The State of Cybersecurity in 2022 with Predictions for 2023

www.returnonsecurity.com/p/state-cybersecurity-2022-trends-predictions-2023

Every year, industry experts, professional investors, and vendors look back at the year that was while also looking at the year to come. This year I also wanted to try my hand at writing a report to reflect on the state of cybersecurity from 2022 and gaze into my crystal ball of what 2023 might hold.

In this post, I'll focus mainly on the macro trends I've observed at the industry level based on conversations I had throughout the year with VCs, other practitioners, and cyber startup founders. I will also lean on personal insights I've taken from the data I collect as a part of the Security, Funded newsletter.

If you're not already subscribed to the newsletter, you definitely should be.

Subscribe to the Newsletter

These thoughts found in this post won't come from the lens of venture capital or private investing but from a cybersecurity practitioner who still buys software and leads security programs today.

You'll find primarily my sentiment analysis, interpretations, inferences, and some ~~wild guesses~~ predictions of my own. This is my first post like this, and it will be exciting to see how many of these concepts come true or fall flat on their face in 2023.

2022 Year in Review

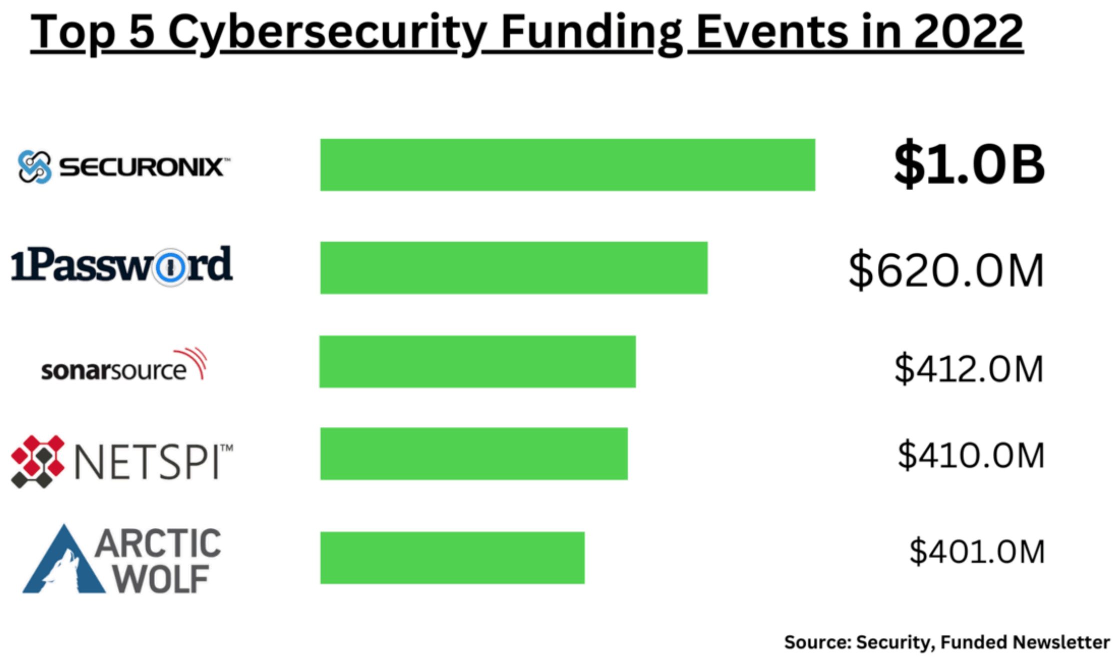
A future-looking post wouldn't be complete without a quick walk down memory lane. Let's take a quick look at how 2022 and the years prior shaped up.

2020 and 2021 were years for the record books with investing in cybersecurity. 2021 specifically saw an influx of non-specialized investors, soaring valuations, low levels of due diligence, and an overall explosion of new cyber companies.

2021 was the largest VC fundraising year in history, and cybersecurity companies got a big portion of that.

