BITSIGHT®

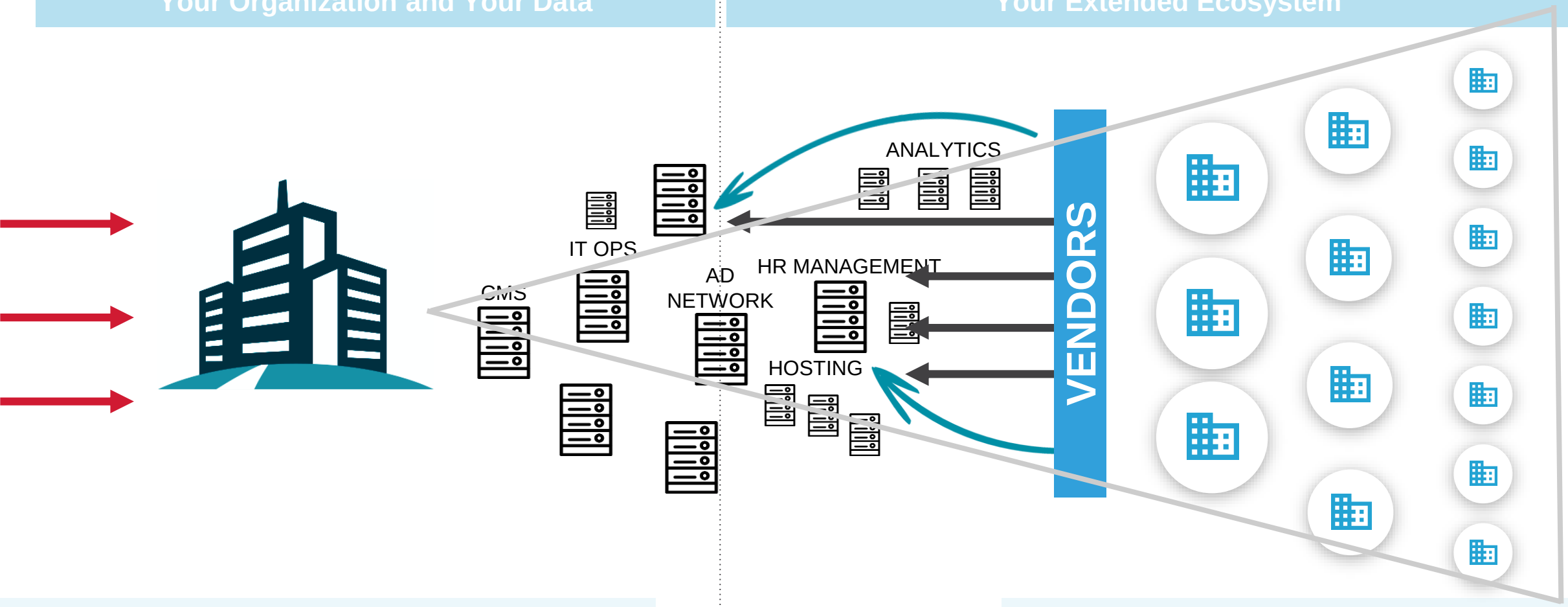
2019 - Year of Supply Chain Risk

S21Sec APD Events

www.bitsight.com

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

2019 - The Year of the Supply Chain Ecosystem

"2019 may be the year the Supply Chain Ecosystem, and **concern about third party risk, officially hit the tipping point**...with Risk, measured in many different ways, becoming the most important letter of the GRC acronym" *- Kirstjen Nielson, Secretary of US Homeland Security @ RSA Conference 2018*

RSA 2019 track on Protecting Data & the Supply Chain Ecosystem

Supply Chain Attacks

15 Experts: Breach at IT Outsourcing Giant Wipro

APR 19

Indian information technology (IT) outsourcing and consulting giant **Wipro Ltd.** [NYSE:WIT] is investigating reports that its own IT systems have been hacked and are being used to launch attacks against some of the company's customers, multiple sources tell KrebsOnSecurity. Wipro has refused to respond to questions about the alleged incident.

Earlier this month, KrebsOnSecurity heard independently from two trusted sources that Wipro — India's third-largest IT outsourcing company — was dealing with a multi-month intrusion from an assumed state-sponsored attacker.

