Managed XDR paves the way for cyber resilience.

Challenges faced by security teams have skyrocketed over the past few years. Massive increases in threats have **expanded workloads** even as **staffing shortages** plague companies struggling to keep pace.

Extended Detection and Response (XDR) systems are growing in popularity, but their complexity can pose a hurdle for shorthanded teams. As a result, outsourcing monitoring and management has become the logical next step for many enterprises. Managed XDR (MXDR) is increasingly attractive as a cohesive platform to address evolving threats while reducing staff burden.

External threats are soaring, and breaches cost more every day.

<60% of breaches stem from Web applications, according to the 2022 Verizon Data Breaches Investigations Report.

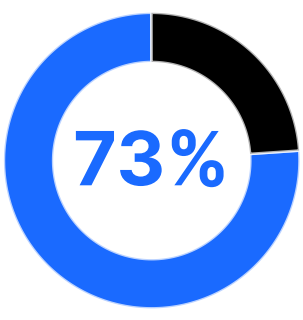
$1.07M million in breach costs on average is added when workers are remote; compared to attacks where remote work was not involved.

$4.2B is what it cost the public for internet crime complaints to be logged by the FBI in 2020 – a 20% increase over 2019.

93% of security professionals expect XDR to significantly improve risk mitigation efforts and lower cost at the same time.

A global survey of security professionals found that the vast majority expect XDR's adoption to reduce their organization's technology and personnel costs.

<98% of respondents either have adopted XDR or are planning to do so soon.

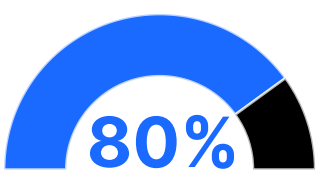


of organizations have been impacted by the global cybersecurity skills shortage.

For respondents in the healthcare and government sectors, 8 in 10 organizations have unfilled security positions.

Most security teams already struggle with limited staff resources. The size of a typical security operations center (SOC) team is between two and 10 staff members regardless of company size.

Meanwhile, the cost of hiring security professionals is rising. Average security analyst salaries rose from $102,000 in 2019 to $111,000 in 2020.



want MXDR to mitigate the impact of staffing issues.

In the context of the skills shortage, it's no surprise that most organizations want to outsource monitoring and management of their XDR.

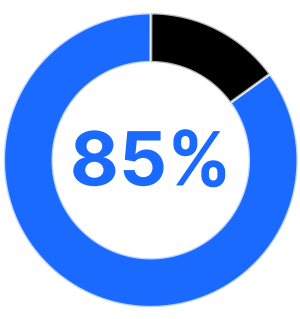
41% of survey respondents want their MXDR to help them automate repetitive tasks.

47% of survey respondents are looking for excellent customer support from their MXDR provider.

51% of security professionals say "ease of use" is the top XDR solution requirement.

100+ More than 100 vendors provide MDR services. Even though most respondents are convinced of the need for a solution, it can be confusing for time-pressed teams to parse offerings and make a choice.

47% of vendors are also looking for excellent customer support with their solution. Understandably they want built-in assistance for the process.



want to reduce risk by leveraging outside XDR expertise.

94% currently outsource XDR monitoring and management or are planning to do so.

Along with reducing the strain on overwhelmed staff, outsourcing also allows companies to leverage their provider's digital forensic and incident response expertise and reduce risk

Reduce staff burden. 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™ MxDR solutions page for more information or to speak with a security expert, contact:

securityservices@opentext.com

DARKReading

Sponsored by: opentext™