SecurityScorecard

# The Legality of SecurityScorecard Data Collection

European Market Edition

SecurityScorecard.com
info@securityscorecard.com

214 West 29th St, 5th Floor
New York, NY 10001
1.800.682.1707

# Executive Summary

SecurityScorecard delivers security ratings that empower enterprises to instantly and accurately monitor, assess and understand their own cybersecurity posture as well as the cyberhealth of all vendors and business partners in their ecosystems.

SecurityScorecard does not collect or use personal data or other personal information related to its product offerings, which limits the applicability of the General Data Protection Regulation (GDPR) to its B2B operations. However, as part of its alignment with best business practices, SecurityScorecard is committed to compliance with GDPR and all applicable U.S. federal regulations, including the Federal Trade Commission (FTC) Act, the Computer Fraud and Abuse Act, and the Electronic Communications Privacy Act, which dictate how SecurityScorecard acquires, uses and discloses data. Since SecurityScorecard engages with clients in heavily regulated industries that are subject to GDPR and U.S. federal laws on personal data privacy, the company also focuses on requirements of laws that impact customers and how those laws apply to its own business operations.

SecurityScorecard believes it is critical to be responsible, transparent and compliant with applicable global and federal laws, and respectful of third-party notices and agreements regarding data collection, storage and aggregation. SecurityScorecard understands that the collection and protection of data in accordance with applicable laws and identified best practices is not only a legal requirement but is also key to business success and of paramount importance to customers. SecurityScorecard remains committed to ensuring adherence to all laws and regulations, and providing customers with information that helps them reduce risk and enhance security.

# General Data Protection Regulation

GDPR, effective May 25, 2018, replaces the 1995 Data Protection Directive (DPD), a patchwork of national laws, with a single legal framework to protect the privacy and security of EU citizen personal data. GDPR supersedes all laws passed by EU member states and it applies to every organization that accesses, collects, processes or uses personal data of EU residents in any way, within or outside the EU.

**Personal Data:** *Any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Examples include but are not limited to name, home address, email address, identification card number, location data, IP address, cookie ID, financial data, medical information, and much more.*

# How does SecurityScorecard collect data to calculate scores?

SecurityScorecard uses its proprietary data engine, ThreatMarket, to collect threat data from multiple intelligence feeds and identify vulnerabilities across the internet. **The company collects only externally accessible and publicly available data, and only nonintrusive techniques are used to gather information.** "Collection" in this context refers to the use of tools like scans, data feeds, sensors, honeypots and sinkholes. In addition, SecurityScorecard uses external surveillance methods, which look at the following critical threat indicators:

- Web Application Security
- Network Security
- Endpoint Security
- DNS Health
- Patching Cadence
- Hacker Chatter
- IP Reputation
- Leaked Credentials
- Social Engineering
- Cubit Score

Collection also refers to using SecurityScorecard's proprietary technology to interact with IP addresses and other communication ties that companies create to post data and information, and to provide access between a company's network and the internet.

## How does SecurityScorecard protect data?

SecurityScorecard employs the following security controls to protect data:

- Network isolation techniques
- Encryption for data at rest (AES 256) and in transit (HTTPS and TLS 1.2)
- Strong user authentication protocols including two-factor authentication and least privilege and division of duties access controls

SecurityScorecard performs background and criminal checks on all employees and educates them via security awareness programs and annual training on published security and privacy policies and standards. Additionally, all employees and business partners sign strict non-disclosure agreements (NDAs) and other contracts, which include requirements regarding the protection of sensitive data.

## How does SecurityScorecard protect its platform?

SecurityScorecard maintains protection and security during customer engagement with the platform by providing access and user controls. The platform allows customers to limit access via user and admin profiles. Read-only access allows users to view but not alter company profiles or portfolios, which can also be set to “Private,” making them visible only to the portfolio creator. The platform can also be integrated with the customer’s single sign-on software.

SecurityScorecard does track customer activity within the platform to better understand how users operationalize the offering. This capability can be turned off at any time per customer request.

# Website Scanning Legal Issues

## *Overview*

An emerging class of cybersecurity rating solutions is helping companies assess their own security posture as well as the cyberhealth of vendors and partners in their third-party partner ecosystems. Security rating solutions collect a broad range of relevant data, deploying active scanning techniques to monitor the cybersecurity of publicly accessible systems. When companies learn that their public digital assets have been "actively scanned," they often ask about the legality of that process. This paper was developed to provide perspectives on this topic from industry and legal experts, as well as SecurityScorecard.