Looking into 2022, however, the cybersecurity market started to feel the pull from the reigns of macroeconomic forces and over-corrections as the year moved on. Private and public markets, macroeconomic forces, and the state of global affairs affected everything and everyone.

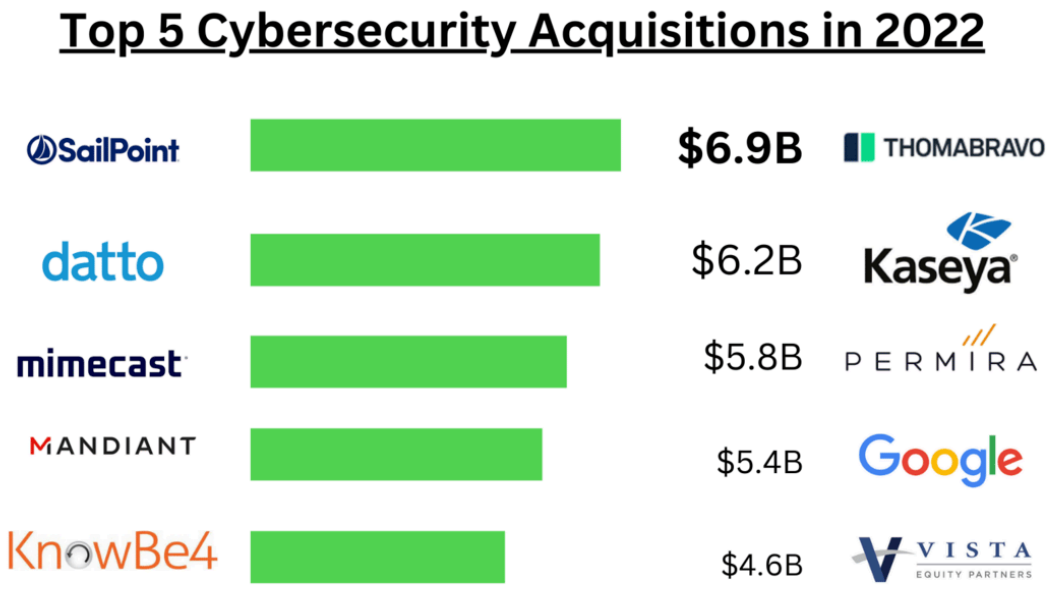
While cybersecurity funding in 2022 saw a noticeable dip from 2021, that didn't stop it from still having a few major funding transactions:


