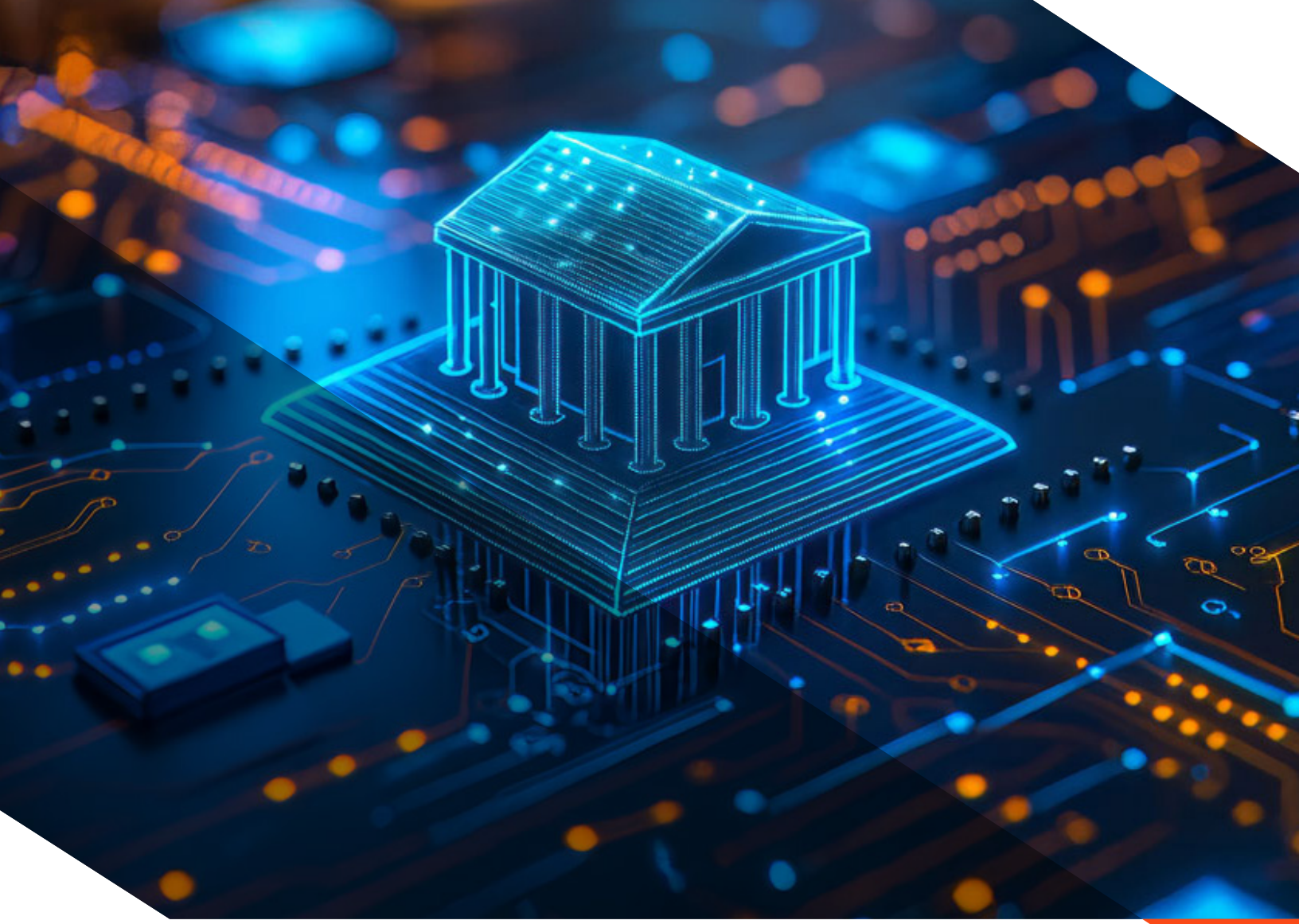

Exposed Cyber Risk in the Financial Sector and its Supply Chain

By Jake Olcott and Ben Edwards

November 2025

BITSIGHT TRACE

The Financial Sector continues to be one of the most targeted industries by sophisticated cyber threat actors, and the providers that serve the industry are increasingly under attack.

But who are these technology providers that comprise the Financial Sector's global supply chain? What are the sector's most significant technological dependencies and greatest risks? And how can Finance leaders remediate these risks?

Bitsight analyzed observable technical connections between financial organizations and their suppliers to develop a view of the digital Financial Sector supply chain.[1] In all, we analyzed 41,511 financial organizations and identified 50,232 third-party technology provider relationships.[2] We then leveraged our cybersecurity performance data collection to assess specific risks to the suppliers.

The findings reveal a sector with critical dependencies, unpatched vulnerabilities, and unmonitored risks that could cause significant harm to individual organizations and the sector as a whole. Read on to learn more, and to see how security leaders can tackle these challenges head-on.