Both sources, who spoke on condition of anonymity, said Wipro's systems were seen being used as jumping-off points for digital fishing expeditions targeting at least a dozen Wipro customer systems.


RANSOMEWARE
Petya

Supply Chain Attacks - NotPetya

05:00 – 06:00 EDT – JUNE 27, 2017

The first signs of a digital attack campaign emerge on Twitter. Early in the morning, Dragos founder and CEO Robert M. Lee tweets out reports indicating that Kyivenergo, an electric power supplier to Kiev, has suffered a hacking attack that's affected Ukrenergo, a Ukrainian power distributor which likely suffered an infection of Industroyer in December 2016.

Supply Chain Attacks - NotPetya

12:00 EDT – JUNE 27, 2017

Ukraine's police confirm MeDoc, an accounting software package that many Ukrainians use to pay their taxes, as a NotPetya infection vector.

The Changing Business Landscape

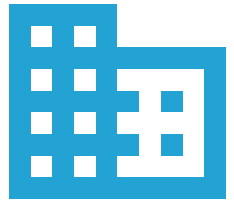
Organizations undergoing digital transformation to better deliver products and services to customers and drive innovation...

40% *of all technology spending will go toward digital transformations.*

$2T *the amount enterprises will spend on digital transformations by 2019.*

New Initiatives to Drive Innovation

Cloud



IoT

Mobile

79% ***Of organizations are adopting new technologies at a rate faster than they can address new security issues*** (Accenture)

Digital Transformation Expands Attack Surface

Companies continue to expand digital ecosystem….

70% *of organizations have "moderate" to "high" dependency on external organizations* [1]

...Which poses new risks to the business

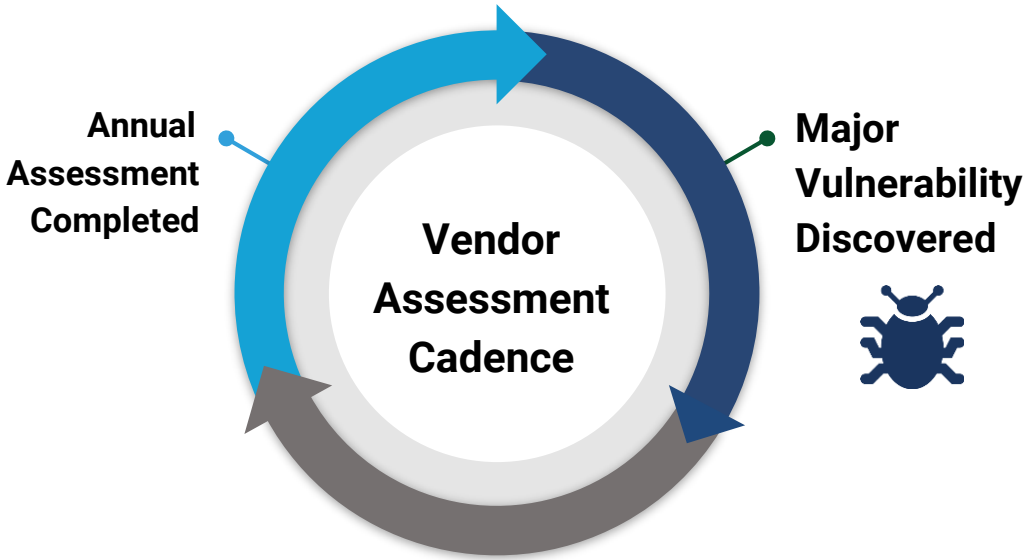
59% *of organizations have experienced a data breach caused by one of their vendors or third-parties* [2]

[1] Results from 2019 Deloitte survey
[2] Ponemon-Opus: 2018 Data Risk in the Third-Party Ecosystem

Lack of Confidence in Current Approaches

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**"

