

Cybersecurity: The Megatrend of the 2020s

Published April 19, 2021

Team8

Global venture group

The world of cybersecurity is changing, and cyber risk is taking on a whole new meaning for enterprises, not only technologically, but also financially, reputationally and operationally. Prior to the COVID-19 pandemic, cybersecurity was already approaching a tipping point—attackers were getting more sophisticated, attack surfaces were expanding and the bad actors' advantage was becoming more asymmetrical. Luckily, the pandemic may have also accelerated some positive shifts in the way organizations fundamentally think about cybersecurity.

The pandemic caused enterprises to become more reliant on their digital infrastructure as a building block critical to business operations. A second-order consequence of the expansion in the scope of digital transformation has been a spotlight on the importance of resilient infrastructure, vetted third-party suppliers and a sound supply chain. The recent SolarWinds attack illustrated how these concepts have been elevated in a digitally transformed and interconnected economy.

Enterprises should seize this opportunity to reexamine their infrastructure and make investments to solve root cybersecurity problems and vulnerabilities, ultimately leading to greater security and resilience.

To help navigate this path forward, we are excited to introduce our 2021 Cybersecurity Brief outlining the main themes, drivers and implications that we believe will be of critical importance to the industry in the next few years. The seven themes help shed light on the forces behind them and the way the overall cybersecurity environment is changing. This brief was created as much for ourselves as it was for innovators, operators and technologists, as we have used it to guide our company-building strategy and detail how we see the world of cybersecurity evolving.

In the coming weeks, we plan to release a blog post for each of the different themes mentioned below.

How we identified our themes

We collaborated with our Village: our community of 350+ C-level security executives from 300 enterprises across 20 countries, 25% of which are Fortune 500 and 55% of which are Forbes Global 2000. We also worked closely with our Team8 cybersecurity experts—many from Israel's elite 8200 military intelligence unit—and our global advisors to highlight the areas of immense future business growth and product depth from a technology, market trend, regulatory and venture funding standpoint. We considered both mature and nascent markets to gather a broad perspective and track early, emerging technologies that will influence the future and lead to high-growth opportunities in the next few years. We also considered Team8's "Attacker Perspective" (our unique insights into how attackers think and operate) and other Team8 internal resources, in addition to publicly available information. We then cross-referenced our findings with

the responses from our proprietary 2021 Chief Information Security Officer (CISO) Survey, confirming the top areas where security leaders are increasing their investment.

Stay tuned for next week, when we will cover the first theme: cloud security.

Important Risks Related to this Article

The views expressed in this blog post are those of Team8. Any reference to “we” should be considered the view of Team8 and not necessarily that of WisdomTree Asset Management.

Team8 is a global venture group with deep domain expertise that creates companies and invests in companies specializing in enterprise technology, cybersecurity and [fintech](#). Leveraging an in-house, multidisciplinary team of company builders integrated with a dedicated community of C-level executives and thought leaders, Team8’s model is designed to outline big problems, ideate solutions and help accelerate success through technology, market fit and talent acquisition. For further information, visit www.team8.vc.