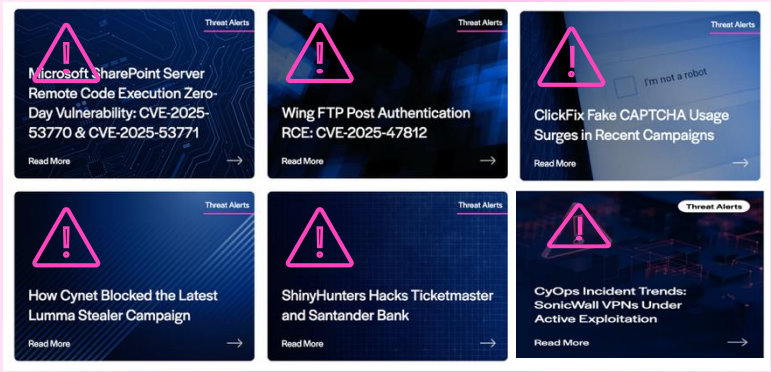
cynet

Unified, AI-Powered Cybersecurity Platform

Threats don’t wait. **Neither do we.**

Four Forces Widening the Cyber Defense Gap



Organizations are under attack.

Partners are overwhelmed.

Accelerating Threat Complexity[1]

Security Talent Shortage[3]

Faster Adversaries[4]

Tool Overload[2]

Sources:

1. sosafe-awareness.com
2. Cybersecurity Dive
3. ISC2
4. Fortinet

Vision and Strategic Pillars

To deliver cybersecurity peace of mind through an AI-powered, All-in-One security platform backed by **24×7 MDR CyOps** security experts, delivered through a single console with AI-automated workflows that **reduce risk, consolidate tools, and drive efficiency.**

All-in-One
Platform

Security
Leadership

AI
Driven

Open
& Collaborative

Co-Managed
By Any Team

Cynet Solutions: Complete Protection

Endpoint

- NextGen Antivirus (AI)
- Ransomware Protection
- Exploit Protection
- Malware Protection
- Credential, Files, Documents Protection
- Device Control
- Endpoint Detection & Response
- Full Endpoint Visibility
- Endpoint Security Posture Management
- Windows Event Visibility
- Secure Remote Shell

Network

- Domain & Phishing Filtering
- Network Scan Detection
- Network Poisoning Detection
- Tunnelling & Exfiltration Detection
- External Attack Surface Management / Port Scanning
- Network Anomaly Detection

Identity & User

- ITDR
- User Activity Visibility
- Lateral Movement Detection
- User Anomaly Detection
- Deceptive Users

SaaS & Cloud Apps

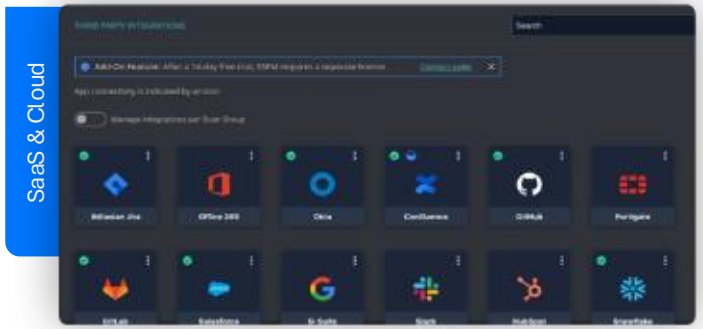
- Security Misconfiguration Detection & Remediation
- Compliance Management
- Reports & Notifications
- Cloud Users & Resource Inventory
- SaaS & Cloud User Behavior Anomaly Detection

Mobile

- Device, Network, App & Phishing Threat Detection
- On-Device Remediation
- Mobile App Risk Detection & Mitigation
- iOS, Android & Chrome OS Devices

