bsi. International Cyber Resilience Exchange 2019

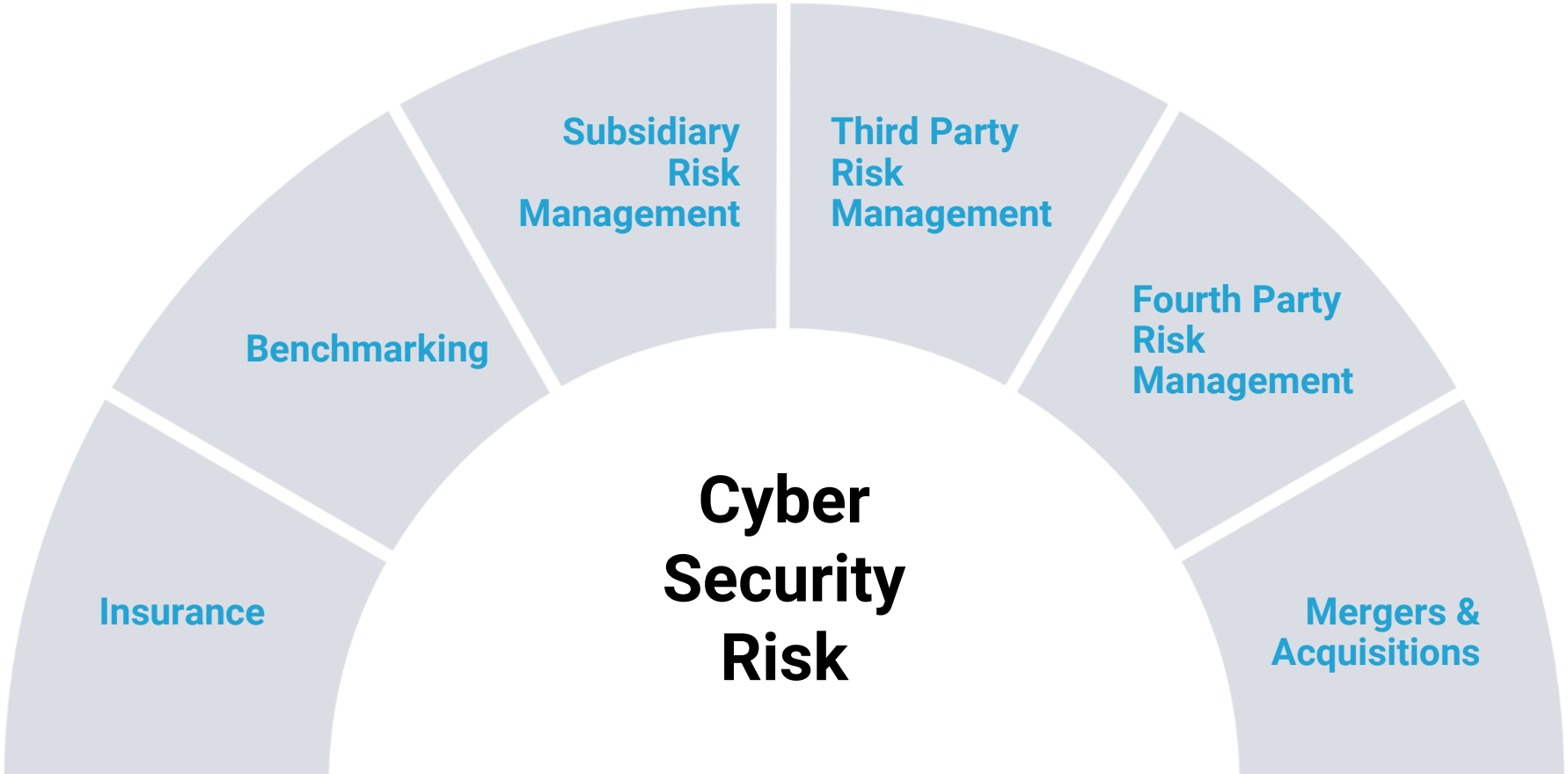
BITSIGHT®

BitSight Security Ratings

BITSIGHT®

Trends

Increasing governance and assurance required



Cyber Risk is Increasing

CYBER INCIDENTS CONTINUE TO INCREASE

- Volume (# of attacks)
- Speed of attacker
- Sophistication of attacker

THE TARGETS ARE BROAD

- 1st party
- 3rd party
- Nth party

THE DAMAGE IS SEVERE

- Financial loss
- Reputational harm
- Legal liability
- Operational disruption

Market Conditions

BOARD EXPECTATIONS

100% of organizations will report to the board on cyber risk at least 1x / year, by 2020

91% of board members can't interpret cybersecurity reports

REGULATORY ENVIRONMENT

Oversight Continues to Increase

GDPR	FFEIC	HK CFI
DFAR	NY DFS	NIST

BUSINESS IMPACT

181 vendors granted access to a company's network per week

63% of all breaches linked directly or indirectly to 3rd parties

MARKET IMPACT

$100B will be spent in 2020 on information security worldwide

$10B in estimated cybersecurity insurance premiums by 2020

$2T cyber crime costs by 2020

The power of objectively measuring cybersecurity performance….