The 99 “most critical” suppliers to the Financial Sector

Understanding which suppliers are ubiquitous is critical to helping organizations understand their own dependencies and mitigate sectoral risk. So which organizations are most important to the Financial Sector supply chain? Data can help answer some of the most fundamental questions we have about the sector’s technological dependencies, including:

- Which suppliers are most commonly used across the sector?
- Which suppliers are used by the financial organizations with the largest market share?
- Which suppliers could be considered “most critical”?

Bitsight developed a methodology to determine the Financial Sector’s 99 “most critical” suppliers. Our goal was to identify the most common technology providers throughout the Financial Sector. We also leveraged revenue and market share data of financial organizations to determine the criticality of a supplier weighted by the revenue of the customers that they serve. The result is a list of the 99 “most critical” suppliers that serve the greatest proportion of—and the most valuable—finance organizations, as can be seen in Figure 1.

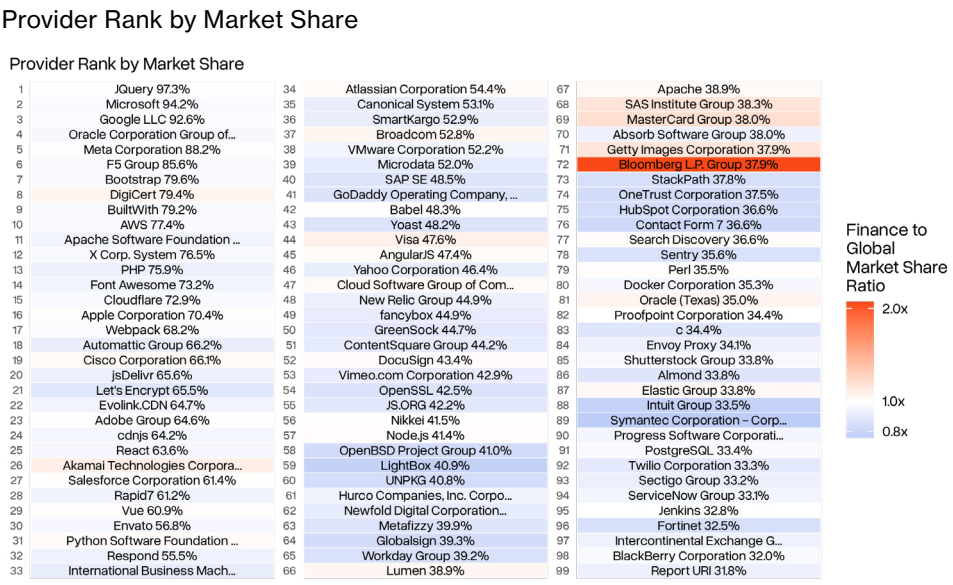

Figure 1. The Financial Sector’s “Critical 99.”

It’s a list with some obvious inclusions as well as some surprises. Many of the identified providers are the same that we observed in our global supply chain analysis. Well-known giants like Microsoft and Google, as well as indispensable Open Source Software like JQuery and Python, are no-brainers. But there are some key differences in Financial Sector dependencies compared to the economy at large. Burning bright red because of their outsized market share in the Financial Sector is Bloomberg L.P. Group, a supplier that provides the necessary tools for financial analysts and traders, which has an outsized footprint in the Financial Sector. And, looking more closely, there are some subtle differences in Financial Sector usage in, for example, Digital Certificate Providers, when compared to the broader market. The Financial Sector was an early adopter of PKI and digital certificates, and this is reflected in their reliance on the older, more traditional DigiCert rather than the newer “Let’s Encrypt.”

While some of these “most critical” providers are well known and obvious, there are others who may not be as recognized. We have witnessed in recent years the rise of supply chain cyber attacks that can have a damaging impact on sectors and industries, and even across the broader economy. In many situations, the breached suppliers are only discovered to be critical after the incident has occurred and the impact can be clearly observed. Our goal with this research is to highlight these “hidden pillars” of the Financial Sector so that the work can be done to remediate risk and improve resilience across the sector.

Notable suppliers with outsized market share in the Financial Sector

There are some large global suppliers who have significant market share in the Financial Sector compared to their presence in other markets. These notable “hidden pillars” are included in Figure 2.