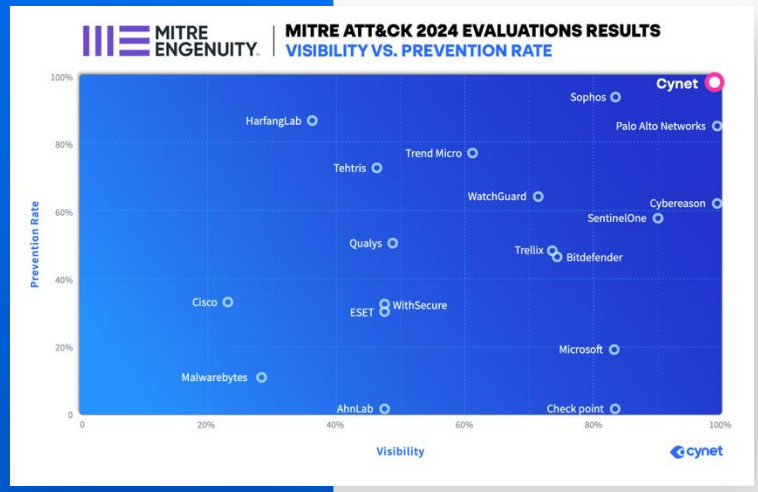
Email

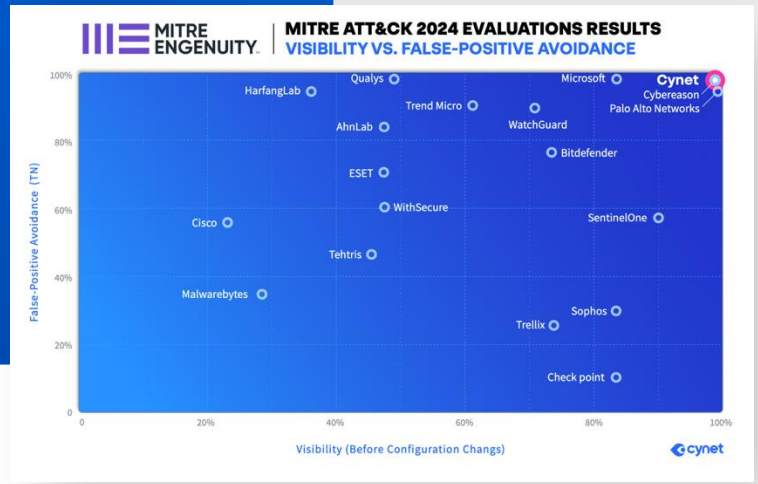
- Integration with Office 365
- Phishing Prevention
- Malware Prevention
- Exploit Prevention
- Unauthorized Senders Management
- Block Malicious File Extensions
- Safe URLs



FIRST to 100%.
ONLY to Repeat.

Cynet made MITRE ATT&CK history as the **first vendor** to achieve 100% Visibility, 100% Context-Rich Detection, 0 False-Positives, and 100% Prevention Rate without any configuration changes, and is the **only vendor** to deliver these results in **back-to-back** years





cynet MITRE | ATT&CK® Evaluations

cynet
GUIDE

2025 MITRE ATT&CK® Evaluations

Exploring Cynet's Continued Strength in Prevention, Visibility, and Accuracy

Cynet achieved exemplary results in the MITRE ATT&CK® Enterprise Evaluations for three years running, showcasing sustained strength across prevention, detection clarity, false-positive reduction, and out-of-the-box readiness.

The consistency reflects a platform engineered for real-world resilience, built for security teams to scale security operations without sacrificing speed, visibility, or protection.