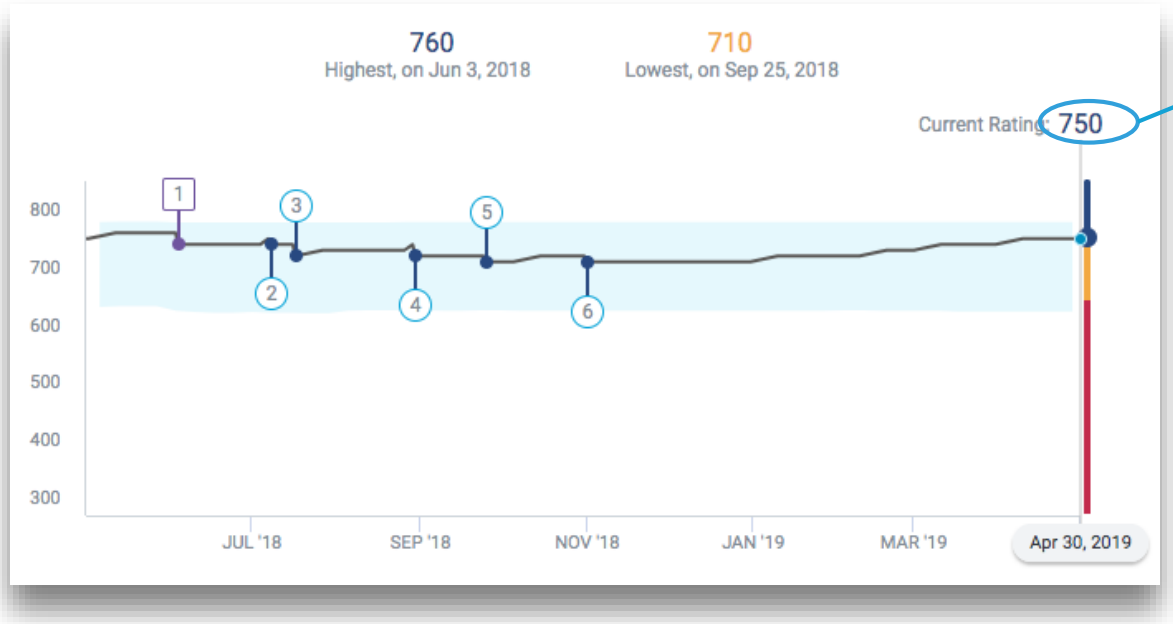
"A **single point-in-time** view of risk is good enough"

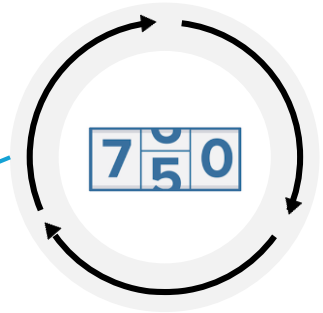
"I only need to **focus on my top tier vendors** - the others don't matter"

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

Translate Complex Cybersecurity Issues into Simple Business Context

Objective, 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*

Manage Third-Party Risk with Confidence

BitSight gives 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.

Demo

Portfolio Overview*

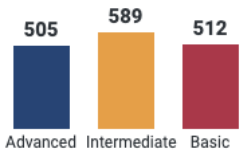
Median Security Rating

700

Companies in Portfolio

1618

Security Ratings Distribution



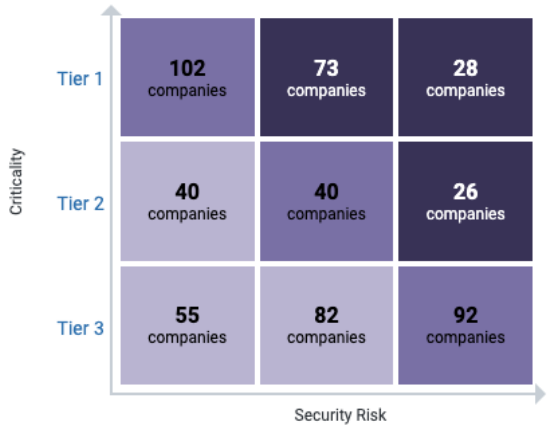
Portfolio Range: 300–810

* Alerts-only companies are not included in overview metrics. Read more...

