

Safeguard your Public Attack Surface with Security Ratings



Fio Lee

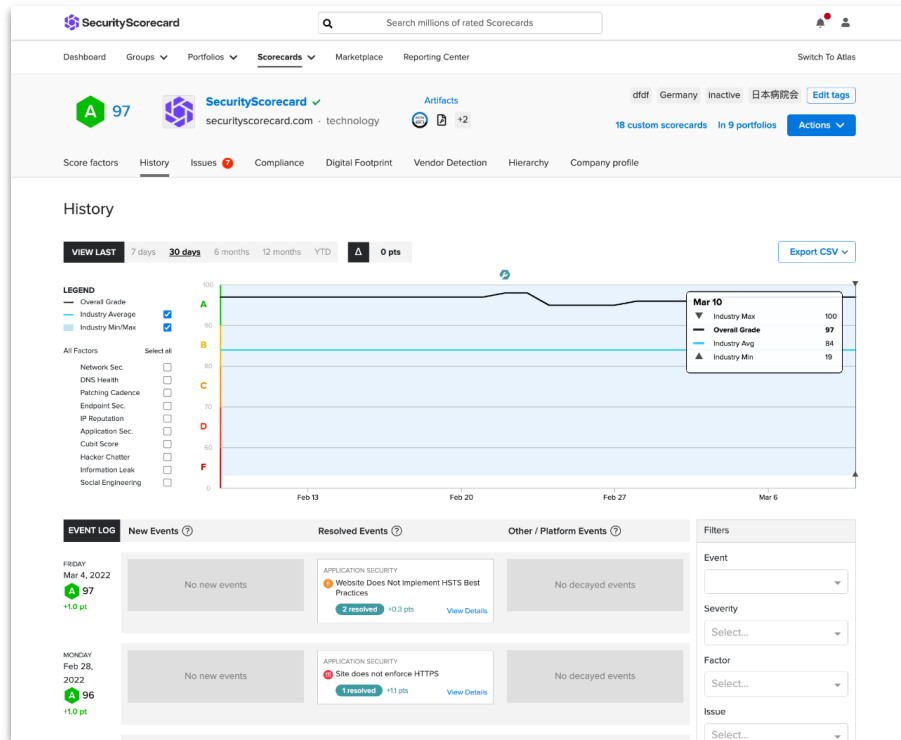
Senior Consulting Engineer,
Asia Pacific



SecurityScorecard



SecurityScorecard is the global leader in cybersecurity ratings. We transform the way that organizations understand, improve and communicate cybersecurity risk to their, boards, employees, and vendors.



FORRESTER
NEW WAVE
LEADER 2021
Cybersecurity Risk
Ratings Platforms



Safeguard requires a novel, holistic approach.

No one offers a more comprehensive suite of solutions.

Cyber Risk Intelligence & Response Platform

Outside-in View of Risk

- Security Ratings
- Attack Surface Intelligence
- Security Data API
- Automatic Vendor Detection

Professional Services

- Third-Party Risk Program Development
- Cyber Threat Intelligence as a Service
- Digital Forensics and Incident Response
- Academy

