Hybrid, multicloud digital frontier requires integrated detection and response.

In the wake of the pandemic-driven transition to the hybrid workplace, companies face an increasingly complex attack surface amid soaring (and expensive) threats. Experts predict that global cybercrime costs will reach $10.5 trillion by 2025 compared to $3 trillion back in 2015. Overstretched security centers already struggling to keep pace also confront debilitating staff shortages that exacerbate the problem.

One thing is clear: the status quo is out of date for the new hybrid, multicloud-dominated frontier. Organizations need to rethink their security strategy and adopt a more integrated preventive approach to bring their security operations up to speed with our evolving landscape.

72% of organizations report that their IT environment has grown more complex

55% attribute this complexity to the shift to remote work, while others pointed to regulations, device diversity and cloud adoption.

shortages that exacerbate the problem.

One thing is clear: the stat

$397.5 billion is the amount Gartner estimates that global spending on public cloud will grow to in 2022 with multi-cloud environments becoming the norm.

92% of IT professionals think their organization is not ready to secure their public cloud services.

200,000 new threats are detected every day on average.
Security teams are tackling a growing deluge of alerts – however, many are false positives.

75% of teams spend just as much time on false positives as they do on real threats. As a result, they struggle to prioritize important vulnerabilities and fix them without delay.

287 days is the average amount of time it takes for teams to identify and contain a threat