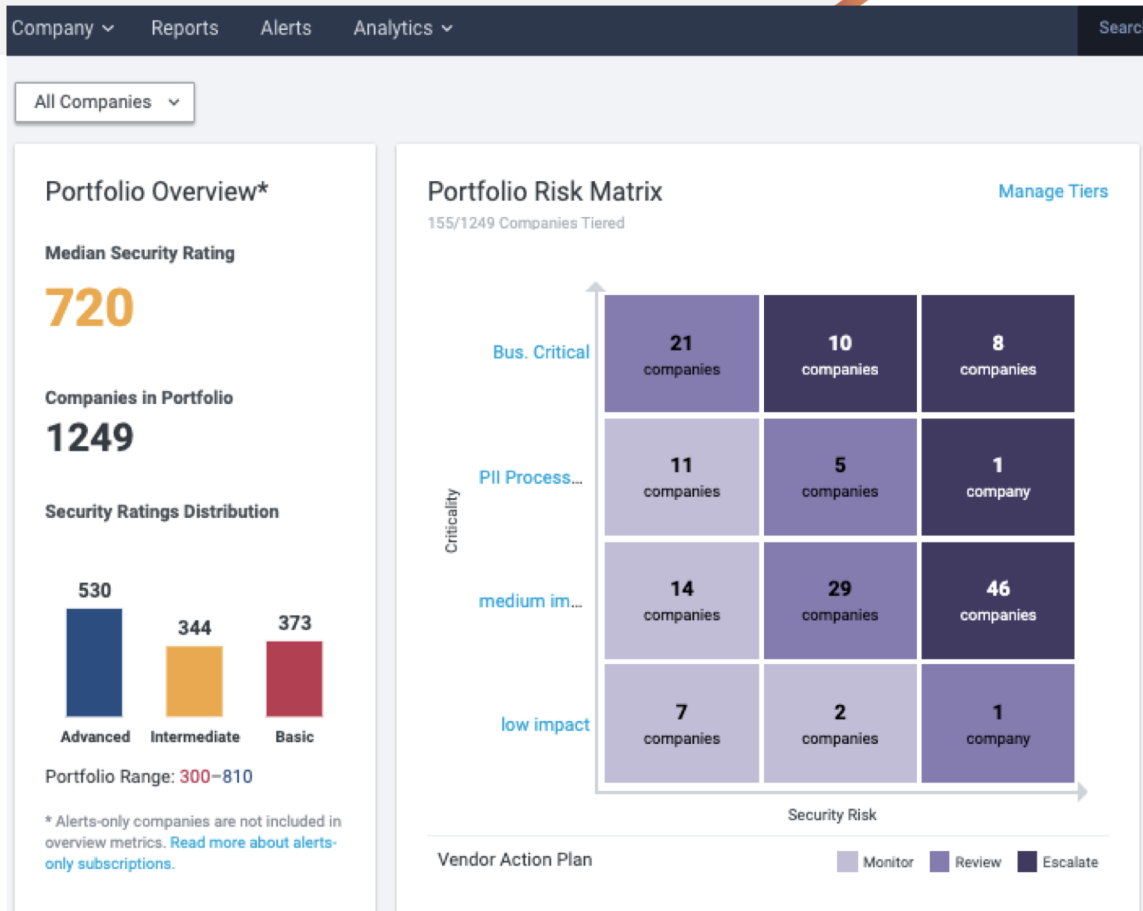
Botnet Infections	F	A	F
Spam Propagation	C	A	B
Malware Servers	C	A	A
Unsolicited Communications	F	A	A
Potentially Exploited	D	A	C

TPRM Risk Oversight at scale

Create real time security risk oversight at scale to:

Manage by exception

Collaborate with vendors to manage risk and improve their security posture



Manage by Exception – ongoing monitoring

The screenshot shows the BitSight interface for a 'Bus. Critical' portfolio. It features a 'Vendor Action Plan' section with 'Monitor' and 'Review' tabs, and a 'Portfolio Quality' section with a bar chart showing risk distribution across tiers. A 'Filters' sidebar on the left lists 39 companies with various attributes like Folder, Subscription Type, Rating Type, Industry, Country, Rating Category, and Vendor Action Plan. The main content area displays a table of companies, including ACTIAM NV, Boston Partners Global Investors, Inc., Brunel Czech Republic, and BUX Technology BV.