100%
Detection Visibility in Initial Run

100%
Technique-Level Coverage in Initial Run

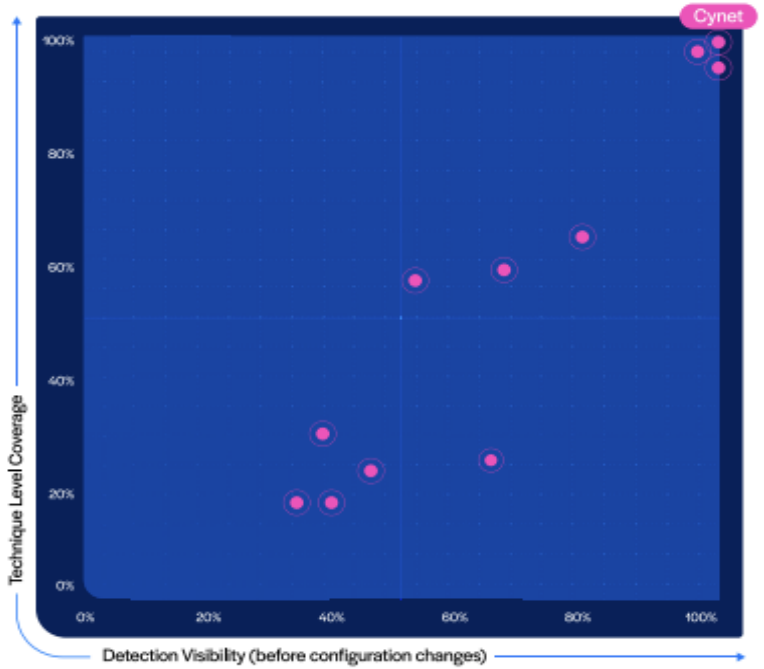
100%
Protection in Initial Run

Zero
Detection False Positives in Inital Run

Zero
Configuration Changes

What the 2025 MITRE ATT&CK Evaluations Measure

The 2025 MITRE ATT&CK Evaluations measures how well security solutions detect and protect against real-world adversary behavior using the ATT&CK framework as a reference. MITRE runs an adversary emulation (this year based on Scattered Spider and Mustang Panda) across multiple platforms and attack stages. Solutions are evaluated on the quality, depth, and accuracy of their detections, including whether they identify activity at the technique level, tactic level, or through general alerts. Solutions are also assessed for what they don't report, as MITRE seeks to identify which participants generate accurate alerts, report false positives, or miss alerts altogether. The ATT&CK Evaluations ultimately aim to help security teams assess participating vendors' visibility, detection accuracy, protection capabilities, and consistency across the full attack lifecycle. Results are evaluated and reported before configuration changes (Initial Run) and after adjustments to configurations (Configuration Change).



Detection Visibility vs. Technique-Level Coverage

MITRE evaluates each platforms' ability to collect all pertinent telemetry during simulated attacks (Detection Visibility) and create actionable, contextual alerts based on those inputs (Technique-Level Coverage). This Detection Visibility vs. Technique-Level Coverage chart demonstrates how Cynet performed in this year's evaluation in regard to data collection and accuracy of alerting. Strong overall results demonstrate a balanced and capable security platform that delivers protection, clarity, and operational efficiency against emulated real-world adversaries.

The Intelligent SOC Agent

AI-Powered Detection, Automation, and Response Natively Built into the Core of Cynet.

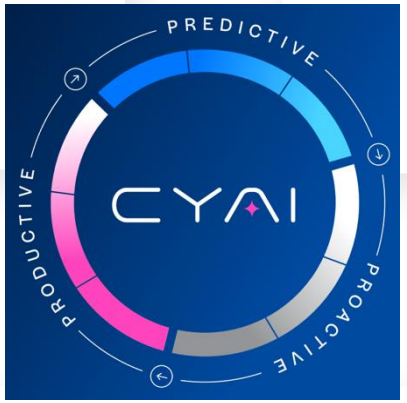
- 97% of advanced threats detected autonomously.
- Detects and contains threats in <1 second.
- 90% of threats remediated automatically.

