WHITEPAPER

Security Ratings Methodology for Telecommunications, Internet Service Providers, and Cloud Providers

Security ratings: A new horizon

CONTENTS

Introduction

Telecom companies, internet service providers, and cloud providers (TICPs) are a pillar of modern connectivity, linking people and companies across the globe. However, these indispensable industries are also prime targets for nation-state actors and motivated cybercrime groups.

And new SecurityScorecard research underscores the urgency for a transformative approach: **A staggering 78% of the top telecom companies in the U.S., U.K., France, and Germany experienced a third-party data breach in the past 12 months alone.** These eye-opening findings emphasize the critical need for a transformative approach to cyber risk management. In light of this, SecurityScorecard, in partnership with industry leaders, is pioneering a new approach to advance security ratings for TICPs.

We chose to enhance our algorithm for telecom companies, ISPs, and Cloud Providers because we recognized that the complexity of their networks demands a bespoke approach. TICPs operate in a highly complex digital ecosystem because, simply put, networks are their products.

T-Mobile

"At T-Mobile, building cybersecurity into everything we do is a critical part of our mission to be the best at keeping customers connected to their world. security ratings are an essential tool that we and other wireless providers use to help create a safer digital ecosystem for our customers, partners and beyond. We applaud SecurityScorecard for their proactive efforts to advance security ratings for the telecom industry, and we believe that together, we can set new standards for cybersecurity."

Jeff Simon,
SVP & Chief Security Officer, T-Mobile

"SecurityScorecard has been an indispensable partner. The company's commitment and dedication to understanding the unique challenges faced by our industry will greatly contribute to our cybersecurity strategy. This collaboration will empower us to strengthen our security posture and foster a sense of shared responsibility across for cybersecurity."

Shinichi Yokohama,
Chief Information Security Officer, NTT

Setting the standard for security ratings

SecurityScorecard, in collaboration with industry giants like NTT, will unveil the first standardized security ratings methodology tailored specifically for these industries. Our security ratings offer a standardized measurement for cybersecurity to foster transparency and trust across the digital ecosystem.

Our security ratings help organizations see weaknesses from hackers' perspectives and strengthen their defenses. We empower organizations with valuable insights into their cyber risk by continuously monitoring open ports, operating system patches, and security posture of the third-party vendor ecosystem.

This paper dives into the tailored scoring methodology we've engineered to align with the unique security landscapes and operational practices of TICPs. We embrace input and feedback, encouraging an evolving approach in tandem with the industry's dynamic nature.

Core principles: Our guiding light

Our mission is to create a safer world. This mission resonates with our dedication to extending security ratings to all organizations, irrespective of customer status. This ensures equal opportunities to enhance data and edit asset categorization.

Transparency is embedded in our ethos. We are resolute in making our methodologies accessible to all without NDAs or restrictive barriers. This commitment underscores our shared journey towards a safer world.

"Cybersecurity risk ratings are key to effectively measuring cyber resilience, and SecurityScorecard is the first to assess organizations based on their unique business models and threat landscapes. These enhancements help ensure that security ratings accurately reflect the complexity of telecom infrastructure. I applaud both SecurityScorecard and the telecommunications industry for their collaborative approach to creating a safer digital ecosystem."

Frank Cilluffo,
SecurityScorecard Advisor

Collaboration: Our path to a safer digital world

Traditionally, telecom companies, ISPs, and Cloud Providers received low cybersecurity ratings due to the intricacies of their digital footprints, often leased to third parties. Consequently, TICPs invariably received low scores across all Security Rating providers, which led to skepticism regarding the overall accuracy of security ratings for these industries.

Security ratings have the power to restore public trust in cybersecurity because they provide a universal and easy-to-understand measurement. In partnership with industry leaders, SecurityScorecard has identified ways to enhance our scoring algorithm, which includes our attribution methodology, to reflect the realities of TICPs' ecosystems.

To ensure fairness and accuracy for these industries, we advocate for three fundamental changes for scoring TICPs across all security ratings companies:

1

Enhancing accuracy with network partitioning

Our approach involves assessing scores solely on corporate assets, excluding customer assets. This granularity ensures a more precise representation of a company's security posture.

2

Introducing industry-specific scoring

Acknowledging the unique dynamics of TICPs, we introduce industry-specific scoring. Our new industry-specific scoring algorithm takes into account the nuances of different industries.

3

Integrating user-contributed data

Our methodology also integrates user-contributed data from organizations, incorporating achievements such as certifications, penetration testing, and cybersecurity training.