Market Share

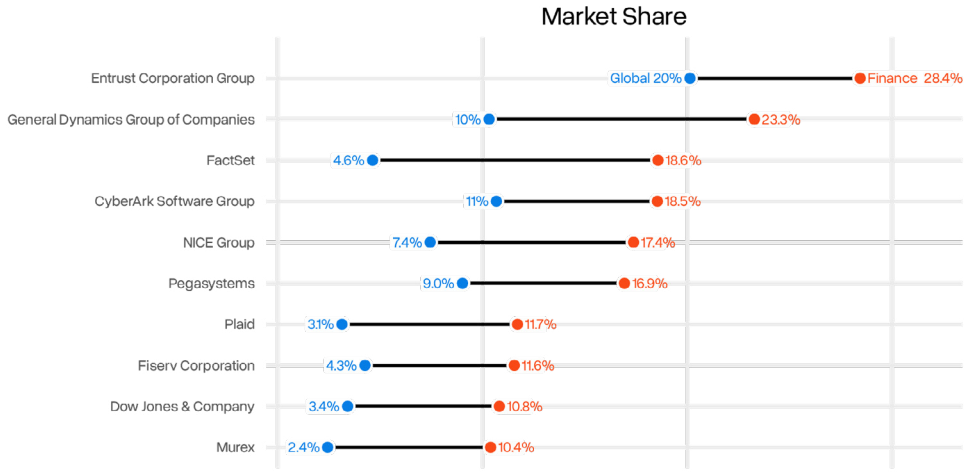

Figure 2. Hidden pillars of the Financial Sector.

The appearance of some of these suppliers is obvious. Plaid, Murex, FactSet, Dow Jones & Company, and Fiserv provide specialized technology and data to the Financial Sector. CyberArk and Entrust deal in Identity and Access Management solutions, which is critical for secure operation at any organization but even more so in finance. Pegasystems provides technical automation services and has also found a niche in the Financial Sector.

But what about suppliers like General Dynamics and NICE Group? Interestingly, General Dynamics provides consulting for COBOL, the programming language used on large mainframes that are still the backbone of transaction processing throughout the sector. NICE Group provides commercial and residential building automation, access control, and security systems, and apparently has a large customer base within the Financial Sector. Once again, data helps illuminate critical dependencies that may not be apparent.

Security performance comparison: Financial Sector organizations vs. their suppliers

Having established a view into the Financial Sector supply chain, we turn our focus to the cybersecurity performance of the suppliers themselves. A critical supplier with a large digital footprint and a high number of security issues could prove a blinking red light for the Financial Sector and the organizations that rely on it.

There are many laws and regulations governing third-party cyber risk management in the Financial Sector. Regulators like the FDIC, Federal Reserve, Securities and Exchange Commission, and FINRA provide guidance and enforce compliance in areas like third-party due diligence and ongoing monitoring. These requirements are designed to ensure that the financial organization is taking advantage of the benefits and efficiencies provided by the third party, while also maintaining responsibility for the risks and ensuring that the third party is carrying out its obligations.

Interestingly, many Financial Sector suppliers tend to perform worse in key cybersecurity risk vectors measured by Bitsight compared to their Financial Sector organization customers. In Figure 3, we analyzed the cybersecurity performance of suppliers across our key cybersecurity risk vectors[3] in order to make the comparison.

