



PERCEPT Cloud Security Platform

**Percept Extended Detection and Response (XDR),
Sequaretek IT Solutions Pvt. Ltd.**

In today's rapidly evolving cyber threat landscape, organizations face an ever-growing challenge to protect themselves from a myriad of cyber threats, both known and unknown. The complexity of the security industry, with its multitude of technologies and services, can overwhelm even the most resourceful organizations. While larger enterprises may deploy dedicated security teams to manage these challenges, small to medium-sized organizations often struggle to allocate the necessary time, resources, and budget for effective cybersecurity measures. Sequestek's innovative solution, Percept XDR, emerges as a beacon of cybersecurity resilience for organizations of all sizes.

Percept XDR harnesses the power of artificial intelligence (AI) to provide real-time visibility into an organization's security posture, enabling swift identification and response to security incidents and cyber threats.

Percept XDR utilizes AI for real-time security visibility and swift incident response. Unlike traditional SIEM (Security Information and Event Management) platforms, it employs an AI-driven

detection engine to analyze evolving cyber-attack patterns effectively. This solution offers 24/7 security monitoring, flexible incident response (automated, semi-automated, and manual), big data security analytics, user behaviour anomaly detection, and global threat intelligence. Recognized by Gartner for its innovative AI-driven approach, Percept XDR adapts to the dynamic nature of cyber threats, allowing organizations to assess security posture and prioritize responses. Leveraging advanced technologies like AI, machine learning, deep learning, and SOAR (Security Orchestration, Automation, and Response), ensures precise detection and comprehensive protection.

Innovative technologies used:

Percept XDR leverages cutting-edge technologies like Artificial Intelligence, Machine Learning, Deep Learning, Big Data Security Analytics and Security Orchestration, Automation, Response (SOAR) for precise detection, comprehensive protection, and automated incident response.

Sequestek's Percept XDR is a part of the Sequestek's Percept Cloud Security Platform which

is based on the latest 24/7 (Continuous) Threat Exposure Management framework and uses MITRE ATT&CK mapping for detection and response

Salient Features:

Percept XDR ensures end-to-end security, threat detection & response while allowing enterprises to focus on their core business growth without the fear of compromise.

It offers a combination of AI based threat detection & incident response technology.

The platform provides 24/7 visibility, detection, and response against new-generation threats, malware, user and entity behaviour for all enterprise security data, telemetry, and events

Impact:

Percept XDR has a transformative impact on organizations, significantly enhancing their cybersecurity posture. By harnessing AI and ML technologies, it reduces the Mean Time to Detect and Respond (MTTD & MTTR) while practically eliminating false positives, allowing IT teams to focus on critical tasks.

With Percept XDR's automated response capabilities, IT teams save valuable time. Moreover, this solution spans across industries, safeguarding businesses from cyber threats, protecting brand reputation, ensuring business continuity, and securing vital data and assets

Implementation Model:

The implementation of Percept XDR involves creating and configuring AI-ML algorithms tailored to specific use cases, along with extensive training using large datasets to enhance detection and response. Challenges included competing with global industry leaders, talent acquisition, and resource constraints. Percept XDR is offered as a SaaS subscription with flexible durations (1, 2, or 3 years).

Sequaretek's team integrates security devices with Percept XDR, enabling 24x7 monitoring and incident ticket generation. Sales efforts include direct sales teams and channel/partner networks worldwide, with strategic partnerships like Ingram Micro for cloud marketplace presence.

Beneficiaries:

Ministries and organizations across industries seek robust cybersecurity, board members, and technology stakeholders, including information security leaders aiming for streamlined security oversight. Information security and IT teams benefit from streamlined incident prioritization and automated resolution, saving valuable time.
