REPORT

An Analysis of the Cyber Security Ratings of the Top 150 Technology Vendors

SecurityScorecard

Introduction

This paper analyzes the cybersecurity ratings of the 150 most frequently and extensively used business-to-business (B2B) technology vendors, according to SecurityScorecard's scoring methodology. The goal is to help these top vendors' customers set priorities for their third-party risk management (TPRM) and vendor risk management (VRM) programs. It aims to achieve that goal by identifying the most significant risk factors and security issues affecting this segment of the technology supply chain for TPRM and VRM programs to prioritize. Security teams at these vendors can also use this report in support of assessments of their own security hygiene.

Many high-profile cyber attacks in recent years have involved technology supply chain compromises. Many threat actors have come to value supply chain attack vectors for two reasons. They enable attackers to scale up their operations by compromising one organization that gives them access to that organization's customers, which may number in the hundreds or thousands, if not more. Supply chain attacks can also give attackers opportunities to circumvent or bypass the security defenses of their customers, which may be more robust than those of their vendors but nonetheless give trusted access to those same vendors. For more information on this subset of third-party breaches, please read SecurityScorecard's latest report on this topic.

Organizations that rely on these vendors can reduce this supply chain risk by addressing identifiable security issues with vendors during the vendor selection process and as customers. SecurityScorecard recently launched its new MAX service to assist customers with these challenges. This paper's findings should give actual or potential customers of these vendors a preview of what overall trends, general risk factors, and specific security issues to expect.

Key Findings

The high concentration of business in the hands of a small number of vendors gives greater significance to any third-party risks that they may pose. The top 150 vendors accounted for **85% of customer relationships and 90% of products** that our platform detected. The top 15 of those 150 vendors accounted for 48% and 62%, respectively.

Endpoint Security is the most common risk factor for which these 150 vendors receive their lowest scores. **The single issue most responsible for these lower Endpoint Security scores is the use of outdated web browser versions.**

The average score for these 150 vendors (84) is the same as our global average. The higher median score (87) for these 150 vendors indicates that **a minority subset of low values reduces that average**, while most values were actually "above-average."

The absence of Sender Policy Framework (SPF) records is the next-most common issue to have the most negative impact on scores. Missing SPF records facilitate email spoofing and thus put an organization and its customers and vendors at greater risk.

8 of the top 15 vendors are also in that minority subset of vendors with below-average scores. This finding is troubling in that the higher risk that these vendors pose can affect larger numbers of organizations via their third-party risks.

IP Reputation was a less frequent but still significant source of lowest scores — only 9% for the whole sample, but doubling to 18% within the subset of below-average vendors.

Key Findings *(continued)*

11% of the total sample had their most negative score impacts from **IP Reputation findings that suggest infections with malware, ransomware, adware, or the malicious repurposing of a machine.** That percentage nearly doubled to 21% in the subset of below-average vendors.

59% of all 150 vendors had no sign of any compromised machines in the past year, whereas **41% had some evidence of at least one compromised machine.** The various types of compromises included adware (35%), other types of malware (32%), maliciously repurposed infrastructure (19%), ransomware (11%), and information stealers (7%).

5 of the 20 product/service categories of these vendors had both below-average scores and increased potential to cause greater harm to their customers via third-party risks by virtue of the nature of their products and services. These categories are: Cloud Services/Computing & Infrastructure as a Service (IaaS); Operating Systems & Computing Languages; IT Infrastructure and Operations Management; Web Content Management System; and Database Management Software & Data Storage.

Vendors can affect the security of their customers in a variety of ways, including: third-party data breaches; as third-party access vectors enabling attackers to compromise customer infrastructure; exploitable vulnerabilities in their software products; lack of availability via DDoS attacks; and the sale of malicious apps in their online stores.

Many key CVEs in the past year affected products from these vendors, including: **CVE-2023-34362, which affected the MOVEit file transfer software** that C10p ransomware operators exploited on a massive scale; and CVE-2023-4966, also known as "CitrixBleed," which LockBit and BlackCat ransomware operators exploited widely.

State-sponsored Chinese cyber espionage groups pose a significant threat to these vendors, which they could use as either third-party attack vectors to target their customers, or as a source of intellectual property for China's own economic development.

Methodology

SecurityScorecard researchers used our platform's new Automatic Vendor Detection (AVD) module to identify the most frequently and extensively used vendors for the pool of approximately 12 million businesses and organizations that we cover. AVD surveys an organization's attack surface and identifies which vendors that organization uses in order to map its supply chain and thus rate the level of third-party risk that it incurs via that supply chain.

SecurityScorecard researchers used a combination of two criteria to determine which suppliers belong in this pool of top vendors. One criteria, frequency, is the number of AVD-detected customers that a vendor has. Another criteria, extensiveness, is the number of AVD-detected instances of that organization's products used in the wild. We then ranked these vendors 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% of organizations from the production detection ranking. We chose a larger percentage from the latter list due to the higher concentration of detections among a relatively small number of vendors on that list, giving us a wider 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 vendors' "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 the sample of 150 vendors for this paper. Having derived this list of top vendors, we queried our platform for each vendor's security rating, as well as its most severe risk factor and the specific security issue that had the most negative impact on its security rating.

Methodology *(continued)*

150 vendors 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. As a whole, these 150 vendors represented 85% of the customer relationships and 90% of the product detections in AVD's total data pool. This high concentration of business relationships and product usage in the hands of a relatively small number of vendors 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 (typically 80%). These top vendors support large shares of the economy vastly disproportionate to their relatively small number. It is worth focusing on these top vendors because their third-party risks, as well as any supply chain compromises at these vendors, are likely to affect the largest numbers of other organizations. Remember that one of the main reasons for threat actors to use third-party attack vectors in the first place is to access as many victims as possible by compromising one vendor.

Furthermore, even within this sample of 150 top vendors, there is a highly disproportionate concentration of customer relationships and product usage in the hands of a few "heavy hitters." For example, the top 10 on the customer detection list alone represented 48% of all detected customer relationships (including those beyond the 150 top vendors). Similarly, the top 10 organizations on the product detection list alone represented 62% of all product detections (including those beyond the 150 top vendors). We merged both top 10 lists and removed duplicates, yielding a sample of 15 "heavy hitters" among the top 150 vendors. We will treat these "heavy hitters" as a subset in the below analysis, as third-party risks and supply chain compromises at these vendors can affect even larger numbers of organizations.