What would it enable for YOU?

Key Questions

How do diverse stakeholders have a sensible conversation about Cyber Security?

- **Language** - Risk posture vs. vulnerability checklist? Impact vs. events. Non technical language
- **Consistency of measurement –** Absolute and relative, Universal Metrics Standard across a critical mass of organizations
- **Business Context –** What is in it for me? How to relate cyber security to business
- **Outcome vs activity –** Results rather than effort
- **Objective versus subjective –** Data centric but in context

BitSight brings data-driven efficiency and automation to the cyber risk evaluation process by providing a **COMMON METRIC** (ratings) to be used in a cyber risk decision framework:

The Key Questions

Who are the consumers of Cyber security information?

- **The Board**
- **Procurement**
- **Compliance**
- **Vendor Risk Management**
- **Audit**
- **Operational Risk**
- **CISO Info Sec Cyber security**
- **Business process owners**
- **Supplier Managers**
- **CIO / CRO**

Common Language

Different perspectives / context

Subject to specific risks

BitSight Security Ratings Enable Measurement

BITSIGHT

BOSTON, MA
HEADQUARTERS

450+
EMPLOYEES

$150M+
CAPITAL RAISED FROM BLUE CHIP INVESTORS

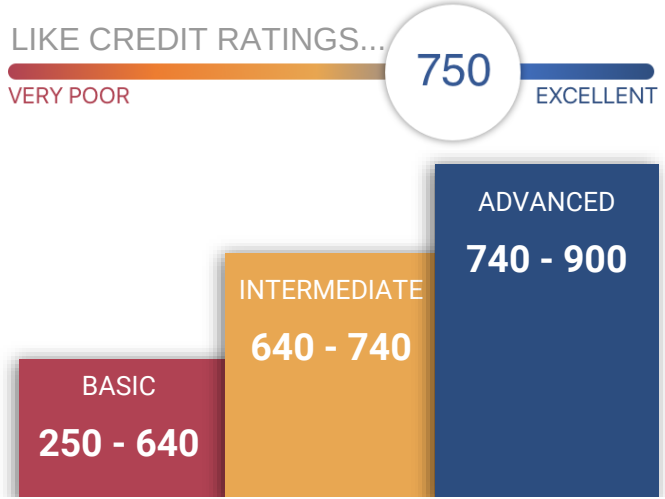
EXPERIENCED
LEADERSHIP TEAM WITH RECORD OF GROWING SUCCESSFUL COMPANIES

GLOBAL
OFFICES IN SINGAPORE, LISBON AND RALEIGH

2011
FOUNDED

BitSight Security Ratings

- Data-driven rating of security performance
- Non-intrusive SaaS platform
- Continuous monitoring
- Objective, quantitative measurement



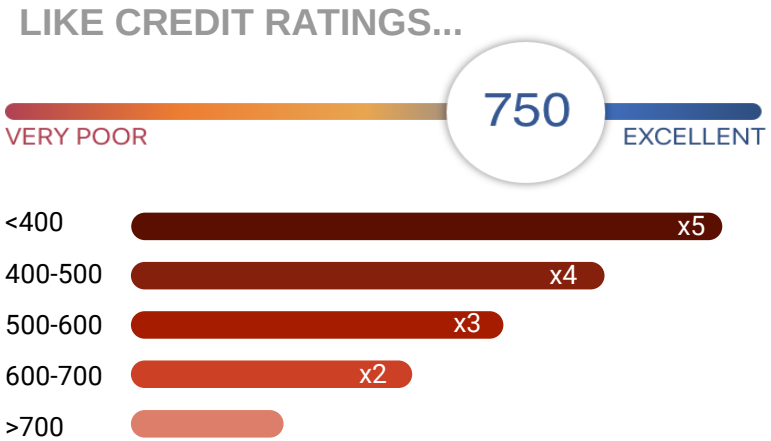
THE LARGEST, MOST ENGAGED ECOSYSTEM

1,500+	25,000+	20,000+	160,000+	105,000+	15M+
Customers Worldwide	Users	Ecosystem Comments & Tags	Monitored Organizations	Pieces of User-Generated Content	Domains

How do security ratings help?

