SecurityScorecard

AVALORA

SEE WHAT A HACKER SEES

Priorizar el riesgo de seguridad y la continuidad del negocio en tiempos de incertidumbre.

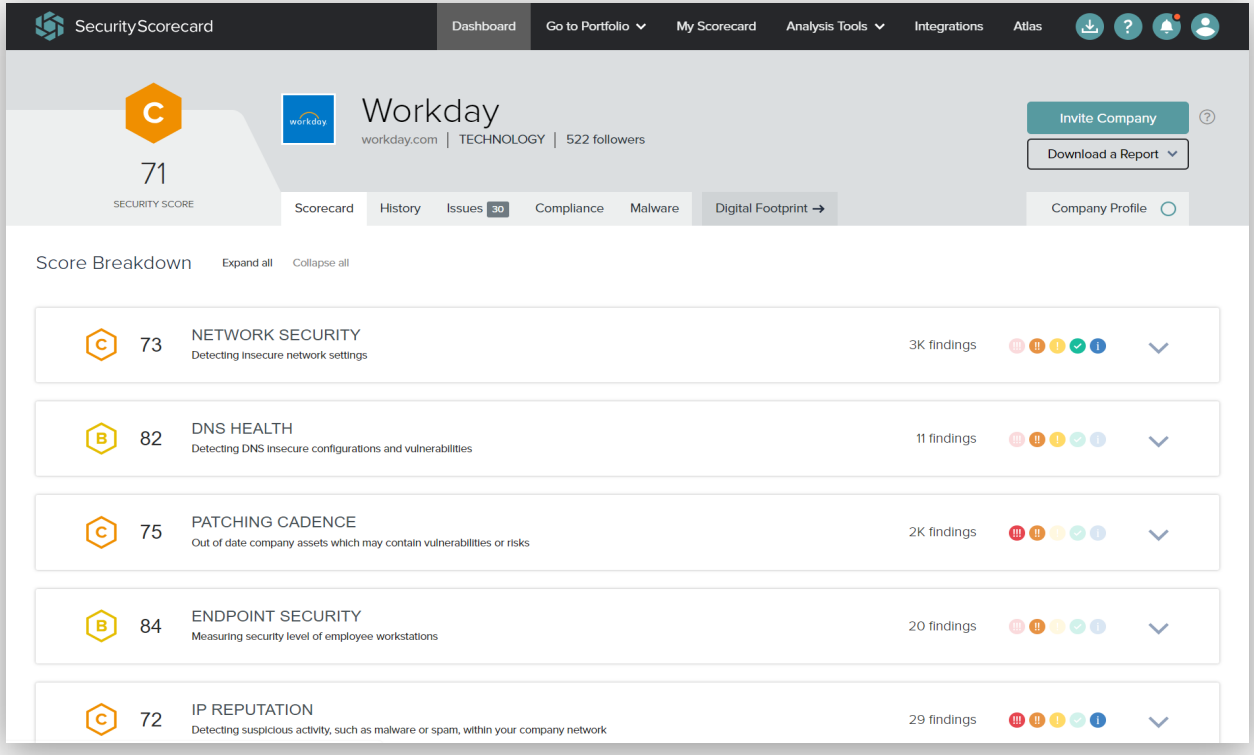
30 Abril, 2020

Overview of SecurityScorecard

- Fundada en 2014, financiada por Google Ventures, Sequoia Capital y Evolution Equity, AXA, Nokia Growth Partners y Riverwood Capital
- 1K + empresas suscritas: **más de 1.3 millones de empresas calificadas diariamente**
- Para 2022, **Gartner** proyecta que las calificaciones de seguridad serán tan importantes como las calificaciones crediticias.
- Las empresas con una mala calificación de “C’ o ‘D’ o ‘F’ tendrán 5.4X más probabilidad de una violación de datos.
- Conjunto de datos histórico de 5 años, que correlaciona los indicadores de compromiso con la probabilidad de una violación de datos

¿Podemos medir de **forma instantánea** y **no intrusiva** la seguridad de **cualquier empresa en el mundo** y mostrar cómo mejorarla?

+1,3 millones de empresas con scores y monitoreadas continuamente por riesgo de seguridad