Portfolio Risk Matrix

538/1618 Companies Tiered

Manage Tiers



Vendor Action Plan — Monitor Review Escalate

All Companies

Quick Links

Most Frequently Viewed

530 Saperix, Inc.
500 Ermenegildo Zegna Corporate
630 REXEL SPAIN, S.L.

Recently Viewed

530 Saperix, Inc.
470 Quimidroga S.A.
760 Lusíadas Saúde

Lowest Ratings

300 Marriott International Corpor...
300 Rackspace Ltd. Corporation
300 BT Group plc

Alerts & News

Alerts

April 07:
Affidea Portugal: SSL Certificates grade decreased from C to D

April 07:
Banco Bilbao Vizcaya Argentaria, S.A. Group: SSL Configurations grade decreased from C to D

April 07:
Befesa Zinc Group: Patching Cadence grade decreased from C to D

More alerts

Featured News

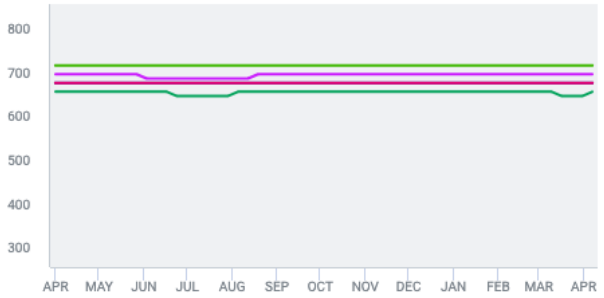
BC Pension Corporation
April 04: A group of microfiches was lost during an office move, compromising the personal information of 8000 individuals.

Bayer Ag
April 04: Malicious software was found on the computer network. The company contained the attack.

More news

Industry Ratings

Industry ratings for the 5 most common industries in your portfolio



Support

Saperix, Inc. 530

Reports Actions

Overview | Rating Details | Compromised Systems | Diligence | User Behavior | Remediation | My Infrastructure | Forensics

BitSight Security Rating

530 BASIC

★ Saperix Corporate is the Primary Rating

About Ratings View Company Tree

Company Info

Set Custom ID

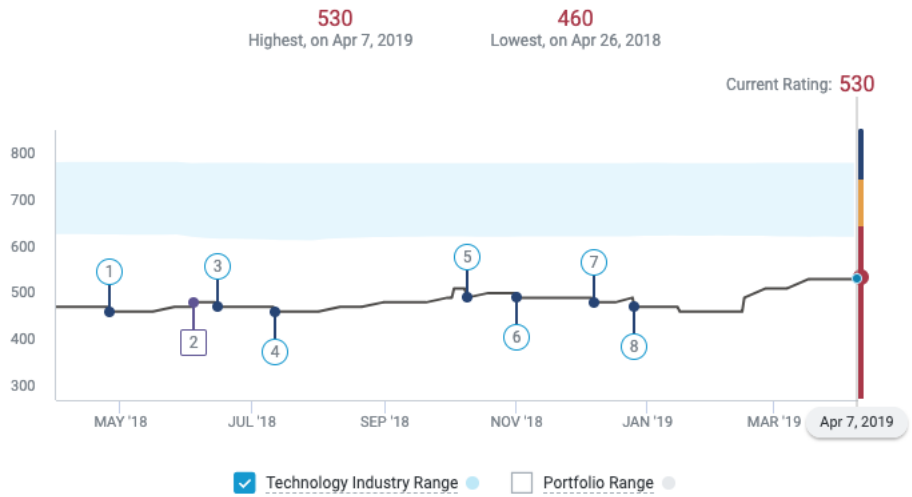
Industry: **Technology** Homepage: saperix.com Monitored by **296 companies**

Subscription: **Continuous Monitoring**

Show Details

Security Ratings

Download Data (.csv)



Rating Highlights

8 Dec 26, 2018
20 point drop, from 490 to 470
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

6 Nov 1, 2018
10 point drop, from 500 to 490
Server Software: minor change, grade remains B

Saperix, Inc. 530

Reports Actions

Rating Overview

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

Compromised Systems

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

User Behavior

File Sharing	A
Exposed Credentials **	N/A

Public Disclosures

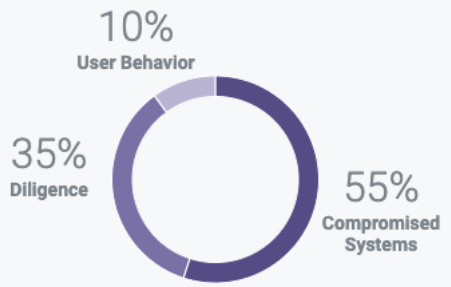
Breaches	A
Other Disclosures*	N/A

Diligence

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

* Risk Vector does not currently affect Security Ratings
** Informational risk vector (will never affect Security Ratings)
Breaches have a negative impact on Security Ratings only if they occur

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.

