Cynet 360 AutoXDR™

Comprehensive cybersecurity has never been easier

Radically simple. Super efficient. Zero resource-drain.

Philipp Schwarz, September 2023

Der klassische Anti-Viren-Schutz reicht nicht mehr!

Cynet und die endpoint- Security steht auf Auto-Pilot!

Philipp Schwarz
Channel Account Manager DACH
PhilippS@cynet.com
+49 176 7458 3169

Agenda

- Exkurs: Anti-Virus und die offenen Scheunentore
- XDR: Nur eine weitere Abkürzung, oder wirklich sinnvoll?
- Cynet 360 AutoXDR -> AutoPilot für die Endpoint- Security
- 24/7, aber nicht nur Support!

Exkurs: Antivirus

Schutz

- Scanner (Echtzeit, manuell, online)
- Reaktiv / Proaktiv
- Signaturbasiert, verhaltensbasiert, maschinelles learning
- Virendefinitionen online

Aber

- Teils hohe Systemauslastung durch scan(s)
- Virendefinitionen aktuell?
- Anwendungen und Seiten werden pauschal geblockt
- Hoher manueller Aufwand
- Reaktiver Schutz durch scan (Zeitfenster / Systemressourcen)

- **Was ist mit dem Schutz im Netzwerk, dem user, in der cloud und weiteren Anwendungen?**

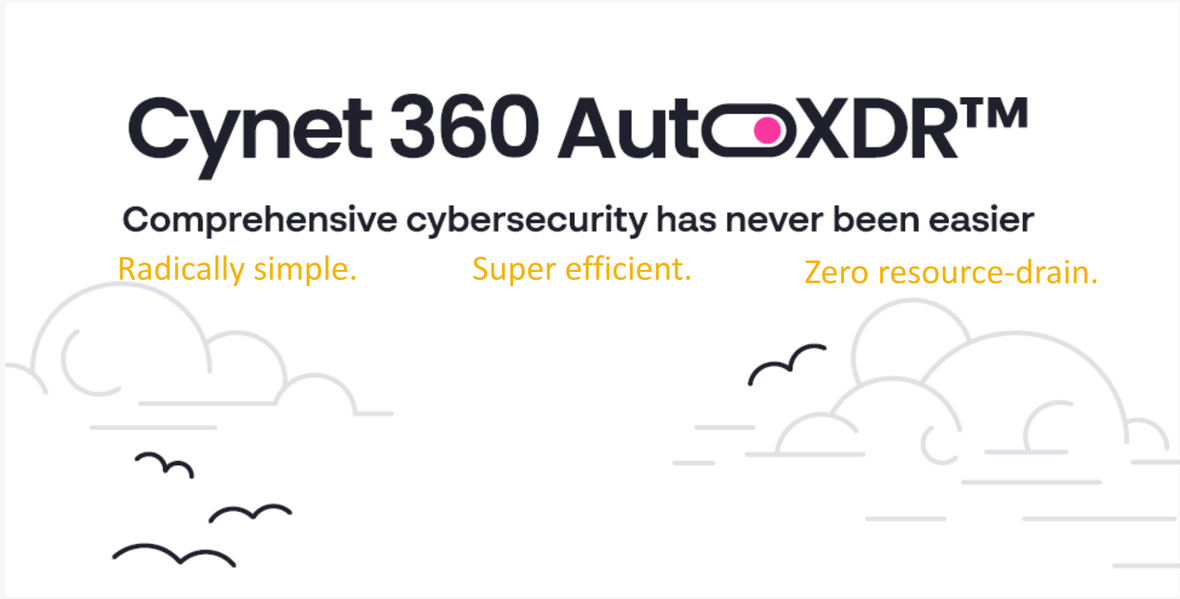
Vom Antivirus über den EDR zum XDR

XDR = X-tended Detection & Response (Erweitert? Aber was denn genau?)