Top 5 Cybersecurity Funding Events in 2022

Source: Security, Funded Newsletter

The big funding rounds

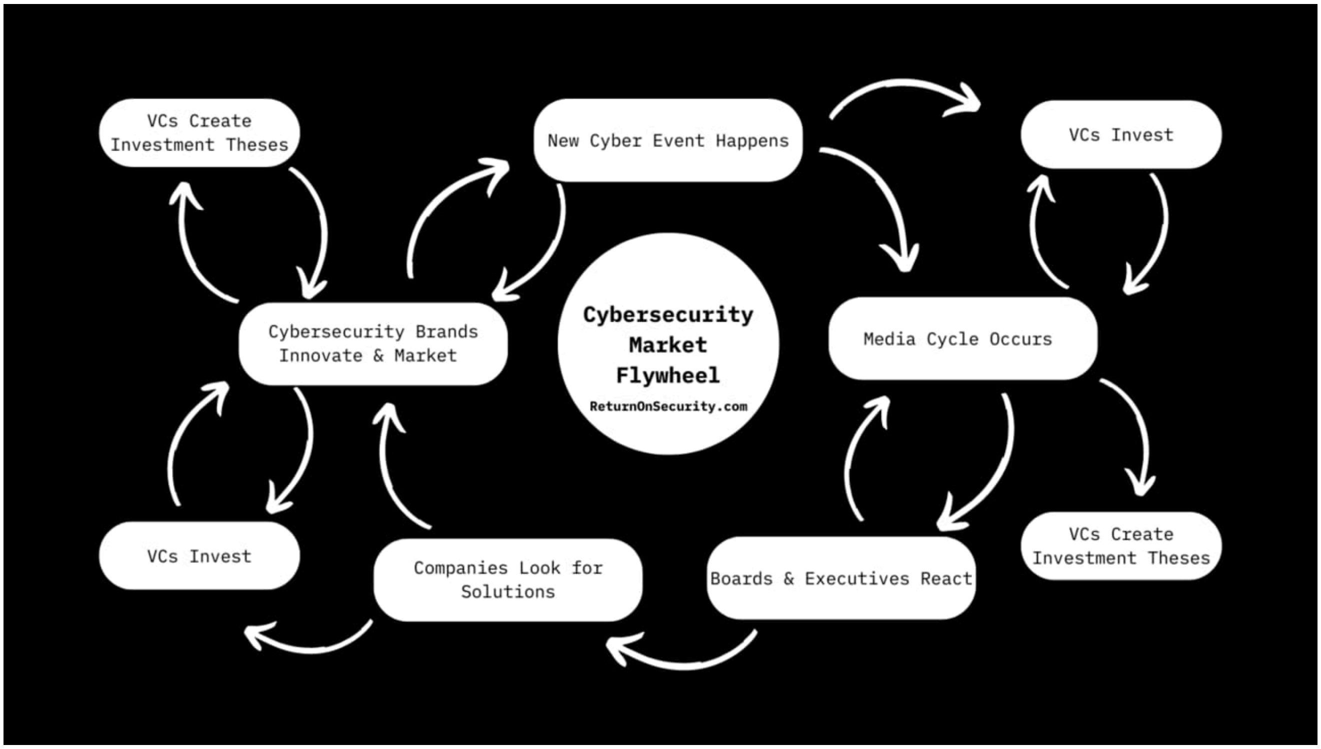
And not to be outdone, there were several huge acquisitions from both private equity firms and individual companies:



Source: Security, Funded Newsletter

Overall funding for 2022 is expected to come in at around **~$18.4B,** with over **700 funding transactions** from **642 unique companies** and **~$50.1B** from over **260 acquisitions and mergers** from publicly available data.

This volume may seem high to the uninitiated, but this is a high-speed, low-drag industry. Here's a visual example I created of how the cybersecurity market flywheel works in general and why there is so much innovation.


VCs Create Investment Theses
New Cyber Event Happens
VCs Invest
Cybersecurity Brands Innovate & Market
Cybersecurity Market Flywheel
ReturnOnSecurity.com
Media Cycle Occurs
VCs Invest
Companies Look for Solutions
Boards & Executives React
VCs Create Investment Theses

The chart above shows how the industry operates in normal times, say, the last 10-15 years.

But 2022 was no normal time for cybersecurity, so this got a bit skewed from outside forces.

Here are some of the things that cybersecurity vendors, investors, and buyers saw that skewed the market in 2022:

- For private and public deals alike, the cost of capital for cybersecurity founders and investors soared, making it unfavorable to borrow money and see returns.
- Tech company valuations across sectors dropped to less than half of what they had been in previous years, making it harder to raise as much money for as good a deal.
- Significantly fewer cybersecurity companies hit unicorn status and went IPO (although lacking IPOs was not just a cyber thing).
- Investors increased their due diligence and were more cautious about deploying capital, so fewer early-stage deals were funded until about midway through Q3 2022.
- Opportunistic investors (those without a cyber focus) resisted entering the cybersecurity market in 2022, whereas, in 2021, they came flocking in search of returns.
- There were over 150,000 layoffs in the broader tech sector, according to data from Layoffs.fyi, and cyber companies were not spared. Companies that had previously raised over $1.0B in funding and had 2-3x their staff from 2020-2021 had to start making layoffs to curb their burn rates.
- Unlike in 2020 and 2021, fewer cybersecurity companies emerged from stealth in 2022 with no defensible positioning or without a more solid product market fit.
- Cybersecurity buyers (CISOs and security teams) were forced to make budget concessions or looked to consolidate their security and tech stacks, a stark reversal from the past 5+ years. However, this wasn't uniform, and smaller companies were hit harder than larger ones.
- Cybersecurity vendors saw longer sales cycles with each customer they did win and longer customer deployment timelines. Relationships depend on existing customers over net new customer growth.
- The small to medium enterprise (SME) market, already underserved in cybersecurity, experienced additional pressure as cybersecurity vendors attempted to expand further upmarket.