Support

Compromised Systems details for Saperix, Inc.

Download Data (.csv)

Graph Type

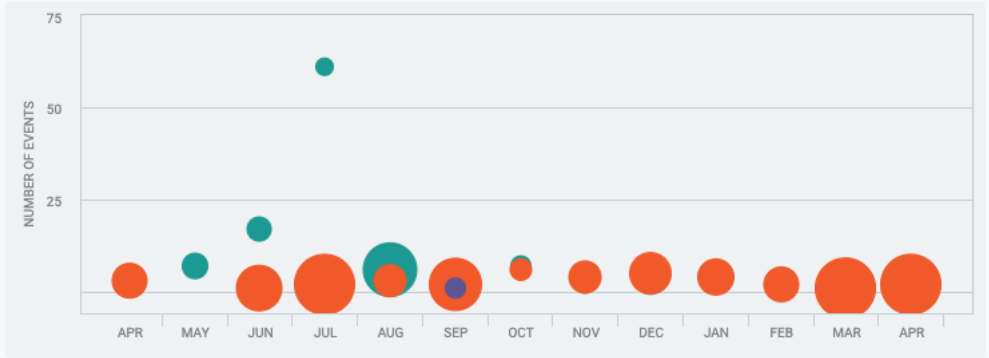
Distribution

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 – 156 events over 12 months



Show:

- All
- Botnet Infections — 35 events
- Spam Propagation — 1 event
- Malware Servers — 0 events
- Potentially Exploited — 120 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
Potentially Exploited SE - ESS	24.6.128.45	US	03-30-2019	04-01-2019	3	**Infection:** CrossRider	Details
Potentially Exploited SE - ESS	24.6.128.45	US	03-24-2019	03-24-2019	1	**Infection:** CrossRider	Details 1
Botnet Infections India HQ Office	45.116.217.90	TH	03-19-2019	04-05-2019	18	**Infection:** Gamarue	Details 1
Potentially Exploited	24.6.128.45	US	03-18-2019	03-19-2019	2	**Infection:** CrossRider	Details

Time range

All Time
Last 7 days
Last 30 days
Custom Date Range

Narrow By Risk Vector

All Forensics
Compromised Systems
Botnet Infections (196)
Spam Propagation (2)
Malware Servers (0)
Potentially Exploited (210)
Unsolicited Communications (0)

User Behavior
File Sharing (57)

Narrow By Tags

- India HQ Office (237)
- SE - ESS (207)
- Webserver Danmark (82)
- agtest2 (82)
- LAB (11)

Show all

Botnet Infections: Gamarue — IP Address/Domain: **45.116.217.90** — India HQ Office

C&C Domain	6kbj7ea9.ru	Date Seen:	04-05-2019
Detection Mechanism	Sinkhole	Location:	Thailand
Last Seen	2019-04-05 01:15:28 UTC		

Botnet Infections: Gamarue — IP Address/Domain: **45.116.217.90** — India HQ Office

Source Port	50518	Date Seen:	04-05-2019
Destination Port	443	Location:	Thailand
Server Name	soplifan.ru		
C&C IP	XXX.38.137.100		
Observations	58		
Detection Mechanism	Sinkhole		
Request Method	POST		
First Seen	2019-04-05 01:15:38 UTC		
Last Seen	2019-04-05 10:21:06 UTC		
Representative Event Timestamp	2019-04-05 10:21:06 UTC		
User Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)		

Details

Botnet Infections: Gamarue — IP Address/Domain: **45.116.217.90** — India HQ Office

C&C Domain	6kbj7ea9.ru	Date Seen:	04-04-2019
Detection Mechanism	Sinkhole	Location:	Thailand
Last Seen	2019-04-04 01:17:15 UTC		

Botnet Infections: Gamarue — IP Address/Domain: **45.116.217.90** — India HQ Office

Source Port	51652	Date Seen:	04-04-2019
Destination Port	443	Location:	Thailand

Remediation Overview

Download Remediation Data

Remediation Strategy

Risk vectors with the highest Rating Impact over a **60-day** period.