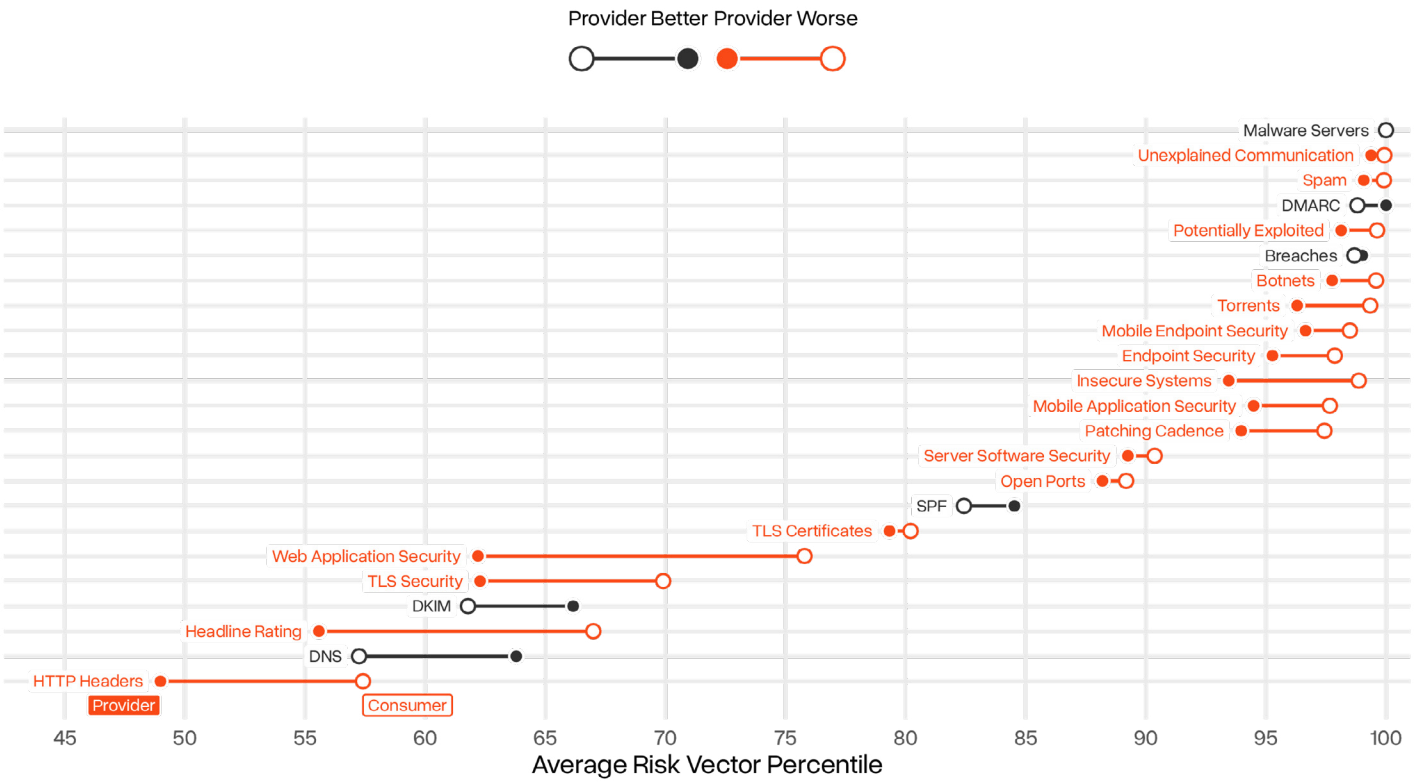

Figure 3. Comparison of Financial Sector providers to consumers.

On average, Financial Sector suppliers tend to have slightly lower security performance than their consumers, with differences of up to 15% in 16 of the 22 Bitsight risk vectors analyzed. Notably, providers perform better in four of the six vectors related to security standards (DMARC, SPF, DKIM, and DNSSEC), which aligns with expectations for larger, more technology-focused organizations.

Considering these observations, we can consider a few root causes for the consistent difference in performance by suppliers compared to their customers. First, providers leverage digital infrastructure as a means of business, meaning they will have a greater digital footprint and likely more digital risk.[4] Second, there is a potential risk transfer occurring, where providers are solving specific business problems for consumers and are also absorbing the cyber risks associated with the problems. Finally, providers tend to have a higher volume of exposures and may have better compensating and reactive controls.

Nevertheless, given the regulatory requirements and risk of exposure, it may be troubling for Financial Sector organizations to learn that their suppliers tend to underperform when it comes to security. Ultimately, consumers of these products and services must perform rigorous diligence and monitoring, assess the operational and reputational risks to their organizations, and determine if these gaps are indeed meaningful.

Suppliers' market size and security posture

It is conventional wisdom that larger organizations—with greater funding, personnel, and mature processes—should display stronger cybersecurity performance compared to smaller organizations. However, larger organizations also tend to have a broader attack surface and risk findings. So we turned to the data to try to answer the question: do larger Financial Sector suppliers (as measured by market share) outperform their smaller counterparts when it comes to cybersecurity?

The answer may surprise you. Bitsight finds that suppliers of all sizes within the Financial Sector supply chain struggle with their security posture. However, we find that Financial Sector providers with larger market share tend to have worse security posture compared with the smaller Financial Sector suppliers that Bitsight monitors.

To arrive at this finding, we divided the Bitsight security rating into the top and bottom percentiles and looked at third-party suppliers across different market share segments, as can be seen in Figure 4.