Predictive

- AI-powered NGAV
- UEBA for Endpoint Behavior
- Environment-Specific Tuning

Proactive

- AI Correlation Engine
- SIEM Behavioral Analytics
- CyOps Integration



Productive

- Automated IR
- GenAI Alert Insights
- GenAI Support Assistant

Cynet Product & Platform Differentiators

AI-Powered Automation

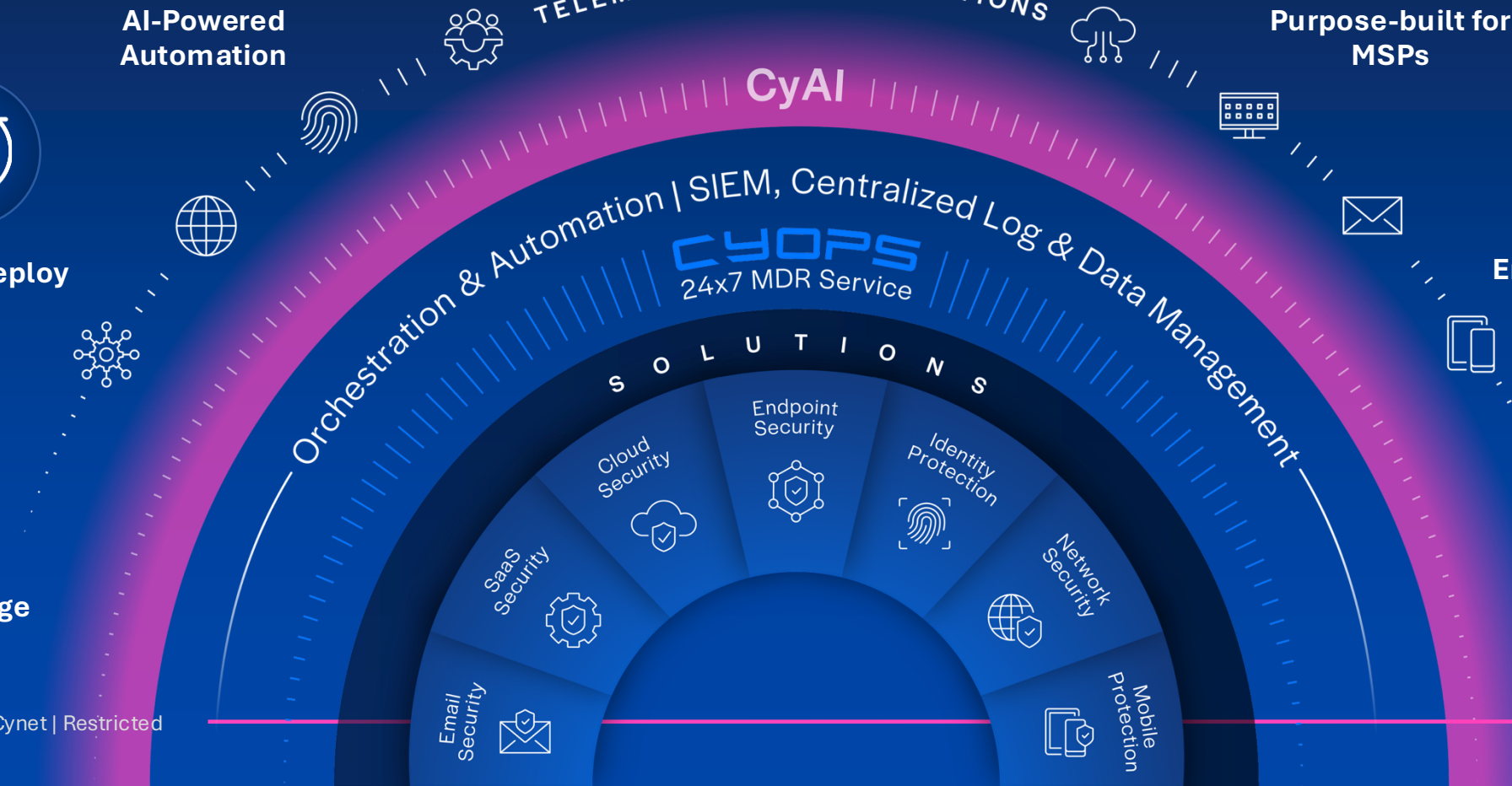
Purpose-built for MSPs

Easy to Deploy

Enterprise Protection for Lean Teams

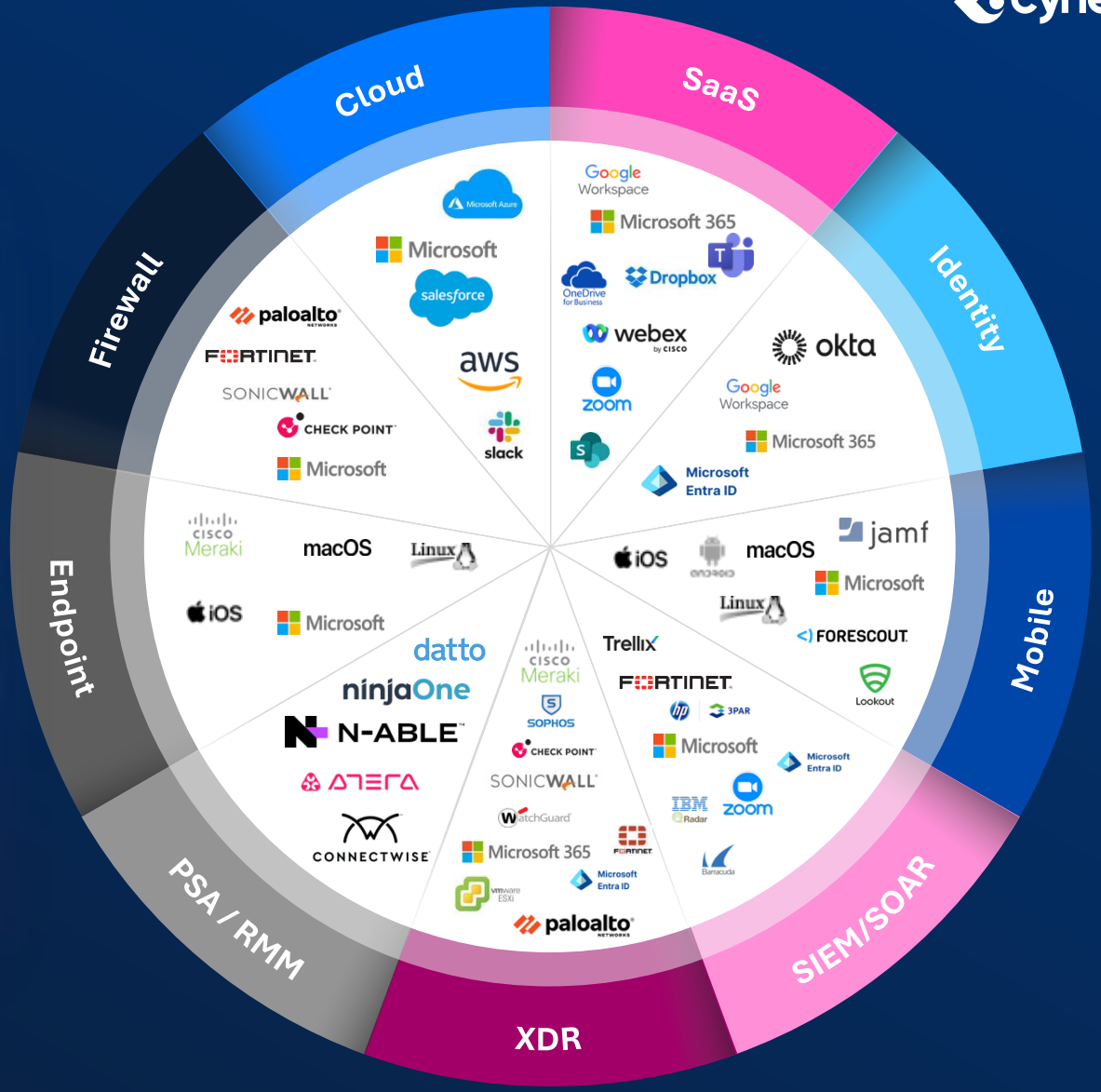
Unified, Broad Coverage

24x7 Expert MDR (CyOps)



