MANAGED DETECTION AND RESPONSE

Condition Zebra's **Managed Detection and Response (MDR)** combines the real-time monitoring and response capabilities of an EDR or XDR solution with highly skilled cybersecurity professionals to conduct 24/7 proactive security actions such as threat hunting, threat intelligence, and managed response.

24/7 Managed Service

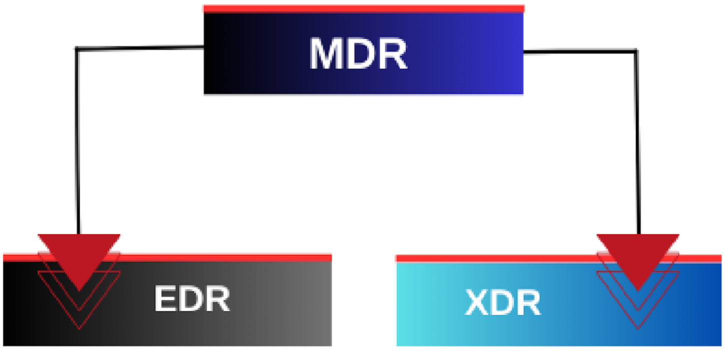
MDR combines advanced threat detection technologies with human expertise to provide a comprehensive defense against a wide range of cyber threats.

More visibility. More power. More control.

MDR upgrades protection against new, unknown and evasive threats through effective detection and response and 24/7 security monitoring, without prohibitive costs or complexity.

EDR or XDR

Based on your needs, our MDR solution will utilize capabilities of an EDR or XDR solution and provide threat monitoring, detection and response functions that offer threat containment capabilities.



EDR - Endpoint Detection and Response

EDR solutions are a core component of every cybersecurity strategy and its foundation. A cybersecurity solution that continuously detects and responds to threats like ransomware and malware in real-time for endpoint devices.

XDR - Extended Detection and Response

XDR is an advanced version of EDR, a full-spectrum, threat-centric security solution that extends detection and response beyond the endpoint to include endpoint, network, server, email, and cloud.

Condition Zebra's EDR

Condition Zebra's **Endpoint Detection and Response (EDR)** is a cybersecurity solution that focuses on monitoring and securing endpoints such as desktops, laptops, servers, and other devices that are connected to a network.

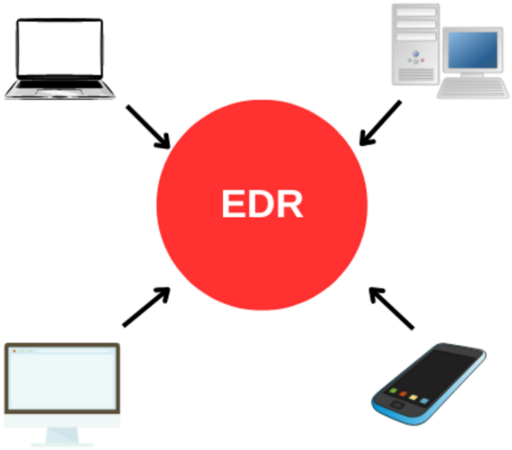
✓ **Endpoint visibility**
Gain unified visibility and real-time insights into all your endpoint devices to understand the threats and their scope.

✓ **Behavioral protection**
EDR involves behavioral approaches that look for indicators of attack (IOAs) and alerts relevant stakeholders to suspicious activities before a breach takes place.

✓ **Rapid response**
EDR that facilitates a rapid response to incidents can prevent an attack before it becomes a breach, allowing your organization to continue to operate as normal.

✓ **Develop expertise**
A simple and efficient EDR solution that will help your team develop expertise in incident response capabilities.

✓ **Save time and resources**
Save time and resources by automating and optimising the most common processes to avoid tedious manual tasks so you can prioritise the important stuff.

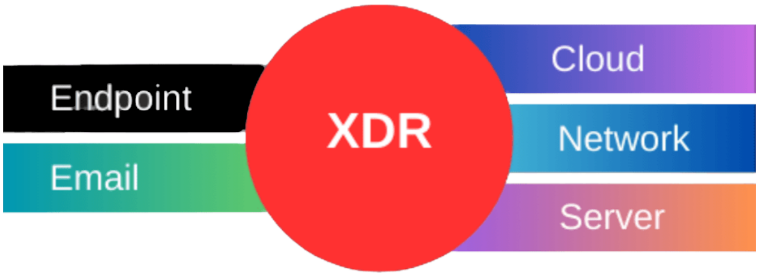


> ***"By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment capabilities."***
>
> **Source**: Market Guide for Managed Detection and Response Services, August 2020, Gartner.

Best suited for: Companies seeking outsourced IT security experts.

Condition Zebra's XDR

Condition Zebra's **Extended Detection and Response (XDR)** is a full-spectrum, threat-centric security solution that extends detection and response beyond the endpoint to provide comprehensive threat detection, investigation, and response across multiple domains like network, server, email, cloud, and others.



XDR Endpoint Security
Focus on endpoint protection from advanced persistent threats (APT), malware & ransomware, IoC (Indicator of Compromise) and IoA (Indicator of Attack) based detection.

XDR Cloud Security
Focus on securing your cloud environments from unauthorised access to cloud mailboxes, admin changes in the environment, impossible logins, brute force attacks, and other types of attacks.

XDR Server Security
Focus on securing your critical server from attacks such as password sprays, brute force attacks, privilege escalation and other types of attack.

XDR Email Security
Focus on comprehensive email protection, which includes gateway security, account compromise, and more, minimising the impact of cyberattacks on your email environment.

XDR Network Security
Focus on securing your network environment from potential threats like command-and-control connections, denial-of-service attacks, data exfiltration, reconnaissance, and others.

> ***"Timely and accurate incident response takes time and skill, which many organizations just don't have, especially when multiple threats need to be addressed simultanenously."***
>
> **Source**: Market Guide for Managed Detection and Response Services, August 2020, Gartner.

Best suited for: Companies seeking managed 24/7 threat hunting.

MDR Key Benefits

✓ **24/7/365 SOC**
Delivers advanced round-the-clock protection from threats that circumvent automated security barriers.

✓ **Empowers businesses by**
Solving the cybersecurity talent crisis, supplying all the major benefits of a SOC 24/7 without the prohibitive costs

✓ **Drives cost efficiencies by**
Focusing expensive inhouse resources on those critical tasks that really demand your IT security staff's involvement

✓ **Maximizes capacity by**
Leveraging proprietary Machine Learning models to significantly increase analyst throughput and minimize the mean-time-to-respond

✓ **Provides peace of mind by**
Delivering continous expert protection against even the most complex and innovative non-malware threats

CONDITION ZEBRA™

www.condition-zebra.com

Condition Zebra (M) Sdn Bhd (701012-T)
Level 3-10, Block F, Phileo Damansara 1,
Jalan 16/11 Off Jalan Damansara,
46350 Petaling Jaya, Selangor, MY.

Email: info@condition-zebra.com
Phone: +603-7665 2021