EDR = Endpoint Detection & Response
Daten beim Endpoint

XDR erfasst und korreliert Daten automatisch auf mehreren Ebenen:

- Endpoint
- Server
- Cloud
- Netzwerk
- User

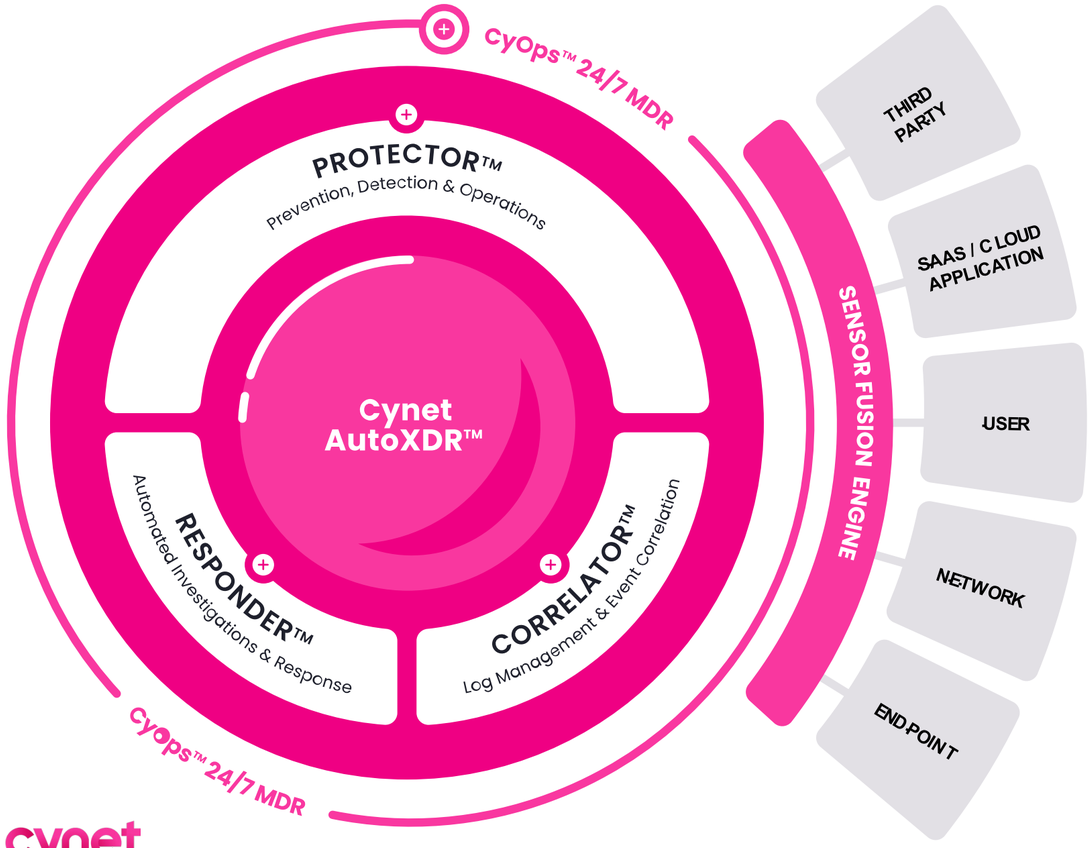


cynet

Cynet 360 AutoXDR™

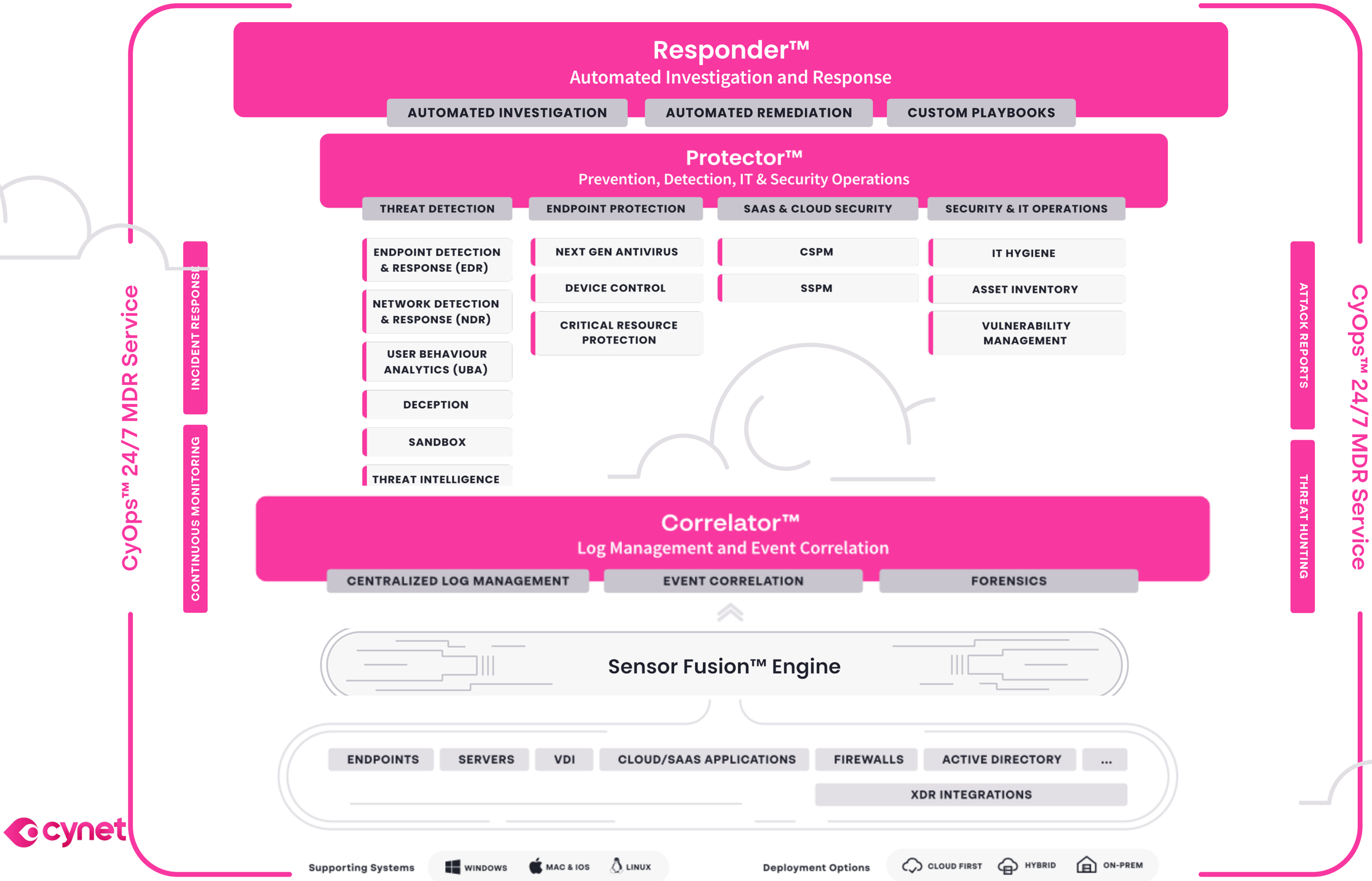
Purpose-built for lean IT Security teams

