Enterprise Cyber Risk Management

Digital acceleration has catapulted businesses beyond the safe walls of the corporate network to rely on third parties and the cloud more than ever before. This has left security teams scrambling to uncover, understand, and quantify the dangers in their expanded attack surface, leaving them at risk to attacks from sophisticated adversaries. Not only were there 31% more cyber attacks in 2021 compared to the previous year but the industry has seen a significant focus on exploiting vulnerabilities of public-facing assets.

31% MORE

cyber attacks in 2021 compared to the previous year

Partner with experts to **minimize your cyber exposure** with a clear and contextual view of your attack surface

Traditional approaches of point-in-time assessments and reactive threat hunting can no longer scale to address the modern attack surface. New technologies have emerged to manage exposure to cyber risk; however, most only address one problem at a time. While some technologies lack the ability to effectively measure risk, others lack the contextual intelligence to provide actionable insights to stop threats or offer a clear path for remediation. To reduce their attack surface, organizations need to turn to a cohesive, intelligent solution that includes expertise to test if your cyber defenses are up for the battle and are resilient.

Industry's Most Comprehensive Enterprise Cyber Risk Management Solution

See What an Adversary Sees

SecurityScorecard provides the industry's most comprehensive Enterprise Cyber Risk Management solution that allows you to stop a cyber attack before it happens. See what an adversary sees with context-rich threat intelligence and human-led analysis to reveal unknown assets, critical vulnerabilities, and active threats. Turn knowledge of your cyber risk exposures into action, empowering your team to make informed decisions faster and speed remediation times. Alleviate future risk by quantifying and reporting on your security program, allowing you to increase cyber risk transparency with stakeholders and build cyber resiliency. Partner with SecurityScorecard, the leading security ratings and cyber resilience services provider, that is uniquely guaranteed to reduce your likelihood of a breach 7.7 times.

guaranteed to reduce your likelihood of a breach by **7.7x**

Business Benefits

Discover Your External Attack Surface by proactively taking control of your public-facing assets and exposing critical vulnerabilities delivered by the industry's most trusted security ratings platform.

Uncover Actionable Insights To Guide Response with context-rich threat intelligence derived from an adversarial point of view and attributed to your organization.

Respond Faster to Threats by Partnering with Industry Experts who can test the effectiveness of your security controls and increase operational efficiency.

Quantify Risk to Stakeholders and help the Board or C-Suite make smarter and faster decisions by showing the financial impact of a past, potential, or active threat.

Key Capabilities

Harness the Power of a Ratings Platform

With SecurityScorecard, harness the power of the most accurate and transparent data to reveal a trusted A-F rating of your own security posture or see how your security stacks up against your top 10 competitors. View the health of 10 security factors that determine your score, including network security, DNS health, patching cadence, endpoint security, IP reputation, application security, cubit score, hacker chatter, information leak, and social engineering. Reduce exposure by drilling down into a factor to understand the findings by high, medium, or low severity and know where to focus your team's efforts to address these findings.
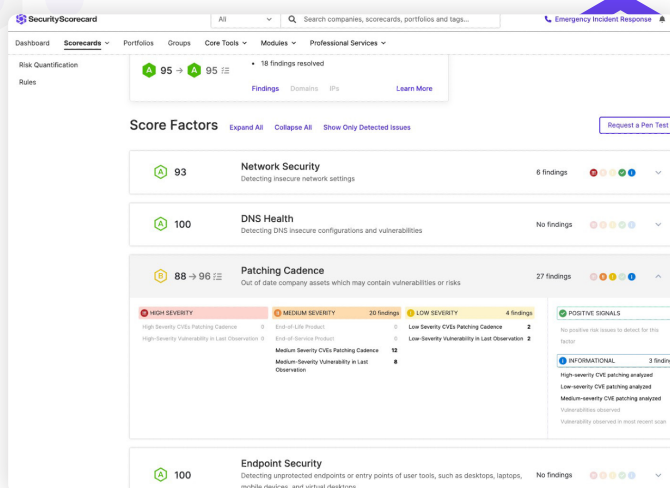