BitSight Security Ratings:

- Provide a **measurable range of risk**
- The only ratings solution with a **third party verified correlation to breaches**.
- **Data-driven** rating of security performance
- **Non-intrusive** SaaS platform
- **Continuous monitoring with 12 month history**
- **Active Oversight AT SCALE**



Strong, Validated Correlation to 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**

Security ratings are an objective, continuous, external measure of an organization's overall cyber security posture

3 levels of information – tailored for stakeholder needs

1. Security Rating - Overall Cyber Risk posture rating

Dashboard, Management reports
'view from the bridge', trending

2 Risk Vectors – Rating for groupings of like events

Compromised Systems		Diligence	
Botnet Infections	F	SPF Domains	F
Spam Propagation	D	DKIM Records	C
Malware Servers	A	TLS/SSL Certificates	F

Risk hunting, thematic reviews,
Audit selection + scoping
Operational reports

3 Events – specific incidents or vulnerabilities

Port	Total Hosts	Grade Distribution	Service
21	2		Detected service: FTP with AUTH TLS and 1 other service
22	10		Detected service: SSH and 1 other service
23	3		Detected service: Telnet

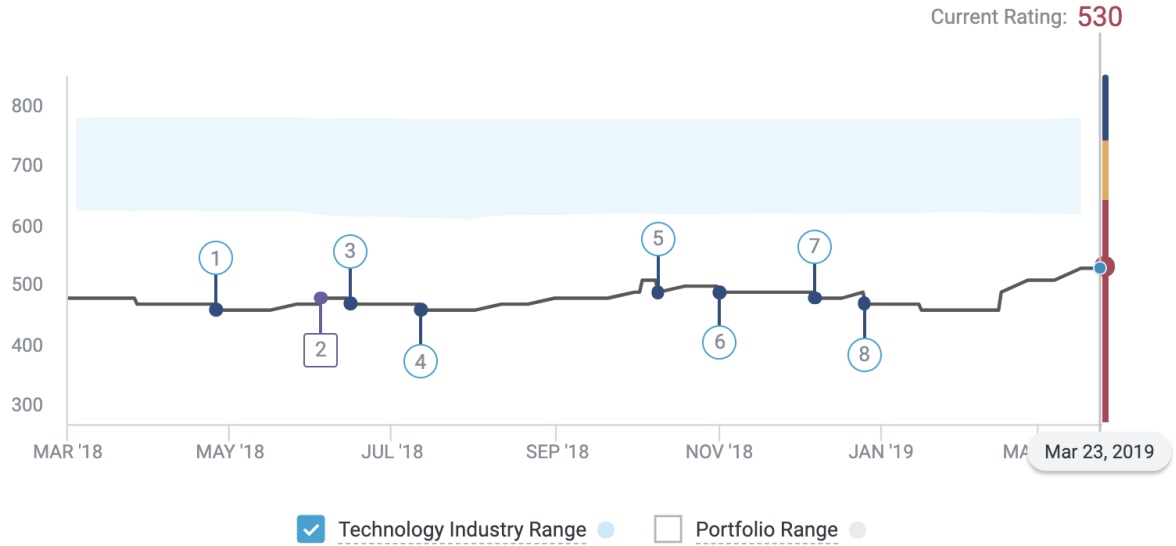
Remediation, preparation for on-site audits
Activity reports

Security Ratings

Download Data (.csv)

530
Highest, on Mar 23, 2019

460
Lowest, on Apr 26, 2018



Rating Highlights

8 Dec 26, 2018

20 point drop, from 490 to 470

Insecure System: grade change from D to B

Open Port: grade change from D to F

7 Dec 7, 2018

10 point drop, from 490 to 480

Desktop Software: grade change from C to D

File Sharing: grade change from B to C

Mobile Software: minor change, grade remains D

Open Port: minor change, grade remains F

6 Nov 1, 2018

Translating Security Data into Actionable Ratings

Security Ratings

Organizational security performance ratings ranging from **250** - **900** derived from verifiable, outside-in security data

Saperix, Inc.

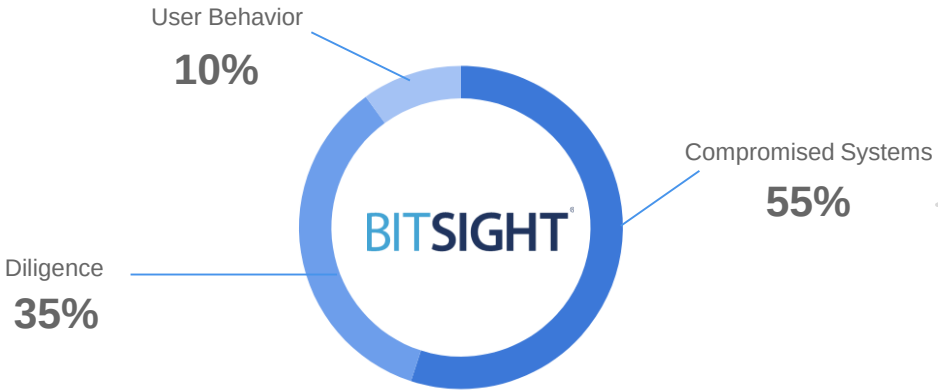
Technology • saperix.com

Monitored by **131** companies

Show details

BitSight Security Rating

720 INTERMEDIATE



Risk Vector Factors within Ratings

Compromised Systems

Botnet Infections	D
Spam Propagation	A
Malware Servers	A
Unsolicited Comm.	A
Potentially Exploited	F

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	C
Open Ports	B
Web Application Headers	C
Patching Cadence	F
Insecure Systems	A
Server Software	B
Desktop Software	D
Mobile Software	N/A
DNSSEC*	C
Mobile Application Security*	N/A
Domain Squatting **	N/A

Botnet event detail

Compromised Systems details for Saperix, Inc.