- Large, publicly traded cybersecurity vendors put significant focus on the US federal sector on the wave of zero-trust initiatives and efforts to secure critical infrastructure. This was additionally heightened by an increased public-private focus from agencies like the CISA and from waves of cyber-physical attacks from the Russia-Ukraine war.

Public sentiment toward cybersecurity has never been higher, and the risks of not having it have never been more apparent. At the same time, macroeconomic forces have provided strong headwinds to progress for many companies.

2022 was a year of contradictions for the cybersecurity industry.

2023 Industry Predictions

It's no surprise that 2022 saw major headwinds from a broader economic perspective.

Raising interest rates, a looming recession or stagflation, increasing (or flat) levels of inflation, weaker-than-normal jobs reports, and general global turmoil made a tall mountain to climb. Many financial analysts, much more attuned to this world than me, believe many of these trends will continue into 2023 and 2024.

While I'm not an economist, I don't think 2023 will be all gloom and doom for the cybersecurity industry, but it will still "feel" different than years before.

If 2022 taught us anything about the cybersecurity industry, it's that while it is still vulnerable to those forces I just mentioned, it's still got deep and healthy pockets of companies still thriving and growing.

Heading into 2023, I believe the funding landscape in cybersecurity looks more promising if the closeout of 2022 is any indication.

A few industry predictions I think we'll see next year include the following:

- More early-stage cybersecurity deals, as seed-stage companies, will lose less inertia from the downward public market trends.
- Additional layoffs at cyber companies as they continue right-sizing operational budgets.
- A decrease in valuations of later-stage companies as they raise additional funding rounds (also known as a "down round") to weather 2023.
- Cyber companies will focus more on net revenue retention (NRR) – that is, trying to get existing customers to buy more modules and increase overall spending – than on new customer acquisition. The higher the NRR, the higher valuations will be.

- There will still be an absence of cyber companies going the IPO route. 2022 made this a less attractive path for private companies and investors, and that's not the only path for a healthy business to take to see healthy returns.
- A more significant wave of private equity leveraged buyouts and consolidations than last year.

Combining this with the sentiment from some financial analysts that inflation will ease slightly and that cyber startup founders, *a very resourceful bunch*, have been operating in a stressed environment for a few quarters, and 2023 has lots of potential.

2023 Product Predictions

I also think it's worth making predictions about the innovation ahead for 2023. The cybersecurity industry loves creating product categories and new acronyms like Pokemon.

> — # (#)

With that in mind, here are the top 11 product predictions I believe we will see in 2023 and where investment dollars will be going (or should be going).

1. Web3 Security

2022 was the early scam days of Web3 and cryptocurrency.

I liken this to the early days of email phishing and scams, and how it affected so many people, only with Web3, it's much harder to know when you're being scammed (or when you're part of a Ponzi scheme).

The technology interactions with Web3 are much more complex. The narratives with Web3 mirror that of the Dot Com era before the bubble, and there is more bandwagon hopping regarding platforms and cryptocurrency that rival religious zealots. Everyone is trying to find the next way to get rich and be a part of the future.

More money and power are up for grabs than ever before. As a result, it appears easier to hide behind the veil of complexity with Web3 and scam people. Individuals and companies can only lose money so many times before market forces create medicine for this ailment.

