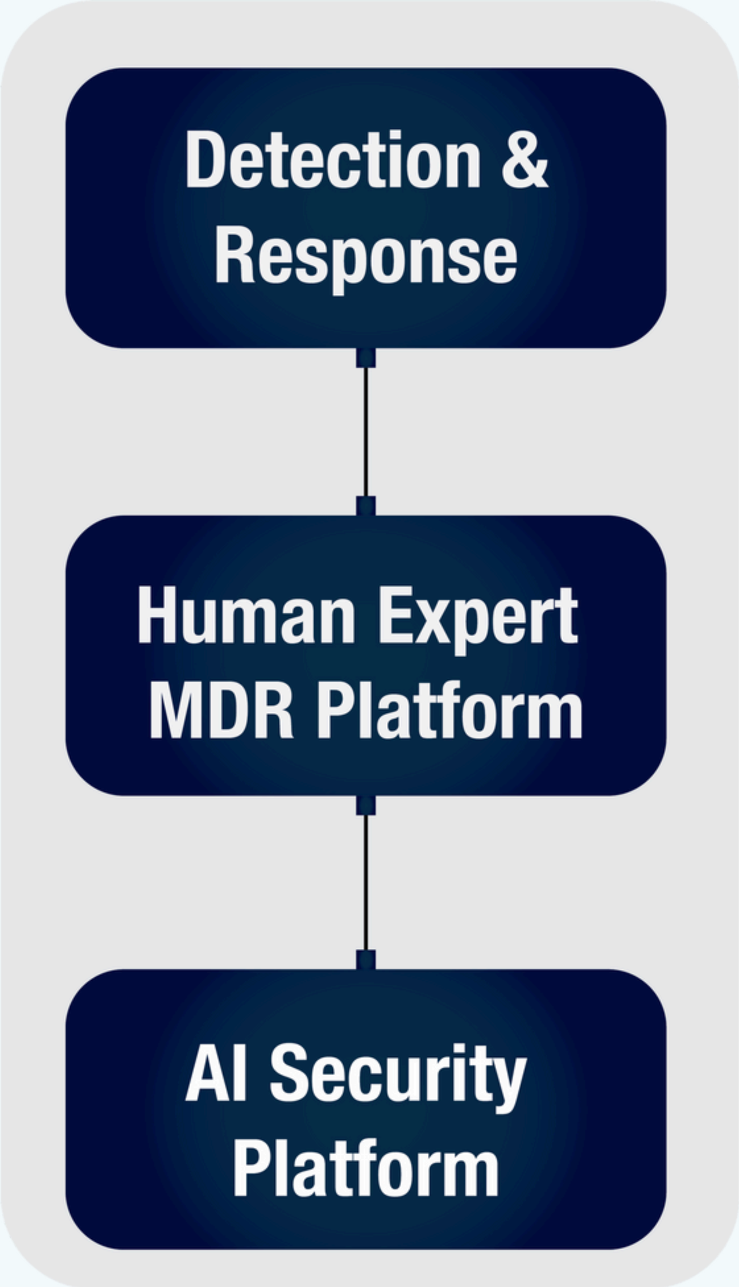
pago CYLANCE

Innovative Cybersecurity Solutions

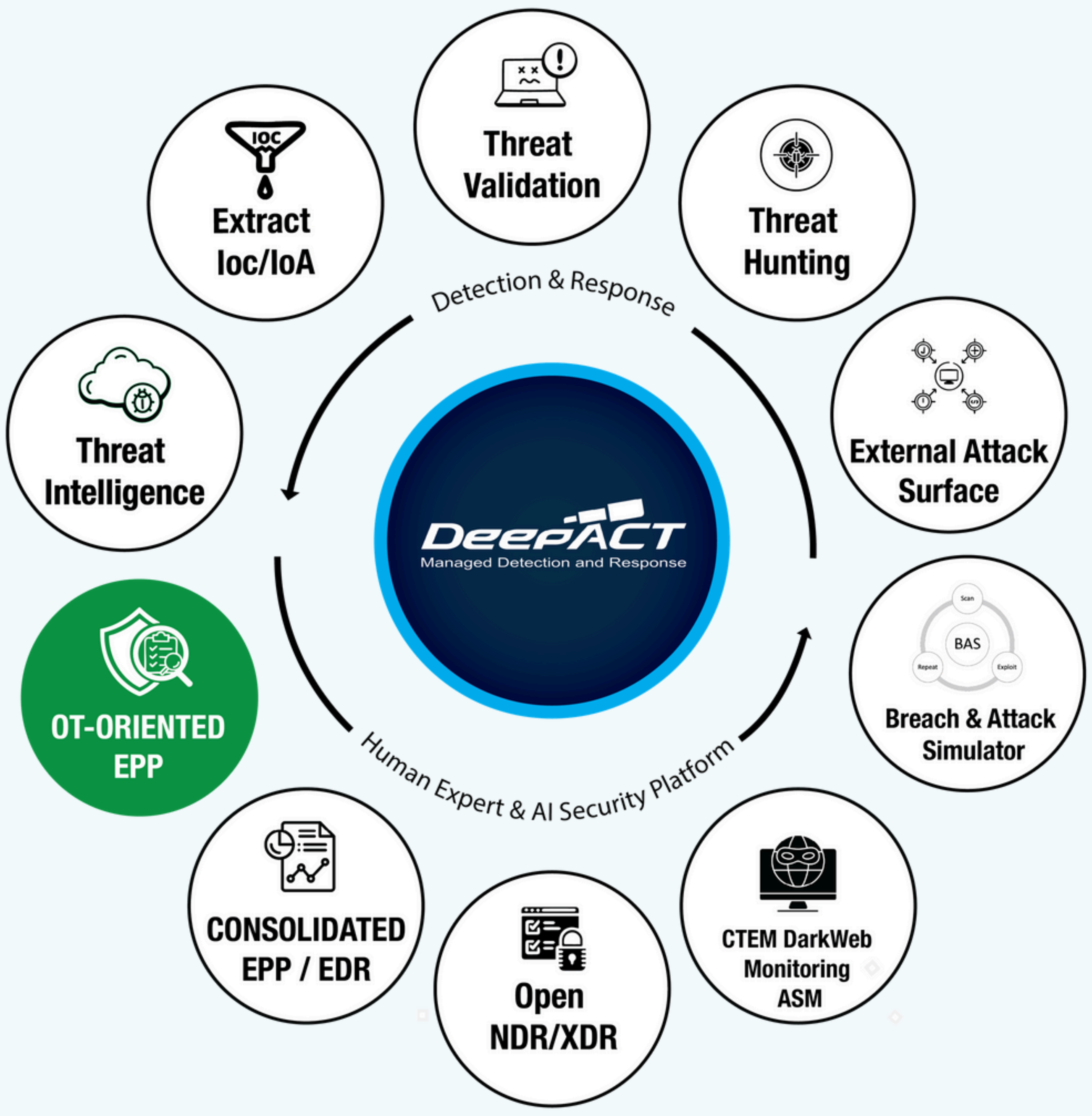
An AI-based Production (OT) and Manufacturing Network (ICS) Endpoint Protection and Prevention Platform provides protection that goes beyond traditional antivirus solutions.