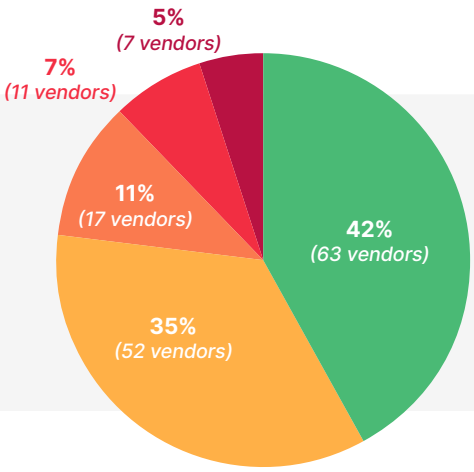
Some suppliers on this list are non-profits. For methodological purposes, we treat them the same as other suppliers, despite their non-profit status. Their software and other contributions to the technology ecosystem make them just as worthy of consideration as their for-profit counterparts. For the sake of simple consistency, our use of the term "vendors" covers them as well.

General Statistics

The average numerical score for the top 150 vendors is 84. The median numerical score for the top 150 vendors is 87. The average score for approximately 12 million worldwide organizations is also 84. The average score for these top vendors is thus the same as our global average. A score of 84 puts these companies collectively in the "B" range. An organization's "B" rating means that the organization is 2.9 times more likely than one with an "A" rating to experience a breach. An organization with a "C" rating is 5.4 times more likely than one with an "A" rating to experience a breach, and so on. Please consult this whitepaper for a more detailed explanation.

DISTRIBUTION OF SECURITY SCORES AMONG TOP 150 VENDORS

- A — 90 or higher
- B — 80 to 89
- C — 70 to 79
- D — 60 to 69
- F — less than 60



The small discrepancy between the mean of 84 and the median of 87 suggests that this data sample has a modest negative skew or is somewhat "left-skewed." In other words, a smaller subset of extreme values at the lower end of the scale are driving down its average, and most data points in this sample are actually above the mean. Indeed, 56 vendor ratings were below the average of 84, while the remaining 94 vendors were above 84. In this case, we thus view the median of 87 as a better overall representation of this sample. As you can see from the above pie chart, the majority of vendors had either strong "A" or good "B" ratings. The vendors with below-average scores nonetheless deserve special consideration as a distinct subset, given the higher risk that they pose, and as a source of clearer insights into risks and issues that affect the whole sample. We will delve further into this special subset below.

It is worth comparing these figures to those of our recently published similar analysis of members of the S&P 500 U.S. stock market index. That sample of companies had a higher average (88) and a higher median (89), with a smaller discrepancy between the two values (1) suggesting a less negative skew. The distribution of letter grades within that sample also had higher proportions of "A" and "B" ratings and fewer "C", "D", and "F" ratings. The gap is not huge but noticeable enough to ask why these top 150 vendors have lower scores, given the critical role they play in the technology ecosystem.

Money is probably a factor, as the S&P 500 includes some of the largest companies in the world's largest economy. Another factor is that technology companies tend to have higher risk levels and more security issues in general, as that other paper demonstrated. They often have larger and more complex attack surfaces, often with more external dependencies and thus more third-party risk. More of their business is in cyberspace, compared to "brick and mortar" businesses in industries like Retail & Hospitality, so they have more cyber risk exposure simply by virtue of the nature of what they do. S&P 500 members are U.S.-based, whereas this list of 150 vendors includes some European and Asia-Pacific organizations. Nonetheless, geography does not appear to be a significant variable in this case.

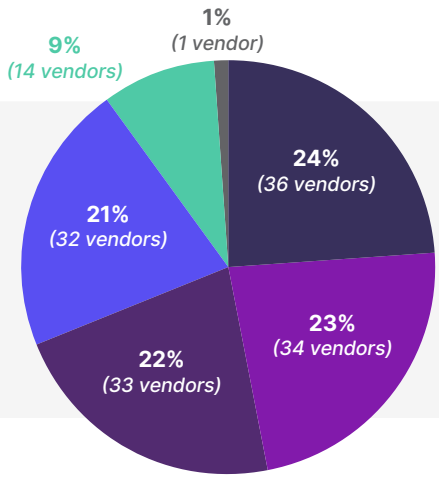
Identified Problem Areas

General Risk Factors

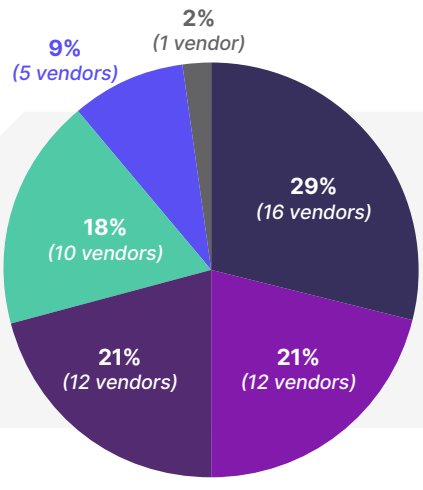
SecurityScorecard ratings reflect evaluations of an organization's observable security hygiene in 10 different security factors or risk areas. Our researchers identified one of these 10 factors for which each vendor had its lowest score, in the hopes of zeroing in on specific areas where they may need more vetting. Below are the percentages and raw numbers of the top vendors whose lowest scores were in each of the 10 security factors.

DISTRIBUTION OF LOWEST-SCORING SECURITY FACTORS AMONG TOP VENDORS

- **Endpoint Security:** 24% (36 vendors)
- **Network Security:** 23% (34 vendors)
- **Application Security:** 22% (33 vendors)
- **DNS Health:** 21% (32 vendors)
- **IP Reputation:** 9% (14 vendors)
- **Patching Cadence:** 1% (1 vendor)



In the hopes of zeroing in more narrowly on those security areas and risk factors with the most negative impact on overall scores, we repeated this query with the above-mentioned subset of 56 vendors with below-average general scores. The distribution resembled that of the full sample of 150 vendors, except that the emphasis on Endpoint Security as the top risk factor was more pronounced in this subset. Network and Application security remained in more distant second and third places in this below-average subset, but IP Reputation and DNS Health switched positions for fourth and fifth place, for reasons that may become clear below.



