transmosis ONE

transmosisONE For

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 and from malicious cyber attack.

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.

transmosisONE for GDPR

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

transmosisONE Autonomous Breach Protection Platform

transmosisONE addresses the full protection life cycle before, during, and after the occurrence of cyber attacks:

Monitoring & Control

Proactive monitoring of endpoint, user, network and file activity to reduce exposed attack surfaces and eliminate potential threats. Organizations take advantage of transmosisONE's Monitoring & Control to assess and enhance their security posture to fend off known threats (GDPR, Article 33).

Prevention & Detection

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

Response Orchestration

transmosisONE 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).

transmosisONE Managed Detection & Response (MDR)

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

transmosisONE Threat Assessment Service

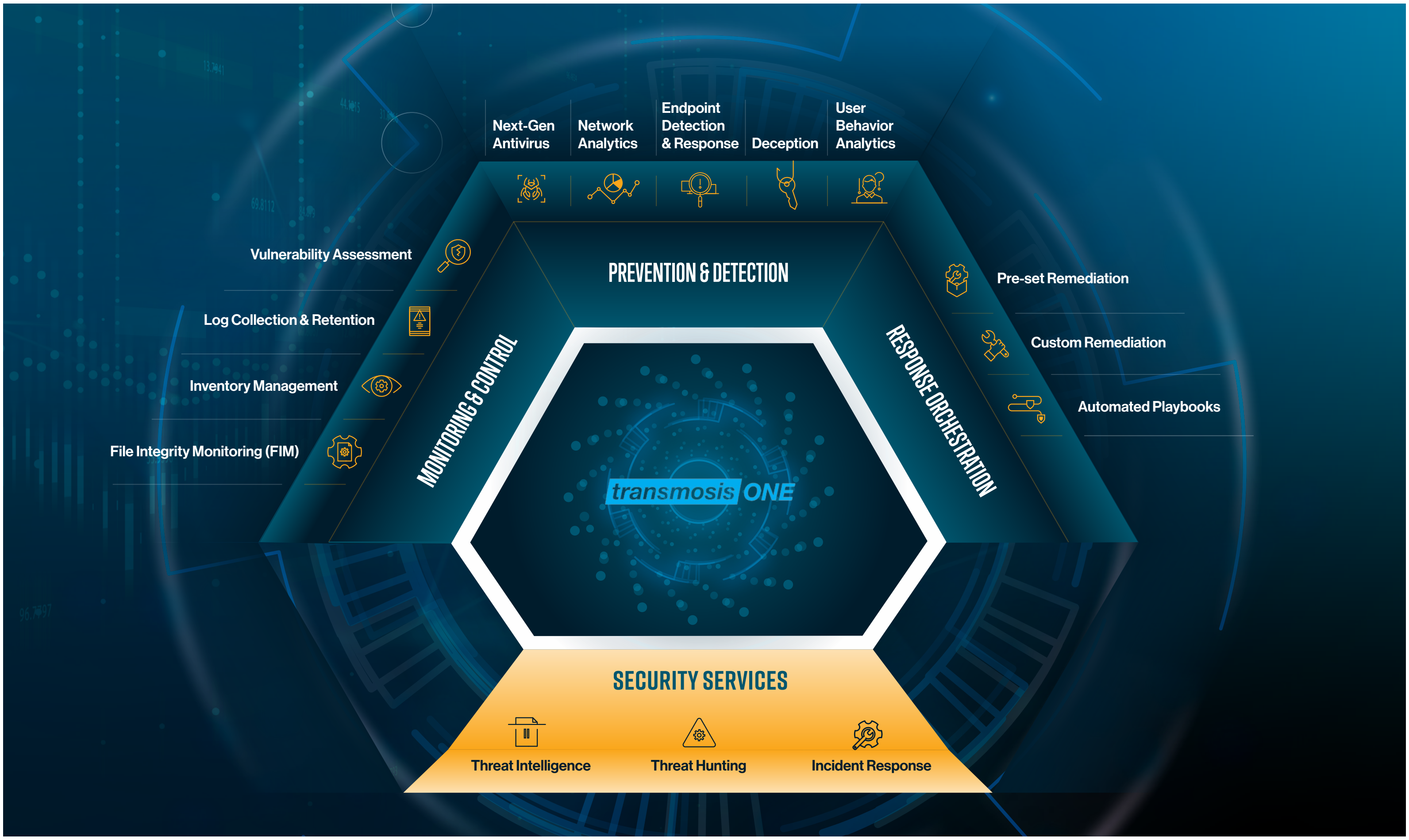
A report that delivers complete and actionable visibility into the organizational security posture and its susceptibility to cyber attack (GDPR, Article 33).

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. transmosisONE has a key role in the breach validation process and determining its scope and impact. Moreover, when properly installed and configured, transmosisONE minimizes the chances of a breach from occurring in the first place.

The following table summarizes where transmosisONE's technology and services fit in:

	Continuous Monitoring	Breach Prevention & Detection	Breach Response
transmosisONE Breach Protection Platform	✓	✓	✓
transmosisONE Managed Detection & Response Services		✓	✓
transmosisONE Threat Assessment	✓		


Next-Gen Antivirus
Network Analytics
Endpoint Detection & Response
Deception
User Behavior Analytics
PREVENTION & DETECTION
Vulnerability Assessment
Log Collection & Retention
Inventory Management
File Integrity Monitoring (FIM)
MONITORING & CONTROL
Pre-set Remediation
Custom Remediation
Automated Playbooks
RESPONSE ORCHESTRATION
transmosis ONE
SECURITY SERVICES
Threat Intelligence
Threat Hunting
Incident Response