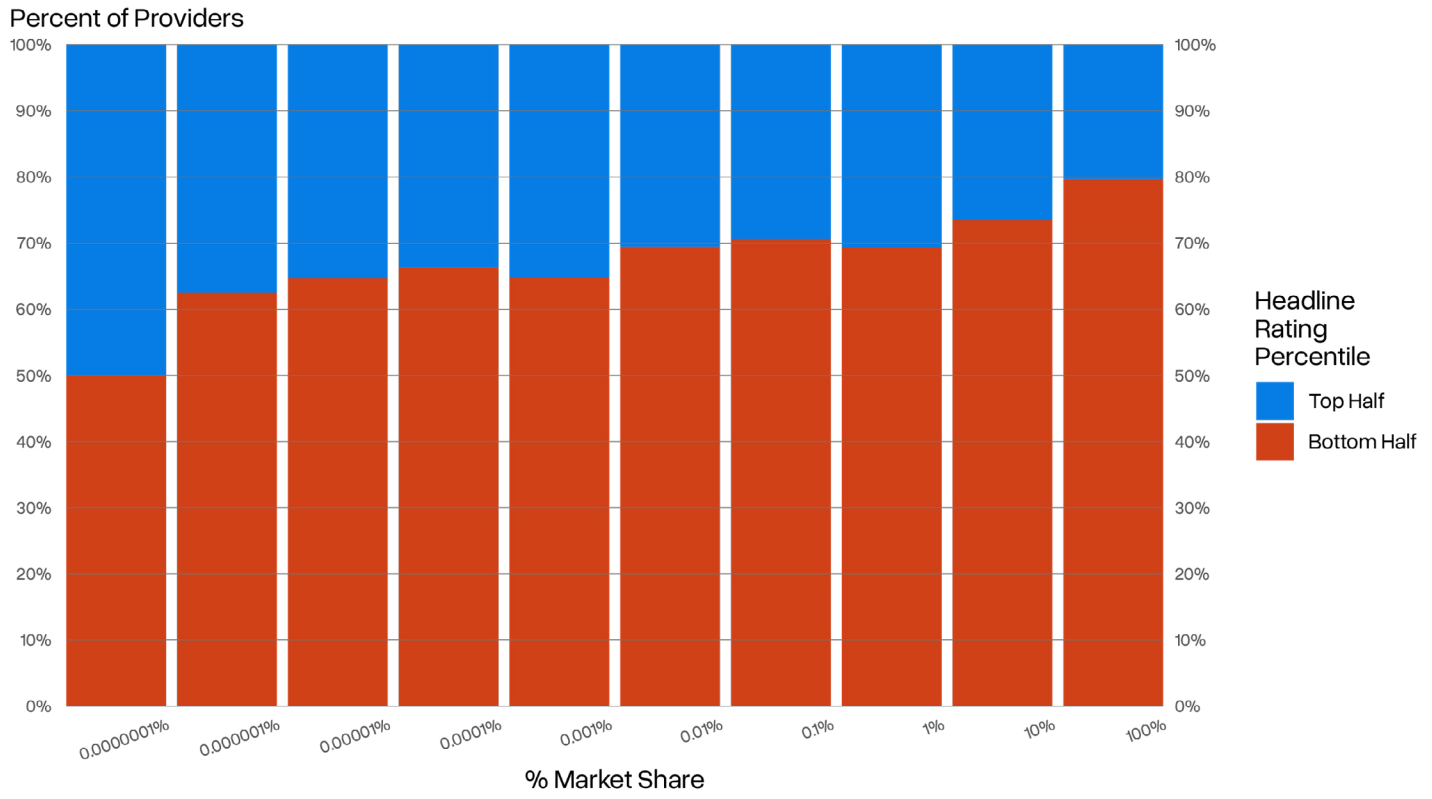

Figure 4. Headline rating percentile by market share for financial sector providers.

We find that Financial Sector organizations are outpacing organizations in other sectors, monitoring on average

36.3%

of their overall supply chain compared to

24.6%

by other organizations.[5]

Financial sector supply chain monitoring rates

Having established a view into supplier criticality and performance, we now turn our attention to steps that organizations are taking to reduce their risk. For this research, we focused on the practice of continuous monitoring: a proactive process to assess performance and risk in real-time. It is generally considered a best practice (and regulatory obligation) within the Financial Sector to continuously monitor cyber risk of critical supply chain organizations. Given the risk that suppliers pose, we wanted to understand how Financial Sector organizations are monitoring their suppliers and whether there are any interesting or meaningful insights around continuous monitoring trends that may be relevant for the broader sector.

How do continuous monitoring rates compare between the Financial Sector and other sectors? Again, we turn to our data. Bitsight counts nearly 600 Financial Sector organizations as customers who are collectively monitoring over 46,000 organizations. Given our ability to infer suppliers based on our own technology, we can calculate for any of our customers what fraction of their supply chain they are monitoring.

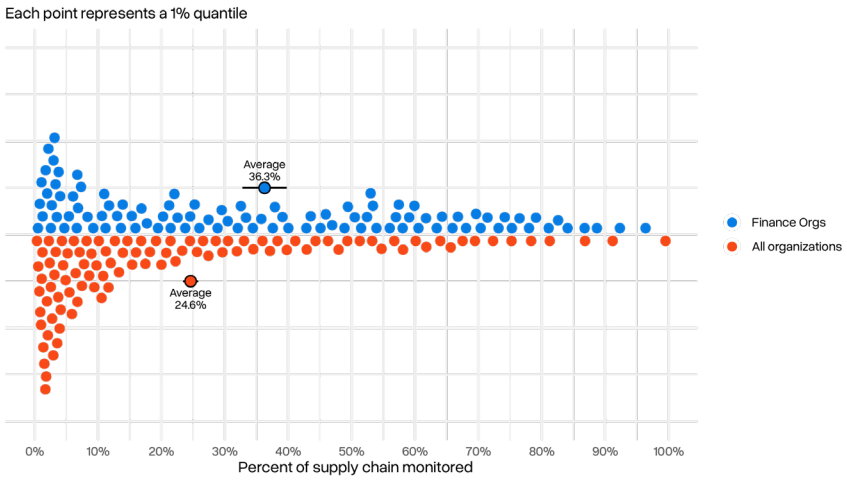

Figure 5. Distribution of percentage of supply chain monitored. Each dot represents 1% of organizations. Higher (or lower depending on side) stacks indicate higher concentrations.