Defining the approach

We believe that these sectors' unique challenges call for a tailored approach to security ratings. Let's dlve into the specifics of these changes:

1. ENHANCING NETWORK PARTITIONING

Currently, TICPs are evaluated on all assets they own, such as IPs and domains – even if their customers control the majority of these assets. As a result, their scores end up reflecting their customers' cyber posture instead of their own.

To solve this, we will exclude customer assets from the digital assets scored. This decision is because customer assets are outside of these organizations' security policies, operational authority, and control, thus posing limited risk to the company. Through segmenting IPs with our proprietary AI model, we use all of our existing insights to determine corporate allocations.

For example:

- Is the digital asset being scored hosting the ISP's corporate infrastructure?
- Are they the ultimately responsible party?

This nuance distinguishes a good cybersecurity ratings company from a bad one and SecurityScorecard from other security ratings providers.

To ensure the highest level of security and privacy, we provide a secure mechanism for companies to communicate their asset classification details confidently. All information shared will be treated as confidential and used solely for the purpose of accurate asset categorization. Assets designated as customer assets will remain private. We advocate for the adoption of this approach by all security ratings companies to ensure precise evaluation of security posture.

About SecurityScorecard network partitioning:

Scoring only corporate assets

For TICPs, we're changing our approach to scoring assets. We'll focus only on scoring the assets directly managed by the company. The assets controlled by their customers won't be considered in the score. SecurityScorecard uses a combination of heuristics and generative AI methods to automatically detect and categorize assets that are leased to third parties. Some of these categories include:

- Residential and mobile IP ranges
- Content Delivery Networks (CDN)
- Shared hosting infrastructure
- Colocated server infrastructure and leased IP ranges

When an asset is identified as falling into one of these categories, SecurityScorecard applies a label that is only visible to the parent organization but not visible to the outside world. This ensures that the parent organization can effectively audit the digital footprint detected by SecurityScorecard and understand how various assets impact their overall score while maintaining customer privacy.

Unengaged and Engaged companies

SecurityScorecard is committed to working closely with engaged companies. We will actively support and empower these companies to modify asset categorization for individual or bulk assets. Any asset a TICP identifies as belonging to a customer will be excluded from their score. In order to maintain our position as a trusted, neutral party, SecurityScorecard conducts regular audits utilizing automated and manual processes to ensure that the categorization of customer assets remains accurate.

For companies that choose to engage with SecurityScorecard, we will provide a streamlined onboarding process that includes comprehensive asset categorization. This applies to new customers and those already part of the SecurityScorecard network.

By limiting scoring only to corporate assets, the accuracy and score should greatly improve. If a company disagrees with our asset categorization, they have the option to collaborate with us at no cost to them.

For companies that choose not to engage, SecurityScorecard will continue actively identifying and categorizing assets belonging to the parent organization or third parties. This asset categorization will still be subject to random audits to ensure quality. However, there is still the possibility that we will classify an asset incorrectly.

As part of our ongoing commitment to precision, SecurityScorecard invites companies to participate actively. Through this engagement, we can continually enhance our categorization methodology, resulting in benefits for all participants.

Protecting privacy and security: Confidentiality of customer assets

TICPs place the utmost emphasis on safeguarding customer privacy. As a measure to uphold this commitment, all customer assets are treated with the highest level of confidentiality.

We are introducing a feature that empowers TICPs to comprehensively view their digital footprint, encompassing both customer and corporate assets. This feature will be exclusively accessible to the individual company, ensuring that the sensitive data remains confidential and secure.

In certain instances, companies might seek to access information about findings related to customer assets (e.g., malware), even if those assets are not scored. SecurityScorecard will allow organizations to access these findings discreetly, keeping them exclusively available to the company and maintaining the highest levels of privacy within the SecurityScorecard platform.

We understand that companies conduct security tests and operations, including honeypots. If assets used for security operations were to be scored, it could affect the company's overall score. To address this, we are committed to collaborating with organizations to establish solutions that prevent these assets from being scored.

Presently, companies have the capability to create private Scorecards for their internal use, granting exclusive visibility to the company only. We are expanding this feature by implementing role-based access control (RBAC) for different Scorecards. This enhancement allows companies to selectively grant visibility of customer assets solely to specific employees as needed.

2. INTRODUCING INDUSTRY-SPECIFIC SCORING

We are proud to introduce an industry-specific scoring methodology that takes into account the nuances of different industries. This enhanced method has two modifications over our previous approach:

1. **Industry-specific factors:** Items that are either irrelevant or not as correlative with incidents given the relevant industry.
2. **Industry-specific cohorts:** Applying these different weights across companies who have the same business practices regarding renting internet infrastructure.

