Trustwave®
a Singtel company

DATA SHEET

Trustwave Cyber Posture Ratings and Benchmarking Programme

UNDERSTAND YOUR OUTSIDE-IN SECURITY POSTURE AND THIRD-PARTY RISK

Benefits

- Continuous visibility into your organisation's outside-in security performance
- Remediate security issues based on actionable findings
- Competitive benchmarking on security performance
- Quantitative and non-intrusive assessment of third-party vendors' cyber posture

For many organisations, the IT infrastructure not only supports corporate needs but also an entire ecosystem of business partners and customers, thereby increasing exposure to cyber risks. This heightens the need to measure, monitor, and maintain cyber health to guard against potential risks from all fronts.

Organisations are often in the dark when it comes to understanding the actual security performance of critical third parties or even assessing the impact of security programmes and policies. This is due to a lack of objective metrics and tools to help measure and mitigate cyber risk across the business ecosystem.

Get Complete, Continuous Visibility on Your Security Performance.

Trustwave's Cyber Posture Ratings and Benchmarking Programme (CPRB) offers a quantitative, non-intrusive measurement of your organisation's outside-in security posture, continuous visibility into security performance, and actionable recommendations to protect the IT infrastructure against all attacks.

CPRB, powered by BitSight Security Ratings, transforms how your organisation evaluates risk and security performance by employing an outside-in model similar to those used by credit rating agencies and leveraging terabytes of global data processed by the world's largest sinkhole.

CPRB comprises three parts:

- Measure and compare security performance against industry peers
- Third-party risk management
- Cyber insurance underwriting

Rating Cyber Posture

CPRB rates your organisation's security performance using high quality, externally observable information on security events such as botnet infections, spam propagation, malware infections, and more.

It also looks at how your organisation exercises due diligence in ensuring its public-facing assets such as SPF domains, DKIM records, TLS/SSL certificates, and the likes are securely configured.

This allows you to quantify cyber risk, measure the programme, and benchmark performance against industry peers.

An Outside-in Approach Leveraging Terabytes of Global Data

- Companies are rated on a scale of 250-900 – high rating indicates strong security performance and low security risks
- Analysis, rating, and monitoring of security performance are done automatically from the outside
- Daily ratings and alerts are provided continuously via a Service Portal

Assess the Cyber Risk of Third-Party Vendors

- CPRB allows your organisation to assess security risks of outsourcing by providing a quantifiable measurement of your third-party vendors' security posture
- Cyber Posture Ratings for third-party management enables organisations to identify, quantify, and mitigate the risk associated with sharing sensitive data with business partners.
- Analysis, rating, and monitoring of third parties' security performance are done from the outside.

Features

- An operational framework that provides guidance on the necessary people, process and technology to address the outside-in security findings.
- 12 months' access to the Service Portal
- Half-yearly onboarding reviews to refine operational framework
- Expert advice and recommendations to address threats and protect assets

Use Cases

Third-party vendor risk management
- Selecting new vendors
- Onboarding process
- Continuous monitoring

Mergers & acquisitions
- Cyber due diligence
- Acquisition onboarding
- Portfolio management

Health check/ Security performance monitoring
- Rating details (compromised systems/diligence/user behaviour)
- Statistics
- Details and remediation instruction

Cyber insurance
- Cyber insurance underwriting
- Risk aggregation
- Insured monitoring

Benchmarking & executive reporting
- Establish a baseline
- Monitor and remediate
- Executive and board reporting

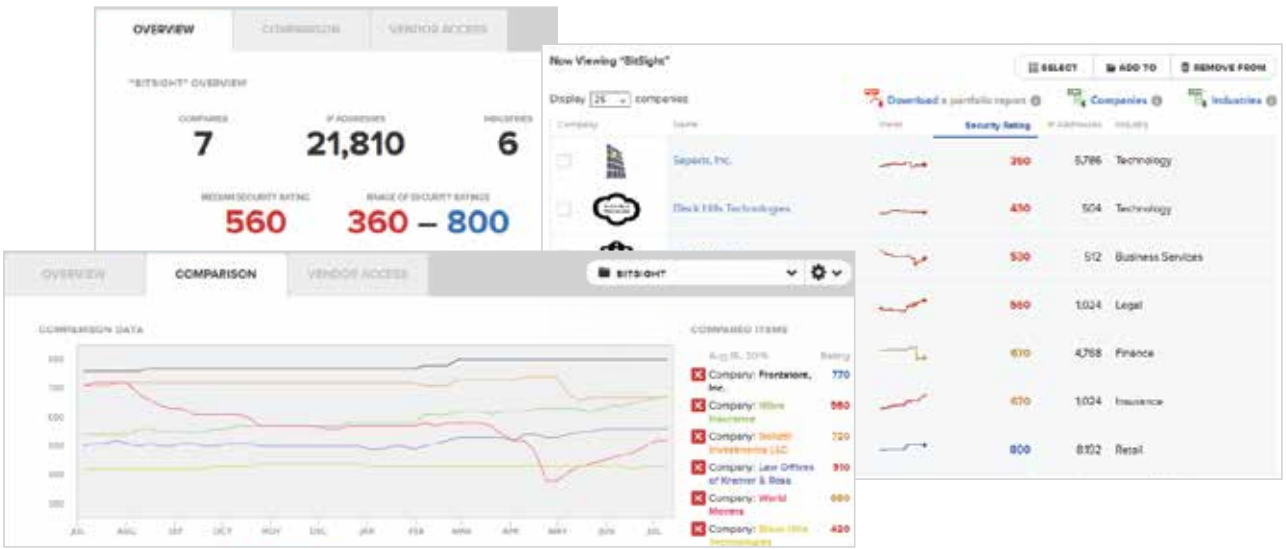
Peer analytics
- Assess relative security performance in context
- Measure & report outcome
- Effectively allocate limited resources