Figure 1: View of your Scorecard and posture against 10 security factors

Gain a Complete View of How an Adversary Sees Your Attack Surface

At a glance, observe all public-facing assets in the Digital Footprint to understand your attack surface including shadow IT and at-risk assets that an adversary could use to gain entry into your network. Assets are attributed through passive scanning of public records such as SSL Certificates, DNS Lookups, WHOIS data, and more. Since SecurityScorecard owns 97% of its data, your Digital Footprint is automatically updated when your infrastructure changes.
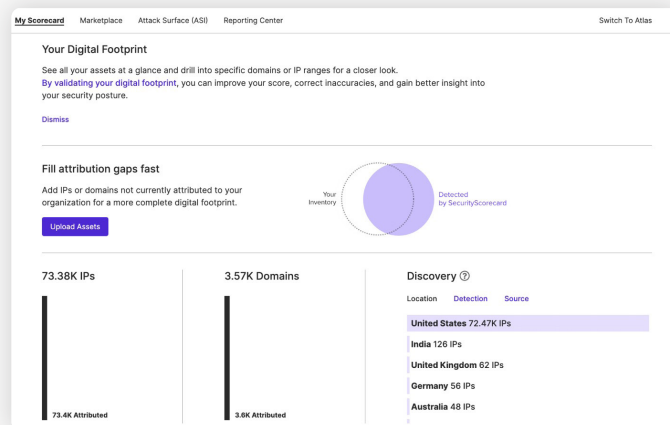

Figure 2: View of your attack surface in the Digital Footprint view

Investigate Further to Drive Actionable Next Steps

Probe into specific IPs or domains for a closer look, and add assets for a more integrated picture of your digital footprint. Track changes of risk associated with your external assets, monitor the attack surface of your vendor ecosystem, and manage misattribution of assets. Access SecurityScorecard's always-on deep threat intelligence built and maintained by world class threat hunters to enrich your attack surface discovery with actionable insights. Drill down into each asset to investigate if it has been compromised, showing associated threat actors, vulnerabilities, ransomware, MITRE TTPs, and more to guide your response in remediation.
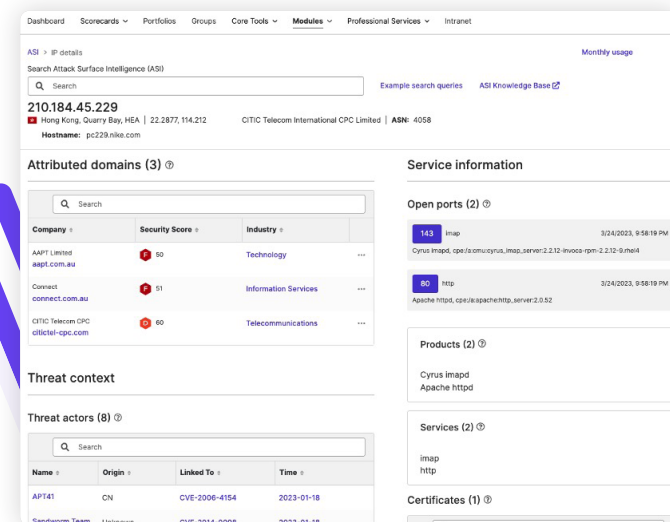

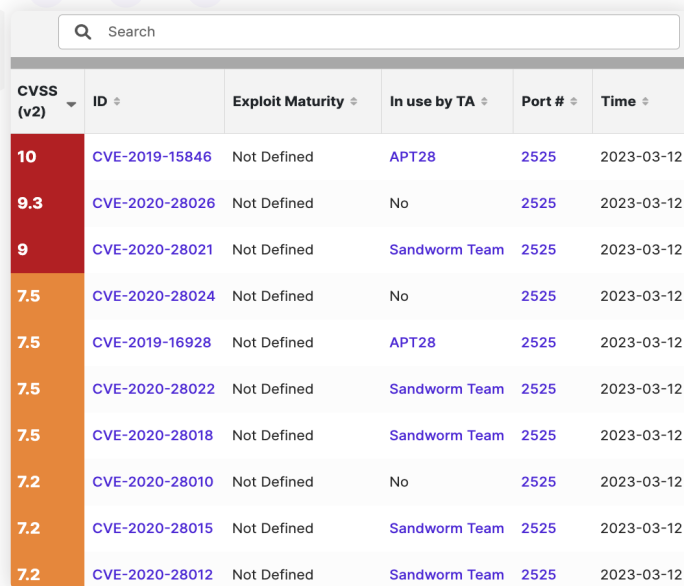**Figure 3:** Detailed view of the asset intelligence