Inside-out View of Risk

- Assessments
- Internal Security Suite

SecurityScorecard Data

Marketplace

- Integrations
- Apps
- Developer Hub

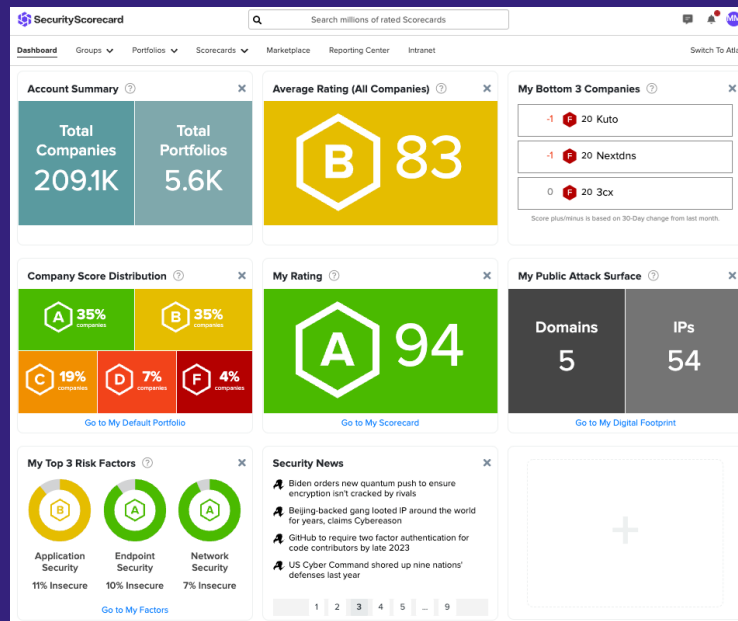
Cyber Risk Reporting

- Cyber Risk Quantification
- Reporting Center



Manage the Security Posture of *any* Organization

- Transparent Data Collection and Accurate Scores with 360° Visibility
- Collaborative Remediation and Powerful Threat Reconnaissance
- Continuous Compliance with Direct Mapping to Frameworks
- Benchmark Risk to Demonstrate Return on Security Investments



Instantly rate, understand, and continuously monitor the security risk of *any* organization

Source Trusted Information About You and Your Third Parties

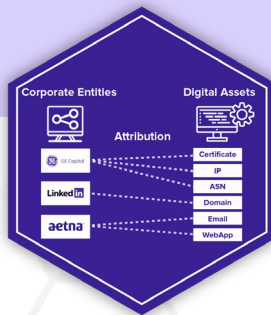
1 Data Collection

- **Global sensor network** crawling the Internet from over 45 locations
- **60B+** vulnerabilities gathered per week and **850M+** hits to sinkhole daily



2 Attack Surface Discovery

- **Patented capabilities** discover an organization's attack surface
- Attribution of attack surface to **any organization worldwide**



3 ML-Powered Data Processing

- Data processing engine aggregates signals to **enhance accuracy**
- **Hundreds of risk factors** over 10 security categories
- **ML based risk severity** model that learns from user feedback



4 Fair, Accurate and Predictive Model

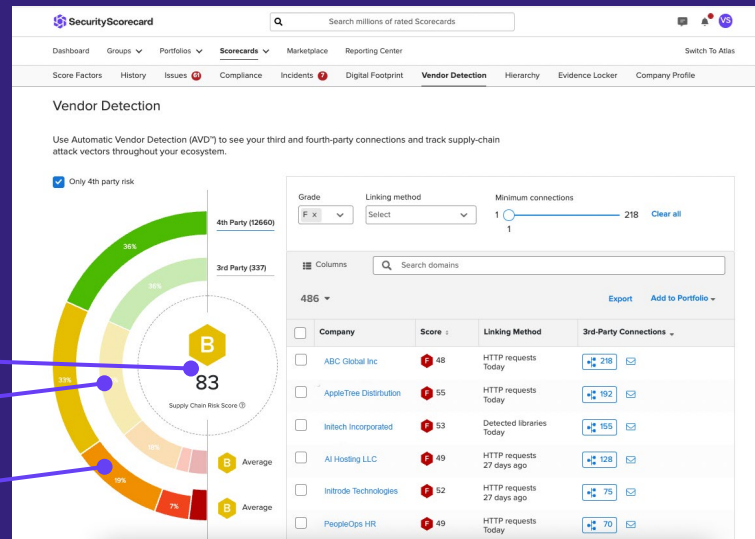
- A-F Rating for **12M+ Companies**
- Low scores **7.7x more likely to breach**
- **9 years** of historical data + user contributed data





Empower Your Organization with an Instant Supply Chain Risk Analysis

- Calculate a Supply Chain Risk Score
- Detect your third-party ecosystem
- Get unparalleled visibility into 4th party and concentration risk.



Mitigate risk and understand potential threats from outside your organization.