Manage by exception:
Create flexible security alerts to follow up when risk in the supply chain needs action

Select Risk Vectors

20 Results

Select All

- Botnet Infections
Compromised Systems
- Spam Propagation
Compromised Systems
- Malware Servers
Compromised Systems
- Unsolicited Communications
Compromised Systems
- Potentially Exploited
Compromised Systems
- SPF
Diligence
- DKIM
Diligence
- SSL Certificates
Diligence
- SSL Configurations
Diligence
- Open Ports
Diligence
- Web Application Headers
Diligence
- Patching Cadence
Diligence
- File Sharing
User Behavior

Cancel

Done

Bus. Critical

Alert Preferences

Receive alerts via email

Receive alerts for

Percent Change

When ratings change by a set percentage

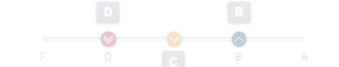
10% 5% 5%

Thresholds

When ratings reach or cross a set threshold

Risk Vector Grades

When grades reach or cross a set threshold



Selected risk vectors (16)

Botnet Infections, Spam Propagation, Unsolicited Communications, Potentially Exploited, SPF [show 11 more](#)

NIST CSF Grades

When NIST CSF grades reach or cross a set threshold

Informational Risk Vectors

When new information is available for an informational risk vector

Cancel

Save Changes

Samenwerking

The screenshot displays the BitSight interface for the company Blohm+Voss B.V. & Co. KG, which has a current rating of 490. The interface includes a navigation bar with options like Portfolio, My Company, Reports, Alerts, and Analytics. A search bar is located in the top right corner. Below the navigation, there are tabs for Overview, Rating Details, Compromised Systems, Diligence, User Behavior, Remediation, Findings, and My Infrastructure. The main content area is titled 'Invite this Vendor to the BitSight platform' and contains a form with fields for Contact Email, Contact Name / Alias, CC own organization (optional), Contact Phone Number (optional), and a message for the vendor. A tip box suggests sharing records from Compromised Systems, Diligence, User Behavior, or Alerts details to make the invitation more actionable. To the right of the form is a rating history chart showing a score of 490 as of Jan 6, 2020, with a lowest score of 490 on Jan 6, 2020. The chart shows a series of points from 11 to 17, with a significant drop from 580 to 560 on Nov 21, 2019, and another drop from 550 to 490 on Jan 6, 2020. A 'Highlights' section on the right lists key events, including a 20-point drop from 580 to 560 on Nov 21, 2019, and a 10-point drop from 550 to 490 on Jan 6, 2020, both attributed to Botnet Infection: Cooee (1). A yellow arrow points from the 'Vendor Access' button in the top right to the 'Invite this Vendor to the BitSight platform' form.

Invite this Vendor to the BitSight platform

Here's a tip...

Share one or more records from Compromised Systems, Diligence, User Behavior, or Alerts details to make your invitation more actionable.

They will have complete platform access for **Blohm+Voss B.V. & Co. KG**, and will be able to see all IP address, Compromised System, and Diligence information including advanced details provided by the Compromised System Forensics and User Behavior Forensics add-ons.

Enter vendor contact details in the form below to enable temporary access to the BitSight Security Ratings platform for **Blohm+Voss B.V. & Co. KG**.