Prioritize Remediation by the Biggest Impact to Your Business

SecurityScorecard's context-rich threat intelligence helps you easily detect and sort CVEs by exploit maturity, weaponized by threat actor, port number, or the time to narrow results into a manageable size of your top priorities to fix. By uncovering actionable insights to guide response SecurityScorecard provides various resources to support remediation efforts including using the Score Planner, a straightforward way to understand which findings will make the biggest impact on the overall score, providing your team with a list of prioritized tasks to patch your systems.

In addition to Score Planner and detecting CVEs, you can use the automated rule builder, create workflows, immediately notifying important changes to your digital footprint, including shifts in your score, new issues found, and new CVEs detected. Enable workflows and notifications across every element of the platform to increase your team's productivity by reducing manual tasks and integrating into your team's existing communication tools, including Teams, Slack, Jira, and ZenDesk.

Finally, effectively mobilize your team with little to no time by integrating any of SecurityScorecard's 90+ integrations, providing incident response and vulnerability management teams with actionable information to increase remediation times – stopping the adversary in their tracks.

CVSS (v2)	ID	Exploit Maturity	In use by TA	Port #	Time
10	CVE-2019-15846	Not Defined	APT28	2525	2023-03-12
9.3	CVE-2020-28026	Not Defined	No	2525	2023-03-12
9	CVE-2020-28021	Not Defined	Sandworm Team	2525	2023-03-12
7.5	CVE-2020-28024	Not Defined	No	2525	2023-03-12
7.5	CVE-2019-16928	Not Defined	APT28	2525	2023-03-12
7.5	CVE-2020-28022	Not Defined	Sandworm Team	2525	2023-03-12
7.5	CVE-2020-28018	Not Defined	Sandworm Team	2525	2023-03-12
7.2	CVE-2020-28010	Not Defined	No	2525	2023-03-12
7.2	CVE-2020-28015	Not Defined	Sandworm Team	2525	2023-03-12
7.2	CVE-2020-28012	Not Defined	Sandworm Team	2525	2023-03-12

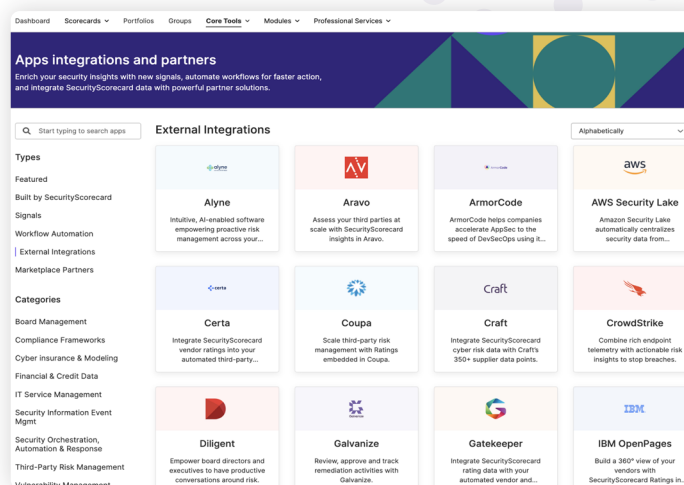**Figure 4:** View of CVEs sorted by Common Vulnerability Scoring System (CVSS)

Figure 5: Snapshot of SecurityScorecard's 90+ integration partners

SEARCH

100s
OF FACETS

including by domain, IP, region, leaked credentials, malicious reputation, and more.