While this is good relative to other sectors, is it enough? Some may have expected that Financial Sector organizations would have a significantly higher rate of monitoring compared to other sectors given the financial industry's longstanding third-party risk requirements. And given the growing number of supply chain incidents involving technology providers, perhaps Financial Sector organizations should be monitoring more of their providers. On the other hand, it is possible that Financial Sector organizations have undertaken a criticality determination and concluded that the vast majority of technology vendors within their supply chain do not need to be continuously monitored. The truth is not entirely obvious from the data.

Security performance comparison: Monitored vs. unmonitored financial sector suppliers

Unmonitored organizations can be a significant, hidden risk to Financial Sector organizations.

We analyzed the security performance of Financial Sector supply chain organizations who are being monitored by Bitsight customers compared to organizations that are not currently monitored by Bitsight customers. We want to understand if there is any correlation between monitored organizations and their cybersecurity performance.

First, we observe a gap in performance between organizations monitored by Bitsight customers and those that are not. This is true whether an organization is a Financial Sector organization or a Financial Sector supplier. We also observe that there is a wider performance gap between monitored and unmonitored Financial Sector suppliers compared to monitored and unmonitored Financial Sector organizations. However, there is no clear performance difference between the Financial Sector and other sectors.

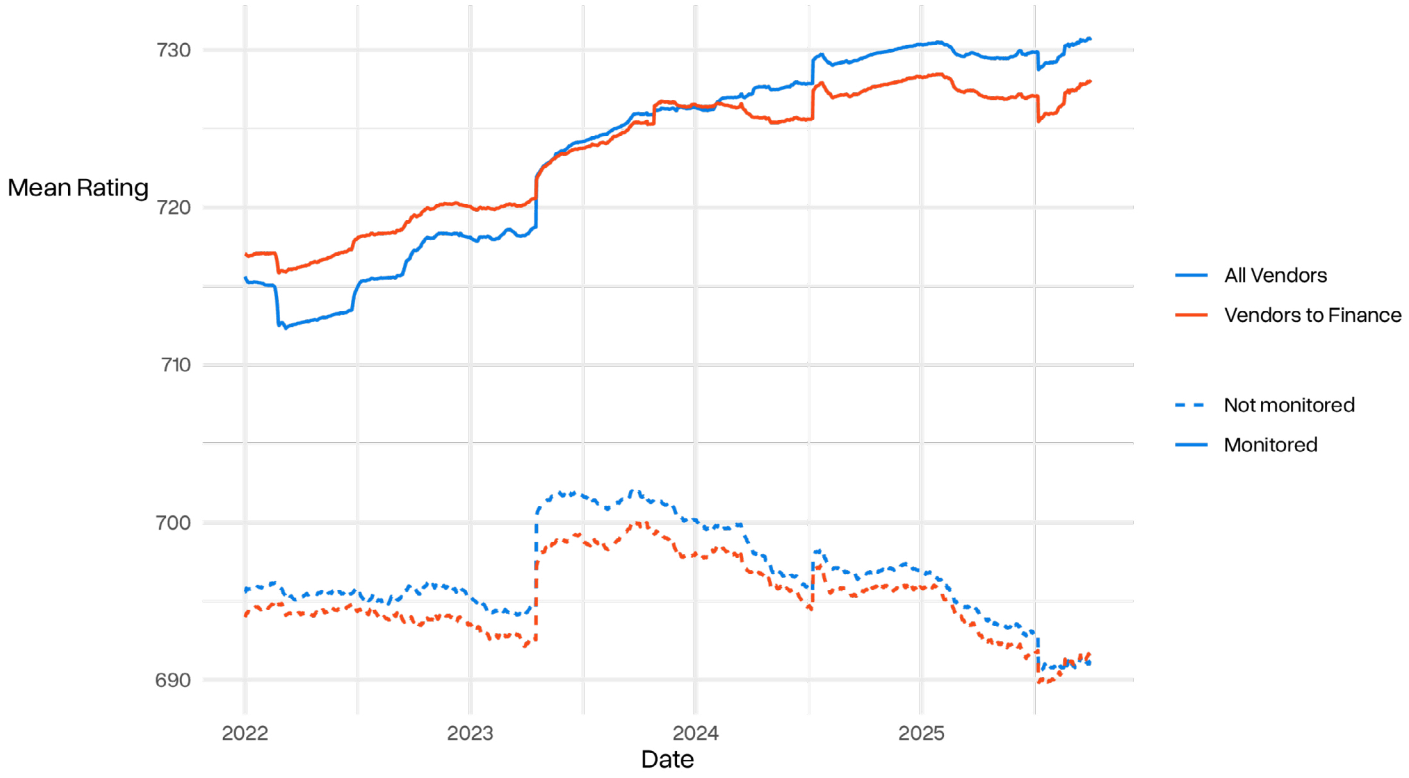

Figure 6. Average headline rating for providers among various categorizations.

We further find that the rate of exposure among Financial suppliers who are not being monitored by Bitsight customers is worse across several key categories related to vulnerability management:

Unmonitored Financial Sector suppliers have

2.9x

more “critical” level CVEs within their environment compared to monitored Financial Sector suppliers.

