**Top Five Security Trends for 2023**

CommunitySolv 2022 brought top experts to the stage. One of the hottest top topics was, of course…. Security: Simplify, reduce risk, educate. To help, we’ve gathered the top solution opportunities to help you gain the edge going into the new year.

1. **Zero Trust Architecture** made waves in 2020 with the rapid shift to remote work environments. In the two years since, many of your customers’ security infrastructures were put to the test. So, 2023 may present an opportune time to help your customers evaluate their current security infrastructure and determine if their existing strategy still makes sense. By implementing a Zero Trust model – which recognizes security threats can exist both outside and inside a network – you may be able to help keep your customer’s business-critical systems safer than ever before.
2. **SD WAN,** also known as a software-defined wide area network, connects users to an organization’s network over a large geographic area. SD-WAN has become a cybersecurity standard given the rapid move to remote work in 2020. No longer needing to rely on physical routers to connect network users, SD-WAN offers your customers the ability to access their network entry points via software, which can be more easily set up and organized.
3. **Everything-as-a-Service,** also known as XaaS, encapsulates various “as a service” offerings, such asSoftware-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). All these services combined are driving the growth of IT business. [Reports indicate](https://www.digitaljournal.com/pr/everything-as-a-service-xaas-market-2378-07-billion-usd-industry-by-2029) that XaaS will experience impressive market growth, increasing from $436 billion in 2021 to an estimated $2.3 trillion by 2029, a compound annual growth rate (CAGR) of 23.4%! XaaS can simplify IT deployments, decrease physical overhead and ultimately lead the way for an organization’s digital transformation.
4. **Automation.** Automation allows network managers and their teams to spend more time investigating and responding to unique security threats. Combining the data from multiple tools to condition logic that “if this happens,” an automated response “to do this” occurs, can help security teams pivot from managing mundane tasks. More providers are implementing proactive [security strategies and tools](https://medium.com/tdsynnex/how-to-soar-your-business-with-soar-b491197850a6), like zero trust and Security Orchestration and Automated Response (SOAR). [According to Gartner](https://www.gartner.com/en/documents/3990720/market-guide-for-security-orchestration-automation-and-r), SOAR refers to solutions that: “…combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform.”
5. **Cloud Access Security Broker (CASB).** With organizations implementing long-term remote office policies, your customers’ work has changed considerably. As a result of hybrid work environments, global public cloud services are projected to grow to $805.5 billion in 2025, up from $387.7 billion in 2021, representing a five-year compound annual growth rate (CAGR) of 21.5%, [according to Gartner](https://venturebeat.com/2021/08/12/takeaways-from-gartners-2021-hype-cycle-for-cloud-security-report/). CASBs essentially wrap a security sleeve around shadow IT.

As the IT industry continues to grow, customers are making a huge investment in security. Stayed tuned as we revisit this in 2023!

*Special thanks to contributing Cybersecurity editor, Kelly Armstrong, from the Copy and Content Team.*