SecurityScorecard: #1 Rated Solution

4.6

Gartner peerinsights™

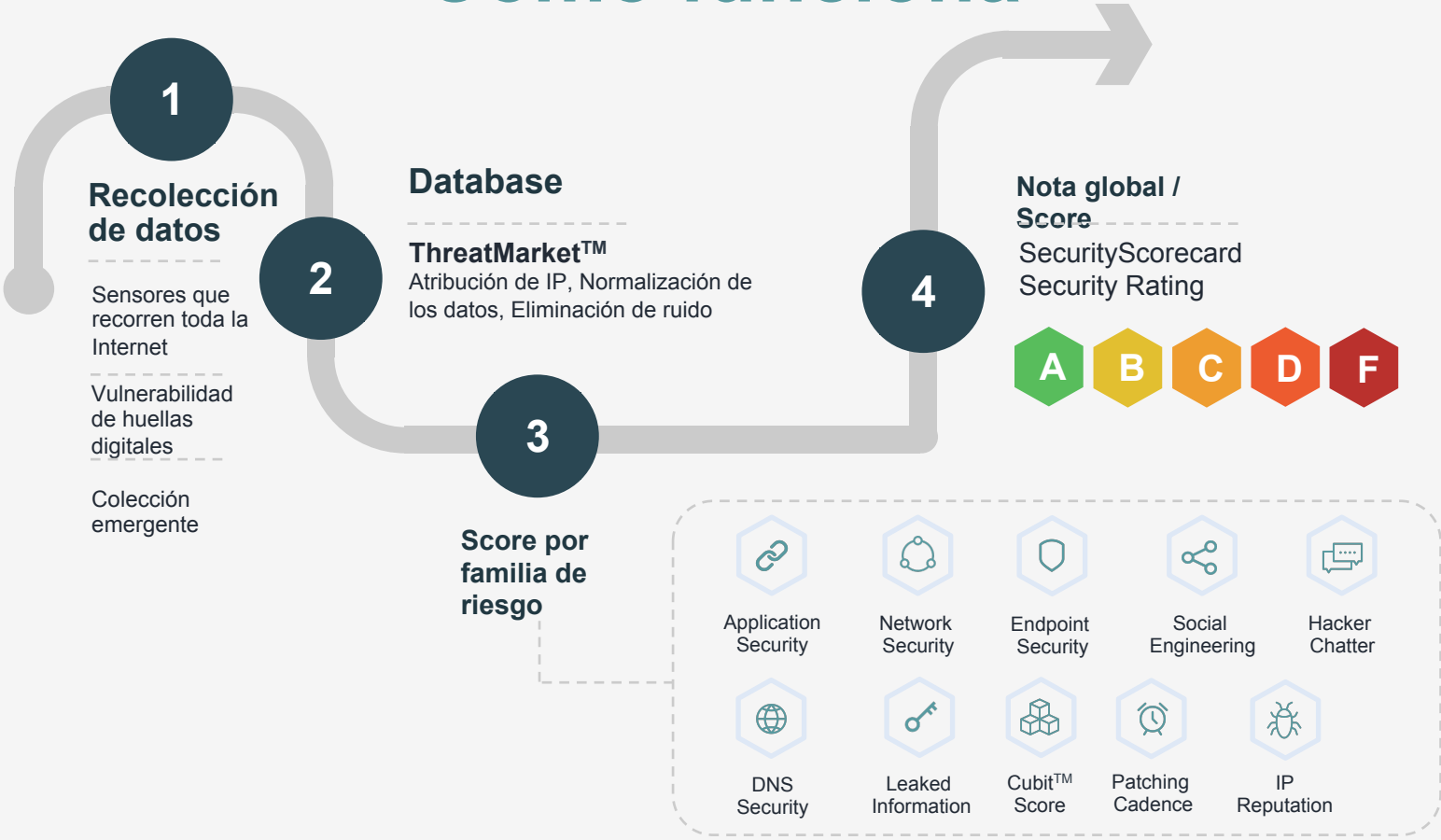
Based on 86 reviews, as of February 2019

Top rated solution for IT VRM on the Gartner Peer Insights customer review website

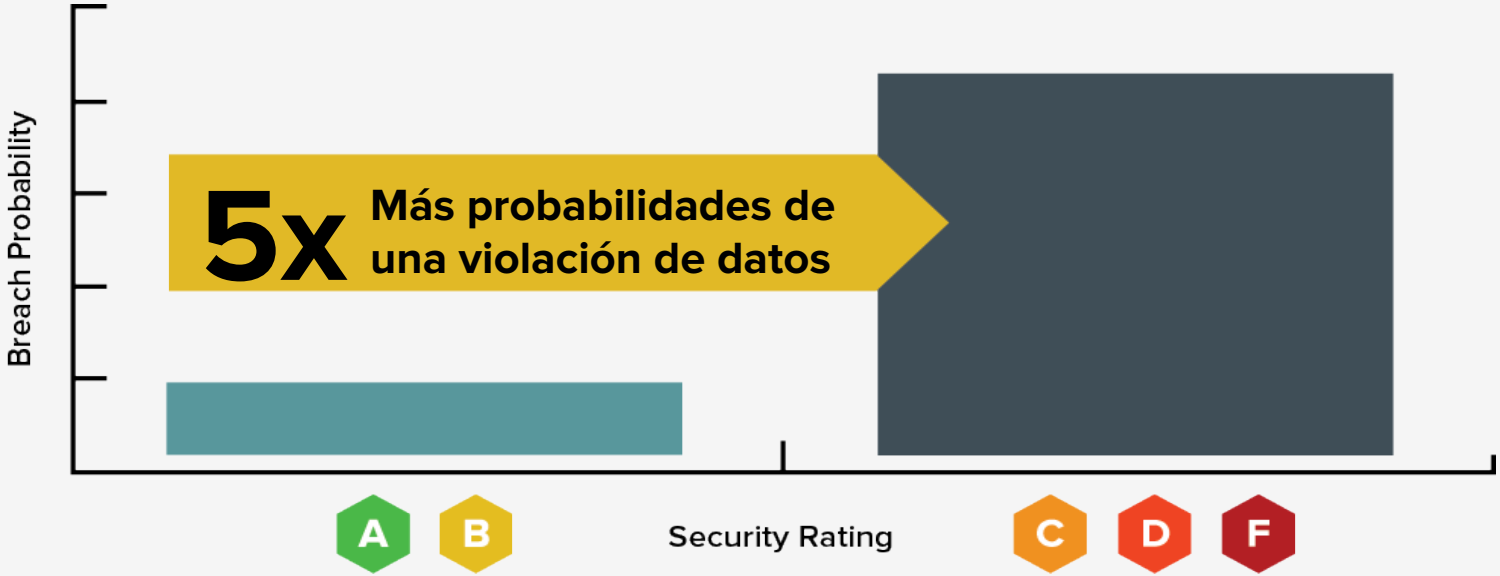
https://www.gartner.com/reviews/market/it-vendor-risk-management/vendor/securityscorecard/product/security-scorecard-platform

SecurityScorecard

Cómo funciona



Correlación estadística con riesgo de incumplimiento/vazamento de datos



Las empresas con calificación C o inferior tienen 5 veces más probabilidades de una violación o incidente de seguridad en comparación con las empresas que son A o B.