Unmonitored Financial Sector suppliers have

2.8x

more Known Exploited Vulnerabilities within their environment compared to monitored Financial Sector suppliers.

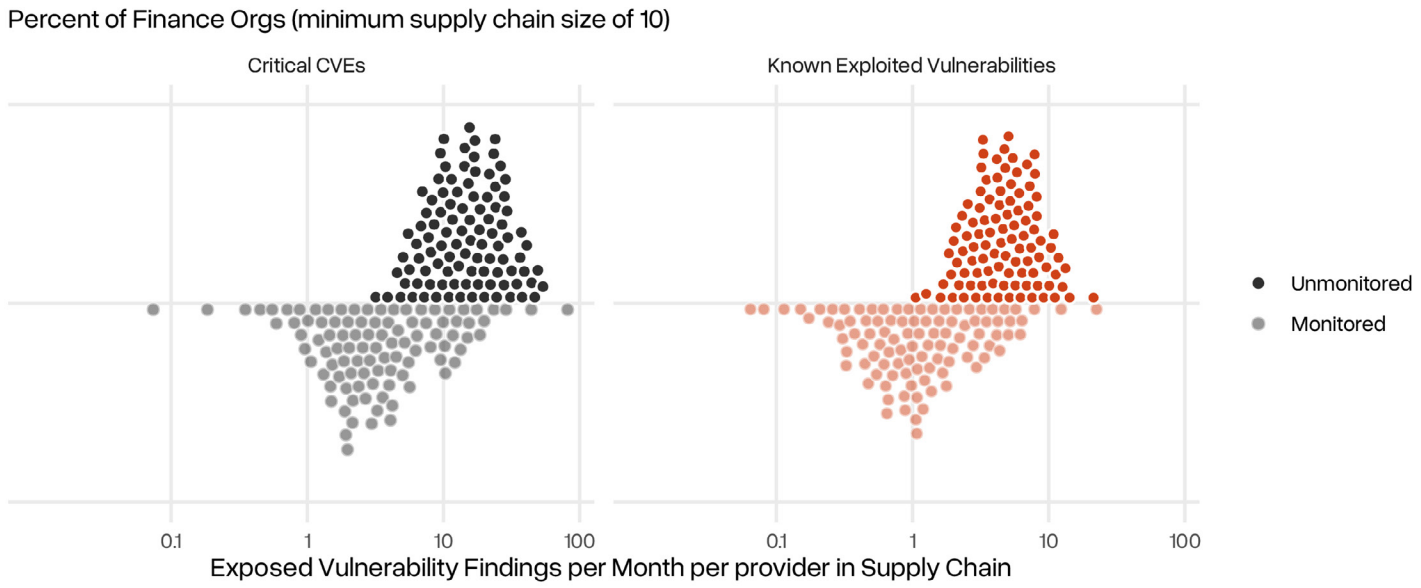

Figure 7. Unmonitored and unmonitored financial organizations as related to identified critical CVEs and KEVs in their supply chain.

Also interesting is that beyond the higher risk in the Financial Sector's unmonitored supply chain, there are also specific exposures that are more prevalent.

