RESEARCH

Redefining Resilience: Concentrated Cyber Risk in a Global Economy

The President's Forum
RSA 2024

In association with McKinsey & Company
Justin Greis, Partner
Charlie Lewis, Partner
Josh Welle, Associate Partner

SecurityScorecard

Introduction

In today's interconnected world, concentrated cyber risk threatens national security and global economies. Much like a precarious house perched on a cliff's edge, the reliance on a handful of vendors shapes the foundation of our global economy.

When zero-day vulnerabilities and emerging threats, like the SolarWinds technology supply chain compromise or MOVEit are discovered, it's a race against time.

SUPPLY CHAIN RANSOMWARE ATTACKS

MONEYWATCH

UnitedHealth says Change Healthcare cyberattack cost it $872 million

https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-hack-ransomware/

WSJ PRO

Companies Take a Closer Look at Supply Chains After Recent Cyberattacks

https://www.wsj.com/articles/cyber-chiefs-are-wary-of-vendor-security-a09cc57e

WIRED

The Untold Story of the Boldest Supply-Chain Hack Ever

https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/

Ransomware attacks cost companies $1 million per day

One example of the cascading effect of a single incident is the 2023 cyberattack on Change Healthcare, a core part of United Health's claims processing unit, in the United States. Medical claims processing ground to a halt. This disruption, termed by the president and chief executive of the American Hospital Association (AHA) as "the most serious incident of its kind" in healthcare, brought many medical providers to the brink of closure. An AHA survey of 1,000 hospitals found that 60% of respondents said the impact on revenue was $1 million per day.

The group behind the attack, known as ALPHV or BlackCat, shares ties with the criminal organization responsible for the infamous Colonial Pipeline attack in 2021. Faced with financial strain, healthcare organizations resorted to drastic measures, including staff layoffs and fire sales.

In the wake of the Change Healthcare incident, companies are doubling down on efforts to bolster supplier oversight and cybersecurity measures. Every organization must scrutinize its data security practices, assess third- and fourth-party access to sensitive data, and identify critical vendors essential to revenue.

75%

of third-party breaches targeted the software and technology supply chain.

SECURITYSCORECARD GLOBAL THIRD-PARTY CYBERSECURITY BREACH REPORT, 2024

Key findings:
Cyber risk concentration

1 **150 companies** account for **90%** of the technology products and services across the **global attack surface**.

2 **41%** of those companies had evidence of at least one **compromised device** in the past year.

3 **11%** had evidence of a **ransomware infection** in the past year.

4 Additionally, a remarkably small subset of just **15 companies** account for **62%** of all products and services.

5 The **top 15 companies** have **below-average cybersecurity risk ratings** – indicating a higher likelihood of breach.

6 **Ransomware operators** C10p, LockBit, and BlackCat systematically **exploit third-party vulnerabilities at scale**.

The cost of a third-party cyber breach is typically

40%

higher than the cost to remediate an internal cybersecurity breach.

GARTNER RESEARCH, 2023

Concentrated cyber risk

Threat actors exploit supply chain attack vectors for two reasons:

1. Scale operations. By compromising one organization, adversaries also gain access to that organization's customers — which may number in the hundreds or thousands, if not more.
2. Circumvent or bypass their customers' security defenses. A company's billion-dollar cybersecurity program is only as good as that of its smallest vendor.

90%

of products detected across the global attack surface are from just **150 companies**.

Third parties can affect the security of their customers in a variety of ways, including:

- Third-party data breaches occur when attackers gain access to customer data by compromising a vendor that retains or has access to it.
- Third-party network breaches occur when the compromise of a vendor enables attackers to compromise their customers' infrastructure.
- Exploitable vulnerabilities in software products.
- Lack of availability via DDoS attacks.
- Sale of malicious apps in their online stores.

Software supply chain vulnerabilities spread like a digital forest fire

Here are just a few examples from 2023:

MOVEit – C10p

$9.9 billion

This is the estimated total cost of the MOVEit mass hacks so far. The number is based on IBM data, which found the average data breach cost $165M last year, coupled with the number of individuals and organizations confirmed to have been impacted.