DISTRIBUTION OF LOWEST-SCORING SECURITY FACTORS AMONG VENDORS WITH BELOW-AVERAGE SCORES

- **Endpoint Security: 29% (16 vendors)**
- **Network Security: 21% (12 vendors)**
- **Application Security: 21% (12 vendors)**
- **IP Reputation: 18% (10 vendors)**
- **DNS Health: 9% (5 vendors)**
- **Patching Cadence: 2% (1 vendor)**

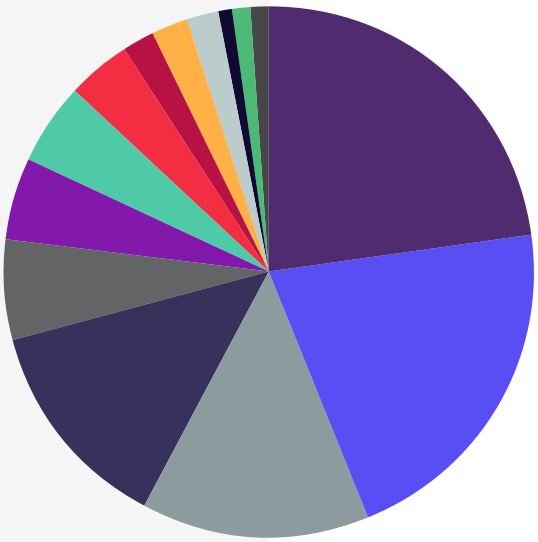
Identified Problem Areas *(continued)*

Specific Security Issues

An organization's score for a given risk factor or security area depends on a combination of specific issues and findings under that rubric. Our researchers thus delved deeper into the specific issues within the various score factors that had the single-most negative impacts on the ratings of the top 150 vendors. This graphic illustrates how many of the 150 vendors had the most negative impact on their ratings from these issues. Within the parentheses are the broader score factors under which these specific issues fall.

DISTRIBUTION OF MOST NEGATIVE SCORE IMPACT AMONG TOP 150 VENDORS

- **Outdated Web Browser Observed (Endpoint Security):** 23% (35 vendors)
- **SPF Record Missing (DNS Health):** 21% (32 vendors)
- **Website Does Not Implement HSTS Best Practices (Application Security):** 14% (21 vendors)
- **Site Does Not Enforce HTTPS: (Application Security):** 13% (19 vendors)
- **SSL/TLS Service Supports Weak Protocol (Network Security):** 6% (10 vendors)
- **Ransomware Infection Detected (IP Reputation):** 5% (8 vendors)
- **Malware Infection (IP Reputation):** 5% (7 vendors)
- **Content Security Policy is Missing (Application Security):** 4% (6 vendors)
- **Content Security Policy Contains Broad Directives (Application Security):** 2% (3 vendors)
- **Insecure HTTPS Redirect Pattern (Application Security):** 2% (3 vendors)
- **Miscellaneous (Network Security):** 2% (3 vendors)
- **Miscellaneous (Endpoint Security):** 1% (1 vendor)
- **Attack Detected (IP Reputation):** 1% (1 vendor)
- **Adware Installation (IP Reputation):** 1% (1 vendor)



The use of outdated web browsers is probably a key factor in why Endpoint Security was the lowest-scoring security factor for the largest percentage of vendors, particularly those with lower scores, as noted above. Indeed, it is one of only two Endpoint Security issues that surfaced as having the most negative impact on any top vendor's score; the only other Endpoint Security issue was so rare, with only one occurrence, that it is not worth mentioning. In any event, outdated web browsers expose organizations to exploitable vulnerabilities that remain unpatched in older browser versions. Threat actors exploit these vulnerabilities to compromise browsers and thus access sensitive data or run malicious code on targeted devices.

Identified Problem Areas *(continued)*

Specific Security Issues *(continued)*

The second-most common issue with the most negative impact on vendor scores was a DNS Health issue, even though that broader risk factor was less common as a source of lower ratings. The absence of a Sender Policy Framework (SPF) record helps threat actors spoof email addresses from that domain, leading to phishing attacks, spam distribution, and other malicious activity. Such malicious activities can damage a domain's reputation and cause recipient servers to mark legitimate emails as spam or reject them. In the absence of SPF records, domain owners have limited control over who can send emails on behalf of their domain.

It is easy to envision a scenario in which the combination of missing SPF records and outdated browsers enables a compromise. An attacker spoofs an email address from an organization's domain, which is easier without a SPF. The attacker sends users an email containing a link with a browser exploit, which is more likely to work because users did not update their browsers.

Four IP Reputation issues appeared with lesser frequency but, when taken as a whole, included the most negatively score-impacting issues for 17 out of the 150 vendors, or 11% of them. **Malware Infection, Ransomware Infection Detected, Adware Installation, and Attack Detected refer to malicious traffic associated with the company's infrastructure, suggesting the compromise of at least one device.** Malware Infection refers to the command & control (C2) communications of malware emanating from an organization's infrastructure. Ransomware Infection Detected and Adware Installation are similar, except that they refer to specialized forms of malware. The most troubling one is Attack Detected, which refers to honeypot data indicating the use of an organization's machine to attack other machines.