Hunt for Potential Threats Like a Hacker Does

Search a database of 10,000 high severity Common Vulnerability & Exposures (CVEs) and 100 billion vulnerabilities and attributions across 100s of facets including by domain, IP, region, leaked credentials, malicious reputation, and more. For deep context, zoom out for a strategic view to find indirect signs of artifacts of an impending attack, or zoom in for a tactical view to dig deeper to find malicious actors in your environment that have slipped past your initial security defenses. As a result of gathering an abundant amount of valuable information, your team or support from SecurityScorecard's threat intelligence experts are ready to perform threat analysis to determine how the business will respond to critical threats.
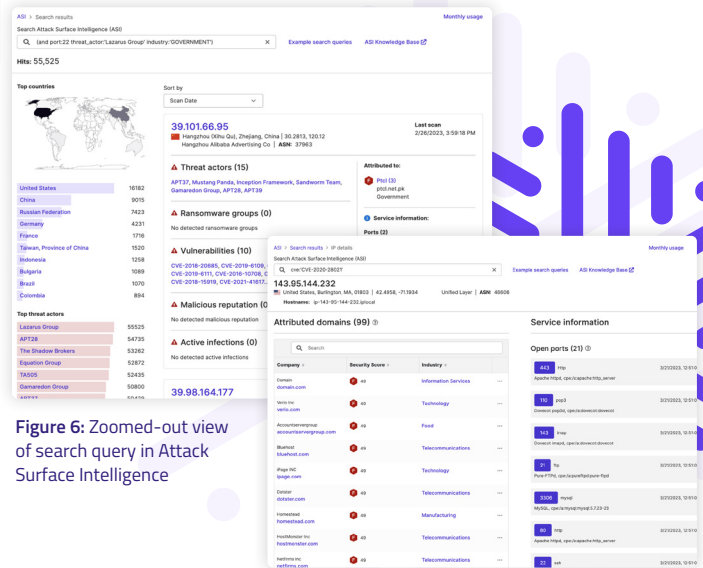

Figure 6: Zoomed-out view of search query in Attack Surface Intelligence

Figure 7: Zoomed-in view of detailed IP information including attributed domains, open ports, CVEs, threat actors, MITRE TTPs, products, and more.

Unify Key Stakeholders with Data to Transform Decisions

Demonstrate the ROI of security initiatives to the Board and key stakeholders by quantifying the financial impact of past, potential or active threats, including ransomware, data breaches, denial of service, or wiper attacks. Gain insight into the probability of these incidents over time and quantify the reduction in expected losses if issues like open ports, outdated browsers, or weak endpoints are not resolved. SecurityScorecard's Compliance capability automatically aligns evidence to various compliance frameworks, allowing you to quickly identify your audit readiness, communicate, and remediate gaps before the audit process starts.
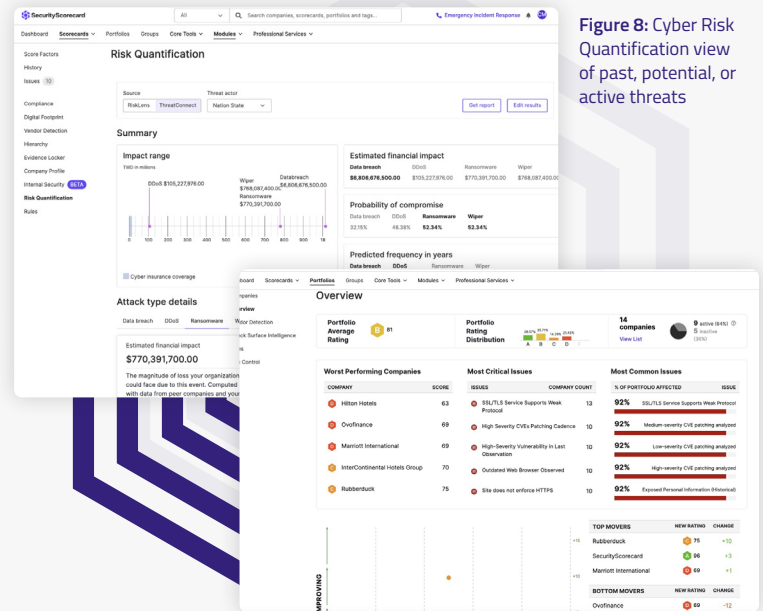