Una plataforma, muchos casos de uso

Compras / Negociación de contratos

Monitoreo continuo y VRM

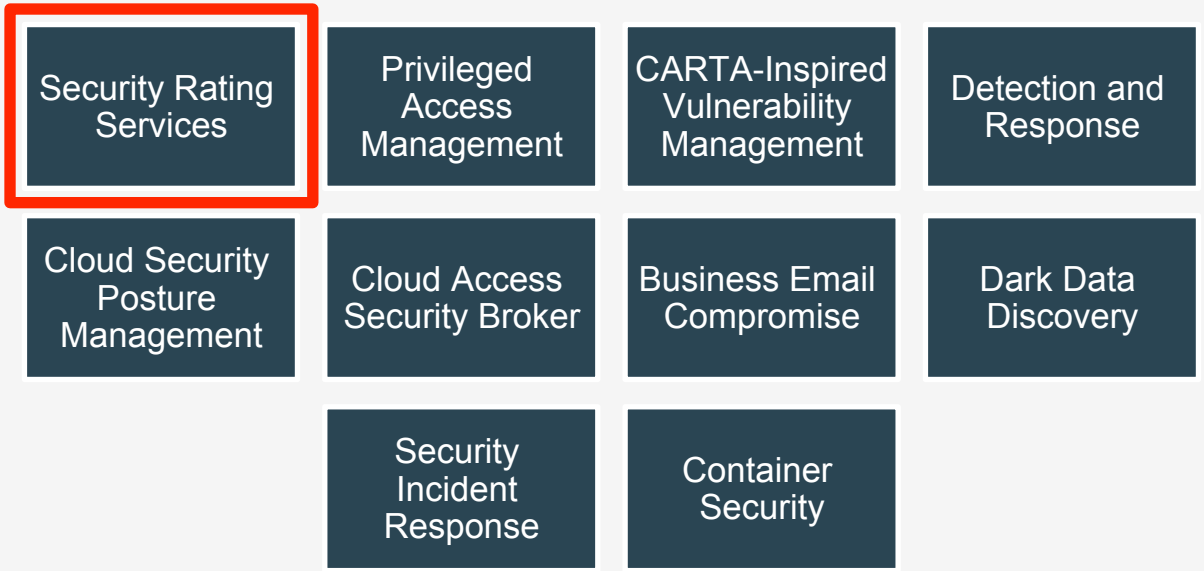
Auto-monitoreo

Incorporación de proveedores

Fusiones y Adquisiciones M&A

Ciberseguro

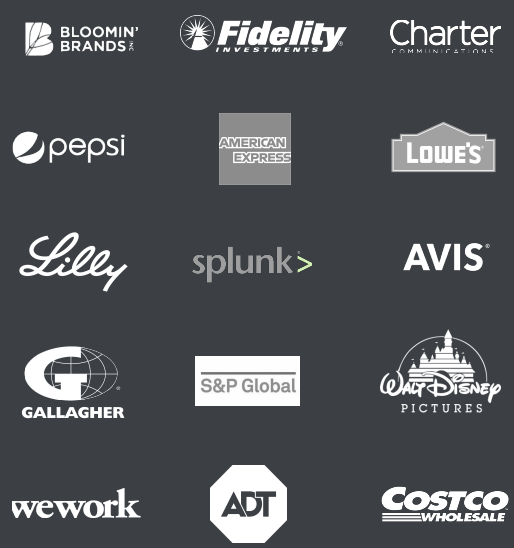
Los 10 proyectos de seguridad principales de Gartner 2019



Hoy cientos de clientes están monitoreando más de 150,000 organizaciones diariamente a través de SecurityScorecard

Gestión de la reputación, cumplimiento e informes ejecutivos

Gestión de riesgos de proveedores



Seguro cibernético y evaluación de riesgos cibernéticos

Somos confiables por:

- **7 de las 10 principales** compañías farmacéuticas son clientes de **SecurityScorecard.**
- **5 de los 6 principales** procesadores de pago eligieron a **SecurityScorecard.**
- **97% de los clientes recomiendan SecurityScorecard,** de acuerdo con **Gartner Peer Insights**, reconociendo su compromiso con el servicio al cliente.
- Los clientes calificaron **SecurityScorecard** con 4.6 de 5 estrellas en el G2, con una calificación de 9.7 de 10 para una fácil configuración y 9.9 de 10 para una atención al cliente de calidad.

TRUPHONE · NOKIA · entel · américa móvil · Claro · intel · Food and Agriculture Organization of the United Nations · UNHCR The UN Refugee Agency · ICC international criminal court · UNITED NATIONS UNCTAD · BoaVista SCPC · WORLD TRADE ORGANIZATION · UN WOMEN · ADB ASIAN DEVELOPMENT BANK · unicef · Banco de Chile · Goldman Sachs · [B]3 BRASIL BOLSA BALCÃO · Banco de la República Colombia · European Investment Bank The EU bank · sumup · cielo · crefisa · AMERICAN EXPRESS · GERU · AXA · GENERALI · MetLife · TOKIO MARINE INSURANCE GROUP · SoftBank Group · Takeda · NOVARTIS · pwc · EY Building a better working world · KPMG · AMADEUS · acciona · edp · pepsi · Neoway · Symantec. · izertis · bemol · NTT Group

... e muchos más!