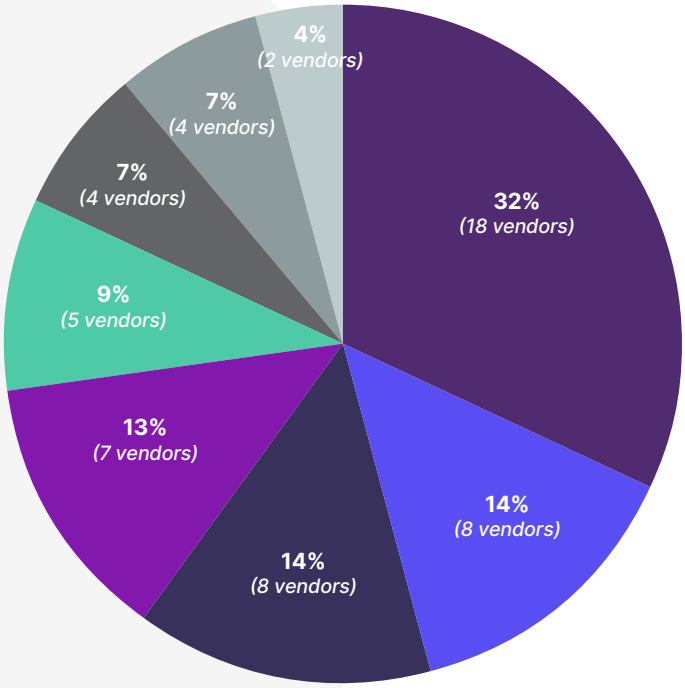
These issues might explain why the IP Reputation factor became more common as a lowest-scoring factor in the below-average subset of 56 vendors. Organizations with lower scores are more likely to experience breaches, and these four issues indicate the potential compromise of at least one machine at that organization. To see if this pattern holds true, and for further analysis of other specific issues with the most negative impact on the scores of the below-average vendors, we repeated the above query but limited it to that below-average subset.

Identified Problem Areas *(continued)*

Specific Security Issues *(continued)*

DISTRIBUTION OF MOST NEGATIVE SCORE IMPACT AMONG BELOW-AVERAGE VENDORS

- **Outdated Web Browser Observed (Endpoint Security):** 32% (18 vendors)
- **SPF Record Missing (DNS Health):** 14% (8 vendors)
- **Site Does Not Enforce HTTPS (Application Security):** 14% (8 vendors)
- **Ransomware Infection Detected (IP Reputation:)** 13% (7 vendors)
- **Malware Infection (IP Reputation):** 9% (5 vendors)
- **SSL/TLS Service Supports Weak Protocol (Network Security):** 7% (4 vendors)
- **Website Does Not Implement HSTS Best Practices (Application Security):** 7% (4 vendors)
- **Miscellaneous (Network Security):** 4% (2 vendors)



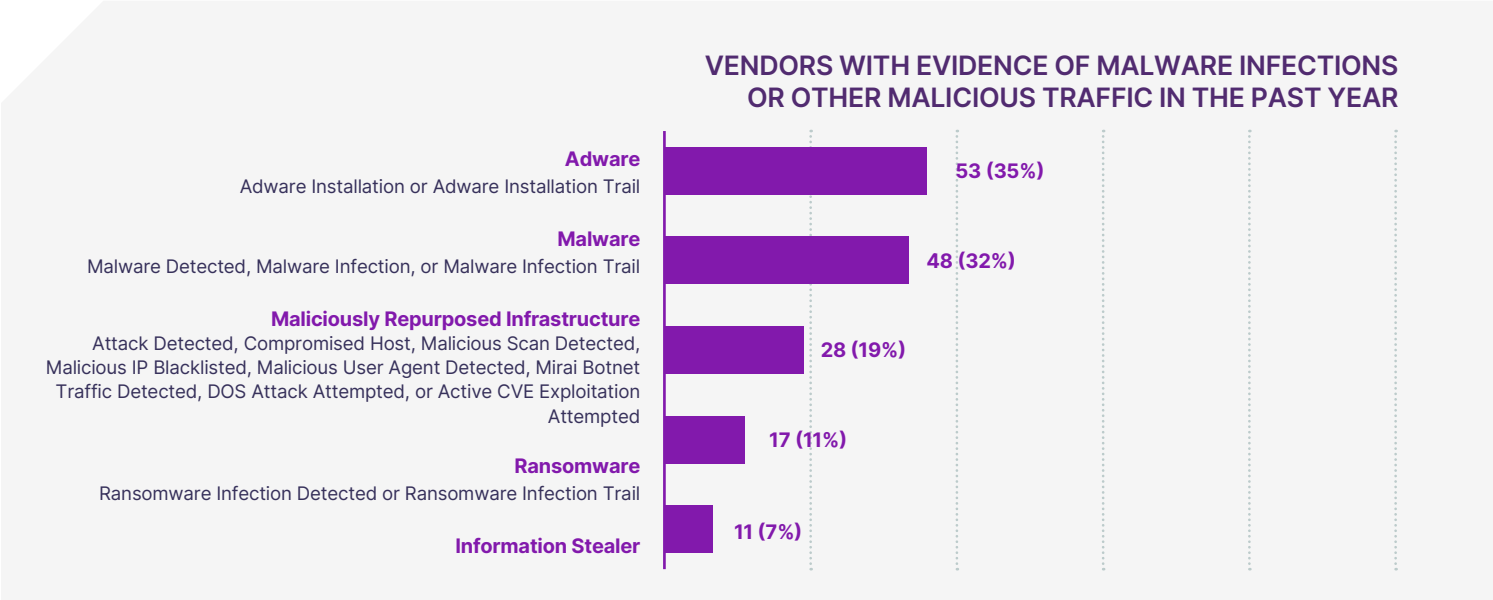
Outdated web browsers are clearly a key source of score-lowering risk, as they represented a notably larger proportion of the individual issues with the most negative impact on those vendors with below-average scores, compared to the total sample of 150 vendors. Missing SPF records still come in second place in this subset of below-average vendors, albeit by a much wider margin than in the total sample of 150 vendors.

This subset's most score-lowering issues included only two of the four IP Reputation issues above that suggest a compromised machine (Malware Infection and Ransomware Infection Detected). **The two of them combined nonetheless constituted a proportion of this subset (21%) nearly twice as large as that of the total sample (11%). This point supports what we posited above: lower-scoring vendors are more vulnerable to compromise and would thus be more likely to have malicious traffic suggesting a compromised device on their network.**

How Many of These Vendors Have Detectable Malware Infections?

The above findings regarding the IP Reputation of some of these vendors poses the question: how many of all 150 vendors have had detectable malware infections of at least one machine within their infrastructure within the past year, regardless of its negative score impact? We reviewed specific IP Reputation findings for all 150 vendors, yielding these results.