Contact Email

Contact Name / Alias

CC own organization (optional)

Contact Phone Number (optional)

Message for Blohm+Voss B.V. & Co. KG (optional)

490
Lowest on Jan 6, 2020

Highlights Export

- Jan 6, 2020 ↔
10 point drop (500 ↘ 490)
Patching Cadence: minor change, grade remains C.
- Nov 27, 2019 ↔
10 point drop (550 ↘ 540)
Botnet Infection: Cooee (1)
- Nov 25, 2019 ↔
10 point drop (560 ↘ 550)
Botnet Infection: Cooee (1)
- Nov 21, 2019 ↔
20 point drop (580 ↘ 560)
Botnet Infection: Cooee (1)
- Nov 19, 2019 ↔

Invite Vendor to get 20 days of access to their BitSight rating and all functionality to discuss:

1: is this risk impacting our security or business continuity

2: if yes – how fast can you remediate

3: how can you structurally improve?

hunt (recent) risk in supply chain

Apply all risk vectors and data as filter to hunt (recent) risks in supply chain and contact those vendors when applicable

The screenshot displays the BITSIGHT interface for a vulnerability hunt. The top navigation bar includes 'BITSIGHT', 'Portfolio', 'My Company', 'Reports', 'Alerts', 'Analytics', and a search bar. Below the navigation, the main area shows 'All Companies' with a search filter and a list of filters including Tier, Folder, Subscription Type, Rating Type, Industry, Country, Rating Category, Vendor Action Plan, Risk Vector Grade, Infection, Vulnerability (with 'Clear (1)'), Open Port, Software, Security Risk, and Service Provider.

The main table displays search results with columns for Company, Trend, and Security Rating. A filter 'CVE-2019-19781' is applied. The table shows a result for MAERSK with a Security Rating of 1.

A 'Vulnerability' modal window is open on the right, showing '1 Result' for CVE-2019-19781. The modal includes a search bar with 'CVE-2019-19781' and a 'Deselect All' button. A list of other vulnerabilities is shown with their counts in circles: CVE-2010-1899 (553), CVE-2017-7679 (552), CVE-2010-1256 (551), CVE-2016-8612 (549), CVE-2016-4975 (536), CVE-2010-2730 (527), CVE-2010-3972 (527), CVE-2012-2531 (527), CVE-2012-2532 (527), CVE-2015-9251 (518), DROWN (511), CVE-2019-0220 (502), CVE-2018-17199 (498), CVE-2017-15710 (491), CVE-2017-15715 (491), and CVE-2018-1283 (491). The modal has 'Cancel' and 'Done' buttons.

Filters used: CVE-2019-19781 Clear all filters

Company	Trend	Security Rating
<input type="checkbox"/> MAERSK		1

Vulnerability

1 Result Deselect All

CVE-2019-19781

CVE-2019-19781 139

- CVE-2010-1899 553
- CVE-2017-7679 552
- CVE-2010-1256 551
- CVE-2016-8612 549
- CVE-2016-4975 536
- CVE-2010-2730 527
- CVE-2010-3972 527
- CVE-2012-2531 527
- CVE-2012-2532 527
- CVE-2015-9251 518
- DROWN 511
- CVE-2019-0220 502
- CVE-2018-17199 498
- CVE-2017-15710 491
- CVE-2017-15715 491
- CVE-2018-1283 491

Cancel Done

Cabela's Gains Efficiency in Vendor Assessments

THE CHALLENGE

Achieving scale with vendor assessments and keeping up with the speed of the business to manage third party risk

THE SOLUTION

BitSight Security Ratings for TPRM



Cabela's®

“

It used to take weeks to complete security assessments. Now it takes us hours. BitSight Security Ratings facilitate security discussions with potential vendors. It's an integral part of our vendor risk management program.

Michael Christian

Information Security Manager
of Risk & Compliance

Third Party Monitoring Produces Measurable Results at Scale for



Goal: Monitor the information security disposition of critical third party service providers