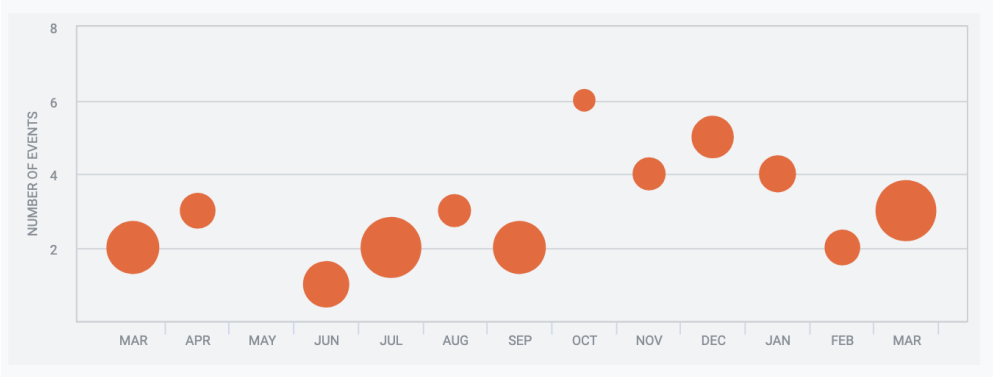
Download Data (.csv)

Graph Type

- **Distribution**
- **Duration**
- **Volume**

This graph displays the number of compromised systems events per month, broken down by type. The size of the bubbles corresponds to the average duration for those events.

Compromised Systems Details – 161 events over 12 months



Show:

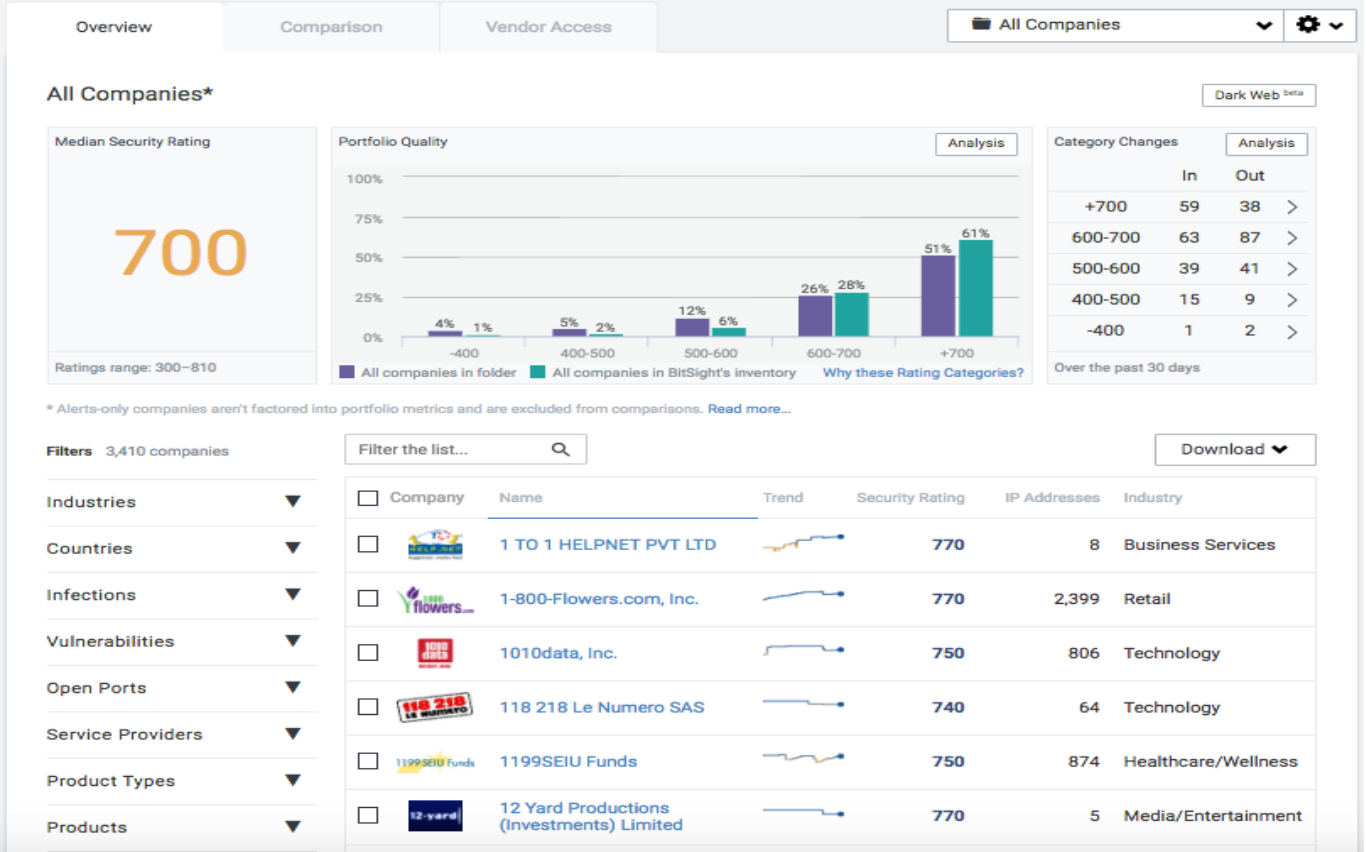
- All
- Botnet Infections — 37 events
- Spam Propagation — 1 event
- Malware Servers — 0 events
- Potentially Exploited — 123 events
- Unsolicited Communications — 0 events

