Have you experienced ‘Tool Sprawl’ in Cyber-security?

Published 12 October 2022

Christopher Gannatti, CFA
Global Head of Research

We recognise we have a diverse array of readers, probably some individual business owners, some employees of large companies, some employees of smaller companies and possibly even some people who are retired or between jobs.

Whatever your situation—how many different cybersecurity tools are you aware of that you interact with? A password manager? A single-sign-on interface? A specialist tool focused on email? Another specialist tool focused on accessing a cloud computing infrastructure?

The fact of the matter is that the more you learn about cybersecurity, the more you are awakened to a large number of providers that each specialise in different types of protection. We saw the term ‘tool sprawl’ used to describe the 2022 cybersecurity landscape—we thought it painted an informative picture1.

How many tools are customers using?

Enterprise customers may be managing portfolios of 60-80 tools, with those on the extreme higher end of the spectrum possibly managing up to 1402. Imagine managing all of these tools over the course of a normal business operation.

One reason why the current environment is characterised by so many tools could relate to the progression of the Chief Information Security Office (CISO) role. 10 years ago, the way a ‘good CISO’ was defined largely had to do with buying and deploying tools. The CISO in 2022 is now much more a top priority for a company’s board and C-suite, and now a ‘good CISO’ is evaluated based on outcomes rather than deploying tools3.

A survey conducted by Gartner found that 88% of Boards of Directors view cybersecurity as a ‘business risk’ rather than a ‘technology risk4.’

Of course, the attack surface in 2022 has also massively expanded, and frequently companies may be launched around new types of artificial intelligence and machine learning techniques, to use one example that could also lead to the proliferation of companies.

Dealmaking is already taking off in 2022

Through 18 August 2022, private equity sponsors and their portfolio companies have backed 162 cybersecurity deals worldwide, valued at $34.9 billion. If this pace continues, it could surpass 2021's tally of $36.4 billion across 308 transactions5.

One driver—valuations. 2020 and much of 2021 saw the most newly public cybersecurity companies, many of which were focused on the cloud, experience massive multiple expansion and therefore premium valuations. The growth was strong, but the prices were not inexpensive in an environment where the cost of capital had been very low for a very long time.

With the rise of inflation and then the shift in policy of many central banks going from expansionary support of growth, many of these companies experienced dramatic multiple compression. This allows private equity players focused on building consolidated product offerings to pick up interesting companies at much lower prices.

Thoma Bravo is one such player that has been quite active. Just in the identity space, Thoma has done deals to acquire Ping Identity for $2.8 billion and SailPoint for $6.9 billion6.

Consolidation is a big desire from customers—possibly a response to the 'tool sprawl' that we mentioned earlier. There is a feeling in the market that there might already be too many companies, so it's not just about more innovation but also building integrated platforms so customers can go to one place and get more services.

Option3 is an example of a firm that has shifted from funding new firms to acquiring late-stage middle-market companies for buy-and-build strategies. They are planning to raise a $250 million buyout fund dedicated to a platform acquisition strategy7.

Private equity firms are attracted to cybersecurity companies for many reasons, but it is noted that they have exhibited lower churn rates than other Software-as-a-Service (SaaS) businesses. They also have tended to generate high margins.

What about the slowing economic environment?

As is the case with many things, historical comparisons can only take us so far. If we think about the state of cybersecurity in 2007-2009, encompassing the 'Great Recession', it was totally different. Cybersecurity budgets are much different in 2022 than they were in 2007 heading into that significant slowdown8.

One doesn't need to look too far to see quotes from experts indicating that even if cybersecurity spending could be impacted by a slower economic environment, it most likely wouldn't be as impacted as other areas. There are many things that are regulatory requirements or viewed as 'table stakes' to the ongoing operation of companies, which make them that much more difficult to cut.

Regulators are also upping the ante. The Securities and Exchange Commission in the US has explored a rule that would require disclosure of a 'material cybersecurity incident' in a public filing. Disclosure would also have to be quite quick after the event—possibly a response to certain types of attacks and breaches like SolarWinds, where months after the fact the scope of potential damage was growing and growing9.

Even if regulators do not mandate spending more on cybersecurity, their pursuit of certain types of rules would be likely to have that impact.

Conclusion: a megatrend for all seasons?

Norges Bank Investment Management, the world's largest sovereign wealth fund at $1.2 trillion, recently indicated that cybersecurity is their biggest current concern, citing that it faces an average of three serious attacks each day. The fund sees roughly 100,000 attacks per year, and they classify about 1,000 of them as serious10.

Firms operating in the financial industry have been increasingly targeted, and firms operating in the Nordic region feel the proximity to Russia during the Ukraine conflict quite tangibly.

While many investment themes might be a bit discretionary or susceptible to delays in a slowing economic environment, cybersecurity is not one of them. We may not know the exact companies or services that will grow the fastest but backing away from focusing on security is not an option.

1 Source: Alspach, Kyle. "Thanks to the economy, cybersecurity consolidation is coming. CISOs are more than ready." Protocol. 17 June 2022

2 Source: Alspach, 17 June 2022.

3 Source: Alspach, 17 June 2022.

4 Source: "Gartner Survey Finds 88% of Boards of Directors View Cybersecurity as a Business Risk." Gartner. Press Release. 18 November 2021.

5 Source: Shi, Madeline. "PE dealmaking thrives in cybersecurity sector." Pitchbook. 23 August 2022.

6 Source: Shi, 23 August 2022.

7 Source: Shi, 23 August 2022.

8 Source: Alspach, Kyle. "Cybersecurity spending isn't recession-proof. But it's pretty close." Protocol. 6 June 2022.

9 Source: Alspach, Kyle. "'Game-changer': SEC rules on cyber disclosure would boost security planning, spending." VentureBeat. 10 March 2022.

10 Source: Klasa, Adrienne & Robin Wigglesworth." Financial Times. 22 August 2022.

Related products

+ WisdomTree Cybersecurity UCITS ETF – USD Acc (WCBR/CYSE)

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an oer for sale nor a solicitation of an oer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can oen lead to a number of dierent interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public oering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.