cynet

TAILORED FOR MSSP SUCCESS

CYNET FOR MSSPS

MANAGED SECURITY-AS-A-SERVICE AT SCALE

Give your customers proactive protection from dynamic and advanced cyber threats

As an MSSP, your customers rely on you to keep them safe from the myriad risks they face each day. But knowing which tools are the optimal fit for the job can be complex. Cynet 360 offers complete breach protection services, providing a single multi-tenant platform that simplifies the task of delivering holistic security across your entire customer base.

Cynet 360 is the ultimate force multiplier, enabling MSSPs to provide their customers with unmatched security, without the need for multiple products and resources. It provides maximum threat visibility and responsiveness, enhancing security team productivity and increasing ROI. Only Cynet 360 gives the power of proactive 24/7 MDR services, continuously monitoring all alerts across your customers' environments to keep them protected at all times, even from the most complex threats.

KEY BENEFITS

DESIGNED FOR MSSP
Scalable tenant-multi platform

SELL A HIGHLY DIFFERENTIATED SERVICE
XDR, Response automation and 24/7 MDR, in one platform

REDUCE MANAGEMENT & DELIVERY COSTS
Extremely rapid deployment

TAILORED TO YOUR SUCCESS
Pricing structure enables high margins for partners

GIVE YOUR CUSTOMERS PROACTIVE PROTECTION FROM DYNAMIC AND ADVANCED CYBER THREATS

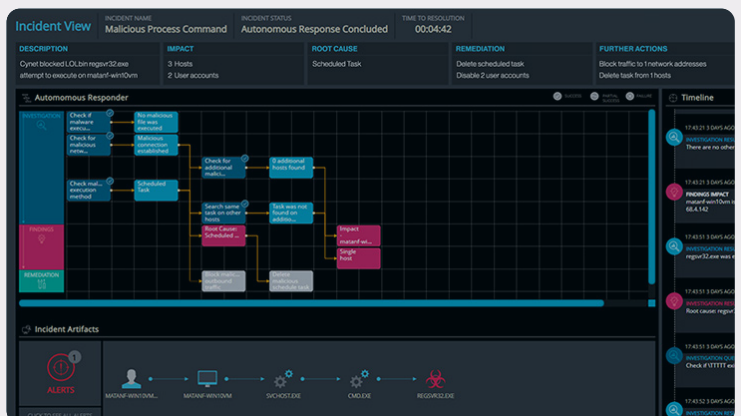Prevention & Detection for endpoints, network, and users

Multi-tenant, scalable platform designed for MSSPs
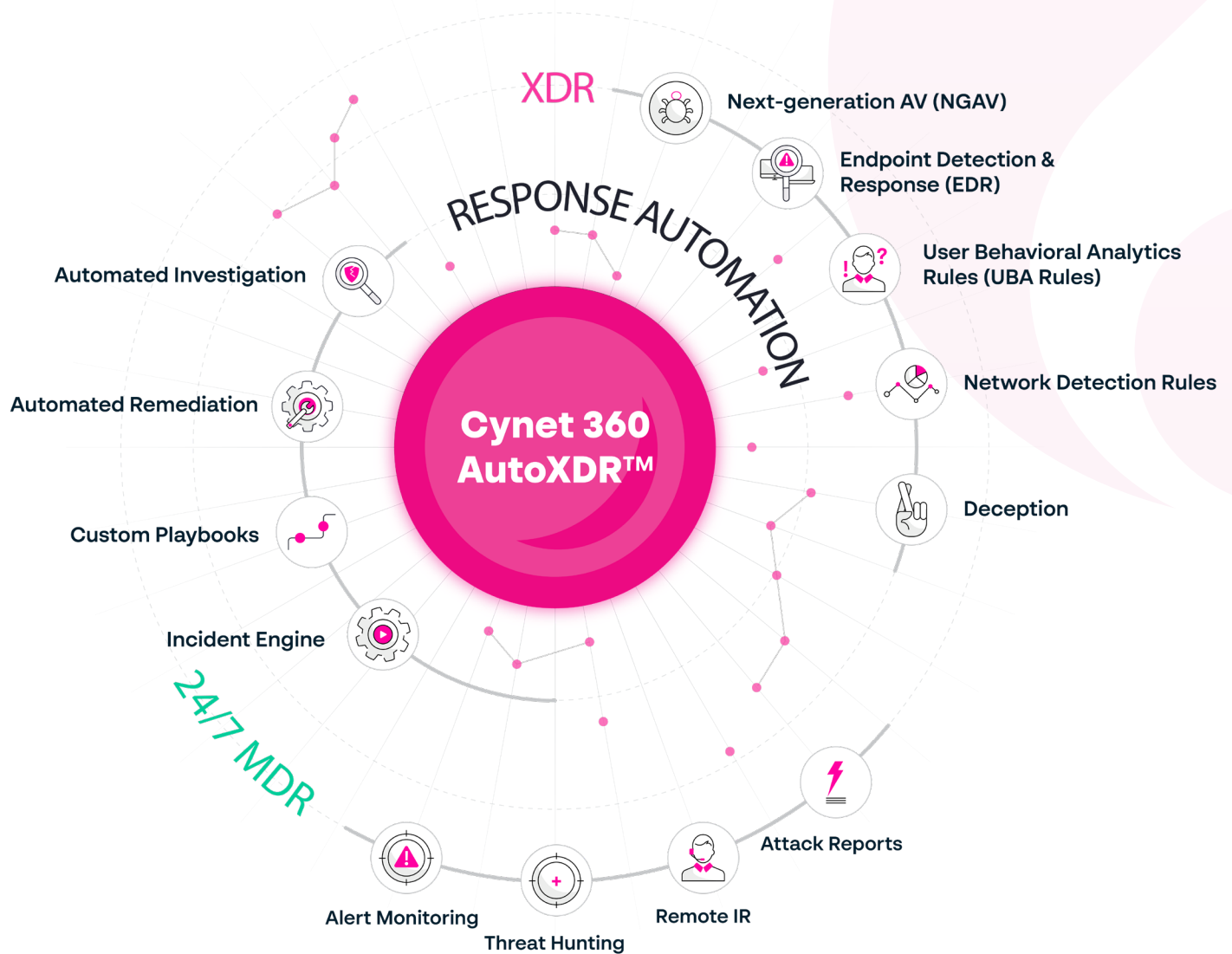
Proactive 24/7 MDR services included