El desafío de gestión de terceros

- Hacer vs decisión de compra ha sido tomada:
  - Las empresas compran + subcontratan siempre que sea posible
  - Los ecosistemas de los proveedores son enormes
- Los vendedores se convierten en una extensión de nuestro perímetro de ataque cuando nosotros:
  - Garantizamos acceso a la red
  - Compartimos datos confidenciales
- No tenemos visibilidad sobre la seguridad de terceros


Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
You

Estadísticas de incumplimiento de terceros

- 70% de las violaciones de datos son causadas por un tercero
- El costo por registro de incumplimiento de terceros es mayor año a año ($ 231 VS $ 188)
- 71% de las empresas no logran gestionar adecuadamente el riesgo de terceros
- 90% de las acciones anticorrupción del "DOJ" de los EEUU involucran terceros
- Las sanciones por incumplimiento son enormes, en ejemplo en la EU , € 800 millones por fallas de GDPR

Desafíos de la evaluación de terceros

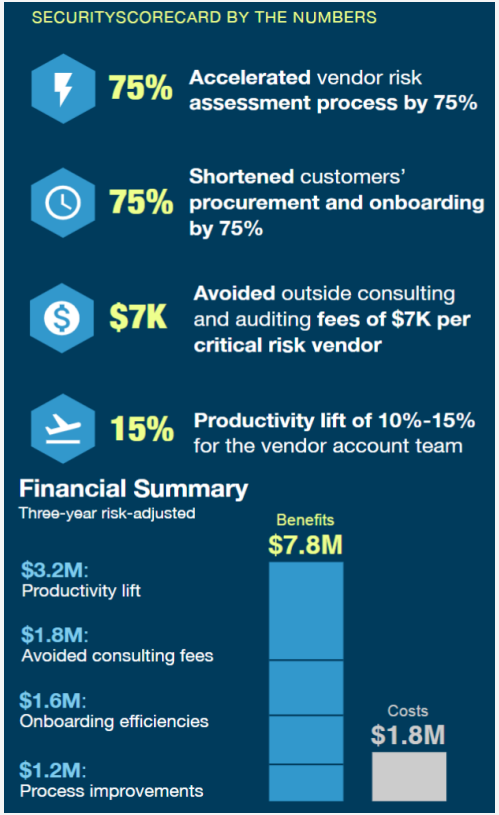
- Utilizamos mediciones estáticas <> la ciberseguridad es dinámica
- El riesgo de error humano es alto
- Las actividades requieren mucho tiempo + tener requisitos presenciales
- Los métodos son caros + carecen de escalabilidad

COVID-19 Challenges

- Increased number of Critical Vendors + need for Continuous Monitoring
    - SAAS vendors that support WFH = critical
- Companies rushing to onboard vendors to support WFH
    - Need are immediate + in-person assessment aren't viable
- Certain issues make companies vulnerable in a WFH environment
- Employees using BYOD from insecure IPs

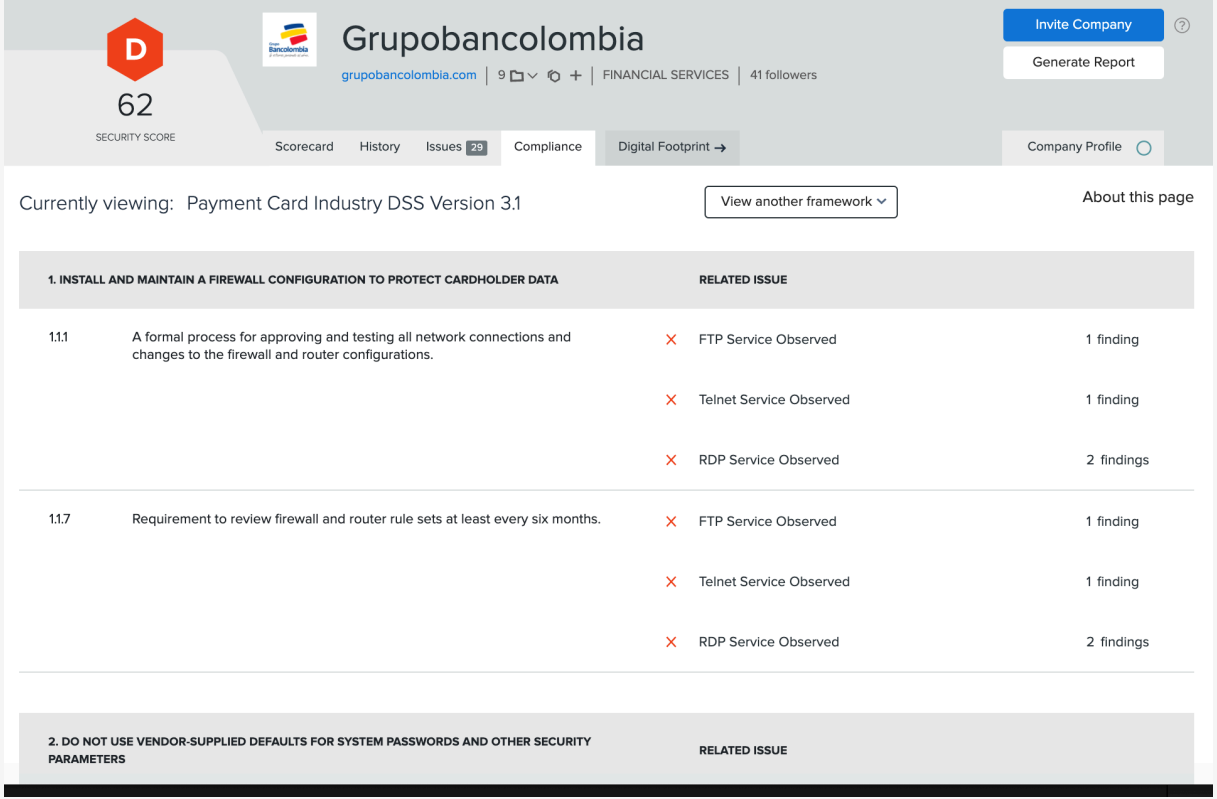
SSC for VRM: Real + Actionable ROI

- Shorten onboarding: Use grades to eliminate activities
- Eliminate unnecessary reassessments: Only survey if score is poor
- Reduce usage of costly 3rd parties: Engage only when needed
- “Right Size” Penetration Tests: Use scores to guide scope
- Simplify onboarding for low critical vendors: Use scores
- Shorten & Shrink RFPs: Eliminate companies with low scores



