Cynet 360 AutoXDR™ Platform Support

GDPR

GDPR Overview

The General Data Protection Regulation (GDPR) is the binding standard to any organization that conducts business operation in the European Union. GDPR includes vast specifications that relate to the responsibility of organizations to safeguard private customer information from both inadvertent exposure, as well as from malicious cyberattack.

GDPR places complete responsibility and accountability on the controller for the customer data it stores and processes. As such, GDPR mostly applies to data access, management, retention, storage and protection, prescribing seven principles for the processing of personal data: Fairness & Transparency; Purpose Limitation; Data Minimization; Accuracy; Storage Limitation; Integrity & Confidentiality; and Accountability.

Cynet for GDPR

Maintaining sound protection from cyberattacks is a key component in keeping customer data secured. In terms of the GDPR principle classification, it maps to **both Integrity & Confidentiality and Accountability.** Cynet enables organizations to ensure that they are covered across all main attack vectors, as well as able to rapidly respond to and recover from detected attacks through both its breach protection technology, as well as managed security services:

Cynet 360 AutoXDR™

Cynet 360 AutoXDR™ addresses the full protection lifecycle before, during and after the occurrence of cyberattacks:

Monitoring & Control

Proactive monitoring of endpoint, user, network and file activity to reduce exposed attack surfaces and eliminate potential threats. Organizations take advantaged of Cynet 360 AutoXDR™ Monitoring & Control to assess and enhance their security posture to fend off known threats **(GDPR, Article 33).**

Prevention & Detection

Cynet 360 AutoXDR™ natively consolidates NGAV, EDR, Network Analytics, Deception and UBA Rules to deliver cross environment protection from all attack vectors that involve endpoints, user accounts and network traffic **(GDPR, Article 25 & 32).**

Response Orchestration

Cynet 360 AutoXDR™ features the widest set of attack remediation tools as either manual operation or automated playbooks, enabling responders to safely address infected endpoints malicious files, compromised user accounts and attacker-controlled traffic **(GDPR, Article 33 & 34).**

CyOps Managed Detection & Response (MDR)

24/7 alert prioritization and monitoring, threat hunting and active assistance in incident response **(GDPR, Article 33 & 34).**

Cynet Threat Assessment Service

A report that delivers complete and actionable visibility into the organizational security posture and its susceptibility to cyber attack **(GDPR, Article 33).**

GDPR 72 Hours Reporting

According to GDPR, **Article 33**, once an organization (data controller) validates an occurred breach that impacts personal data, it must notify the affected individuals with 72-hours without any delays. Both the Cynet 360 AutoXDR™, as well as CyOps MDR have key role in the breach validation process, as well as in determining its scope and impact. Moreover, when properly installed and configured Cynet 360 AutoXDR™ would minimize the chances of a breach form occurring in the first place.

The following table summarizes where Cynet technology and services fit in:

	Continuous Monitoring	Breach Prevention & Detection	Breach Response
Cynet 360 AutoXDR™	✓	✓	✓
CyOps – Cynet Managed Detection & Response Services		✓	✓
Cynet Threat Assessment	✓