Tags | Search | Show events from: MM-DD-YYYY to MM-DD-YYYY

Click infection names for remediation instructions

Type	IP Address/Domain	Location	Start	End	Days	Details	collapse all expand all
Botnet Infections Guest WiFi	45.116.217.90	TH	03-19-2019	03-22-2019	4	**Infection:** Gamarue	Details
Botnet Infections Guest WiFi	45.116.217.90	TH	02-18-2019	03-15-2019	26	**Infection:** Gamarue	Details

Measuring Performance Across a Large Portfolio



Better Data Enables Smarter Prioritization of Risk

Vendor Tiering *enables quick identification of critical vendors with issues* ***….***

… *and* ***Asset prioritization*** *provides context on the most pressing issues facing these critical vendors*

Other ratings providers cannot provide the extensive visibility of security issues (see previous slide) or business critical assets (no API, mail server, or database visibility) meaning customers **don't get the most comprehensive view of the most important issues facing their most critical vendors.**

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

1,500+ CUSTOMERS ACROSS THE GLOBE

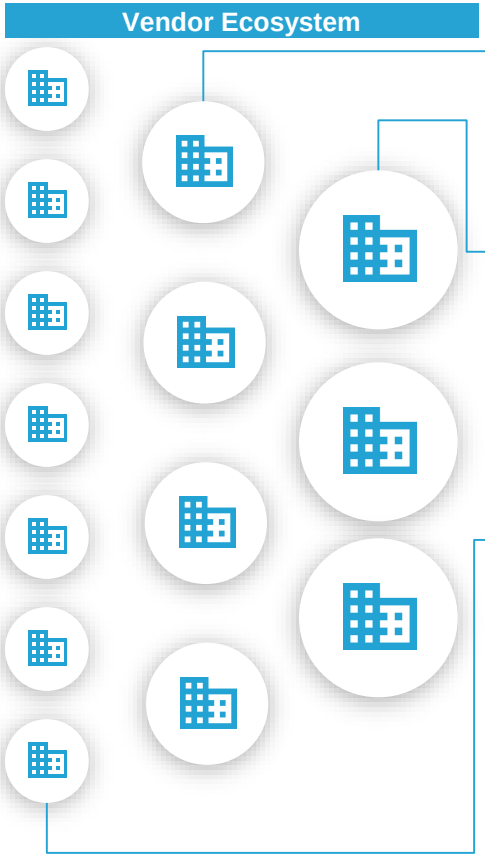
AIG · BERTELSMANN · BNP PARIBAS · FannieMae · TransUnion
E*TRADE · Starbucks · KKR · KPMG · Microsoft
CHUBB · TRAVELERS · pwc · QANTAS · Comcast

BITSIGHT®

bsi. International Cyber Resilience Exchange 2019

Third Party Risk Management

TPRM: Customer Pain Points



Tier 1 Vendors
Critical to business function with potential network access or sensitive data sharing

Tier 2 Vendors
Important vendors that may have access to network, data or company premises

Tier 3 Vendors
Long tail of vendors with less network/technology relationship

Existing processes highly focused on Tier 1 vendors

Customer

Existing Processes

Gather important data through **questionnaires** or **episodic** assessments to learn about vendors policies, procedures, controls

Send risk manager to do **onsite assessments** to verify vendor policies, procedures, controls