The first and most reassuring finding was that **88 of these 150 vendors, or 59%, did not have even a single finding of malware infection or other malicious traffic emanating from their networks within the past year. The other 62 vendors, or 41% of them, did have at least one piece of evidence indicating such security issues with at least one machine in the past year.** For the sake of simplicity and clarity, we have grouped these findings into five categories. Some vendors had findings in multiple categories, so the percentages do not equal 100%.



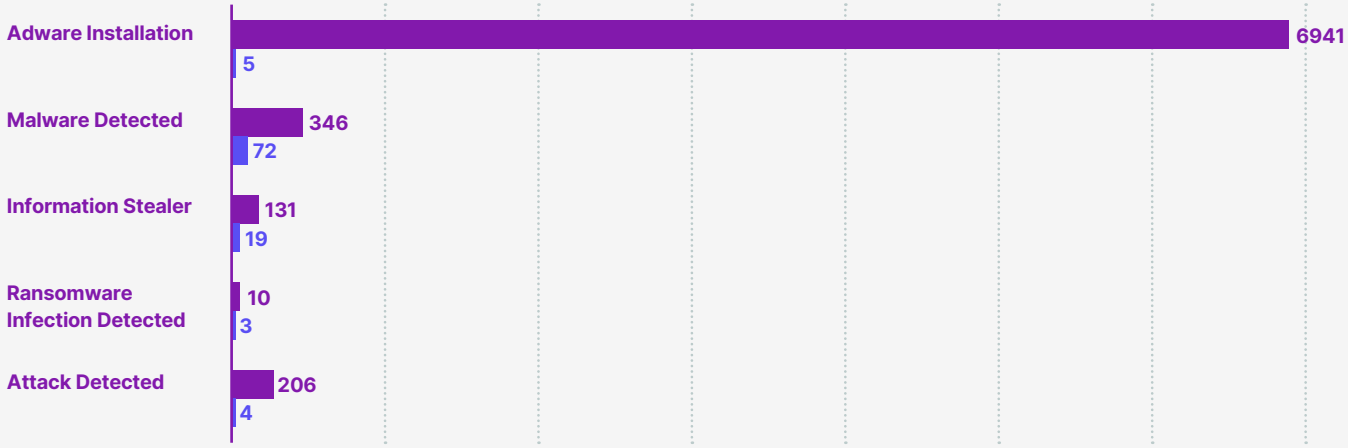
The interpretation of these findings poses challenges. On one hand, these findings include only those malware infections that SecurityScorecard was able to detect with its various data sources, such as sinkholes and honeypots, and are thus probably conservative. In keeping with "the cockroach theory," these findings could be indicators of more substantial compromises. On the other hand, the infection of one machine does not necessarily indicate a compromise or network breach beyond that one machine. Many of these findings could be isolated incidents.

The different categories of findings also have different potential implications. A ransomware infection generally has higher potential severity than other malware due to its disruptive effects, whereas the consequences of an adware infection may be less severe than those of other types of malware. The malicious repurposing of compromised machines is probably the most concerning finding, as it suggests that threat actors have been able to use compromised machines belonging to these vendors to attack other targets without those vendors detecting or stopping it.

How Many of These Vendors Have Detectable Malware Infections? *(continued)*

In an attempt to clarify the potential extent of these compromises, we compiled more statistics on these findings. The below figures represent the average and median numbers of potentially unique compromised machines in the infrastructure of each vendor with relevant findings. For each of the five categories above, we chose one type of finding that we consider the single-best indicator of the potential number of unique compromised devices on a vendor's network.

AVERAGE AND MEDIAN NUMBERS OF UNIQUE COMPROMISED DEVICES



The massive and glaring discrepancies between these average and median numbers indicates that the averages are skewed and significantly inflated upwards by a relatively small number of much higher values. In such cases, the median values are often a better representation of the overall dataset. Furthermore, we note that many of those vendors with much higher values are large service providers whose infrastructure for customers may surface in our findings (our methodology aims to factor out customers whenever that distinction is clear/possible).

Nonetheless, even a conservative interpretation of some of these figures is discouraging. A network with four machines attacking machines on other networks is generally a bad sign and probably a reflection of deeper problems. A network with three machines infected with ransomware can easily get worse, given the tendency of ransomware to move laterally and encrypt as many machines as possible. 19 information stealers on the same network have a strong chance of collecting credentials or other data that attackers can use to expand their access.

Other Variations by Subset

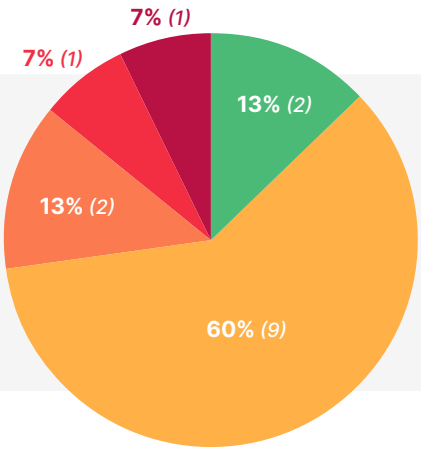
"Heavy Hitters"

We already delved into the below-average scores of that subset of vendors searching for factors responsible for heightened risk. We will now examine another subset of vendors that may pose higher supply chain risk simply for the vastly disproportionate concentration of customers and product usage in their hands: the "heavy hitters" described above in the Methodology section. Security issues at these vendors could jeopardize their enormous customer bases. We repeated the above queries on these 15 "heavy hitters," with the following results.

First of all, it is worth emphasizing that a majority of these "heavy hitters" (8 out of 15) are also members of the above-mentioned subset of 56 vendors with below-average scores. The average score for these "heavy hitters" is 80, and the median is 84. Those two figures are notably lower than those of the overall sample, and the slightly larger gap between the average and the median also suggests a slightly more negative skew than that of the overall sample. The distribution of letter grades among these "heavy hitters" is in the below pie chart.