Citrix Bleed – LockBit and BlackCat

36 million users' data exposed

That number of Xfinity users exposed through a single third-party data breach involving the exploitation of the "CitrixBleed" vulnerability (CVE-2023-4966) is staggering. Citrix now faces a class-action suit. The zero-day vulnerability was exploited by hackers in secret for weeks before it was found and a fix issued. The vulnerability was exploited without any authentication or privileges on the affected network. One of the significant companies targeted was Boeing's parts and distribution business.

Change Healthcare – BlackCat and RansomHub

$1 million per day

According to a survey by the American Hospital Association, 60% of hospitals experienced a revenue impact of $1 million per day or more due to this cyberattack. More consequentially, 74% of hospitals reported impacts on direct patient care. Change Healthcare is alleged to have paid a $22 million ransom to ALPHV following the incident – a claim made by researchers monitoring a known ALPHV crypto wallet and one backed up by RansomHub. However, Change Healthcare has never officially confirmed this to be the case. Weeks after Change Healthcare recovered from the ALPHV attack, the company was allegedly being extorted by a second ransomware group, RansomHub.

Atlassian Confluence Data Center and Server Software – DarkShadow

75,000 customers at risk of exposure to state-sponsored threat actors

As of early October 2023, state-sponsored actors had exploited this Atlassian Confluence Data Center and Server Software vulnerability (CVE-2023-22515) to create new administrator accounts. Researchers attributed this activity to the state-sponsored Chinese group DarkShadow, whom the U.S. Justice Department had previously indicted for trying to steal COVID-19 intellectual property (IP). Confluence's use for development projects would make it a valuable source of the IP that state-sponsored Chinese actors often seek. The actively exploited vulnerability potentially impacted 75,000 Atlassian customers.

JetBrains Software Development Platform – Russian Foreign Intelligence Service

15.9 million developers

CVE-2024-27198 is a critical zero-day authentication bypass vulnerability in the JetBrains TeamCity software development platform, and CVE-2024-27199 is a related high-severity zero-day authentication bypass vulnerability in the same platform. JetBrains says over 15.9 million developers use its products and counts 90 Fortune Global Top 100 companies among its customers. The March 2024 disclosure of this vulnerability by TeamCity and the security vendor that discovered it is an unfortunate case of what happens when the coordination of vulnerability disclosures fails. The security vendor released proof-of-concept (PoC) exploit code so quickly after TeamCity issued its advisory and patch that many customers did not have time to update. Several customers thus experienced compromises, including ransomware infections and the creation of unauthorized accounts, some of which had administrative privileges.

> The variety of victim types was notably diverse, with no discernible pattern or trend in their selection, aside from the common vulnerability of an unpatched, Internet-reachable JetBrains TeamCity server.

62% of the global external attack surface is concentrated in 15 companies

A striking 62% of the measurable market share for technology products and services belongs to just 15 companies. This extreme reliance on a select few “heavy hitters” creates precarious single points of failure. In the event of a major outage or security breach, the vendor’s entire customer base is at risk.

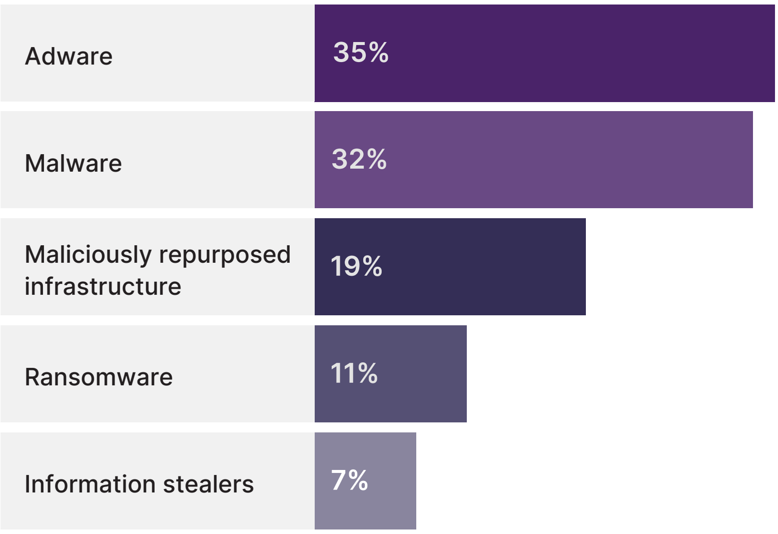
The more established a vendor is, the likelier it is to have privileged access to networks housing highly sensitive and often business-confidential information. Top global companies are inherently trusted, making them particularly tempting targets for sophisticated threat actors.

