PRISMA CLOUD | paloalto NETWORKS

The State of Cloud Native Security Report 2022

Executive Summary

As the cloud's unique capabilities continue to evolve, so have the ways in which we employ it to drive business forward. As such, this report includes research that pays special attention to the latest top-of-mind concerns and narratives in the cloud native security community, including automation, DevSecOps, security posture, the use of open source and more. Our goal each year in the production of this report remains the same: for you to come away with valuable insights that help guide your cloud adoption and security journey in 2022 and beyond.

Cloud Expansion and Strategy

- Organizations rapidly **expanded their use of clouds during the pandemic by more than 25% overall** but struggled with comprehensive security, compliance, and technical complexity.
- Organizations expanded with less budget, with **39% of organizations spending less than $10M on their cloud** (up 16% from 2020) and **only 26% spending more than $50M** (down 17% from 2020).
- While organizations continue to use diverse compute options, **platform as a service (PaaS) and serverless approaches rose 20%**, likely supporting the rapid transition to the cloud, while the use of containers and containers as a service (CaaS) saw more moderate growth.

Security Posture and Friction

- **Organizations with a strong security posture are more than 2X more likely to have low levels of security friction**—the degree to which organizations believe cloud security supports or limits their operations. This highlights the need for a two-pronged approach to cloud security, with effective security capabilities that don't disrupt teams outside of security.
- Organizations with best-in-class security operations see the greatest benefits to their workforce in terms of productivity and satisfaction. **Eighty percent of those with strong security posture and 85% of those with low security friction reported increased workforce productivity**.
- A majority of organizations **(55%) report a weak security posture** and believe they need to improve their underlying activities—such as gaining multicloud visibility, applying more consistent governance across accounts, or streamlining incident response and investigation—to achieve a stronger posture.
- **Eighty percent of organizations that primarily use open-source security tools have weak or very weak security posture**, compared to 26% of those who primarily leverage their cloud services provider and 52% of those who depend on third parties, highlighting that piecing together a platform using disparate tools leaves an organization less secure.

Security Drivers

- Organizations are consolidating their security approach. **Nearly three-quarters use 10 or fewer security tools**, and we see a **27% increase from the 2020 data in the number of organizations using just one to five security vendors**, suggesting that they are looking to fewer security vendors for more capabilities.
- **Organizations that have implemented a high level of security automation are 2X more likely to have low friction and strong posture** than their counterparts with low levels of security automation.
- How well organizations adopted and implemented DevSecOps methodologies is the primary indicator of best-in-class security. **Organizations that tightly integrate DevSecOps principles are over 7X more likely to have strong or very strong security posture and are 9X more likely to have low levels of security friction**.

Download the full report