DISTRIBUTION OF LETTER GRADES AMONG "HEAVY HITTERS"

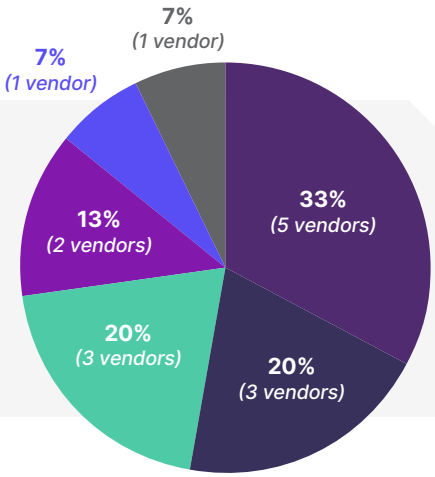
- A — 90 or higher
- B — 80 to 89
- C — 70 to 79
- D — 60 to 69
- F — less than 60



These grades clearly skew lower than those of the general sample, although the majority of these "heavy hitters" still had respectable "B" grades. Furthermore, to be fair, many of these organizations are responsible for massive amounts of instructure that may make it easier for security issues to fall through the cracks or remain undetected. Nonetheless, by the same token, these large vendors should also have more resources to devote to security. As Securityscorecard researchers previously demonstrated, there is a strong positive correlation between financial means and security hygiene. One would expect larger and more well-resourced companies to have better security hygiene, but this tendency does not always hold true, as in this case. In any event, **the tendency of these organizations with such vastly disproportionate technology market share to score lower does pose some serious concerns about its supply chain risk implications for the technology ecosystem and the broader economy.**

Other Variations by Subset *(continued)*

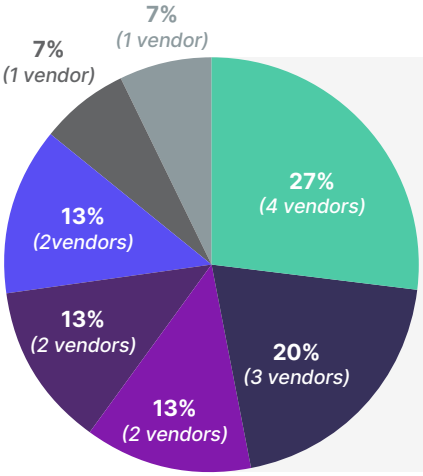
The distribution of lowest-scoring risk factors for these "heavy hitters" also differed from that of the overall sample. It is also worth noting that **one of these "heavy hitters" was the only vendor in the entire sample to receive its lowest factor score in Patching Cadence.**



LOWEST-SCORING SECURITY FACTORS FOR HEAVY HITTERS

- **Application Security:** 33% (5 vendors)
- **Endpoint Security:** 20% (3 vendors)
- **IP Reputation:** 20% (3 vendors)
- **Network Security:** 13% (2 vendors)
- **DNS Health:** 7% (1 vendor)
- **Patching Cadence:** 7% (1 vendor)

The issues that had the most negative impact on the scores of these "heavy hitters" **echo the above findings about IP Reputation issues**, particularly for vendors with below-average scores.



SECURITY ISSUES WITH MOST NEGATIVE IMPACT ON SCORES OF HEAVY HITTERS

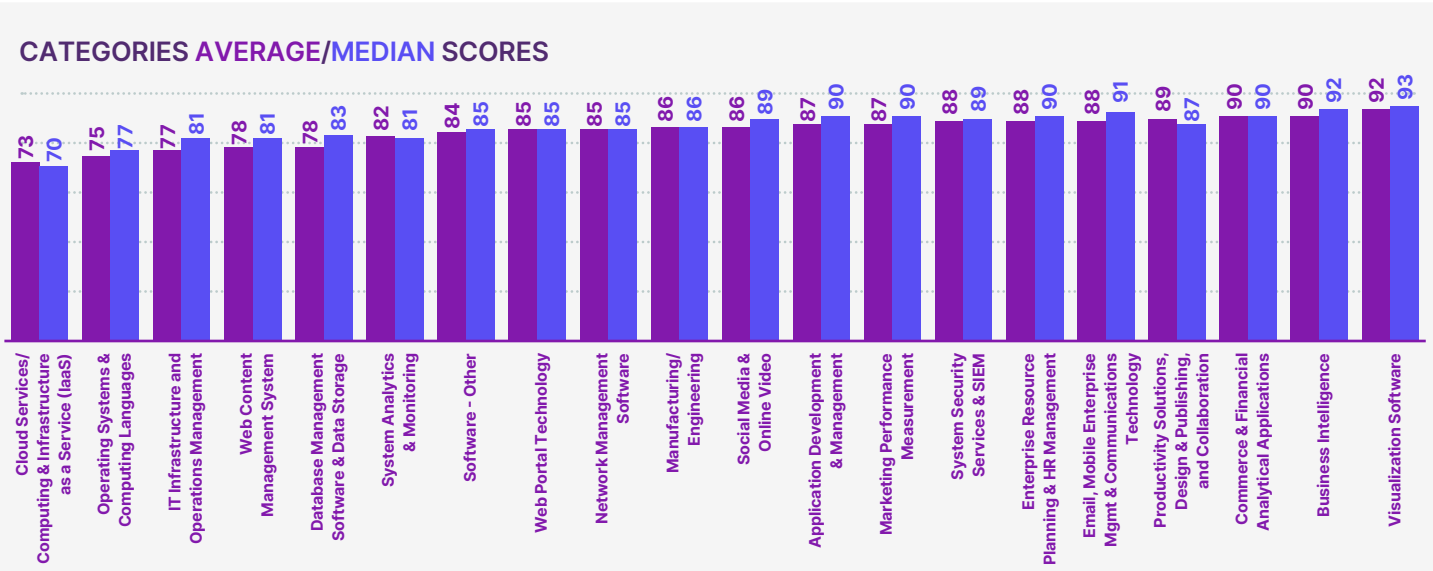
- **Malware Infection (IP Reputation):** 27% (4 vendors)
- **Site Does Not Enforce HTTPS (Application Security):** 20% (3 vendors)
- **Ransomware Infection (IP Reputation):** 13% (2 vendors)
- **Outdated Web Browser Observed (Endpoint Security):** 13% (2 vendors)
- **SPF Record Missing (DNS Health):** 13% (2 vendors)
- **Content Security Policy is Missing (Application Security):** 7% (1 vendors)
- **Website Does Not Implement HSTS Best Practices (Application Security):** 7% (1 vendor)