Attractive margins

THE CYNET 360
AUTONOMOUS BREACH PROTECTION PLATFORM

Cynet 360 is the world's first Autonomous Breach Protection platform that natively integrates the endpoint, network, and user prevention & detection of XDR with automated investigation and remediation, backed by 24/7 MDR services—placing end to end breach protection within reach of any organization, regardless of its security team size and skill.

Cynet 360 AutoXDR™

XDR

RESPONSE AUTOMATION

24/7 MDR

- Next-generation AV (NGAV)
- Endpoint Detection & Response (EDR)
- User Behavioral Analytics Rules (UBA Rules)
- Network Detection Rules
- Deception
- Attack Reports
- Remote IR
- Threat Hunting
- Alert Monitoring
- Incident Engine
- Custom Playbooks
- Automated Remediation
- Automated Investigation

KEY BENEFITS
OF CYNET 360 FOR MSSPS

DESIGNED FOR MSSPS

- Scalable multi-tenant platform
- True client separation down to the data
- Centralized dashboard: alerts, forensics & remediation
- Supports both full-management and end-client management

SELL A HIGHLY DIFFERENTIATED SERVICE

- A complete XDR platform - including NGAV, EPP, EDR, UEBA, NTA, and Deception
- Fully Automated Threat Response Workflows - Investigation, Root Cause Analysis, Impact Analysis, Remediation - providing SIEM and SOAR capabilities
- Single solution, providing full coverage of Users, Hosts, Files, & Network
- Proactive 24/7 MDR services included for all clients
- Single license with all features and services included

REDUCE MANAGEMENT & DELIVERY COSTS

- Extremely rapid deployment – up to 5,000 endpoints in 1 hour
- Replace multiple solution providers with a single pre-integrated offering
- Lightweight agent minimizes maintenance requirements
- Multiple agent deployment methods
- Entire environment monitored 24/7 by Cynet

TAILORED FOR YOUR SUCCESS

- Cynet's partner pricing structure enables higher margins to partners
- Marketing – tailored collateral, webinars, and case studies
- Sales – expert sales reps and SEs across the entire sales cycle
- Technical support across deployment, management, and maintenance
- Partner Portal access to Cynet Academy which includes Sales & Technical training, tech & sales videos, and certification

AUTONOMOUS BREACH PROTECTION
ESSENTIALS FOR MSSPS

XDR

ENDPOINT PROTECTION
Multilayered protection against malware,ransomware, exploits, and fileless attacks

NETWORK PROTECTION
Protecting against scanning attacks, MITM, lateral movement, and data exfiltration

USER PROTECTION
Preset behavior rules coupled with dynamic behavior profiling to detect malicious anomalies

DECEPTION
Preset behavior rules coupled with dynamic behavior profiling to detect malicious anomalies

RESPONSE AUTOMATION

INVESTIGATION
Automated root cause and impact analysis

REMEDIATION
Eliminate malicious presence, activity, and infrastructure across user, network, and endpoint attacks

PLAYBOOKS
Automate comprehensive responses across the environment for any attack scenario

INCIDENT VIEW
Intuitive graphical layout of the attack and the automated response actions

MDR

ALERT MONITORING
Prioritize and notify customer on critical events

ATTACKS INVESTIGATION
Detailed analysis reports on the attacks that targeted the customer

PROACTIVE THREAT HUNTING
Search for malicious artifacts and IoC within the customer's environment

INCIDENT RESPONSE GUIDANCE
Remote assistance in isolation and removal of malicious infrastructure, presence, and activity