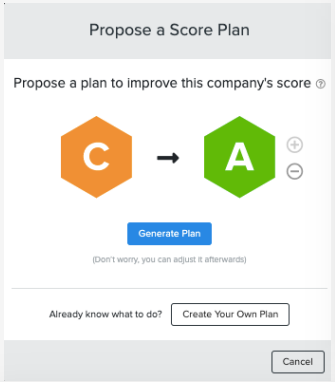
SSC for PCI: Gap Analysis + Monitoring

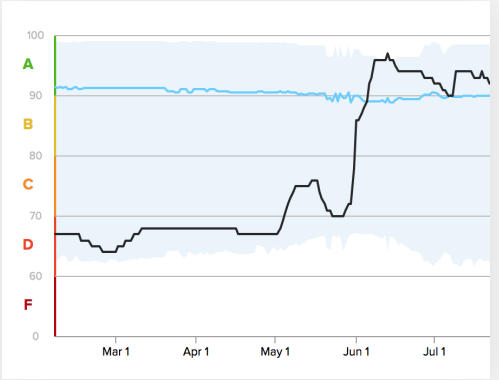
- Identify controls that are accessible from outside
- Map controls to relevant issue(s) in platform
- Instant measurement of 1st & 3rd party compliance
- Continuously monitor 3rd & 1st party compliance
- Satisfy PCI “Continuous Assurance” requirements

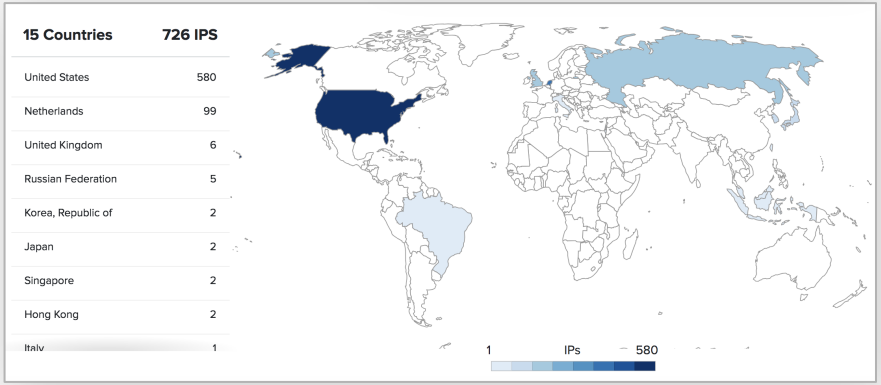


SSC for Self-Monitoring

- “Hacker-eye” view of your organization
- Identify and track publicly facing assets
- Grade assets + signals in accordance with NIST
- IP-Level detail for all issues surfaced
- Build remediation plans using score targets
- Visibility into historical scores + issues
- Receive alerts re: changes that require action
- Report to stakeholders + non-tech audiences







Summary Report

Security Summary Report

Report generated 4/27/20 by SecurityScorecard

We are sharing this independently-gathered confidential business insight that may help inform your policy decision.

A 90

Banco de Chile

bancochile.cl

Threat Indicators

A 92 **NETWORK SECURITY**
Detecting insecure network settings

A 100 **DNS HEALTH**
Detecting DNS insecure configurations and vulnerabilities

A 91 **PATCHING CADENCE**
Out of date company assets which may contain vulnerabilities or risks

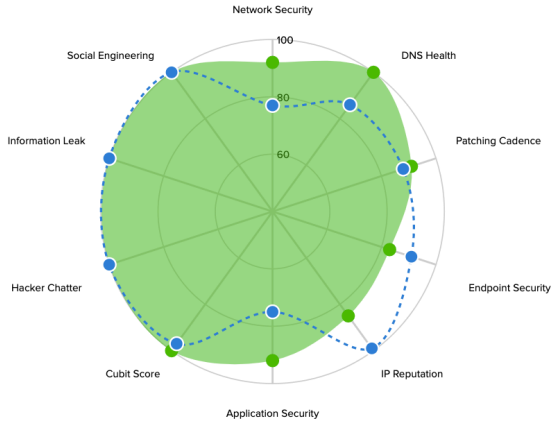
B 83 **ENDPOINT SECURITY**
Measuring security level of employee workstations

B 85 **IP REPUTATION**
Detecting suspicious activity, such as malware or spam, within your company network