Why are some risk vectors not listed?

Open Ports 10 Points

Asset Risk Matrix

Assets for Saperix, Inc.

Search...

Assets	Importance	Warn/Bad Findings	Total Findings
kennedymotors.com	High	0%	1
nibrainsurance.com	High	0%	1
parallelsig.com	High	0%	1
kramerandross.com	High	100%	1

Support

Peer Analytics

Company: Saperix, Inc.
Peer Group: Technology Industry | Similar Employees | 868 Companies

Export CSV | Edit Comparison

Overview | Risk Vectors

Saperix, Inc. **530**

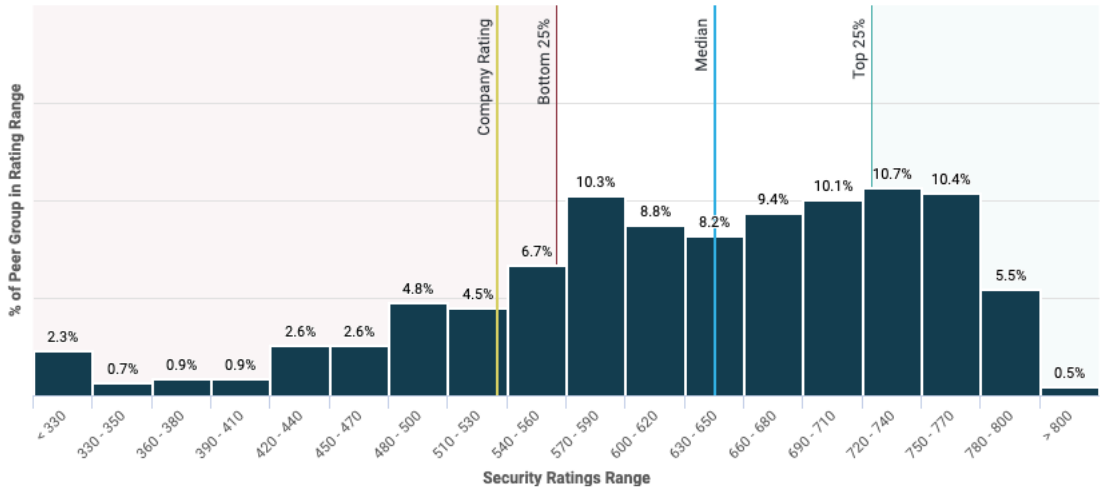
Bottom **20%**
of the Peer Group

Bottom 25% **560**
↑ 30 points more
than Saperix, Inc.

Median **640**
↑ 110 points more
than Saperix, Inc.

Top 25% **720**
↑ 190 points more
than Saperix, Inc.

Peer Group Distribution over Rating Ranges



Risk Vector Performance

6 **Worse** than Peer Group
4 **In Line** with Peer Group
6 **Better** than Peer Group

Worse Risk Vectors

	Company	Median	Top 25%
Botnet Infections Bottom **11%** of the Peer Group	F	A	A
Spam Propagation Bottom **19%** of the Peer Group	B	A	A
Potentially Exploited Bottom **20%** of the Peer Group	D	B	A

View all Risk Vectors

Better Risk Vectors

	Company	Median	Top 25%
File Sharing Top of the Peer Group	A	A	A
Malware Servers Top of the Peer Group	A	A	A
Unsolicited Communications Top of the Peer Group	A	A	A