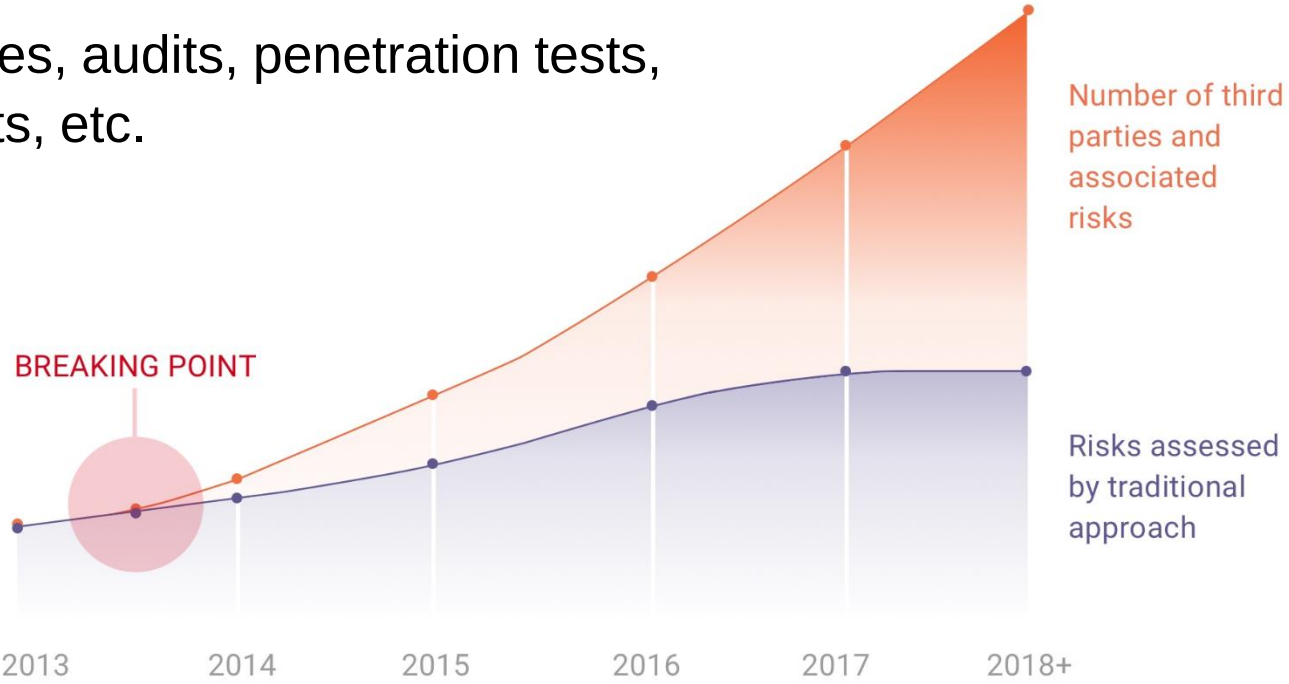
Perform **penetration tests** to get point-in-time analysis of vendor security vulnerabilities

Current processes are expensive, time consuming, and don't provide continuous visibility across an organization's entire ecosystem of vendors.

Cyber Security Challenge

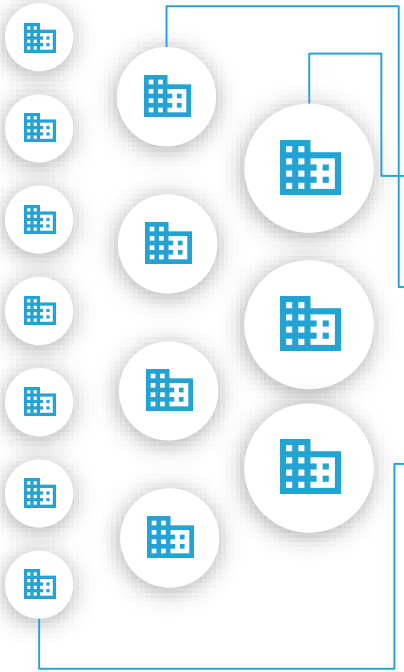
Difficult to scale traditional approaches:

Questionnaires, audits, penetration tests, manual efforts, etc.



BitSight Value in TPRM Program

Vendor Ecosystem



Tier 1 Vendors
Critical to business function with potential network access or sensitive data sharing

Tier 2 Vendors
Important vendors that may have access to network, data or company premises

Tier 3 Vendors
Long tail of vendors with less network/technology relationship

Cost-effective continuous visibility across all tiers

BITSIGHT®
The Standard in SECURITY RATINGS

- **Expand visibility** across all vendors to identify highest-risk vendors
- **Drive efficiency** and automation across existing workflows and processes
- **Prioritize action** and **allocate resources** to address dynamic risks across vendor population
- **Integrate ratings data throughout vendor lifecycle** processes including selection, onboarding, ongoing monitoring and termination