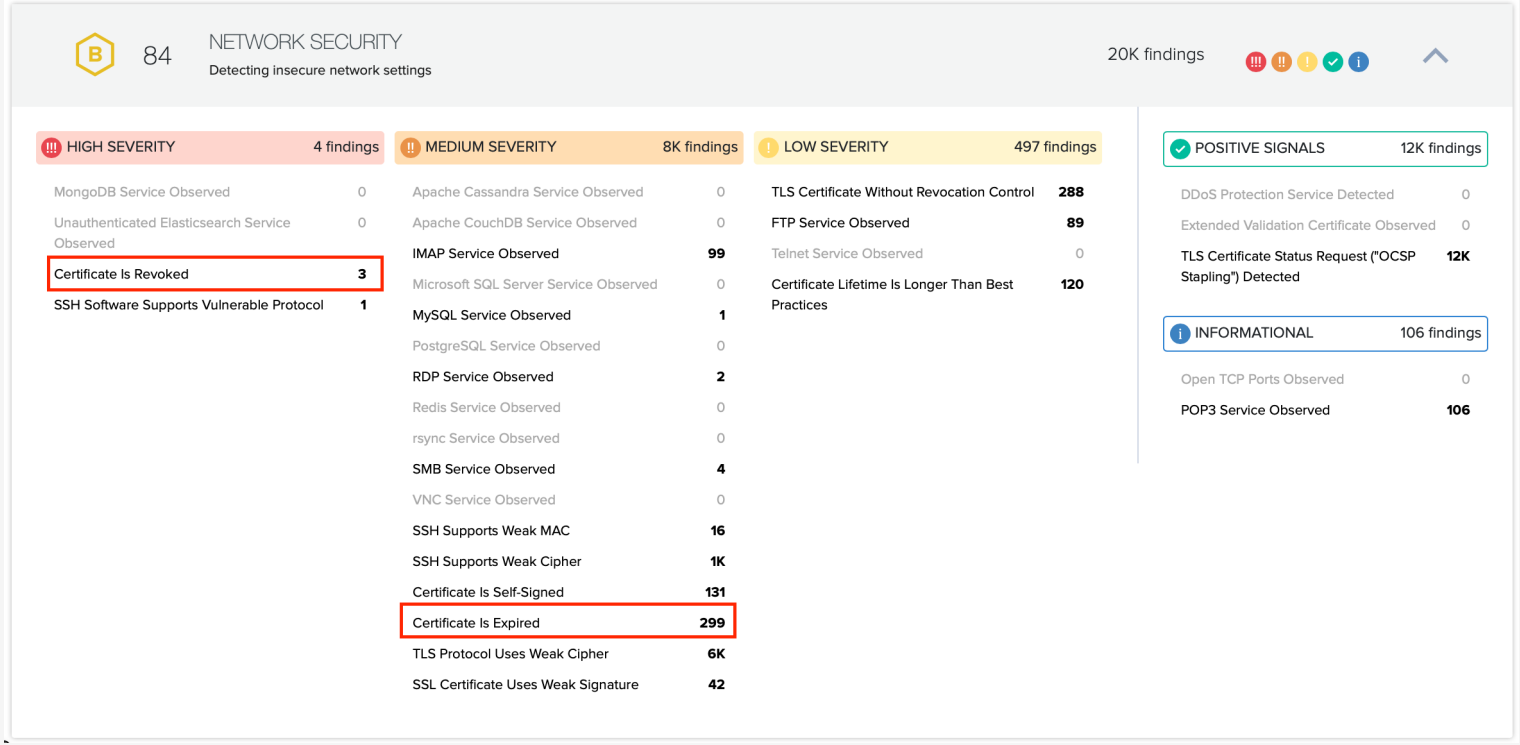
A 92 **APPLICATION SECURITY**
Detecting common website application vulnerabilities

A 100 **CUBIT SCORE**
Proprietary algorithms checking for implementation of common security best practices