WHEN IT COMES TO CONCENTRATION RISK, THE QUESTION TO ASK IS:

> *“Have we concentrated a mission-critical service to a single vendor — creating a single point of failure?”*

41% of the 150 companies had some evidence of at least one compromised computer or other device on their networks

The various types of compromises included:



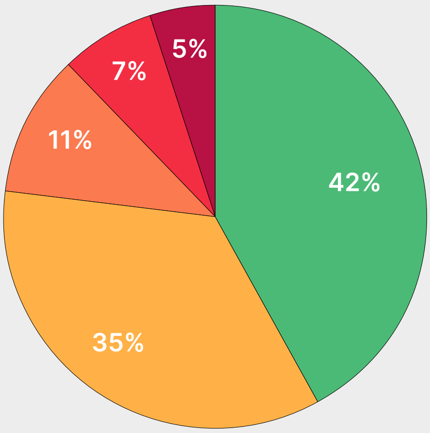
Some companies had findings in multiple categories, so the percentages add up to more than 100%.

The top 15 companies have below-average cybersecurity risk ratings

SecurityScorecard researchers identified not only a pool of 150 top vendors – based on their detectable market share of products and customers – but also a subset of 15 "heavy hitters" with an even higher market share concentration.

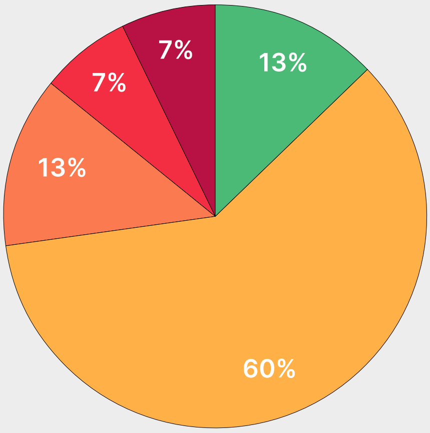
A	B	C	D	F
90 OR HIGHER	80–89	70–79	60–69	LESS THAN 60

DISTRIBUTION OF SECURITY RATINGS: TOP 150 COMPANIES



A: 63 VENDORS
B: 52 VENDORS
C: 17 VENDORS
D: 11 VENDORS
F: 7 VENDORS

DISTRIBUTION OF SECURITY RATINGS: TOP 15 COMPANIES



A: 2 VENDORS
B: 9 VENDORS
C: 2 VENDORS
D: 1 VENDOR
F: 1 VENDOR

These top 15 companies alone have a market share of 62% of technology products and services detected.

These 15 companies had security ratings that were below-average, compared to the broader pool of 150 top vendors. This finding is concerning, as these companies have greater potential to inflict third-party harm on their customers due to their lower security ratings and extremely large market share.

Companies with a "C" rating are 5.4 times more likely to experience a breach.

As our researchers previously demonstrated, there is a strong correlation between financial means and cybersecurity posture. Buyers expect more prominent and well-resourced companies to have better security hygiene, but this set of companies was different. The tendency of these organizations with such vastly disproportionate technology market shares to score lower cybersecurity risk ratings poses serious supply chain risk for the technology ecosystem and the broader economy.

The sheer scale of these companies amplifies their risk of compromise, posing significant third-party risks to their extensive customer bases. Enormous attack surfaces make it extremely difficult for even the largest and most well-funded and vigilant security teams to defend them. They have to get it right every time, whereas an attacker only has to find one entry point in their vast attack surfaces to compromise them. In other words, the sheer scale of these largest vendors increases their risk of compromise, which they pass on to their enormous customer bases as third-party risk.