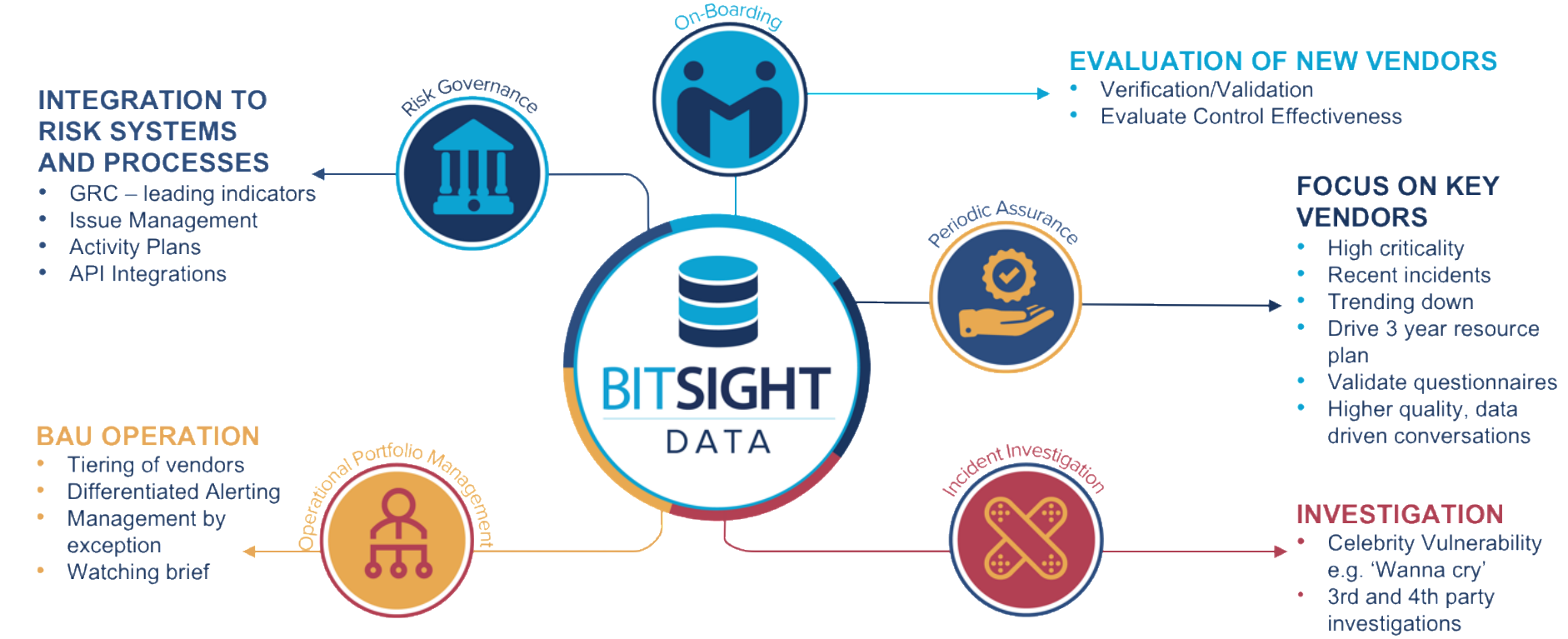
Customer

Existing Processes

- Questionnaires
- Onsite assessments
- Penetration tests

BitSight Security Ratings are a cost-effective, data-driven metric that enables better prioritization of risk and allocation of resources to make effective risk decisions within an organization's TPRM program

BitSight TPRM



EVALUATION OF NEW VENDORS
- Verification/Validation
- Evaluate Control Effectiveness

INTEGRATION TO RISK SYSTEMS AND PROCESSES
- GRC – leading indicators
- Issue Management
- Activity Plans
- API Integrations

FOCUS ON KEY VENDORS
- High criticality
- Recent incidents
- Trending down
- Drive 3 year resource plan
- Validate questionnaires
- Higher quality, data driven conversations

BAU OPERATION
- Tiering of vendors
- Differentiated Alerting
- Management by exception
- Watching brief

INVESTIGATION
- Celebrity Vulnerability e.g. 'Wanna cry'
- 3rd and 4th party investigations

Third Party Monitoring Produces Measurable Results at Scale for TransUnion

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

9x

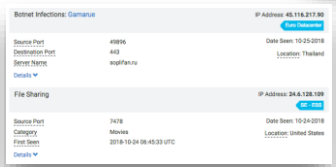
Third party expansion coverage
with same FT employees