Voll ausgestattete, automatisierte, einfach zu bedienende Plattform

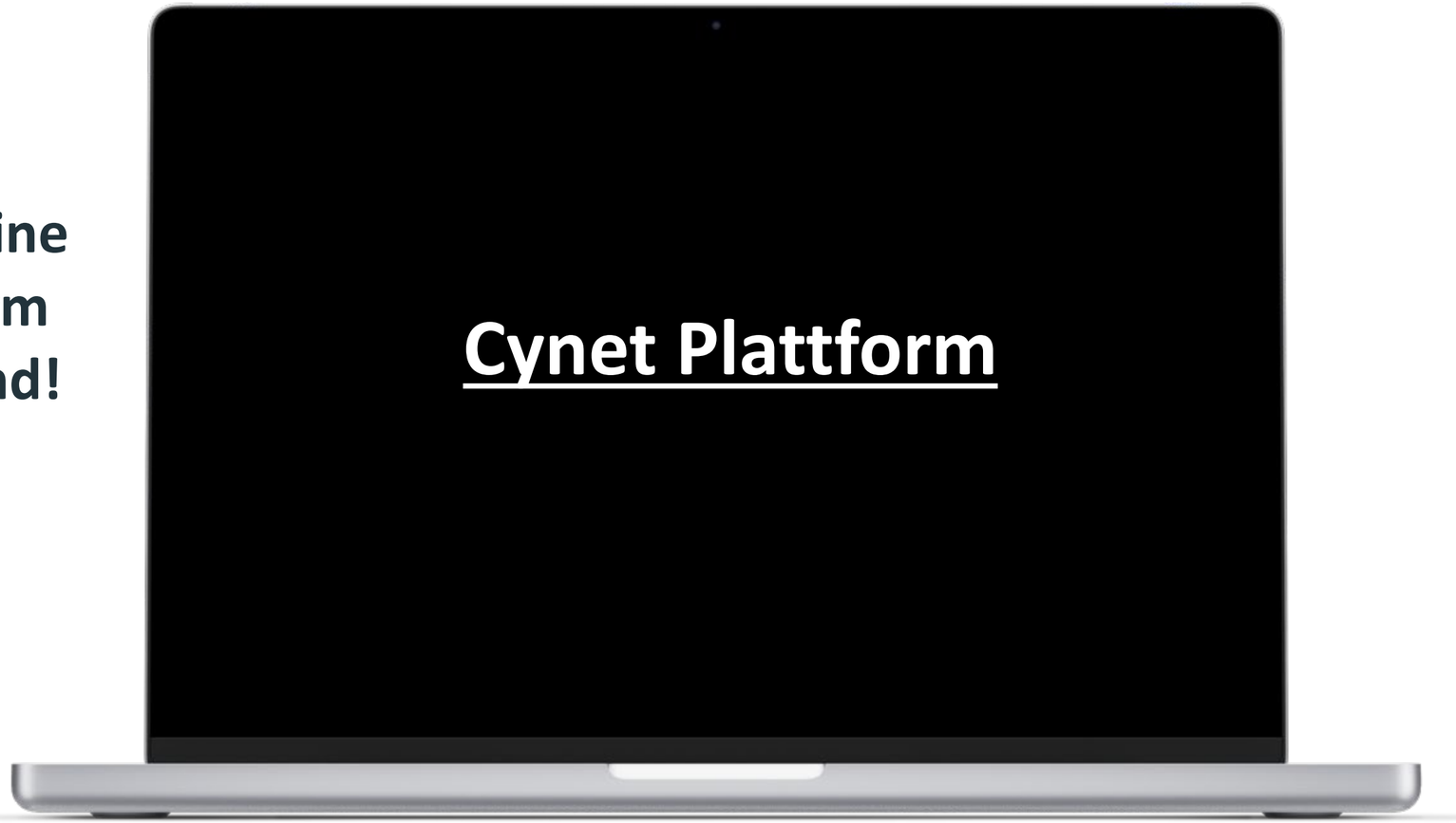


Cynet Vorteile / Kundenanforderungen

- End-to-end
- Benutzerfreundlich
- Nativ, automatisiert
- Sehr guter TCO TransparenteLizenzkosten
- Höchste Genauigkeit
- 24/7 MDR- Service inkl.
- Unmittelbar zu installieren / kein reboot!
- Minimale Voraussetzungen


Responder™
Automated Investigation and Response
AUTOMATED INVESTIGATION
AUTOMATED REMEDIATION
CUSTOM PLAYBOOKS
Protector™
Prevention, Detection, IT & Security Operations
THREAT DETECTION
ENDPOINT PROTECTION
SAAS & CLOUD SECURITY
SECURITY & IT OPERATIONS
ENDPOINT DETECTION & RESPONSE (EDR)
NETWORK DETECTION & RESPONSE (NDR)
USER BEHAVIOUR ANALYTICS (UBA)
DECEPTION
SANDBOX
THREAT INTELLIGENCE
NEXT GEN ANTIVIRUS
DEVICE CONTROL
CRITICAL RESOURCE PROTECTION
CSPM
SSPM
IT HYGIENE
ASSET INVENTORY
VULNERABILITY MANAGEMENT
Correlator™
Log Management and Event Correlation
CENTRALIZED LOG MANAGEMENT
EVENT CORRELATION
FORENSICS
Sensor Fusion™ Engine
ENDPOINTS
SERVERS
VDI
CLOUD/SAAS APPLICATIONS
FIREWALLS
ACTIVE DIRECTORY
...
XDR INTEGRATIONS
CyOps™ 24/7 MDR Service
INCIDENT RESPONSE
CONTINUOUS MONITORING
ATTACK REPORTS
THREAT HUNTING
CyOps™ 24/7 MDR Service
Supporting Systems
WINDOWS
MAC & IOS
LINUX
Deployment Options
CLOUD FIRST
HYBRID
ON-PREM

Für weitere Informationen und eine kurze Demonstration der Plattform besuchen Sie mich gerne am Stand!



24/7, aber nicht nur Support!

24x7 MDR

CyOps - 24x7 Managed Detection and Response Team

Erweitern Sie ihr Security Team

Nutzen der Erkenntnisse von den anderen Endkunden weltweit

Zugewinn von erstklassigem Know-How in der Cybersecurity

Bereits inklusive, ohne Mehrkosten

Detection

- **Kontinuierliches alert monitoring** zur Validierung und Optimierung von Präzision und Handlungsfähigkeit
- **Proaktives threat hunting** um verborgene Bedrohungen zu finden
- **Lateral Movement** Erkennung