Ransomware operators like Cl0p, LockBit, and BlackCat methodically exploit third-party vulnerabilities at scale

State-sponsored Chinese cyber espionage groups also use third-party attack vectors

Threat groups operate globally, but their operational infrastructure is concentrated in some countries more than others; 24% originate from China, and the Russian Federation accounts for 15%. These insights shed light on the geopolitical dimensions of cyber conflict.

The frequency with which reports of attacks on these companies and their products mention state-sponsored Chinese cyber espionage needs to be a higher priority for threat intelligence coverage. The scale and severity of the Russian SolarWinds breaches may have distracted some cybersecurity defenders from the longer track record and greater demonstrated interest of Chinese actors in the technology and telecommunications industry, including the pioneering use of MSPs as third-party attack vectors and the critical importance of technical intellectual property to China's development goals.

State-sponsored Chinese counterparts have a much longer history of third-party supply chain compromises. For example, Chinese APT10 pioneered using compromised MSPs to gain access to their ultimate targets in other industries well before this strategy became popular among ransomware operators. More broadly, competing foreign technology and their businesses are critical targets for state-sponsored Chinese actors because of their relevance to the Chinese government's ambitious economic development goals.

Nonetheless, one should not discount the impact of the subtler state-sponsored Russian actors, whose usually less "noisy" attacks are often more likely to go undetected. The discovery of the SolarWinds third-party technology supply chain compromises put state-sponsored Russian actors on the map.

Lessons learned

Product vulnerabilities can have an equal or more significant impact on their customers than actual breaches of those vendors.

Exploitation of these Common Vulnerabilities and Exposures (CVEs) has been the root cause of many high-profile and large-scale third-party breaches. Such vulnerabilities in standard software are popular attack vectors because of the potential to infect so many victims with relatively little labor input. For example, in October 2023, Citrix disclosed CVE-2023-4966, known popularly as "CitrixBleed," a critical zero-day sensitive information disclosure vulnerability in Citrix NetScaler ADC and NetScaler Gateway. CitrixBleed went on to become one of the most widely exploited vulnerabilities of the year, after CVE-2023-34362. It was associated in particular with the LockBit and BlackCat ransomware groups.

The most egregious example was CVE-2023-34362, a critical zero-day SQL injection vulnerability in the MOVEit file transfer software of Progress Software. The ransomware group C10p exploited it in an unusually large-scale campaign in May-June 2023 that affected a large number of victims both directly and via third-party breaches. Many organizations that used MOVEit experienced direct compromises. Many organizations that did not use MOVEit themselves but relied on vendors that used it experienced third-party data breaches via those vendors. SecurityScorecard research identified CVE-2023-34362 as the most widely exploited vulnerability of 2023 and a top third-party attack vector.

Separately, Microsoft disclosed in July 2023 that state-sponsored Chinese threat actors that it calls Storm-0558 had compromised email accounts for approximately 25 customer organizations, including government agencies. Microsoft believes that Storm-0558 is a distinct group but may have some overlap with the separately reported APT31 (AKA Zirconium, Violet Typhoon). The actors used a novel technique; a code validation error enabled the actors to abuse a consumer signing key to forge Azure Active Directory (AD) authentication tokens with which to access customers' Exchange Online data via Outlook Web Access (OWA).

Lessons learned *(continued)*

A company does not have to be a customer to suffer a third-party compromise.

A July-August 2023 “EvilProxy” phishing campaign used an open redirection vulnerability in the job posting website Indeed to compromise credentials for senior executives in various industries, particularly banking, insurance, and real estate. The redirection from Indeed via an email message aimed to provide further credibility to the phishing page, which acted as a reverse proxy between the victims. The phishing page stole session cookies that enabled attackers to bypass multi-factor authentication (MFA).

Customer exposure varies depending on the degree of adversary access.

For example, in December 2023, MongoDB disclosed a breach that exposed customer account information, as they acknowledged. The company nonetheless emphasized that there was no indication of the attackers gaining access to the more sensitive information that customers stored on MongoDB’s database products, which were on separate infrastructures that the attackers did not reach.