Industry Comparison: Financial Services



Risk Factor View

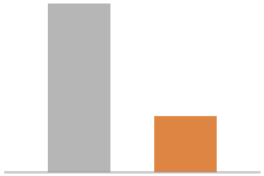


Issue-Level View

COMPARISON TO SIMILAR COMPANIES

54% have this issue, **just like this company**

46% do not have this issue



45 findings on average

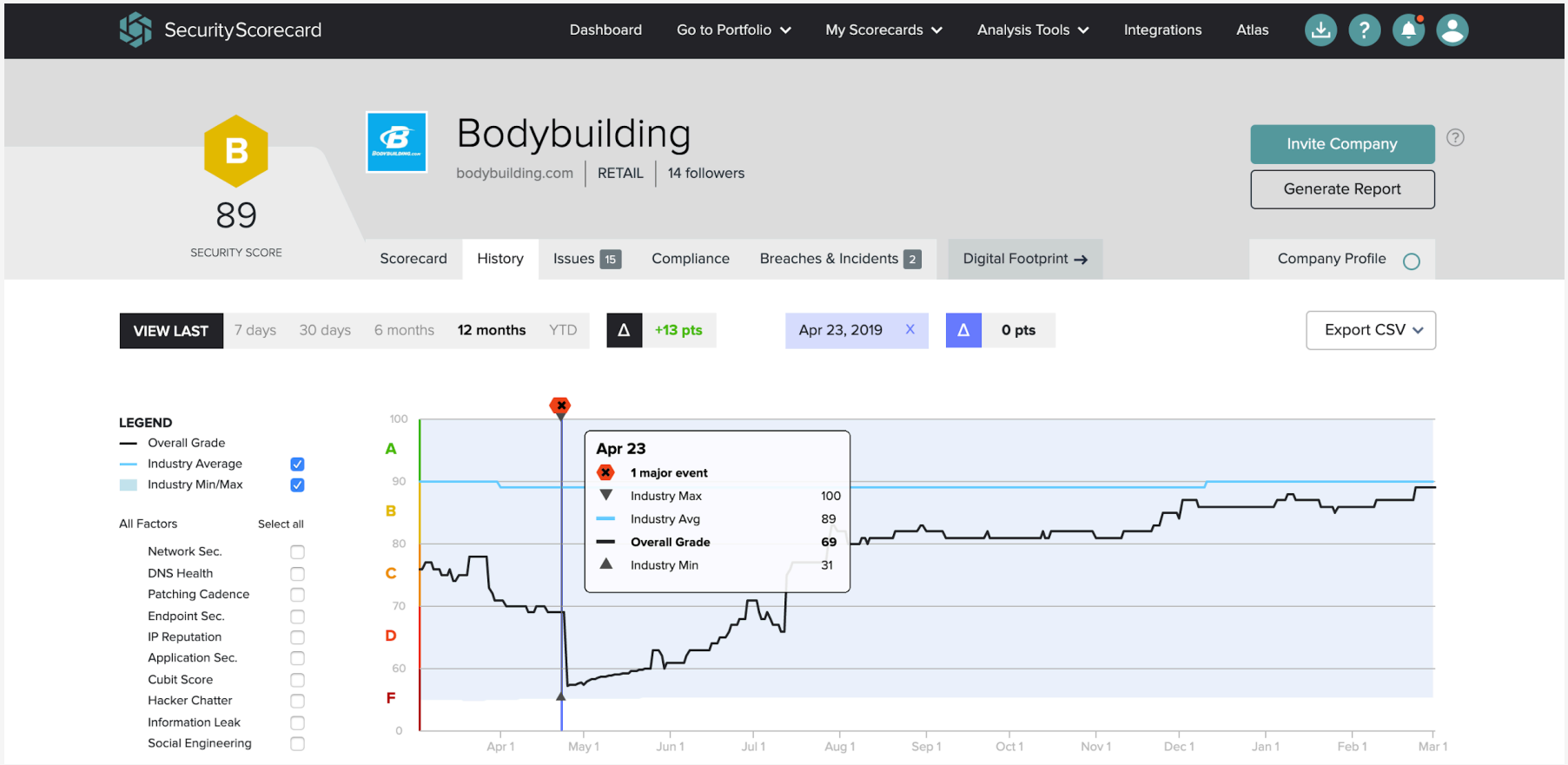
15 findings for this company

15 findings Download as CSV

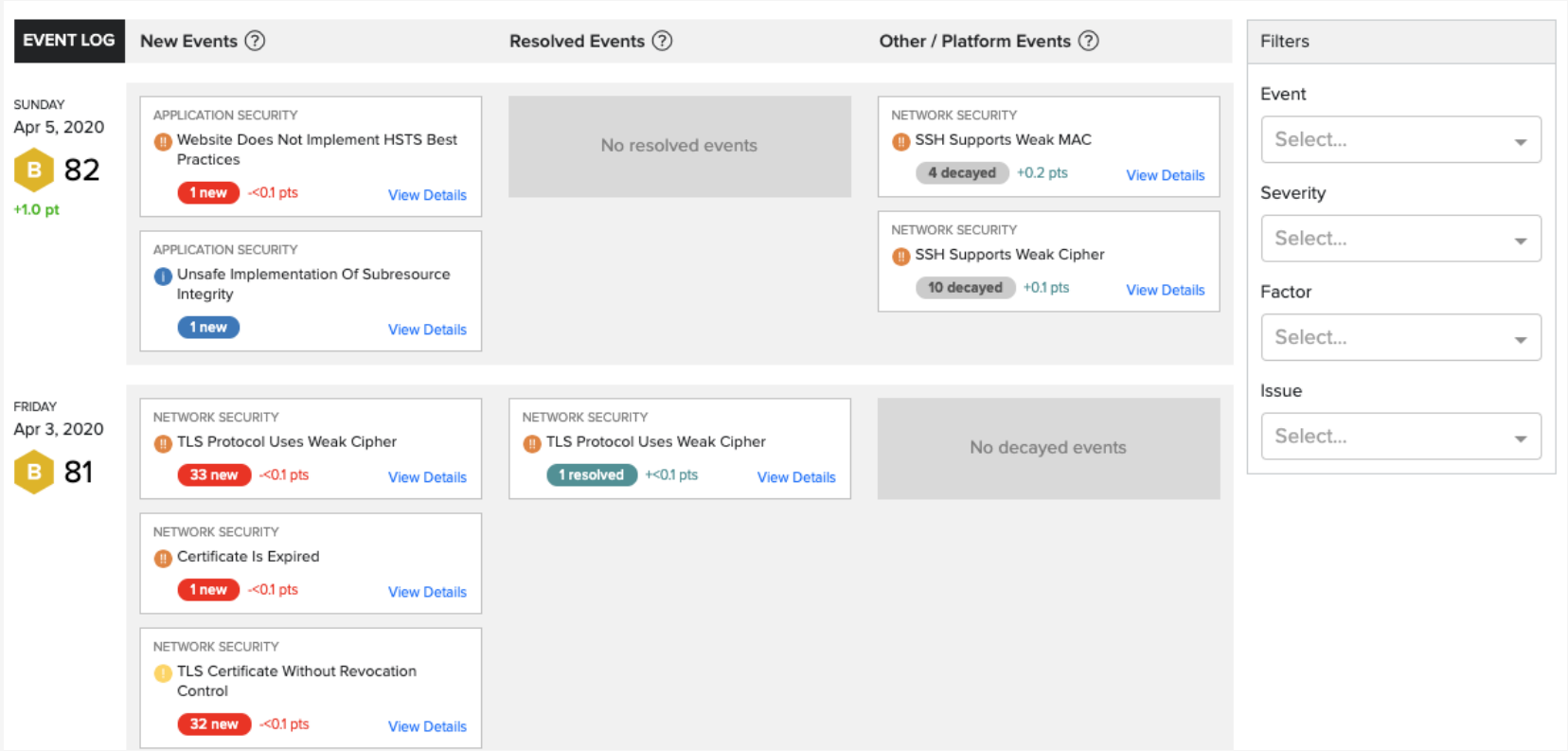
Resolve

	VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY DESCRIPTION	VULNERABILITY PUBLISH DATE
☐	CVE-2017-3737	35.160.114.188	443	Feb 10, 2020 10:33:33 am	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.	Dec 7, 2017