Security Performance Management

Security Performance Management Capabilities

Operational Value → **Business Management Value**

Remediation



Prioritization

Benchmarking

Peer Analytics

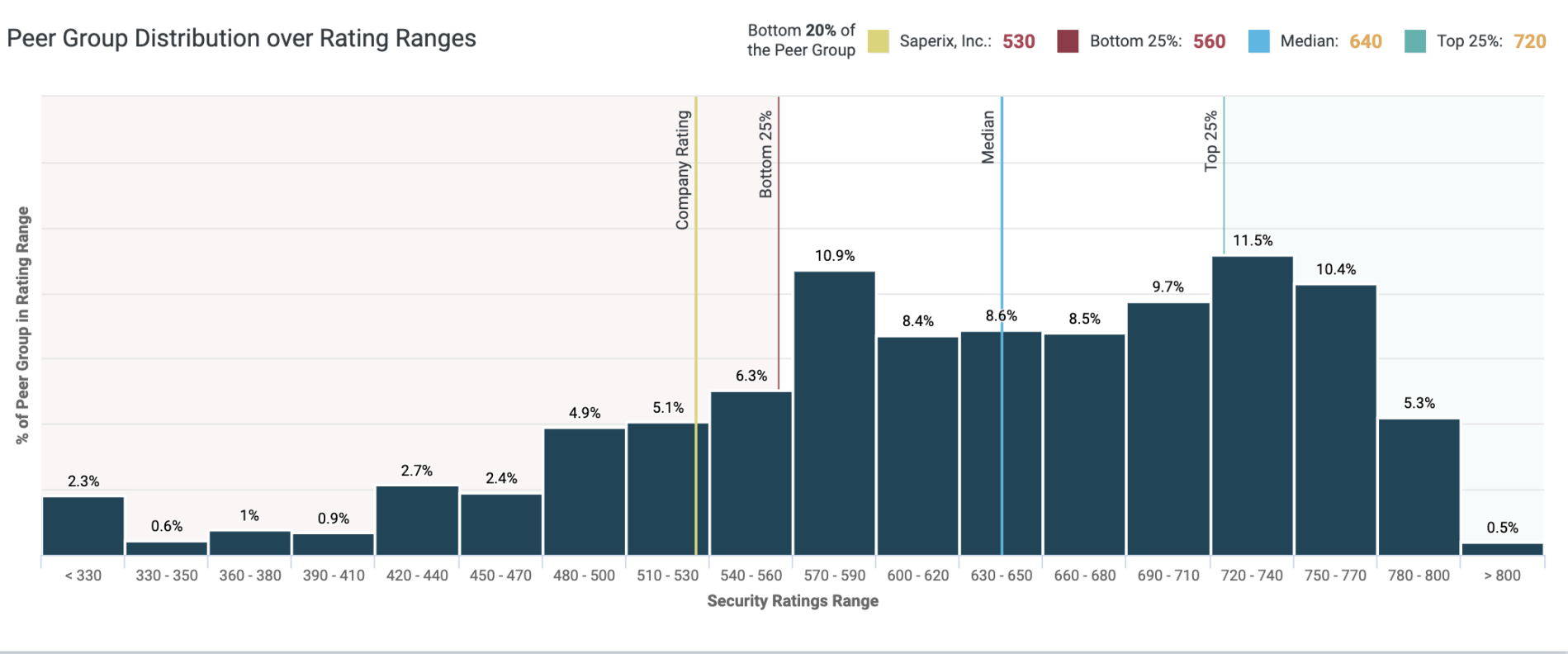
Launch in Q1

Forecasting

Progress Tracking

Future Enhancement

Peer Analytics



BitSight Technologies

https://service.bitsighttech.com/app/ratings-forecast/65daac90-610a-4814-8201-3dc9312f9449/

Apps | BitSight Platform | BitSight Global Pa... | Gmail - Inbox offli... | BitSight Technolo... | Inbox (137) - jame... | Google Drive - Ac... | Campaign: Q417 ... | Partner Comms

BITSIGHT | Portfolio | My Company | Reports | Alerts | Forecasts | Search and Add Companies | 351

Cyber Security Forecast

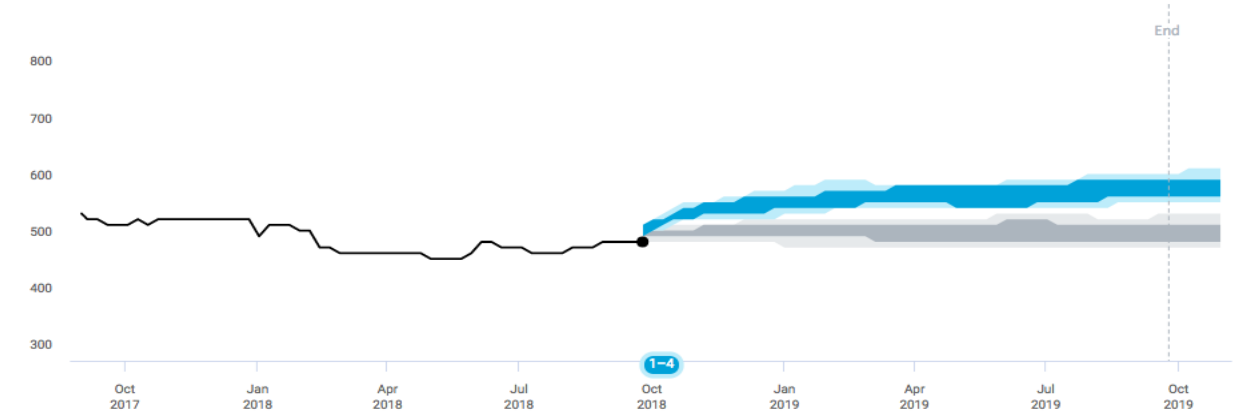
Last saved on September-26-2018 23:01

Define Scenario

Forecast Timeline	Improvement Forecast	Elapsed Time	Forecast Status
September-25-2018 → September-25-2019	480 → 560 - 590	Not Started	Inactive Active

Forecast for Saperix, Inc.

Current Rating — Improvement Forecast — No Action Forecast



Date	Improvement Forecast	No Action Forecast
07-31-2018	N/A	N/A

Support

One Example of Impactful Results from Vendor Collaboration

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

56%

Saw a Rating Increase

276

50

Average points increased across this group

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

How BitSight Security Ratings are Calculated