Highly Specialised Services from the Experts

Trustwave consulting services matches you with experienced professionals who will help to interpret the reports, identify security gaps, and propose best-suited services to improve security postures of your organisation and third-party vendors.

Our consultants will:
- Assist in the interpretation and application of the report
- Explain how the security posture ratings are derived
- Recommend methods to improve your security posture ratings (versus industry average)
- Work with you to architect a more holistic cybersecurity strategy with a defence-in-depth approach, leveraging the "outside-in" intelligence provided by the reports, to eliminate attack vectors from within and outside of the network.

Sample report: Vendor Risk Management



Sample report: Health Check and Security Performance Monitoring

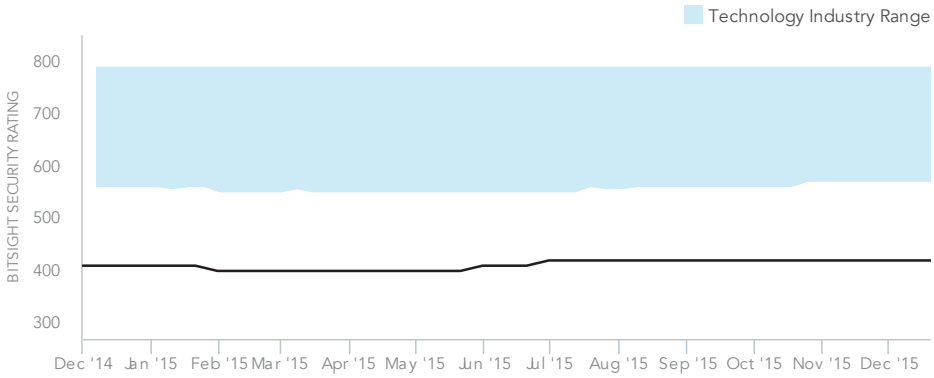
SECURITY RATINGS

BITSIGHT SECURITY RATING

420

Our ratings measure a company's relative security effectiveness.

ADVANCED	900-740
INTERMEDIATE	740-640
BASIC	640-250



The Security Rating for Saperix, Inc. has varied from 400 to 420 over the past 12 months. The blue band represents the range of ratings for all companies within the Technology industry. Outliers are excluded. Sudden drops in ratings can be due to publicly disclosed data breaches, an increase in observed events, or poorly configured diligence records.

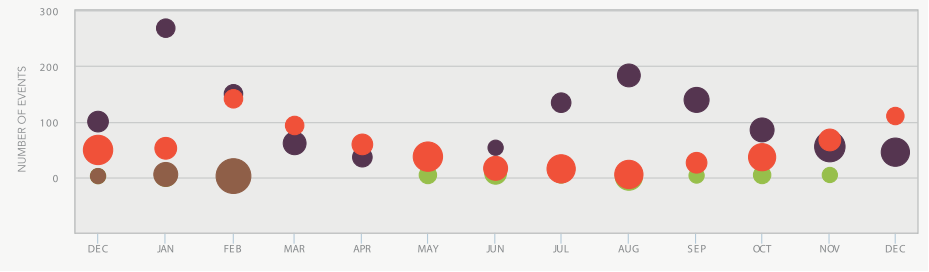
BOTNET INFECTIONS

F	24	696	2.8 days	SAPERX, INC.
GRADE	THIS WEEK	THIS YEAR	AVERAGE DURATION	
In the **bottom 10%** of all companies	7	421	2.1 days	TECHNOLOGY INDUSTRY AVERAGES
	THIS WEEK	THIS YEAR	AVERAGE DURATION	

EVENT DISTRIBUTION

2049 events over 12 months

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



EVENT REMEDIATION

Infection Name	Description	Targeted Platform	Risks
Alureon Aliases: DNSChanger, Tidserv, TDSServ, TDSS, Zlob	Alureon is a trojan designed to exfiltrate specific data, such as usernames, passwords, and credit card information. Remediation Instructions: http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2fAlureon	Win32	Data Exfiltration, Unauthorized Access, Implies Other Infections, Resource Abuse

Trustwave®
a Singtel company

For more information: www.trustwave.com