Figure 8: Cyber Risk Quantification view of past, potential, or active threats

Figure 9: Report financial risk with SecurityScorecard's reporting dashboards

Alleviate Future Risk Alongside Trusted Advisors

Proactively battle-test and validate your security controls are working effectively alongside industry-leading security experts with 100+ cumulative years of experience working with security agencies, special operations units, and Fortune 50 threat intelligence teams to eliminate risk, strengthen cyber defenses and boost resilience. SecurityScorecard Cyber Resilience Services include:

Tabletop Exercises to help organizations practice their cyber incident response plans with simulated real-life scenarios, uncovering gaps and ensuring they're ready to respond effectively and efficiently if a real incident occurs.

Penetration Testing and Red Teaming to learn how vulnerable you are to an attack by understanding the adversary's tactics, techniques, and procedures (TTPs) and confirm vulnerabilities are resolved.

Cyber Risk Intelligence to lean on SecurityScorecard to augment or outsource your threat analysis to some of the toughest cyber defenders in the industry today. Combine expert-led human analysis with dark web intelligence sources to deliver in-depth customized and actionable reports that provide visibility into the most critical threats to your organization.

Digital Forensics & Incident Response to partner with combat-proven experts who are ready to jump into action to diligently triage the incident, restore operations, collect evidence to solve the case, reducing financial impact and disruption to business operations.

Understand Your Most Critical Threats Including...

- Ransomware
- Malware
- Supply Chain Attacks
- Breach Information
- Leaked Credentials
- Imposter Domains
- APT Reconnaissance
- Hacker Chatter
- Malicious Email
- Cyber Campaigns
- Active Investigations including Cyber Bullying, Botnet Tracking, Attack Attribution, and more.

Cloud Delivered

## Reduce Risk with Accurate and Transparent Cloud-Delivered Ratings Data

SecurityScorecard provides a single cloud-delivered platform protecting your organization with a flexible Enterprise Cyber Risk Management solution that helps reduce risk across your ecosystem. SecurityScorecard has been named the leader in security ratings by Forrester and has scored over 12M+ companies. Find comfort in knowing the depth and scope of the collected data is unmatched, accurate, and transparent enough that you can trust!

Generating meaningful cybersecurity ratings data consists of four distinct processing stages: Signal Collection, Attribution Engine, Cyber Analytics, and Scoring Engine.

Single cloud-delivered Platform protecting your organization with a flexible Enterprise Cyber Risk Management solution

Signal Collection
- IPv4 Scans
- Malware Sinkholes
- DNS data
- External data feeds

Attribution Engine
- RIR, DNS, SSL data
- Domain discovery
- Subdomains
- IP-domain pairing

Cyber Analytics
- Study emerging threats
- CVEs
- Machine Learning

Score Engine
- Digital Footprint
- Size normalization
- Factor scores
- Total score

A B C D F

The Most Transparent, Trusted, and Easy-to-Understand Cybersecurity Ratings

SecurityScorecard leverages data mined with the market's leading capabilities, and relies on a global network of sensors to monitor signals across the internet. Our customers have access to the greatest volume and quality of intelligence available with our global network that collects data from over 1,500 ports globally. SecurityScorecard has honeypots in over 87 countries and leverages 120 distinct malware sinkholes that detect hundreds of millions of active attacks every day. Using this data we map out every organization's digital footprint with a historical look back of over 10 years. From there, we categorize the hundreds of singles and issues we collect across 10 key security categories which we call risk factors. Through this process we generate an A-F rating for over 12 million organizations globally which makes up the basis of our Scorecard. For full transparency we publish our methodology, the formulas we use to calculate our scores, and our refute rate on our public trust portal: https://securityscorecard.com/trust/.
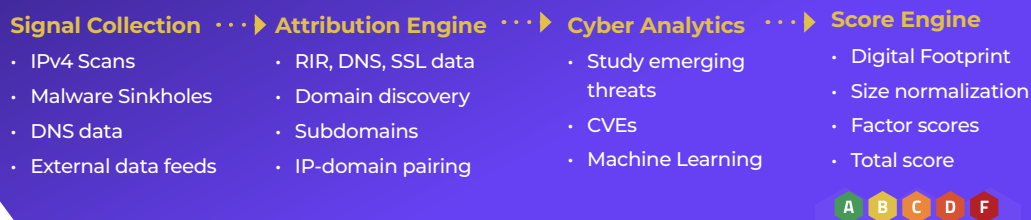
Operational Benefits