> *“Companies must identify the business processes, and the business criticality of those processes, of their third parties and then identify single points of failure.”*
>
> **JOSH WELLE**
> **ASSOCIATE PARTNER**
> **MCKINSEY**

DDoS attacks are another threat to these companies and their customers.

Distributed denial-of-service (DDoS) attacks are technically not breaches, but the loss of availability can nonetheless impact companies with low tolerance for downtime. While many DDoS attacks are the low-impact efforts of hacktivists with modest capabilities, more sophisticated adversaries can have a more significant impact. For example, the group Anonymous Sudan (which many researchers believe to be a cover for the pro-Russian group Killnet, despite its name and ostensible affiliation) reportedly took down the website of Cloudflare in November 2023. Other targets of Anonymous Sudan have included Microsoft, Telegram, and OpenAI.

The dissemination of malicious software via the app stores of technology companies may not be a breach per se, but represents the violation of policies aiming to protect users from such attacks. For example, in February 2024, a cryptocurrency investor lost $490,000 using a malicious app posing as the legitimate Linux version of the Exodus cryptocurrency wallet on Canonical’s Snap Store. Canonical had marked the app as “Safe.”

Take action to protect against third-party risk

Considering the severity of Nth party risk, cybersecurity (and business) leaders can act by taking two steps: first, increase top-level buy-in on why defending critical business processes against Nth party risk matters. Next, CISOs should bolster defenses to reduce risk to protect what matters most.

Increase top-level buy-in

The cybersecurity landscape is constantly evolving (e.g., transition to digital enterprise and next-generation technologies), and many companies are not sufficiently prepared to respond to the evolution of threats from Nth parties.

The CISO, in partnership with other C-staff leaders (Chief Risk Officer, Chief Legal Officer, and Business Leaders) should elevate cybersecurity as a senior leadership priority because of the growing impact, volume, and rate of threats; in doing so, this should be a board-level agenda item, one that has proper oversight and governance. Once alignment is created across the company's leadership, there should be a commitment to increasing digital resilience against Nth party risk. This means increasing cybersecurity capabilities, identifying gaps, and capitalizing on opportunities to improve over time.

> *"Despite the many advances and innovations made in cybersecurity, there still remains a large gap in most organizations: a deep understanding of the business. Once this alignment is achieved, CISOs can take a risk-based approach and prioritize the controls needed to secure that which matters most to the business and apply differential levels of protection to its systems, processes, personnel, and third parties."*
>
> **JUSTIN GREIS**
> **PARTNER**
> **MCKINSEY**

Bolster defenses to reduce risk and be prepared for the worst

Companies spend hundreds of thousands of dollars per year managing cyber risk within their vendor and third-party ecosystem and millions on cyber programs, yet their billion-dollar business is only as good as the cybersecurity of their smallest vendor. Mitigating supply chain cybersecurity requires four key steps: identifying single points of failure; continuous monitoring; automatic vendor detection; and operationalizing vendor cybersecurity communication.

1 Identify single points of failure

The first action will be to map the critical business processes and technologies to the people that power them to identify any single points of failure. Zero in on the third parties that business continuity depends on. Create a watch list with these "single point of failure" vendors. Automate continuous monitoring, action plans for improvement, collaboration, and vulnerability remediation validation. Knowing these critical processes and building capabilities to prepare for a potential cyber attack is paramount because when an incident similar to the one at Change Healthcare happens, and the healthcare industry can't pay claims, the industry is "on fire."

2 Automatically detect new vendors

Identify cybersecurity concerns across the global vendor landscape and partner with those vendors to improve. You can't control your vendors, but you can prove that you know their security posture matches your risk tolerance. Using an automated solution that passively monitors your vendors' IT deployments gives you valuable visibility into how well they manage cybersecurity risk.

3 Continuously monitor external attack surface

Cybersecurity monitoring is a threat detection strategy that uses automation to constantly scan your IT ecosystem for control weaknesses, sending alerts to a security information and event management (SIEM) system. Companies can use the same threat intelligence they use for their defense against their critical suppliers and inform vendors if they become aware they are at risk.

