# ENZOIC INTEGRATION WITH EDR, MDR, AND XDR SOLUTIONS
Strengthening Defense Against Dark Web Threat

Recent findings from IBM's Cost of a Data Breach Report and Verizon's DBIR have identified compromised credentials as the leading cause of data breaches. For EDR, MDR, and XDR solutions, confronting this vulnerability directly is key to ensuring the safety of their end users' environments. Organizations are particularly at risk when credentials are exposed on the Dark Web, making them prime targets for cybercriminals. Enzoic provides an advanced integration of Dark Web intelligence and compromised credential data into these solutions, boosting your competitive edge and your customers' security.
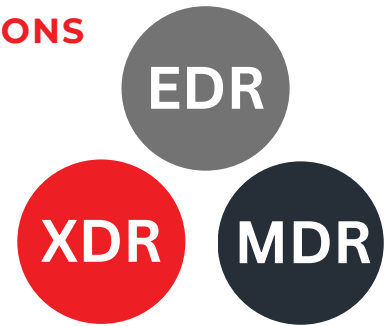
Enhancing EDR, MDR, and XDR with Enzoic

Real-Time Compromised Credential Monitoring
Enzoic's proprietary tools and threat research team continuously scan the Dark Web and other illicit sources for compromised credentials, providing real-time alerts when users' account details are compromised. This integration enables EDR, MDR, and XDR solutions to promptly notify end users of compromised accounts, prompting immediate password changes and securing accounts before they can be exploited.

Automated Response and Remediation
Integrating Enzoic allows EDR, MDR, and XDR solutions to automate responses to compromised credentials. This includes enforced password resets, account lockouts, and MFA enforcement, ensuring that compromised accounts are quickly secured. These proactive measures significantly mitigate the risk of unauthorized access and data breaches.

IP Address Monitoring
Enzoic's integration enhances threat intelligence by continuously scanning the Dark Web and other illicit sources for your exposed IP addresses. This proactive monitoring helps EDR, MDR, and XDR solutions detect and flag suspicious activity linked to your IPs, allowing for timely alerts and automated responses.

Extending Reach Beyond Endpoints
By incorporating Dark Web data, Enzoic extends the reach of EDR, MDR, and XDR solutions from merely monitoring endpoints to encompassing external sources and deeper areas of the internet. This broader scope enhances overall threat visibility and protection, allowing security solutions to detect and respond to threats originating from outside the organization.

Business Credit Card and Bank Account Protection
Monitor business credit card numbers and bank accounts for exposure on the Dark Web. Trigger alerts and implement protective measures such as freezing cards or accounts if they appear in compromised data sets, protecting financial assets from fraud.

Incident Response Enhancement
Utilize Enzoic's data to provide context to security incidents, helping responders understand if compromised data found during an investigation has appeared on the Dark Web. This enables quicker identification and mitigation of threats.

Password Hygiene and Policy Enforcement
Enzoic's password database integration ensures that strong password policies are enforced and detects the use of compromised passwords in real-time during user creation and password updates. This prevents the use of known compromised passwords, enhancing overall security.

Automated Threat Intelligence Enrichment
Automatically enrich threat intelligence feeds with Dark Web data to provide deeper insights into threats and enhance the context of security alerts.

Threat Hunting
Enhance threat hunting capabilities by integrating Dark Web data into threat hunting tools and processes to identify and investigate potential threats originating from the Dark Web.

Insider Threat Detection
Monitor Dark Web data for mentions of internal employee data being sold or discussed, which might indicate an insider threat or data leakage, allowing for early detection and response.

YOUR COMPETITIVE ADVANTAGE

Contemporary compliance standards and industry research show the important role of compromised credentials in data breaches. As organizations prioritize this area of risk, the integration of Enzoic's enhanced security features into XDR, MDR, and XDR solutions is increasingly necessary. By addressing credential-based threats comprehensively, these solutions align with market demands for robust security measures, thereby driving higher sales and revenue for EDR, MDR, and XDR providers. Additionally, incorporating Enzoic's Dark Web data helps providers stay competitive with other solutions that are beginning to include this functionality.

EDR, MDR, and XDR solutions can stay ahead of attackers by providing the best protection and peace of mind to their end users.