Eliminate the Uncertainty of a Potential Threat with actionable intelligence when a business event requires immediate insights. Confirm if you are at risk of the latest publicized threat, confirm risk in your supply chain, identify issues in business events, perform M&A due diligence, and discover new unknown assets when shadow IT occurs.

Bolster Your Cyber Resilience by partnering with the industry experts to enhance your security program, improve remediation times, and get help when you need it most.

Effectively Mobilize your Entire Security Operations Team by automating rules and alerts for your critical exposed assets and enhancing existing workflows via point-and-click integrations into 90+ certified technology partners.

Enhance Your Threat Team with Customized Intelligence to Get Ahead of Threat Actors. Our elite group of experts create curated reports revealing your hidden exposures from leaked credentials, hacker chatter, imposter domains, and APT reconnaissance.

Products and Services
Reduce Your Cyber Risk Exposure

Ratings

Continuously monitor and measure the security posture of any organization and even improve your own, with the industry's most accurate and transparent ratings platform. Each organization is scored based on a standard A-F grading scale to help simplify and better understand and address vulnerabilities in your own environment and those in your digital supply chain.

Attack Surface Intelligence

Prevent cyber attacks by reaching clear decisions from the industry's only global threat intelligence with context from your ecosystem. By analyzing billions of sources to provide deep threat intelligence and visibility into any IP, network, domain, or vendor's attack surface risk, customers can identify all of an organization's connected assets, expose unknown threats, conduct investigations at scale, and prioritize vendor remediation.

Cyber Risk Intelligence

Gain clarity to proactively eliminate cyber risk with customized, actionable threat intelligence about emerging and active threats specific to your organization. Delivered by SecurityScorecard STRIKE Threat Intelligence team, Cyber Risk Intelligence fills critical intelligence gaps and illuminates cyber risk trends, enabling cyber security teams to deploy limited cyber resources to the most efficient areas.

Proactive Security Services

Defend your organization with a range of proactive services, including: penetration testing, red teams, and tabletop exercises. Battle-test your security controls, identify gaps in your attack surface, and enhance your ability to defend against cyberattacks.

Digital Forensics & Incident Response

Be ready to respond to any threat confidently and mitigate business interruptions from a cyber attack by partnering with industry-leading experts in digital forensics and incident response (DFIR) capabilities to augment your security team's capabilities with SecurityScorecard on demand.

Cyber Risk Quantification

Be seen as a business leader and justify your security budget to the Board with the most scalable and actionable cyber risk quantification solution. Instantly quantify the financial impact of cyber risk by leveraging FAIR or attack path modeling frameworks.

VRM Jumpstart

Lean on experts to help you maximize the ROI of the SecurityScorecard platform and scale your organization along the TPRM maturity curve with services that help you configure the SecurityScorecard platform to suit your organization's needs along with best practice workshops to help you level-up.

Compliance

Evaluate the impact of IT and its associated security risks on your organization's adherence to regulatory requirements or security standards. Compliance centralizes evidence collection for faster, more effective audits.

Marketplace

Optimize your security workflows and deliver intelligence everywhere you work with the largest ecosystem of over 90 integrated technology partners. Whether you're looking to embed security ratings into your third-party risk management tool, integrate ratings data into your SIEM, or simplify workflows in your IT service management platform, our Marketplace has the connection for you.

CONTACT US TO LEARN MORE
Request a demo today.

GET STARTED

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1701
International: +1(646) 809-2166