Outside In: Attack Surface Intelligence

Scan Billions of Data Sources to Provide Deep Threat Intelligence

- Identify and respond to threats faster
- Save time with 10x faster analysis
- Scale your Security and Risk Management teams
- Reduce tools costs, licensing fees and free up staff

12M+ Digital Footprints

200K+ Campaign Events

1,300

Scanned Ports in Six (6)
Continents

>200

Threat Actors

62M

Indicators of
Compromise (IOCs)

9 Critical CVE-2020-0688

Current Description

A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.

[Detail](#) [Products](#) [Assets](#)

Risk

CVSS v3.0 score: **9 Critical**
CVSS vector: AV:N/AC:L/Au:S/C/C/I/C/A/C
CVSS date: Jul 12 2022
Confidentiality impact: Complete
Integrity impact: Complete
Availability impact: Complete
Access complexity: Low
Authentication required: Single
Access vector: Network
Common weakness CWE-287
enumerator ID:

Publication information

Published in NVD: Feb 11 2020
Last modified in NVD: Jul 12 2022
Source: [secure@microsoft.com](https://secure.microsoft.com)

Connection to Threat Actors

Unrecognized campaigns

Jun 03 2022
[CISA/CERT] - Public Feed

Jun 01 2022
Metasploit exploits with CVE assigned feed

Jul 21 2021
Ongoing Campaign Leveraging Exchange Vulnerability Potentially Linked to Iran

Jun 28 2022
CISA - KNOWN EXPLOITED VULNERABILITIES CATALOG

Jun 28 2022
CISA - KNOWN EXPLOITED VULNERABILITIES CATALOG feed

Jun 28 2022
CISA - Known Exploited Vuln Catalog Enrichment

**Identify all of your connected
assets and expose unknown
threats to prioritize remediation.**



Build a Comprehensive Security Ecosystem with the SecurityScorecard Marketplace

Discover and deploy **trusted partner solutions and pre-built integrations in our one-stop shop**, so you can optimize your security workflows, access even more security intelligence, and accelerate risk mitigation.

Marketplace

Developer Hub

Help

Apps integrations and partners

Enrich your security insights with new signals, automate workflows for faster action, and integrate SecurityScorecard data with powerful partner solutions.

Start typing to search apps

Alphabetically

Types

Featured

Built by SecurityScorecard

Signals

Workflow Automation

External Integrations

Marketplace Partners

Categories

Board Management

Cyber insurance & Modeling

Financial & Credit Data

Alyne

Intuitive, AI-enabled software empowering proactive risk management across your...

Aravo

Assess your third parties at scale with SecurityScorecard insights in Aravo.

axio

Axio360 Cyber Risk Platform

Quantify cyber risks in seconds to see your financial exposure to catastrophic scenarios.

Certa

Integrate SecurityScorecard vendor ratings into your automated third-party workflo...

CFG

CFG delivers 'Security Risk Monitoring Services' to clients to improve their security posture...

Cloud Security by SecurityS...

Identify and prioritize issues in your cloud that have the greatest impact on your security posture.

