XDR: A REVOLUTION IN CYBERSECURITY

The threat landscape is constantly evolving, yet many organizations still rely on disconnected, static security solutions to protect against dynamic attacks.

34% of cybersecurity professionals are dealing with 26 to 50 security incidents daily, with a further 25% managing twice that amount

60% admit security threats evolve so rapidly they're struggling to keep up

89% of cybersecurity experts are working with siloed security solutions

New research from Trellix reveals the cost of siloed security: inefficient protection and significant blows to the bottom line

84% report that their organization has lost up to 10% revenue due to security breaches in the last 12 months

60% said their current tools don't enable SecOps teams to work with maximum efficiency

57% admitted that their current security model needs to be updated to predict, detect, and respond to attacks in real time

36% say that their organizations' security ecosystem is fit-for-purpose today—not tomorrow

Extended detection and response (XDR) is revolutionizing the future of security. XDR simplifies cybersecurity by integrating multiple security tools into a single platform, offering improved detection, response, and remediation capabilities.

23% of organizations have already implemented XDR, with over half (58%) of them citing the ability to automate processes and prioritize critical concerns as a key benefit

SecOps teams see critical advantages with XDR:

real-time detection of threats across vectors	54%
greater operational efficiency	44%
adaptive security	40%
quicker remediation of cyber incident	33%

**Trellix 'XDR: Revolutionising SecOps' Research, 2022. 9000 cybersecurity professionals polled across 15 markets*