PAGO MDR (Managed Detection and Response) platform, DeepAct, combined with Cylance AI's cutting-edge artificial intelligence security technology, offers customers a differentiated security experience. This integrated solution proactively manages cyber risks through predictive threat detection and real-time response, ensuring fast and accurate 24/7 response in the event of a security incident.


Detection & Response

Human Expert MDR Platform

AI Security Platform



Over the past few years, most security products have blocked threats using signature-based and behavior-based detection methods. The traditional signature-based approach could only respond to known threats, and behavior-based detection had limitations in identifying suspicious activities. However, modern malware is evolving every day and every hour, with technologies emerging that bypass traditional security methods. In this environment, security that goes beyond traditional antivirus is required.

Cylance AI is an innovative security solution that addresses these very challenges.

pago's choice

- AI-Based Predictive Threat Detection Provides predictive security capabilities to anticipate and block unknown malware or zero-day attacks in real time.
- Independent Protection Without Cloud Sandboxing.
  Blocks real-time threats locally without relying on cloud sandboxing or external servers.
- Minimal Impact on System Performance Features a lightweight architecture that minimizes the use of system resources.
- Efficient and Intuitive Management.
  Offers a simple management interface with a single-agent design, ensuring intuitive and efficient security monitoring.
- Optimized for Production and Manufacturing Environments
  Delivers exceptional performance in manufacturing and Industrial Control System (ICS) environments.

pago's Added Value

- **Customizable Security Strategy Development**
  Provides precise threat analysis and risk response plans tailored to the specific industry environment and requirements of each company.
- **Integrated Security Operations Management**
  Centralizes security operations for customers, enabling effective threat monitoring and response.
- **In-Depth Threat Intelligence and Response**
  Offers customized response strategies for potential security incidents based on thorough analysis.
- **Security Optimization for Various Industry Environments**
  Delivers security solutions optimized for industries such as manufacturing, production networks, finance, healthcare, and more.
- **Operational Efficiency and Cost Reduction**
  Maximizes security operations efficiency through automated threat detection and response technologies, with real-time response capabilities provided by PAGO 24/7 MDR Center.
- **Incident Response and Compliance Support**
  Assists with security incident management and compliance requirements, ensuring adherence to regulatory standards.

Fully Integrated

Beyond Chatbots

No Additional Costs

Responsible AI

Cylance PROTECT: Next-Generation Endpoint Protection

Cylance PROTECT is an AI-based endpoint protection platform (EPP) that blocks not only known threats but also unknown zero-day attacks. The latest AI models predict the behavior of malware in advance and block it in real time, ensuring system security. It provides predictive security without relying on signature-based or behavior-based methods.

Cylance PROTECT – EPP Key Features

- **AI-Based Threat Detection and Blocking**
- Cylance PROTECT uses artificial intelligence technology to predict and block unknown malware or zero-day attacks in real time. By utilizing machine learning algorithms, it learns the normal operating patterns of the system and detects malicious code and suspicious activities based on that data.

- **Protection Without Cloud Sandboxing Dependency**
- Cylance PROTECT blocks threats in real-time locally, without relying on cloud sandboxing or data transmission. This ensures effective protection, even in environments with unstable network connections, and helps prevent unknown zero-day threats.

- **Minimized System Performance Impact**
- Since it operates based on AI, Cylance PROTECT does not impact system performance while keeping security features active. It does not interfere with the end-user experience and ensures business continuity. Security is strong, while the effect on system resources or performance is minimal.

- **Single Agent, Simple Management**
- Cylance PROTECT is composed of a single agent, and all endpoints can be easily managed via its cloud-based SaaS console. Without complex configurations, security statuses can be monitored in real time through a centralized management dashboard, allowing for swift responses.

- **Optimized for Production/Manufacturing Networks**
- Cylance PROTECT excels in specialized environments such as manufacturing, OT (Operational Technology), and industrial control systems (ICS). It provides continuous protection for production networks, effectively defending against cyber threats that manufacturers face by predicting and blocking risks in advance.