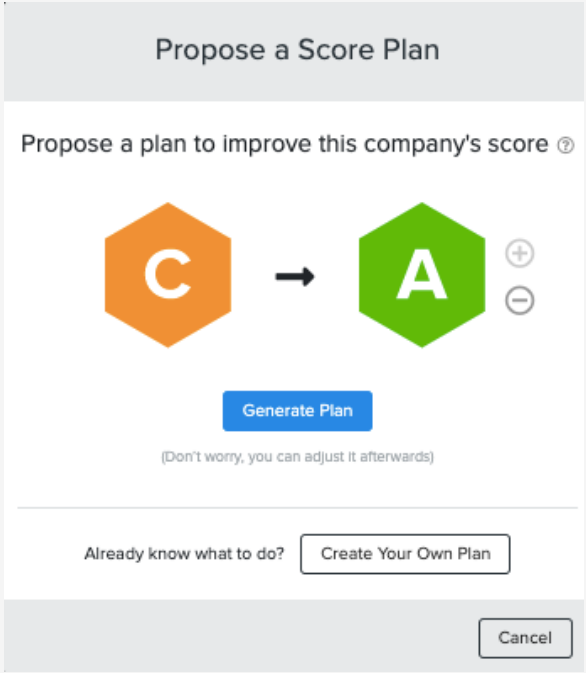
Score History View

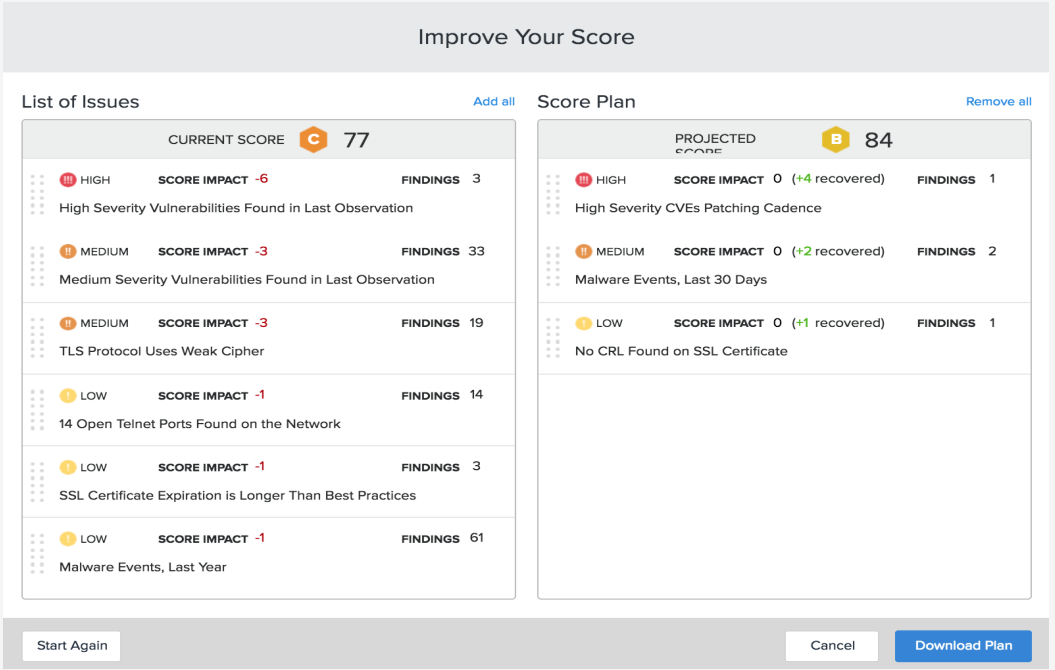


Event Log View



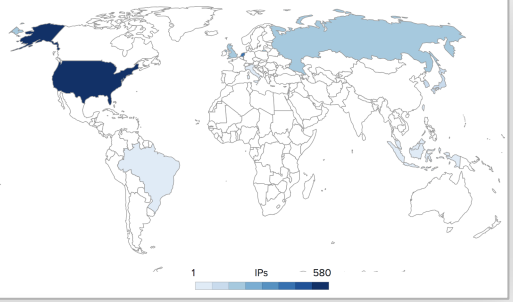
Prescriptive Remediation Plans





Digital Assets Views

15 Countries	726 IPS
United States	580
Netherlands	99
United Kingdom	6
Russian Federation	5
Korea, Republic of	2
Japan	2
Singapore	2
Hong Kong	2
Italy	1



IP ADDRESS	LOCATION
2.21.103.14	ZA
42.119.185.72	VN
118.68.81.92	VN
3.210.250.43	US
3.220.185.227	US
3.232.62.86	US
13.91.40.166	US
13.109.162.190	US
13.109.167.128	US
13.111.18.27	US

2.16.39.11

CDN / Shared IP

Remove IP

Attributed to **mindbodyonline.com** (Next observation on **Apr 19, 2020**)

Issues 1 | IP Details

SSL CERTIFICATE

Name	MindBody, Inc.
Domain	mindbodyonline.com
Location	San Luis Obispo
Common Name	*.mindbodyonline.com
Key Type	RSA
Key Length	2048
Issued By	DigiCert Inc
Time of Validty	02/13/2019, 12:00 am - 01/25/2021, 7:00 am
MD5	713d563210d10bfeec35e917d9e5b0e3
SHA1	297da004effd3602d9937ee54052486a56fabef6
Subject Alternative Names	*.mindbodyonline.com, mindbodyonline.com

Last updated: 03/05/2020, 8:02 pm

Show Full Source

To determine this finding we considered data from these sources:

- NA WHOIS
- ✓ **SSL Certificate**
- NA DNS Lookup
- NA Published Data
- NA SSC Research
- NA Third Party

Q&A

Jose Ferreira da Costa
Latam Regional Director
jcosta@securityscorecard.io

XXXXXXX
xxxxxxx@xxxxPARTNER.com

Competitive Differentiators

	SecurityScorecard	Other Security Ratings
Breach Insights Concentrated Risk	✓	X
1,000,000+ companies rated	✓	X
Rate any new company, even SMB, not in a database in minutes	✓	X
Robust API and bulk for security intelligence data exporting	✓	–
ThreatMarket engine collects our own data going into a score	✓	X
Score Planner showing steps to get an "A"	✓	–
Integration Center with 3rd party apps (ServiceNow, Splunk, Qradar, etc.)	✓	✓
Compliance Mapping	✓	–
4th party risk	✓	X
Risk exchange repository with AI analytics for internal data	✓	X
Customizable Alerts	✓	✓