

WHITE PAPER

Charting the Course for IT and Security: Unveiling the Trends Shaping 2024

2024




WHITE PAPER

IT and Security Data Predictions for 2024

The world of information technology (IT) and cybersecurity is constantly evolving, and 2024 is sure to be no different. With new threats and technologies emerging all the time, it can be difficult to predict what the future holds, but we've made a few educated guesses, based on current trends and emerging data.

Before looking forward to 2024, however, it's important to reflect on the year we've had. We published our 2023 Trends and Predictions for Observability and Security with a few key predictions for this past year, which are below. Overall, our team was pretty accurate in predicting the top challenges for IT and Security. Check it out!

The 2023 Year in Review

PREDICTION	REALITY	VERDICT
Data breaches within managed service providers will shift risk unpredictably for MSP customers.	Breaches have impacted J&J through IBM , VoIP providers , financial and energy providers , and many more. MSPs and MSSPs continue to be one of the most desirable targets for attackers due to their level of access to and inherent trust of the customers they manage.	 Correct
The cost of catastrophic cyber attacks will be 10x that of all other disasters combined.	Global warming has given this one a run for its money , but high profile cyber attacks on MGM and Johnson Controls have helped even the score and the fallout from MOVEit has still not fully been assessed. Most recently, Clorox advised investors that ongoing issues from their attack will impact earnings by more than 20%. With a few months left in the year, the losses are adding up, but the jury's still out.	 Correct / Undetermined
Antitrust investigations will materially impact large public cloud companies in 2023 and 2024.	This one has really started to come true in the second half of the year. From NVIDIA to Microsoft and Amazon , antitrust regulators are aggressively going after cloud companies.	 Correct

IT SECURITY MARKETS
ARE EXPECTED TO
UNDERGO SIGNIFICANT
CONSOLIDATION IN THE
NEXT YEAR, WITH NEARLY
HALF OF THE COMPANIES
EITHER FAILING OR
BEING ACQUIRED



CONSOLIDATION
WILL HAVE A NUMBER
OF NEGATIVE
CONSEQUENCES
FOR CUSTOMERS,
INCLUDING LESS CHOICE,
LESS INNOVATION,
AND POTENTIALLY
UNEXPECTED VENDOR
REPLACEMENT PROJECTS



TREND ONE:

Vendor Consolidation

A rising tide lifts all ships, but unfortunately, we think a rising yield curve has the potential to **sink half of them**. One of the key trends that we see continuing through 2024 is a consolidation among vendors. As enterprises have struggled to modernize their tech stacks, we've seen historically high levels of VC and private equity investment in companies trying to solve different pain points along the way. Innovation is imperative and investment is necessary for innovation, but with that said, the markets have become saturated with companies that provide features, not products, and will likely not survive any sustained economic slowdown.

We've already seen a steadily increasing deal flow heading into Q4'23. Some of 2023's notable activity:

- Cisco's acquisition of Splunk **(\$28B)**
- Silver Lake's acquisitions of Qualtrics **(\$12.5B)** and Software AG **(\$2.4B)**
- Databricks acquisition of MosaicML **(\$1.3B)**
- Thales acquired Imperva **(\$3.6B)**
- Sumo, New Relic, Toshiba and Qualtrics went Private
- IBM acquired Apptio **(\$4.6B)**
- Optiv Acquired Clearshark (*undisclosed*)

By this time next year, we expect that nearly half of the companies currently in the IT and security markets will either have failed or been acquired. What will this mean for customers? Unfortunately, less choice, less innovation, and potentially unexpected vendor replacement projects. While larger companies have deep pockets, as products transition from a small company's main source of revenue to a line item on a much larger balance sheet, it becomes less critical, and therefore less likely, that innovation will take place quickly. Bigger companies have slower processes and competing projects. We've already heard from several customers in the process of replacing newly acquired vendors due to concerns about future innovation and support.

ADOPTION OF DATA LAKES WILL ACCELERATE IN 2024, FUELED BY ADVANCES IN QUERY CAPABILITIES, AS WELL AS RISING STORAGE COSTS



DATA LAKE VENDORS, ON THE OTHER HAND, WILL SEE CONSOLIDATION AS THE MARKET MATURES AND CUSTOMERS CHOOSE BEST OF BREED TECHNOLOGY



TREND TWO:

Rise of Data Lakes and Fall of Data Lake Vendors

If you've spent any time with a Cribl Goat, you've probably heard (herd?) that the compounded annual growth rate of enterprise data is over 20%. If you've spent any time in the real world, you know that security and IT budgets are most definitely not growing at over 20%. While some companies may choose to collect less data, increasing regulatory requirements mean that most teams have no choice but to do more with less. As they struggle to find cost-effective means to store data of unpredictable value, we see companies increasingly reconsidering data lakes.