Expect over-correcting regulation and more Web3 Security companies in 2023.

2. Artificial Intelligence (AI) & Machine Learning (ML) Security

AI/ML has long been on a collision course with cybersecurity. Cyber vendors have been touting the benefits of using AI/ML in their product offerings for years, but much of it has been vaporware.

Security researchers have warned of nation-state and criminal gang usage of AI/ML for several years. Only now are the potential ramifications starting to hit home.

❝

ChatGPT has entered the chat

If the potential ChatGPT isn't enough reason to start securing how these systems are built, how they learn, and how they interact with the general public, I don't know what is.

3. API Security Part Deux

The first iterations of API Security took off like a rocket in 2021 and 2022, but 2023 and beyond will enter the second wave of innovation.

API Security as we know it today will be engulfed by the broader Web Application and API Protection (WAAP) product category (thanks for yet another long acronym Gartner 🙄).

WAAP players will take on a broader suite of capabilities focused more on resiliency and availability of customer-facing services. This will contrast with the pure application security and observability-driven approach of v1 API Security players.

Look for the emergence of players, both new and established, who combine API Security blocking and monitoring capabilities with content distribution networks (CDNs), bot protection, runtime application security protection (RASP), intrusion detection systems (IDS), distributed denial of service (DDoS), and web application firewall (WAF) offerings.

Add a hosted or managed services option, and you've got some serious firepower.

4. Securing No-Code

While no-code and low-code tools have undeniably become a significant shift in how companies and products are built, the cyber risks of using these platforms are not well understood.

All applications have vulnerabilities, and all no-code and low-code platforms run on one of the major cloud service providers (CSPs).

As an industry, we are already familiar with the challenges of securing the cloud. Not to mention the massive amount of funding poured into the cloud security space year after year.

I expect players to enter the no-code security scene similarly to other emerging realms. It will start with visibility and transparency of what kind of data these no-code platforms can view, store, and edit, and then a risk-based picture will begin to emerge from there.

The first step to overcoming a problem is admitting you have a problem. From there, we will see recommendations and scoring of no-code platforms that allow for more transparent security practices and visibility.

5. More Managed Services

With continued budget pressure for security leaders and challenges in hiring, managed services will continue their adoption. The more one-stop-shop and managed the solutions are, the better.

Customers will be more willing to consolidate vendors, buy more managed services, spend through cloud-based marketplaces (e.g., AWS Marketplace), and spend more with the vendors they have for deeper discounts.

Security leaders will be challenged to make the most of budget and resource constraints that will likely extend through 2024 (on top of what might already be present).

6. Security Program Value Realization

The rise of tools that help showcase the value of cybersecurity investments and decisions.

Programmatically make and track investments for your security program to industry frameworks and decision models.

This could fall under various product category names, such as Threat Informed Defense (TID), Continuous Threat Exposure Management (CTEM), or even Threat and Risk Prioritization.

However it's named, it will all come down to cost management and allocation, especially in 2023. In the cloud computing world, they call this "FinOps" or the practice of becoming as efficient as possible with your cloud spending (*hopefully, there are no "FinSecOps" or "SecFinOps" terms that come out of this* 🤦).

Cost in the cloud results from architectural decisions (good or bad), and now security programs need their version of this. CISOs need to be seen as good stewards of corporate capital, and tools like this will become more critical to show the value of cyber programs.

7. Identity Threat Detection

A common theme with cyber vendors is to take a new approach to an existing problem space that continues to plague the industry.

Just as how cloud security posture management (CSPM) looked at cloud (mis)configurations, identity threat protection will look at how roles and permissions of various identities impact security and compliance gaps.

Backing into a blast radius by way of compromised credentials, the most common form of attack still in 2022 (and I would bet in 2023), will give a more tactical remediation approach to findings that may not involve architectural or application changes.