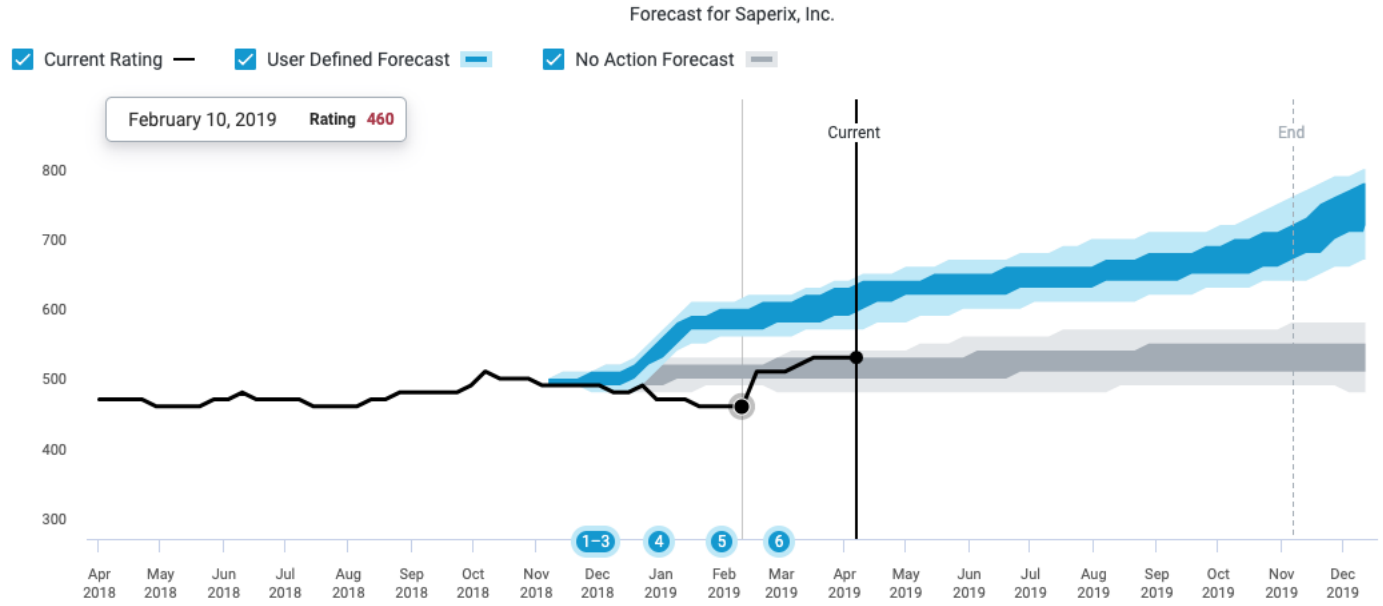
View all Risk Vectors

Support

Budget approval Forecast

Last saved on April-08-2019 15:25 Share Stop Monitoring

Forecast Timeline	User Defined Forecast	Elapsed Time	Forecast Status
November-07-2018 → November-07-2019	530 → 670 - 720	151 days	Active



Budget approval Forecast

Last saved on April-08-2019 15:25 Share Stop Monitoring

Forecast Scenario

1 Botnet Infections

Updated Yesterday

Your goal is to **Reduce the yearly rate of Number of Events from 35 to 0** and to **Reduce the Average Duration from 10.2 to 1.4 Days**.

Due Date

November-30-2018

4 months and 1 week ago

0% complete

Number of Events (Yearly rate)

0%
COMPLETE

35 Events Remaining

INITIAL	TARGET	CURRENT
35	0	35

Average Duration in Days

0%
COMPLETE

8.8 Days Remaining

INITIAL	TARGET	CURRENT
10.2	1.4	10.2

2 Mobile Software

Updated Yesterday

Your goal is to **Reduce the Total Number of BAD Records from 8 to 0** and to **Reduce the Total Number of WARN Records from 12 to 0**.

Due Date

November-30-2018

4 months and 1 week ago

21% complete

BAD Total Number of Records

25%
COMPLETE

6 Records Remaining

INITIAL	TARGET	CURRENT
8	0	6

WARN Total Number of Records

16%
COMPLETE

10 Records Remaining

INITIAL	TARGET	CURRENT
12	0	10

3 SSL Certificates

Updated Yesterday

Your goal is to **Reduce the Total Number of BAD Records from 82 to 0** and to **Reduce the Total Number of WARN Records from 24 to 0**.

Due Date BAD Total Number of Records WARN Total Number of Records

BITSIGHT

Questions

BITSIGHT

info@bitsight.com