The two IP Reputation issues indicate that **6 out of the 15 "heavy hitters" (40%) had malicious traffic consistent with a ransomware or other malware infection emanating from their infrastructure as their most score-lowering issue.** This proportion was almost twice as high as we saw above in the subset of below-average vendors (21%) and many times larger than in the overall sample (11%). To be fair and to put this finding in context, some of these "heavy hitters" have massive amounts of infrastructure. Their size gives them more attack surface to exploit and may make it easier for a compromise to slip through the cracks but may also make it less significant in the grand scheme of things. One compromised device could serve as a foothold for a broader network breach but could also amount to little more than an easily remediated and isolated nuisance. As for other issues highlighted above, outdated web browsers and missing SPF records are still a problem for these "heavy hitters," but in lower proportions.

Other Variations by Subset *(continued)*

Market Niche and Company/Product Type

Many security research publications use quantitative methods to divide their data samples by industry in search of industry-specific trends or variations. This approach would not work for our sample, as most vendors would fall under the Technology vertical. AVD nonetheless has more granular categorizations for technology vendors and their various products in its data collection. We compiled average and median scoring data for vendors on the basis of these 20 categories.



These figures suggest that the categories of vendors with some of the greatest potential to cause inadvertent harm to their customers via compromises also have some of the lowest-trending scores and thus have the greatest risk of compromise in the first place. Consider these risks that could result from compromises of vendors in the five lowest-scoring categories above, all of which have average scores below that of the total sample (84).

- The lowest-scoring category, Cloud Services/ Computing & IaaS, puts customer data at risk of exposure when using such services. Compromised cloud infrastructure can also facilitate attacks aiming to gain access to customer environments.
- The next-lowest category includes developers whose compromise could enable supply chain attacks via the discovery of vulnerabilities in source code or the insertion of backdoors via unauthorized changes to source code.
- The next-lowest category includes vendors to whom businesses outsource their IT operations and infrastructure. These vendors, such as managed service providers (MSPs), have become popular targets for ransomware operators to use as a convenient way to gain access to numerous victims at once in large-scale third-party attacks.
- Content management systems (CMS), the focus of the next-lowest category, are popular attack vectors for threat actors seeking to exploit vulnerabilities in an organization's public-facing web infrastructure.
- The next-lowest category of vendors, for database management and data storage, can put customers and their data at risk in the event of a compromise by giving attackers access to data storage or by enabling access to their environments via a compromise or exploitation of database management software.

How Can the Security of The Top 150 Vendors Affect Your Business?

Compromises at these vendors can result in third-party data breaches for their customers. In a textbook example of such a breach, the healthcare platform of a subsidiary of a major U.S. pharmaceutical company with over 1 million users experienced a compromise of user/patient information via IBM as of August 2023. The compromised data included PHI, such as conditions, medications, and health insurance details, as well as regular PII. It was not clear how the attackers compromised the relevant IBM database, but the investigation suggested that they may have exploited a vulnerability or security misconfiguration.

The degree of customer exposure from a third-party breach may vary from one case to another, depending on the degree of access that attackers manage to obtain. For example, in December 2023, MongoDB disclosed a breach that exposed customer amount 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 infrastructure that the attackers did not reach.

Distributed denial of service (DDoS) attacks are another threat to these vendors and their customers. They are technically not breaches or compromises per se, 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 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 vendors may not be a breach per se but nonetheless represents the violation of policies aiming to protect users from such attacks. For example, in February 2024, a cryptocurrency investor lost the equivalent of $490,000 by 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."

Software and Other Vulnerabilities

One does not have to be a customer or other third-party of these vendors to suffer a compromise from its security flaws. In fact, a July-August 2023 "EvilProxy" phishing campaign used an open redirection vulnerability in the website of the job posting website Indeed to compromise Microsoft credentials for senior executives in a variety of industries, particularly banking, insurance, and real estate. The redirection from Indeed via an email message aimed to give greater credibility to the phishing page, which acted as a reverse proxy between the victim and Microsoft. The phishing page stole session cookies that enabled attackers to bypass MFA.

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). Storm-0558 has historically focused on U.S. and European governmental, diplomatic, and economic targets, as well as individuals with access to information on Taiwan and Xinjiang.

Product security vulnerabilities in the software that many of these companies sell can have an equal or greater impact on their customers than actual breaches of those vendors. Exploitation of these CVEs has been the cause of many high-profile and large-scale third-party breaches. **Such vulnerabilities in common software are popular attack vectors because of the potential to infect so many victims with relatively little labor input on their part.** Below are some of the most significant CVEs in products from these top vendors in the past year.

- **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 usually large-scale campaign in May-June 2023 that affected an unusually large number of victims both directly and via third-party breaches. Many organizations that used MOVEit experienced direct compromises. Furthermore, 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 the most widely exploited vulnerability of 2023 and a top third-party attack vector.**
- **CVE-2023-4966, known popularly as "CitrixBleed," a critical zero-day sensitive information disclosure vulnerability in Citrix NetScaler ADC and NetScaler Gateway** that Citrix disclosed in October 2023. 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.
- **CVE-2023-3519, a separate critical zero-day remote code execution (RCE) vulnerability in Citrix NetScaler ADC and NetScaler Gateway** that Citrix disclosed in July 2023. It later emerged that, in June 2023, unidentified actors had used this vulnerability against a U.S. critical infrastructure organization to install a webshell. Other researchers determined that at least 640 servers had been compromised by "China Chopper" webshells, a tool **typical of state-sponsored Chinese cyber espionage.**

Software and Other Vulnerabilities

(continued)