Once considered the final resting place for unstructured data, we see the migration to data lakes accelerating in 2024, driven by increasing storage costs, as well as advancements in query capabilities (like Cribl Search!) across data lakes and object storage, and the comparative ease with which data can be routed into them. With the ability to quickly and cost-effectively search large data stores, companies will start using data lakes as a first stop, rather than a final destination for their data. We see this causing a shift of data volumes out of analytics platforms and hot storage into data lakes.

In contrast to this growth, we anticipate data lake vendors who are not best-of-breed may see slowing growth and consolidation next year, as the market matures from theory and deployment to reality and utilization. As we mentioned earlier, 2024 is likely to be a year of consolidation in general, but for the segments of industries that experienced outsized growth leading into the looming economic downturn, this pain will be more acute, and data lake vendors are definitely on that list.

MONITORING AND
PROTECTING APIS WILL
BECOME INCREASINGLY
IMPORTANT IN 2024 AS
API-ASSOCIATED DATA
VOLUME DOUBLES



THE AVERAGE USER
HAS INCREASED THEIR
API USAGE BY OVER
50%, RESULTING IN
EXPONENTIAL INCREASE
IN DATA VOLUMES AND
COMPLEXITY



TOOLS LIKE CRIBL
STREAM WILL BE
ESSENTIAL TO ENABLE
ENTERPRISE-SCALE
LOGGING, MONITORING,
AND ANALYTICS FOR APIS



TREND THREE:

All Eyes on APIs as Volume and Complexity Explode

APIs, or Application Programming Interfaces, are a way for software applications to communicate with each other. They act as a middleman, allowing two or more applications to share data and functionality and almost everything cloud-based - from banking to wearable medical devices, to self-driving vehicles - relies on APIs. In 2024, we see APIs as being both the cause of, as well as a potential answer to, several security problems, as **API-associated data volume doubles**.

According to one survey, the average developer is using 17 APIs in 2023, up from 11 just three years ago and Gartner estimates the API economy will reach \$1 trillion USD by 2030. Unsurprisingly, with so much data and money moving around, attacks on APIs have steadily increased. This has necessitated more robust logging and analytics for monitoring and security, as well as to prevent potential abuse. We anticipate the **data volume being produced by API transactions and management will at least double in 2024**, compounding the problem many teams are already facing. Establishing and maintaining data quality and standardization will be imperative, resulting in an allocation of more budget and labor to data engineering.

On the protection side, we think APIs will be an indispensable tool in helping organizations to identify gaps in their programs and visibility, establish and maintain more effective log management for their cloud-based tools, and achieve and maintain compliance with data privacy and retention standards and regulations. While this will require its own data engineering lift, we think it will ultimately make enterprises safer and look forward to seeing how the creative use of APIs shapes 2024.

NEW SEC DISCLOSURE
RULES ARE FOCUSING
ATTENTION ON THE
COMMON DENOMINATORS
AMONGST HIGH-PROFILE
HACKS, AS WELL AS THE
EXTENT TO WHICH SUPPLY
CHAIN DISRUPTIONS ARE
CYBERSECURITY-RELATED



MONETARY PRESSURE
ON PUBLICLY TRADED
COMPANIES WILL SPUR
CHANGES IN BEHAVIOR
WHERE REGULATIONS
AND BEST PRACTICES
HAVE FAILED



WHILE THESE RULES MAY
CAUSE SHORT-TERM
PAIN, WE SEE LONG-TERM
GAIN AND, ULTIMATELY,
A MORE SECURE
ENTERPRISE AS A RESULT
OF NEW REGULATIONS



TREND FOUR:

The SEC Shines a Spotlight on Systemic Risk

2024 may very well become the year of dirty laundry, as a [new SEC requirement](#) that registered companies disclose material cybersecurity events within four business days lays bare just how interconnected and systemic risk in cybersecurity can be. In the few months since its passing, we have already seen several high-profile disclosures from Clorox, Johnson Controls, MGM, and Okta rattle the securities markets and send teams scrambling. While breaches are nothing new, the level of disclosure the SEC is now requiring ensures that enterprises feel a level of financial pain as punishment for their security misdeeds. It also makes far more public the common threads among various breaches, be they threat actors or vendors.

Such is the case with Okta, who disclosed a breach of its Support System on Oct. 20, 2023 that Cloudflare and 1Password both publicly stated was the source of their own breaches. Okta was also a common thread in the jacks of MGM, Caesars Entertainment, and [three other undisclosed companies](#) in retail, manufacturing, and technology. These attacks are all also linked to ALPHV / Scattered Spider, a notoriously aggressive and effective hacking group. Our own [Jackie McGuire warned in March this year](#) that 'single points of failure', like the Single Sign On provided by Okta, had the potential to be massively disruptive, and the new SEC regulations are likely to make the reality of that disruption very public.