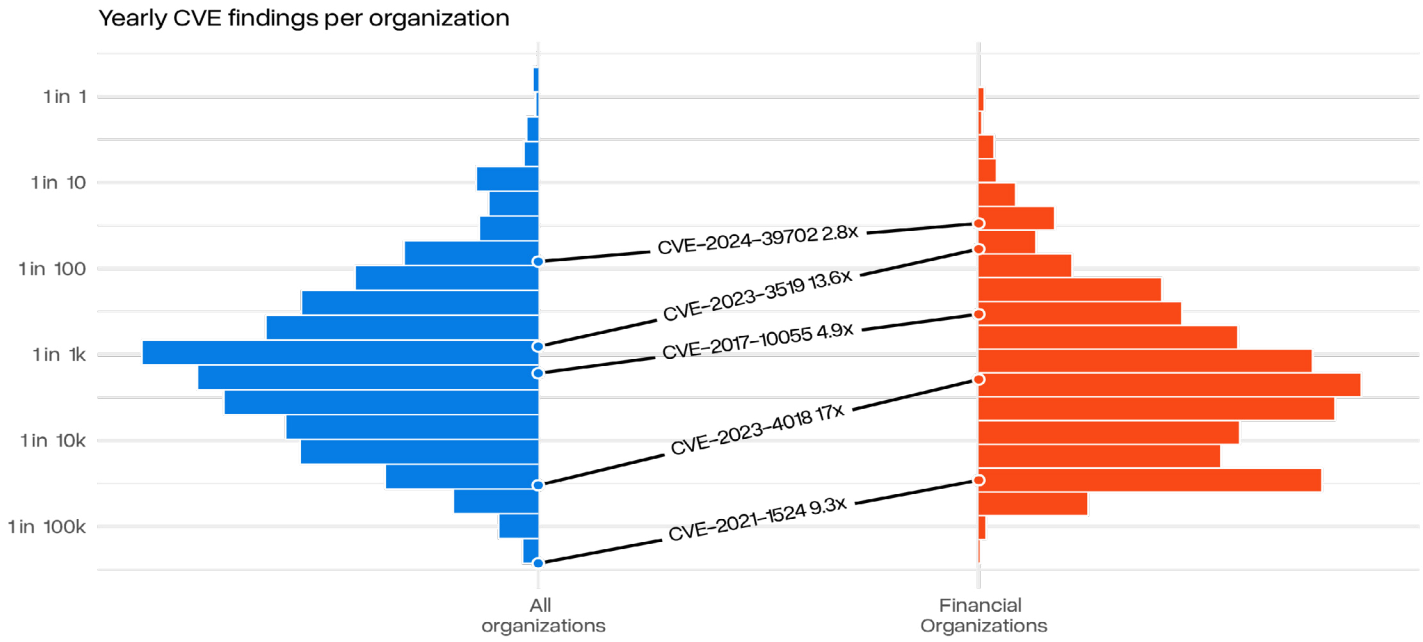

Figure 8. Yearly CVE findings per organization.

Do the number of organizations monitoring a supplier have any impact on the supplier's performance? Interestingly, we found that there is a slight decrease in the security performance of organizations who are monitored by more organizations.

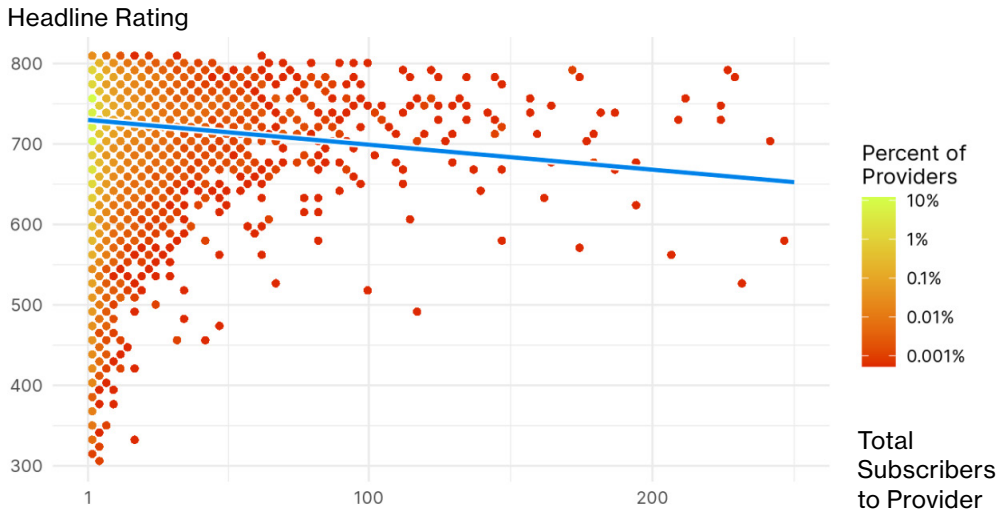

Figure 9. Security performance of organizations based on supplier monitoring.

There may be many reasons for this finding, including that some of the most heavily monitored organizations in the Bitsight platform are also the world's largest organizations. We believe this is a trend worth more analysis and we will be doing additional research into this area, including the impact that direct engagement with organizations has on security posture.

Conclusion

With the acceleration of cyber attacks targeting critical Financial Sector vendors, it has never been more important for Financial Sector leaders to assess and monitor the risk and exposure of organizations within their supply chain. Bitsight data shows that critical Financial Sector suppliers are indeed at risk, often underperforming Financial Sector organizations themselves in critical areas of security like vulnerability management. The challenge for Financial Sector leaders is to implement a comprehensive supply chain risk management program that continuously monitors key organizations. While data shows that Financial Sector organizations are better than others when it comes to continuous monitoring, there are still significant gaps that result in critical suppliers going unobserved. Unfortunately, these unmonitored suppliers could pose the greatest risk to the organization.

For greater visibility into your supply chain, help with identifying unknown risks and exposure, and prioritization based on validated analytics and unique threat intelligence, you can trust Bitsight. Talk to our team to learn more.

[1] We use the terms vendor, supplier, and provider interchangeably

[2] For full details about methodology and the broader supply chain, please refer to Bitsight's report, "Under the Surface: Uncovering Risk in the Global Supply Chain," March 2025

[3] For a detailed breakdown of Bitsight's risk vectors and their correlation to breach likelihood, see https://www.bitsight.com/security-ratings.

[4] For a deeper analysis of the correlation between providers and risk, see Gallagher Re, "Scanning the Horizon."

[5] We arrive at this number by calculating the number of technical supply chain connections that we can observe, adding the number of organizations Bitsight observes of 3rd/4th parties, plus the number of organizations observed to be monitored by our customers. This gets us a total number of possible supply chain organizations.

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE