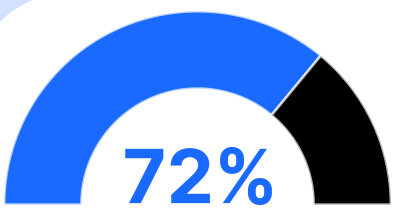
Hybrid, multicloud digital frontier requires integrated detection and response.

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One thing is clear: **the status quo is out of date** for the new hybrid, multicloud-dominated frontier.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.



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.

$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.

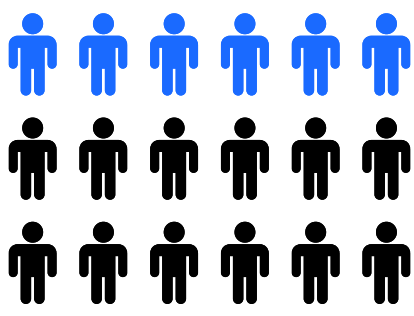
Security teams are tackling a growing deluge of alerts – however, many are false positives.

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

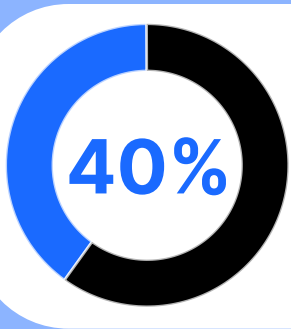
Almost one third of security professionals are overwhelmed and stressed by their jobs.

Alert fatigue carries a hefty human resource cost.



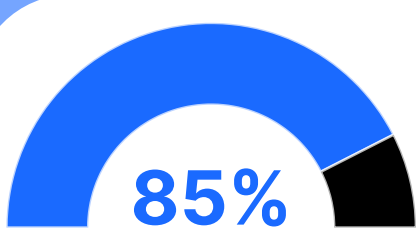
8 out of 10 organizations have unfilled cybersecurity positions in government and healthcare.

65% of SOC professionals are considering quitting their jobs.

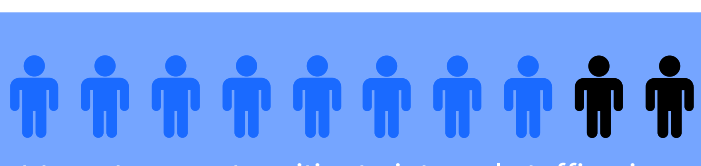


of fatigued security professionals care most about the ability to automate repetitive tasks when turning to extended detection and response (XDR) solutions

28% say that an over-reliance on manual or informal processes is their organization's greatest security challenge.



of security professionals want to outsource managing XDR so they can leverage best practices from an XDR expert and reduce risk.



Eight out of ten want to outsource to mitigate internal staffing issues. The accelerating skills gap and shortage is likely a major factor in their decision-making.

40% **are eager to integrate network detection and response (NDR) capabilities into their XDR solutions.**

39% want solutions to integrate threat intelligence platform capabilities. These priorities reflect the growing complexity of the cybersecurity landscape.

Empower the analyst. Harness best practices. Become cyber resilient.

OpenText, The Information Company™, offers a suite of products and capabilities for a comprehensive and robust cyber resilience strategy. OpenText focuses on risk and compliance, product readiness, digital forensic and incident response (DFIR), and managed security services to help organizations become cyber resilient by identifying security risks, optimizing forensic workflows, and keeping systems safe, available and protected.

Visit the OpenText Threat Detection and Response solutions page for more information or to speak with a security expert, contact:

securityservices@opentext.com

DARKReading

Sponsored by: opentext™