Extended detection and response, or XDR, is an open cybersecurity architecture that integrates security tools and unifies security operations across all security layers—users, endpoints, email, applications, networks, cloud workloads and data.

With XDR, security solutions that aren't necessarily designed to work together can interoperate seamlessly on threat prevention, detection, investigation and response.

XDR eliminates visibility gaps between security tools and layers, enabling overburdened security teams to detect and resolve threats faster and more efficiently, and to capture more complete, contextual data for making better security decisions and preventing future cyber attacks.

XDR was first defined in 2018, but the way security professionals and industry analysts talk about XDR has been evolving rapidly ever since. For example, many security experts first describe XDR as endpoint detection and response (EDR) on steroids, extended to span all enterprise security layers. But today experts see XDR's potential as much more than the sum of the tools and functionalities it integrates, emphasizing benefits such as end-to-end threat visibility, a unified interface, and optimized workflows for threat detection, investigation and response.

Also, analysts and vendors have categorized XDR solutions as either *native XDR*, which integrates security tools from the solution vendor only, or *open XDR*, which integrates all of the security tools in an organization's security ecosystem regardless of vendor. But it has become increasingly clear that enterprise security teams and security operations centers (SOCs) expect even native XDR solutions to be open, providing the flexibility to integrate third-party security tools they use now or may prefer to use in the future.

BEBEFITS UF XDR

Today organizations are bombarded by advanced threats (also called advanced persistent threats). These threats sneak past endpoint prevention measures and lurk in the network for weeks or months—moving around, gaining permissions, stealing data, and gathering information from the different layers of the IT infrastructure in preparation for a large-scale attack or data breach. Many of the most damaging and costly cyber attacks and data breaches—ransomware attacks, business email compromise (BEC), distributed denial of service (DDoS) attacks, cyber espionage—are examples of advanced threats.

Organizations have armed themselves with scores of cybersecurity tools and technologies to fight these threats and close off the attack vectors, or methods, that cybercriminals use to launch them. Some of these tools focus on specific infrastructure layers; others collect log data and telemetry across multiple layers.

In most cases these tools are siloed—they don't talk to each other. This leaves security teams to correlate the alerts manually to separate the actual incidents from false positives and triage the incidents according to severity—and coordinate them manually to mitigate and remediate threats. According to IBM's Cyber Resilient Organization Study 2021, 32% of organizations reported using 21 to 30 individual security tools in response to each threat; 13% reported using 31 or more tools.

As a result, advanced threats take too long to identify and contain. IBM's Cost of a Data Breach 2022 report reveals that the average data breach took 277 days to detect and resolve. Based on this average, a breach that occurred January 1 would not be contained until October 4.

By breaking down the siloes between layer-specific point solutions, XDR promises overextended security teams and SOCs the end-to-end visibility and integration they need to identify threats faster, respond to them faster and resolve them faster—and to minimize the damage they cause.

In the relatively short time since its introduction, XDR is making a difference. According Cost of a Data Breach 2022, organizations with XDR deployed shortened their data breach lifecycle by 29 and lowered breach costs 9% on average compared to to organizations