The good news here is that the SEC and cyber risk providers will likely succeed where guidelines and best practices have failed; financial punishment and shareholder angst cause changes in businesses' security investment and behavior—fast. [The reason we have seatbelt laws is because of the auto insurance industry](#), and security incident disclosures will likely have the same impact. As several high profile material disclosures in 2023 have shown, investors and shareholders are unlikely to tolerate the immediate share price impact for very long before demanding change or divesting. As much as it shouldn't be the case, hitting companies in the wallet is typically the best way to influence behavior, and in 2024, we think the SEC's new rules will do just that.

CURRENT MODELS FOR ASSESSING AND VALUING DATA ARE OUTDATED AND WILL NEED TO CHANGE IN 2024, SHIFTING FOCUS TO THE UNDERLYING INFORMATION DATA REPRESENTS



INCREASING USE OF AI AND MACHINE LEARNING, AS WELL AS THE NECESSITY TO SHARE DATA ACROSS AN ENTERPRISE WILL NECESSITATE DEVELOPING AN AUDIT TRAIL FOR DATA



ACCURATELY IDENTIFYING, CATEGORIZING, AND ESTABLISHING SOURCES OF ORIGIN AND TRUTH FOR DATA WILL BE CRITICAL IN 2024 TO AVOID UNINTENDED DATA BREACHES OR LEAKS, AS WELL AS THE EFFECTIVE REMOVAL OF DATA FROM ACROSS THE ENTERPRISE



TREND FIVE:

Data as an Asset

In many senses, data is the new oil. It's a finite resource that needs to be mined and managed strategically, and its value is highly dependent on your ability to refine and manipulate it for specific applications. For this reason, we see 2024 as being a critical year in the transition of data from being 1s and 0s on a screen to an actual asset to be managed, tracked, and optimized within an enterprise.

If we look past data as the space it takes up and consider each data point (IP, port number, customer name, city name, temperature reading) as an asset in and of itself, it becomes clearer that the way we are mining and storing data is incredibly wasteful. The same data points are often collected repeatedly, stored more redundantly than necessary, and contain no single source of truth. With the increasing use of AI and machine learning, as well as more stringent regulatory requirements that both require you to hold some data longer, as well as delete some data sooner, it will become crucial that data is managed as an asset.

To accomplish this, the accurate identification and categorization of data will be essential, as well as establishing the sources of origin and current truth. Organizations will also need the ability to track and organize vast amounts of decentralized data that is scattered across endpoints, on-premises storage, and the cloud, as centralizing massive amounts of data won't always be possible. We see an entire industry dedicated to data identification developing over the next few years, and companies becoming increasingly more focused on what the sole source is for any piece of information. This will ensure changes to data propagate, unexpected output from data science models can be traced to the training source, and ensure that any data that a company no longer has the right or desire to hold is actually deleted. Alongside these companies, technologies like Cribl Search will be necessary to efficiently search this scattered data.



Conclusion

One of the things many of us enjoy about working in IT and security is that it's an exciting, challenging, constantly evolving landscape of innovation. This challenge and evolution is going to reach a fever pitch in 2024, and while some of these changes will be strategic innovation, we anticipate that teams will be kept busy with a steady stream of unexpected changes. From forced vendor migration, to AI-powered threats, and complex new regulations, it will be critical for teams to remain agile and keep enough fuel in the tank for these unexpected sprints.

The time to formalize an enterprise data strategy is now, and establishing best practices for data collection, storage, and processing, as well as a strategy for addressing backlog are the most important things you can do in the upcoming year. Often, it's not the data you have, it's the data you can find and use, so we also encourage teams to establish a search strategy that ensures valuable information isn't lost at the bottom of a data lake or file tree.

ABOUT CRIBL

Cribl makes open observability a reality for today's tech professionals. The Cribl product suite defies data gravity with radical levels of choice and control. Wherever the data comes from, wherever it needs to go, Cribl delivers the freedom and flexibility to make choices, not compromises. It's enterprise software that doesn't suck, enables tech professionals to do what they need to do, and gives them the ability to say "Yes." With Cribl, companies have the power to control their data, get more out of existing investments, and shape the observability future. Founded in 2018, Cribl is a remote-first company with an office in San Francisco, CA. For more information, visit www.cribl.io or our [LinkedIn](#), [Twitter](#), or [Slack](#) community.

©2023 Cribl, Inc. All Rights Reserved. 'Cribl' and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries. All third-party trademarks are the property of their respective owners.
WP-0007-EN-4-1123