## *Nonintrusive Versus Intrusive Network Scanning*

Nonintrusive or passive scanning techniques utilize standardized and publicly available network-based protocols to query hosts and learn one or more attributes about the host. Examples of passively scanned attributes include:

- **Open Ports:** Networked applications typically communicate via a "network port," using one of the 65,536 available TCP ports. For example, web traffic typically uses TCP port 80. Similarly, secure web (HTTPS) typically uses TCP port 443. Security practitioners recommend configuring public digital assets to deny all TCP ports except those that are actively in use. Scanning ports helps determine if ports have been inadvertently left open and susceptible to vulnerabilities.
- **SSL Certificates:** SSL certificates provide encryption keys that enable encrypted network communications. Security practitioners and online providers like Google recommend that public websites that transmit sensitive data ensure HTTPS (i.e., secure web communications) is in use and that SSL certificates are current. Scanning for SSL certificates helps validate that sites are using appropriate SSL certificates.

- **Web Content:** Browsing the "web" has become ubiquitous. Information that a company displays on its public website can reveal information security concerns. For example, publishing an individual's email address on a public site can expose the person or company to unwanted SPAM. Scanning a website for public information helps assess web content that could pose a security risk to the company.

The above three types of scans are considered "nonintrusive" since the data they collect is publicly available and accessible by anyone using a web browser or other programmatic methods. In contrast, intrusive or active scans often attempt to compromise a system and thereby highlight a security vulnerability. For example, a nonintrusive scan might determine there is a login capability available on a web server whereas an intrusive scan might attempt to login using common usernames and passwords, or attempt multiple failed login attempts to ensure the configuration of account lockout settings in place. Penetration tests often use intrusive methods to uncover potential vulnerabilities to a host. Solutions that claim to be using only noninvasive techniques should not perform penetration tests or deploy intrusive scanning methods.

## *Public Versus Private Data*

The use of cloud-based services (e.g., software, infrastructure and platform as a service) and sophisticated websites have blurred the demarcation between networking and security. **Public data** is any information that is known to be available for public consumption. In contrast, **private data** is any information that should not be available publicly (e.g., records considered private by some defined entity). Organizations should work diligently to ensure sensitive data is not displayed or made available on any public-facing host. Similarly, all private data should be accessible only after a user properly authenticates to a host. Additional layers of multifactor authentication

can increase the security of private data. A nonintrusive scanner should not attempt to authenticate to a host. The demarcation between public versus private data is an important consideration when assessing the legality of an entity that is performing active scanning. Opinions on the legality of nonintrusive scanning vary depending on the type of legal proceeding (e.g., criminal versus civil) and legal jurisdiction (e.g., U.S. versus EU).

## *EU Jurisdiction*

Beyond the personal data privacy laws dictated by GDPR, European governments can establish their own laws regarding network security and port scanning. Many emerging laws focus on reducing cybercrime. For example, Germany and England have enacted strong legislation. It is beyond the scope of this article to cover all EU laws that could provide the basis for litigating port scan activity. However, it is important to note that industry and legal scholars recognize that the legality of security scanning should be measured based on intent. Any intention to interrupt the confidentiality, integrity and availability (CIA) of digital assets is illegal. In contrast, any intention to use nonintrusive scans to detect and report system vulnerabilities – as often done by ethical hackers – is seen as a positive contribution and not perceived as being illegal.

## *Industry Perspective*

An informative article on this topic is available from the SANS Institute, supporting much of the information discussed in this paper, but in more depth.

Since chatty scanning (i.e. scanning thousands of ports) can impact host integrity and availability, and scanning multiple times in a short time frame can be viewed as unacceptable, security experts recommend tightly scoping scanning activities in terms of their frequency and depth. These practices can reduce or eliminate a company's concerns regarding ethical port scanning activities.

## *SecurityScorecard Perspective*

SecurityScorecard has invested heavily in developing a security rating solution that relies entirely on security telemetry data that is available in the public domain and is acquired using nonintrusive scanning methods. SecurityScorecard continually interfaces with legal experts on the methods and techniques in use to ensure the ethical collection of all data. SecurityScorecard maintains a staff of industry security experts to continuously verify that data gathering practices are nonintrusive and transparent. Any company can obtain its SecurityScorecard at any time and review the security data collected for the company's digital assets. SecurityScorecard empowers companies to manage their cybersecurity risk using a wealth of public security-related data that is already available to hackers. SecurityScorecard recognizes the sensitivity around this topic and is committed to transparency in all scanning activities.

# Summary

Port scanning is not new. It has been a foundation of information security since the advent of computer networks. The legal lines for port scanning usually align with the scanner's intent. Hackers typically use scanning to perform an illegal act that compromises the integrity, confidentiality or availability of systems. Legal activities include ethical (white hat) security professionals focused on discovering and reporting system vulnerabilities that hackers could use for illicit purposes. SecurityScorecard is committed to full transparency in this area and is helping thousands of companies manage the cybersecurity health of public digital assets using ethically and publicly sourced security data, including nonintrusive scanning techniques.