There will be multiple iterations of this, trying to tie cloud configurations, attack surfaces, and cloud entitlements to an identity-centric approach.

8. The Rise of Automation Integrators

Everything in the cloud can be automated through an API, and a new class of vendors will emerge focused on secure business enablement.

These players will offer "1-click" architectures to create secure, compliant, and production-ready infrastructures. The sales pitch will be less on specific security capabilities and more on letting businesses run ahead, knowing they have a compliant and secure infrastructure to start from.

Passwordless Authentication workflow? **1-click**.

Secure Service Edge network deployment? **1-click**.

This will let businesses focus on their core values and less on managing overhead. Speaking of managing, this will be an easy parlay for tech-focused MSSPs to add to their service offerings.

They build, you deploy, they operate and maintain, and you run your business.

9. It's VAR Morphing Time

What constitutes a Value-Added Reseller (VAR) will change considerably.

The "value" in value-added is often light in VAR relationships. Next is adopting vertically integrated and managed software services, not just bespoke consulting or staff augmentation.

Every VAR will become an MSSP. Every MSP will become an MSSP.
Every MSSP will become a VAR.
Every VAR will become an Automation Integrator.

And Private Equity firms will buy all of them.
Expect to see a lot more private equity acquisitions in the VAR space next year as these spaces munge into one and create attractive cash-flowing businesses.

10. Consumer Protection Gets New Life

New and revised data privacy laws and rules are sweeping across the globe (unfortunately, not in a uniform fashion).

Consumers also have no control over the algorithms used against them in general technology, AI applications, and social media platforms.

As a result, we will see an explosion in the consumer-focused digital privacy and security product market.

This will be on the personal data privacy front that serves both business-to-consumer (B2C) and business-to-business (B2B), but also on securing critical individuals outside of their day jobs.

❝

The company you work for might secure your 9 to 5, but who is securing your 5 to 9?

Business-to-business-to-consumer (B2B2C) platforms will emerge and increase as companies come to terms with the fact that humans are consistently targeted and the subject of threats.

There are no off days here, and consumers will be increasingly interested in taking the security and privacy of themselves and their families into their own hands.

Add onto this global unrest with protests and censorship growing in parts of the world, and digital sovereignty and mobility become very important.

11. War on Information Warfare

As we learned from 2020 to 2022, misinformation and disinformation can be a matter of health and public safety, especially regarding social media platforms and their role in all of this (whether they agree or not).

ChatGPT and other generative AI have entered the chat again

Look for the evolution of products designed to identify, filter, and otherwise dispute misinformation campaigns to be applied at a large scale.

This will likely be harder to tackle since most information people consume these days, good, bad, or otherwise, come from social media sites. It's been no easy feat for social media platforms to sort out what is freedom of speech, what hate speech is, and what constitutes harmful or foul play on individuals or groups.

It won't be an easy job, but it could benefit the rest of society if it can be done even in a small way.

Wrapping Up

2022 brought new and unchartered waters for many, and 2023 will continue to bring more of the same kinds of uncertainty.

Keep an eye out for startups and companies that are positioning themselves as leaders in these emerging areas of the cybersecurity industry.

For the VCs, I hope the predictions outlined in this post can help guide your investment decisions and identify potential growth areas in the coming year. If you've found any of these ideas helpful or want to dig deeper, let's chat.

Found the founders or soon-to-be-founders reading this, I hope this gives you a gauge on where to point your sails (or steer clear of). If you're interested in funding any idea like these, let me know, and I'll do my best to help you connect the dots with investors.

I write these kinds of posts for free, just like I do with the Security, Funded newsletter, because I want to add value to the cybersecurity industry and because I find it personally fascinating.

As it turns out, many others have found it interesting and helpful and shared it along the way. If you liked this post, please subscribe to the newsletter and share it with your friends.

Thanks for reading, have a great New Year, and I'd love to hear any feedback you may have.

Cheers,

Mike P