Integration Partners: Leverage Connected Security Ecosystem

Third-Party Risk Management



Workflow Automation



Vulnerability Management



Digital Risk Intelligence



Security Orchestration, Automation, & Response



IT Service Management



Cloud Access Security Broker



Security Information & Event Management



Service Provider



Risk Quantification



Business Intelligence



Cyber Insurance & Modeling



Financial & Credit Data

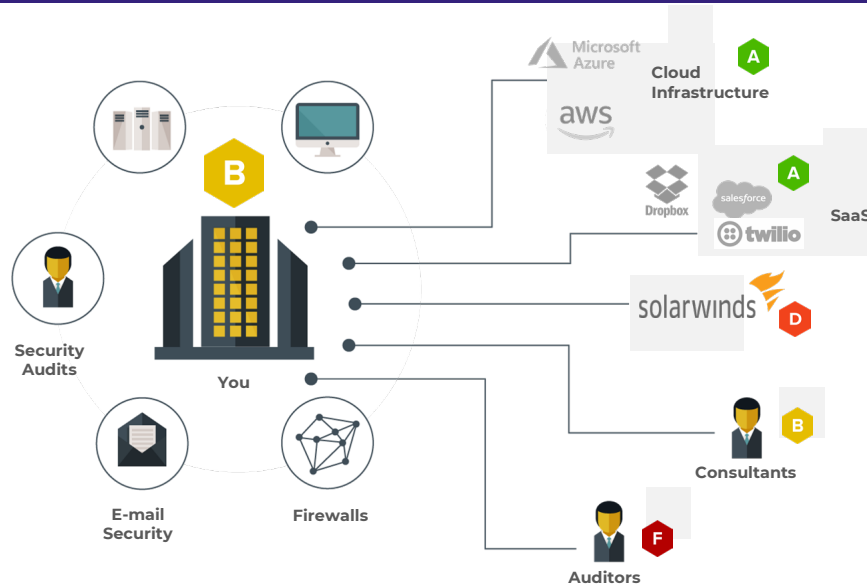


Board Management



Problem: It's becoming increasingly difficult to keep up with the security posture of new and existing vendors

How do I understand risks in my own security program?



How do I know who my third and fourth party vendors are and if they are diligent about protecting their data?

63% of data breaches are linked to third parties*

Think third-party risk is Important, fourth-party risk is the Horizon

Third parties we
know about.

Third and Fourth
parties we don't
know about



Hyperconnected companies on the risk Horizon

583

The average number of
of third parties with
access to organizations'
sensitive data.

$$N*N = 339889$$



4th Party Companies

C 79
↑ 8 ▲

Propose Plan

No artifacts shared

Create Custom Scorecard · In 22 Portfolios

Contact Company

More !

Score Factors

History

Issues 23

Compliance

Incidents 3

Digital Footprint

Vendor Detection

Hierarchy

Evidence Locker

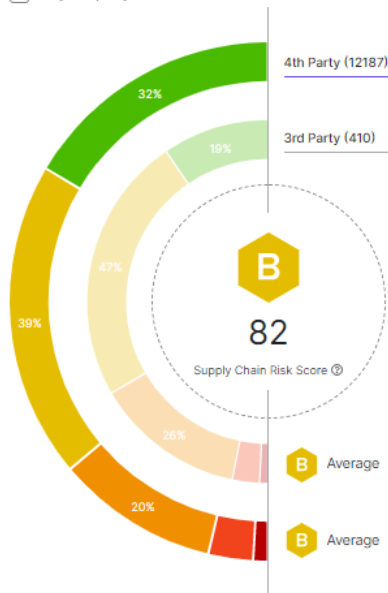
Company Profile

Financial Impact

Vendor Detection

Use Automatic Vendor Detection (AVD™) to see your third and fourth-party connections and track supply-chain attack vectors throughout your ecosystem.

☐ Only 4th party risk



Scorecard: Tesla · Products used: Apache Flink (+1837)

Grade

Linking method

Minimum connections

Select

Select

1 361 Clear All

Columns

Search domains and products

2K

Export Add to Portfolio

| <input type="checkbox"/> | Vendor | Score | Products used | Linking Method | 3rd-Party Connections |
|--------------------------|---|-------|---------------|---|-----------------------|
| <input type="checkbox"/> | Cityonlinebd | F 24 | -- | HTTP requests 14 days ago | 1 |
| <input type="checkbox"/> | Indian Institute Of Technology , Bombay | F 26 | -- | HTTP requests 7 days ago | 1 |
| <input type="checkbox"/> | litk | F 29 | -- | HTTP requests 7 days ago | 1 |
| <input type="checkbox"/> | Smatechnologies | F 29 | 90 | Enhanced illumination 31 days ago | 1 |
| <input type="checkbox"/> | Unt | F 31 | -- | HTTP requests 7 days ago | 1 |
| <input type="checkbox"/> | Kinsta | F 32 | -- | HTTP requests 7 days ago | 2 |

Alerting

- Notification of breach in connected companies
- Assess impact of extended vendor breach
 - Tier one vendor
 - High efficacy breach