Investigation

- **Deep-dive** in den Angriff zur vollständigen Aufdeckung von Ursache, Umfang, Verweildauer und dessen Auswirkungen
- Den client mit **aktuellen IOCs versorgen**
- **Expert Advice**, Playbooks, White/Black-Listing, Ausschlüsse ... per E-Mail, Telefon oder direkt aus der GUI

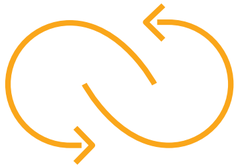
Response

- Unterstützung bei **Remote Incident Response** mit Untersuchung, umfassenden Abhilfeplänen und Anleitung
- **Bewertung der Sicherheitslage** über die gesamte Organisation
- **Threat Detection** detailierte attack reports

*Premium services with dedicated analyst are available

Cynet AutoXDR - Der umfassendste autonome Schutz vor Sicherheitsverletzungen

- Schnelle Wertschöpfung
- Ein einziger Blickwinkel für Endpunkte, SaaS und Drittanbieter
- Vereinfachung von SecOps für kleine Sicherheitsteams
- Bestes Preis-Leistungs-Verhältnis



Eine Plattform

- ✓ SaaS-first
- ✓ MSSP Partner
- ✓ Einfache UX
- ✓ CyOps MDR
- ✓ Geringer TCO
- ✓ Plattform- agn.

Autonomes IR

- ✓ Incident Workflows
- ✓ Anpassbare Remediations
- ✓ Out-of-the-box Playbooks
- ✓ Anpassbare Alerts

Umfassender Schutz

- ✓ SaaS Security Posture
- ✓ URL Filtering & Phishing
- ✓ SIEM + Data Lake
- ✓ Win, Linux & Mac
- ✓ Über alle Angriffsvektoren
- ✓ MITRE ATT&CK

SOAR Integration

- ✓ Anpassb. Playbooks
- ✓ Identity: AD, Azure AD, OKTA
- ✓ Netzwerk: Proxy, RMM, TCP->HTTP
- ✓ Security: FW, SWG
- ✓ Ops: Ticketing

CyOps 24/7 MDR Team

- ✓ Neue Erkennungsmethoden
- ✓ On Demand Analyse
- ✓ Remediation Anleitungen
- ✓ Proaktives Monitoring
- ✓ Keine Bots, aber Experten

cynet

CYNET Market Recognition – Independent Validation

IDC
ANALYZE THE FUTURE

"Cynet emphasizes the benefits of its ground-up development approach in building a truly unified platform that effectively delivers numerous essential security capabilities through a single user interface"
Read More

Gartner peerinsights™

Gartner®

Recognized as an Automated EDR in Gartner's
EDR Market Guide 2019
Read More

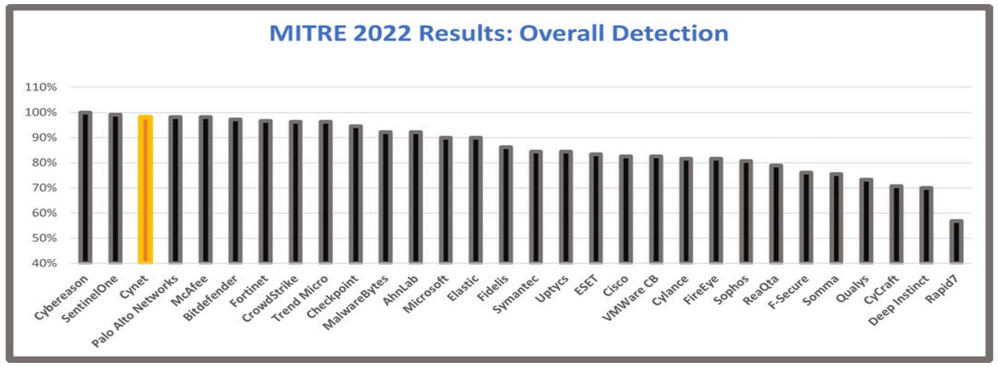
Ovum

On the Radar: Cynet Autonomous Breach Protection automates core functionalities for breach protection

2021 MITRE ATT&CK Evaluation

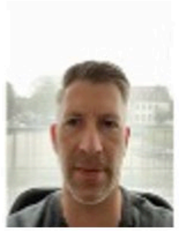
MITRE 2022 ATT&CK Evaluation Results

G2 WINTER REPORT: CYNET RATED #1



cynet

Vielen Dank für Ihre Aufmerksamkeit!



Philipp Schwarz

Channel Account Manager

+49 176-74583169

philipps@cynet.com | www.cynet.com

--