Because of the nature of their business telecom, internet service providers (ISPs), hosting providers, and cloud providers may need to provide services that would otherwise be viewed as risky. Take for instance, "open DNS resolvers." An open DNS resolver is a DNS server that responds to queries from any IP address on the internet. For most companies, this would be considered a security risk because it increases the likelihood of accidental information disclosure that could be used to further an attack. However, for these companies, it is an essential component of their business. SecurityScorecard recognizes this nuance and will only apply the relevant factors specific to a given industry.

These industries can be scored very accurately, yet they pose distinctive challenges that require a refined approach. The problem isn't cybersecurity ratings; it's ratings companies that rely upon human effort, treat all companies the same, or utilize unsophisticated methods.

3. INTEGRATING USER-CONTRIBUTED DATA

Cybersecurity is not a static pursuit; it's a journey of continuous improvement. While external signals offer critical indications into an organization's cyber health, we acknowledge that certain security efforts come from sources that are not easily scannable. Our new scoring methodology also factors in certifications, pen testing, and cybersecurity training.

Championing comprehensive cybersecurity efforts

Certifications such as SOC 2 or ISO 27001, along with proactive measures like penetration testing, lay the foundation for enhanced scores — an embodiment of progress and commitment to cybersecurity.

As part of our ongoing evolution, we provide a secure repository for certifications like SOC 2 and ISO 27001 in our Evidence Locker. While these certifications are presently included on Scorecards without directly impacting scores, we're exploring avenues to enable organizations to improve their scores with these badges of security excellence.

Valuing the impact of penetration testing

The varied tiers of penetration testing efforts — ranging from baseline to advanced — reflect different levels of dedication to security. As we consider introducing the option to upload pentest results, we envision a scaling mechanism that awards a more significant boost to organizations that undertake comprehensive security measures, encouraging a proactive cybersecurity ecosystem.

Recognizing cybersecurity training

Organizations invest in training programs to defend against phishing and social engineering. Our journey forward involves providing organizations with ways to validate their cybersecurity training efforts. By aligning scores with training programs, we champion holistic cybersecurity.

Looking ahead, we aspire to incorporate a broader spectrum of user data into our scoring framework. This collaborative journey seeks to define and integrate additional data points, ultimately enhancing the scoring granularity and rewarding comprehensive cybersecurity.

SecurityScorecard AI analysis

SecurityScorecard provides an objective method to continuously monitor the cybersecurity practices of organizations, including their vendors. SecurityScorecard assesses whether an organization's security posture is improving or deteriorating over time. To achieve this, our algorithm leverages AI techniques to fine-tune the weighting of various scoring factors. This ensures that the overall score aligns optimally with the relative likelihood of a data breach.

SecurityScorecard scores are computed as a weighted average of 10 factor scores, each evaluating a distinct aspect of an organization's cybersecurity posture.

THESE FACTORS ARE:

1. Application Security
2. Cubit Score
3. DNS Health
4. Endpoint Security
5. Hacker Chatter
6. IP Reputation
7. Information Leak
8. Network Security
9. Patching Cadence
10. Social Engineering

The numeric values for these factors weights were initially determined by cybersecurity experts. Subsequently, SecurityScorecard applied machine learning to adjust the factor weights to optimally align the score with the likelihood of a breach.

As an organization's grade decreases, the likelihood of experiencing a publicly disclosed breach increases. Utilizing the ML-tuned factor weights, we found that organizations graded as 'F' were 7.7±0.9 times more likely to experience a breach compared to those with an 'A' grade. This analysis underscores the effectiveness of our Machine Learning-driven approach in providing actionable insights into an organization's cybersecurity risk.

Your input is invaluable as we collectively navigate the ever-evolving landscape of cyber threats.

Why partner with us? A roadmap defined by partnership

We believe in co-creating the future of cybersecurity. Collaborating closely with organizations is our modus operandi, and their input fuels our continuous improvement. Together, we'll steer the conversation on cybersecurity through joint keynote talks and thought leadership.

Availability

The enhanced scoring algorithm is available now globally. In 2023, we applied this specific algorithm on an on-demand basis.

Your voice matters: Join the conversation

We are inviting both customers and non-customers to share their insights and perspectives.

REACH OUT TO US AND CONTRIBUTE TO SHAPING THE FUTURE.
Email our CEO & Co-Founder: alex@securityscorecard.io

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com
United States: (800) 682-1707
International: +1(646) 809-2166