Actions by BitSight



Monitor thousands of third parties

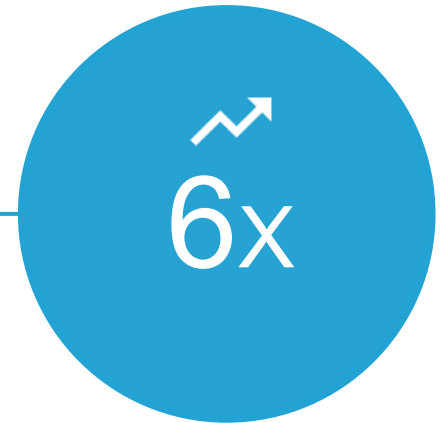


Evaluate risk rating for each provider



Determine risk areas for action

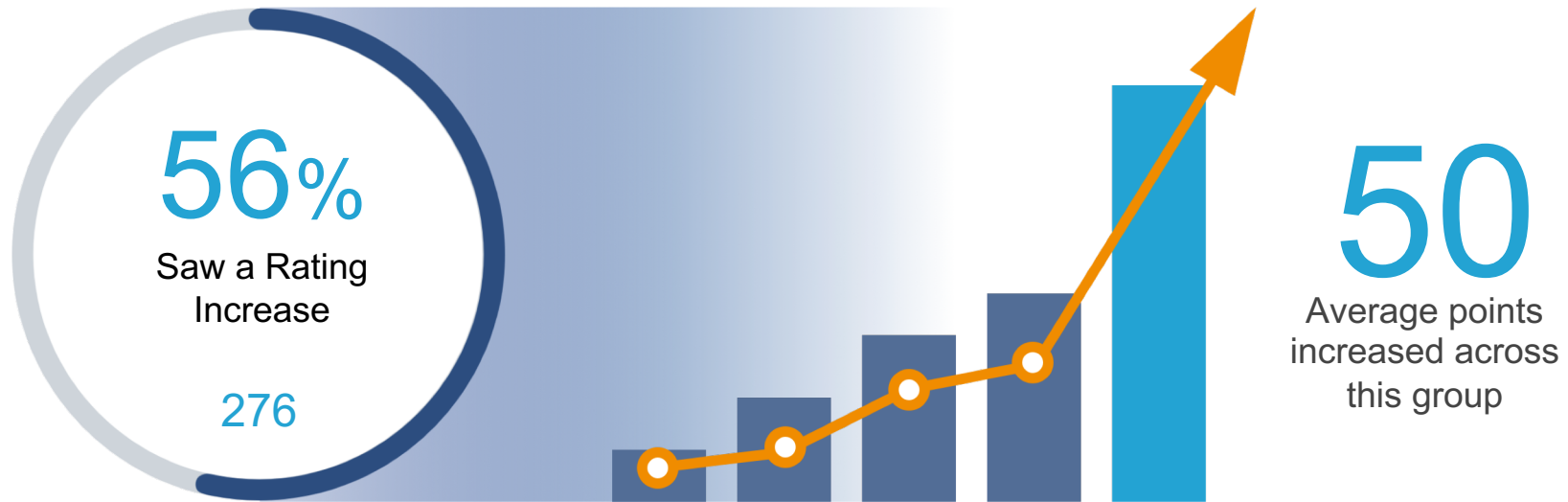
Results



Third party expansion coverage
with same FT employees

Impactful Results from Vendor Collaboration

Onboarded **496** suppliers and engaged with BitSight Security Ratings as part of this process



*Suppliers on-boarded between May 1st and October 31. Ratings compared between May 1st and Dec 4th

Leading Organizations Use BitSight

20%

of Fortune 500
companies use
BitSight

4

of the top 5 Investment
Banks use BitSight for
Vendor Risk
Management

40+

government agencies,
including US and Global
Financial Regulators,
use BitSight

4

of the Big 4
Accounting Firms
use BitSight

50%

of the world's cyber
insurance premiums
are underwritten by
BitSight customers

GLOBAL, BLUE CHIP CUSTOMER BASE

MS&AD
INSURANCE GROUP

HITACHI

 **BNP PARIBAS**

 **STERIS**
Healthcare

 **HAECO**

HCL

VERACODE

 **AIRPORT
AUTHORITY
HONG KONG**

 **TransUnion**

MIZUHO

SHISEIDO

 **CHART**

 **pwc**

Cabela's

 **Colonial Pipeline Company**