- **CVE-2023-22515**, a critical zero-day broken access control vulnerability in **Atlassian's Confluence Data Center and Server Software**. As of early October 2023, state-sponsored actors had exploited this vulnerability to create new administrator accounts. Researchers attributed this activity to the state-sponsored Chinese actors 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 useful source of the IP that state-sponsored Chinese actors often seek.
- **CVE-2023-20198**, a critical zero-day privilege escalation vulnerability in Cisco's IOS XE operating system for networking devices, and **CVE-2023-20273**, a high-severity zero-day privilege escalation vulnerability used in the same attacks as of September-October 2023. The actors exploited the former to create new accounts on vulnerable and then exploited the latter to inject commands with root privileges. Such compromises enabled attackers to monitor traffic, move laterally into networks, and conduct man-in-the-middle (MITM) attacks. Researchers determined **these attacks had compromised approximately 40,000 devices** worldwide, with the highest concentrations in the U.S., South America, and South and Southeast Asia. Attackers had begun using at least 120 of these compromised devices for attacks on other machines.
- **CVE-2024-27198**, a critical zero-day authentication bypass vulnerability in JetBrain's TeamCity software development platform, and CVE-2024-27199, a related high-severity zero-day authentication bypass vulnerability in the same platform. **Compromises of this software development platform could have enabled supply chain compromises by giving attackers access to source code in development.** 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 above examples contained multiple references to state-sponsored Chinese cyber espionage. These actors are probably among the most prolific attackers of U.S., European, and East Asian technology sectors to which these top vendors belong. 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 Solar Winds third-party technology supply chain compromises put state-sponsored Russian actors on the map in this field, so to speak.

Their state-sponsored Chinese counterparts nonetheless have a much longer history of third-party supply chain compromises. For example, Chinese APT10 was a pioneer of 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 its businesses are key targets for state-sponsored Chinese actors because of their relevance to the Chinese government's ambitious economic development goals. These actors seek to steal foreign IP that reduces their research & development (R&D) costs, as well as competitive intelligence that enables them to undercut foreign businesses in global markets.

Conclusions and Recommendations

Data-Driven Vetting vs. Brand Name Recognition

Vendor vetting should be fact-based and data-driven. This principle is the foundation of our platform and our MAX managed service. One should not adhere to the common misconception that large companies with well-known brand names, which may have a "halo effect" on perceptions of them, are somehow inherently better or more reliable from a security perspective or otherwise. As we have seen above, the evidence does not support this perception, and in some cases the opposite may be true. On one hand, the large budgets that often come along with well-known brand names may give their security teams more resources with which to tackle security challenges. By the same token, the greater size, complexity, and often public-facing nature of their infrastructure also gives them more challenges as well. Greater size and more resources do not necessarily make them better at security or any other field, but they can help.

"The Bigger They Are, the More Likely They are to Fall...on You!"

To take the above point further, not only are bigger companies not necessarily any better than their smaller counterparts at security, they may actually pose greater third-party risk simply because of their size and market share, through no fault of their own. Those qualities often make them more appealing targets for threat actors, including: ransomware operators seeking larger ransoms from larger companies; those that seek to maximize the number of targets that they can access by compromising a single third-party vendor or product; and state-sponsored threat actors seeking access to sensitive communications or infrastructure or high-value intellectual property.

Outdated Web Browsers

The salience of outdated web browsers deserves further consideration as not just a security issue to address in its own right, but perhaps as a symptom of broader or deeper problems. It is worth asking why outdated browsers are so common at many organizations. Is it because users are either unaware of or unconcerned about the implications of using older and thus more vulnerable browsers? Are they thus in need of further security education? Is it because organizations do not have the resources or policies to monitor user update cadence, require timely updates, and enforce those requirements? Answering such questions might not just result in more frequently updated browsers but also improve the overall security culture of an organization, such as with changes or additions to user security education or update mechanisms and policies.

Missing SPF Records

Our researchers were surprised to discover the degree to which missing SPF records were a problem. DNS Health overall was not that salient of a risk factor in this sample, so it is curious that this particular DNS Health issue stood out so prominently in second place overall, after outdated web browsers. In any event, it deserves priority consideration in vendor vetting, given its potential to enable email spoofing that could result in compromises of either the vendors themselves, their customers, or other parties. Email is such a common attack vector that any measures that organizations can take to make it harder for threat actors to use are welcome.

Conclusions and Recommendations *(continued)*

IDS/IPS , Sinkholes, and Honeypots

The number of potentially infected or maliciously repurposed machines that our sources revealed raises the obvious question: how many of these vendors or other parties have detected (or not detected) these compromises, and what if anything have they done about it? One would hope that their intrusion detection systems and intrusion prevention systems (IDS/IPS) and other security solutions would have identified these incidents for remediation. The scale of activity on some of these networks nonetheless suggests that at least some of these compromises may have gone unnoticed or unaddressed for non-trivial amounts of time. Sinkholes and honeypots were our main sources for these findings. If your threat intelligence program does not already have such sources, it should acquire them to enhance its coverage. Such data feeds can also be useful to your TPRM programs as a source of information on possible compromises at vendors.

Categories of Vendors to Prioritize for Vetting

We identified above five of the 20 categories of vendors with both below-average scores and the potential to inflict greater third-party damage in the event of a compromise (which is more likely, given their lower scores). Out of those five categories, we recommend making three of them higher priorities for TPRM and VRM programs: Cloud Services/Computing & Infrastructure as a Service (IaaS); IT Infrastructure and Operations Management; and Database Management Software & Data Storage. Compromises of these vendors have the greatest potential for the most direct and severe third-party impact on their customers, such as by enabling access to customer infrastructure or data, given the nature of the services they provide and the more "intimate" access they require. The other two categories of vendors (Operating Systems & Computing Languages and Web Content Management System) also deserve special consideration, but with more of a focus on product or application security issues, rather than network breaches per se (which could nonetheless enable attackers to discover vulnerabilities or insert backdoors).

China

The frequency with which reports of attacks on these vendors and their products mention state-sponsored Chinese cyber espionage suggests that it should be a high priority for threat intelligence coverage, or at least higher than its Russian counterpart. The scale and severity of the Russian SolarWinds breaches may have distracted some threat intelligence consumers from the longer track record and greater demonstrated interest of Chinese actors in the technology & telecommunications industry, including: their pioneering use of MSPs as third-party attack vectors; and the key importance of technical intellectual property to China's development goals.

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

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