4 Operationalize vendor cybersecurity management

Cybersecurity managed services can own communication directly with third parties to resolve issues on your behalf, including providing support that enables risk resolution. Making sure the response is ready and linked to the Incident Response (IR) playbook. Be able to identify, contain, eradicate, and recover from a cyber attack; if we were to replay Change Healthcare, companies must have an alternative payment process on standby OR be prepared to manage paper claims internally.

"The interconnected nature of our digital landscape requires a shift in how companies think about their cyber ecosystem risk — it is no longer just about your resilience, you need to consider the broader system and how to build mutual support with peers, competitors, and your vendors"

Charlie Lewis
PARTNER
MCKINSEY

Digital disruption is inevitable and leads to rapid technology-driven change as companies strive to better serve their customers and win market share As organizations make large-scale investments in technology — whether in the spirit of innovation or out of necessity — they do it in partnership with a web of third-party companies which all bring inherent cyber risks. It is here where CISOs have been thrust into the spotlight and are now serving as partners to the overall business strategy. CISOs know attackers are exploiting the vulnerabilities that new technologies introduce, and even the best cyber controls can become dated as attackers adapt. Organizations that seek to position themselves most effectively for the next five years must take a proactive posture to building over-the-horizon defensive capabilities.

"For instance, consider common vendors, shared infrastructure, communications and cloud/software services with the goal of identifying where risk is most concentrated in only a small number of common providers and then work with those providers to minimize the risks in their services. Consider expanding supplier diversity to avoid common-mode vulnerabilities."

President's Council of Advisors on Science and Technology
Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World, February 2024

SecurityScorecard Methodology

Threat researchers used SecurityScorecard Automatic Vendor Detection (AVD) to identify the most frequently and extensively used companies of approximately 12 million public and private sector organizations. AVD surveys an organization's attack surface and identifies which companies it uses to map its supply chain and identify and resolve cybersecurity risks.

SecurityScorecard researchers used a combination of two criteria to determine which suppliers belong in this pool of top companies.

1. Frequency is the number of AVD-detected customers that a vendor has.

2. Extensiveness is the number of AVD-detected instances of that organization's products used in the wild. We then ranked these companies by the percentages of their respective "market share" of detections for both criteria.

We took the top 0.1% of organizations from the customer detection ranking and the top 1% from the production detection ranking. We chose a more significant percentage from the latter list due to the higher concentration of detections among a relatively small number of companies on that list, giving us a more comprehensive sample for greater statistical validity. We note that the respective cut-off points for both ranked lists were also close to the points on both lists at which companies' "market share" decreased to below 0.1% of all detections. This cut-off point made those with lower rankings as insignificant as a rounding error and thus not worth including in our sample. We merged the organizations above both cut-off points into one list and removed the duplicates, yielding a sample of 150 companies for this paper. Having derived this list of top companies, we queried our platform for each vendor's security rating, its most severe risk factor, and the specific security issue that had the most negative impact on its security rating.

150 companies may sound like a small sample size, but keep in mind the degree to which this small number of companies has an enormous market share in the aggregate. These **150 companies represented 85% of the customer relationships and 90% of the product detections in the total AVD data set**. This high concentration of business relationships and product usage in the hands of a relatively small number of companies is an example of the "Pareto Principle," known popularly as the "80-20 rule" (although actual percentages may vary). This "law of the vital few" or "principle of factor sparsity" states that a minority of causes (typically 20%) are responsible for a majority of effects or results (normally 80%). These top companies support large shares of the economy, vastly disproportionate to their relatively small number. It is worth focusing on these top companies because their third-party risks and any supply chain compromises at these companies are likely to affect the largest numbers of other organizations.

Remember that one of the main reasons adversaries use third-party attack vectors is to access as many victims as possible by compromising one vendor.

To learn more and create your free account, visit SecurityScorecard.com

ABOUT STRIKE

The SecurityScorecard STRIKE threat intelligence team combines unique intelligence, incident response experience, and supply chain cyber risk expertise. Backed by SecurityScorecard technology, STRIKE is a strategic advisor to CISOs worldwide, empowering the entire digital ecosystem to identify, measure, and resolve cyber risk.

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io