Incidents

| DATE | DESCRIPTION | FURTHER DETAILS |
|-------------|---|---|
| May 5, 2022 | BREACH Internal data hack discovered [REDACTED] | Global News Copy External Report URL |
| Aug 5, 2019 | LEAKED The [REDACTED] has issued an apology to Singapore-based customers that may have been adversely impacted by a data breach the firm suffered. The data breach occurred after the company mistakenly pasted 410 customers' email addresses into a promotional communication which was then sent out to others who had signed up to receive marketing material. The data breach took place as... | Copy External Report URL Show more |
| Aug 4, 2019 | BREACH [REDACTED] says sorry for customer data hack, Singapore News & Top Stories The Straits TimesSwedish retailer [REDACTED] yesterday apologised to affected customers in Singapore after the company inserted 410 individual e-mail addresses in the wrong ... | Copy External Report URL |

Contact Vendor

- Visibility first step
- Awareness and Action is just as important
- Contact Vendor Free for any company



Connect with an invitation

Improve your own security posture by encouraging companies to improve theirs with a free SecurityScorecard account.

Invite them to connect.

Add a contact for each company you want to invite:

▼ Yandex 0

First name

Last name

Email address

Use corporate addresses

[Save Contact](#)



2

Select contacts



[Do This Later](#)


[Continue](#)

Remediate Issues

- Generate your own score plan
- Setup your goal for example improve score from B to A
- Follow the suggestions and priorities the items


List of Issues

[Add all](#)

| CURRENT SCORE  86 | | |
|--|----------------------|--|
| !!! HIGH | ENDPOINT SECURITY | |
| Outdated Web Browser Observed | | |
| SCORE IMPACT -6.9 | FINDINGS 1 | |
| !!! HIGH | NETWORK SECURITY | |
| SSL/TLS Service Supports Weak Protocol | | |
| SCORE IMPACT -0.9 | FINDINGS 9 | |
| !!! HIGH | PATCHING CADENCE | |
| High Severity CVEs Patching Cadence | | |
| SCORE IMPACT -0.1 | FINDINGS 2 | |
| !!! HIGH | PATCHING CADENCE | |
| High-Severity Vulnerability in Last Observation | | |
| SCORE IMPACT -0.2 | FINDINGS 2 | |
| !! MEDIUM | APPLICATION SECURITY | |

Score Plan

[Remove all](#)

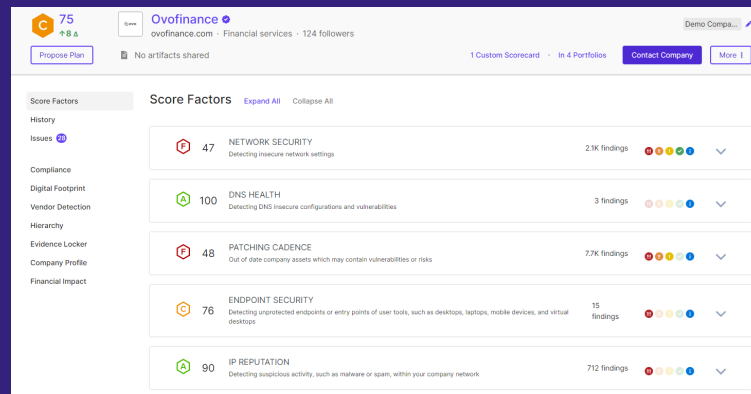
| PROJECTED SCORE  91 | | |
|--|----------------------|--|
| !!! HIGH | ENDPOINT SECURITY | |
| Outdated Web Browser Observed | | |
| RECOVER +6.1 (-0.8 remaining) | REMEDiate 8 out of 9 | |

[Start Again](#)[Cancel](#)[Download Plan](#)

Take control of your 4th parties.

Sign up for your free account to:

- Minimize your cyber risk with continuous monitoring
- Discover vulnerabilities and security gaps in real-time
- Instantly see cybersecurity analytics that highlight risk areas



Contact flee@securityscorecard.io to get started!



Thank you.