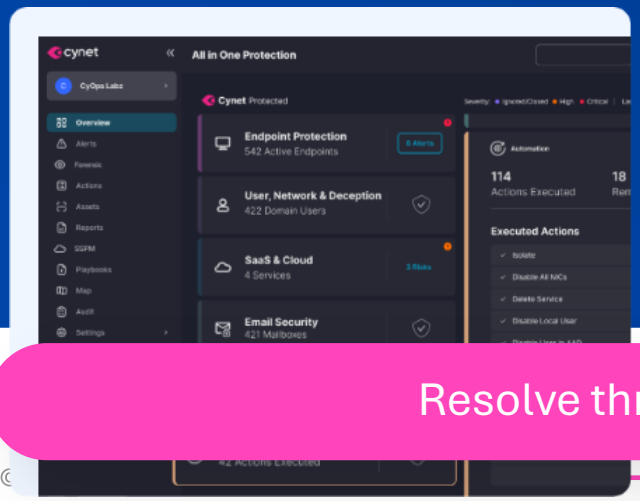
Cynet Integrations: Ingest, Operate, Extend.

- **Security Data Ingestion (INGEST)**
  Collects telemetry and signals across the security ecosystem for complete visibility and protection
- **Business Platform Alignment (OPERATE)**
  Works with existing IT and security systems used to operate and deliver services (e.g., PSA, RMM, ITSM)
- **Ecosystem Extension (EXTEND)**
  Connects with adjacent technologies unify and optimize IT and security operations.



Security Orchestration, Automation, and Response (SOAR)

Cynet SOAR puts security on autopilot by unifying detection, investigation, and response across the entire environment.



Integrate

Combine third party log data into investigation flows and extend remediation action to switches, firewalls, active directory, and more.

Investigate

Automatically determine attack root cause with graphical timelines and attack layout details.

Consolidate

A single screen to Investigate alerts, remediate threats, orchestrate, and automate incident response workflows.

Orchestrate

Remediation Playbooks automate comprehensive multi-action responses across the environment for any attack scenario.

Remediate

Eliminate malicious presence and activity across endpoints, networks, users, SaaS applications, and other IT components.

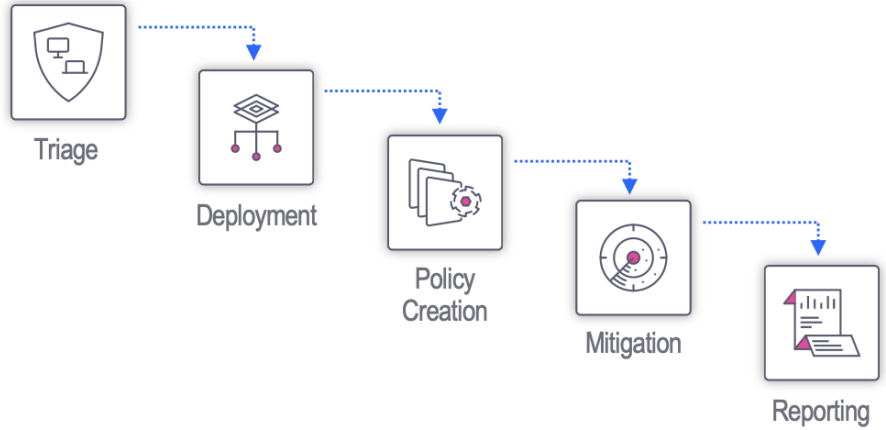
Resolve threats 50x faster and reduce manual incident handling by 90%.

Managed SOC - activate 24/7 monitoring

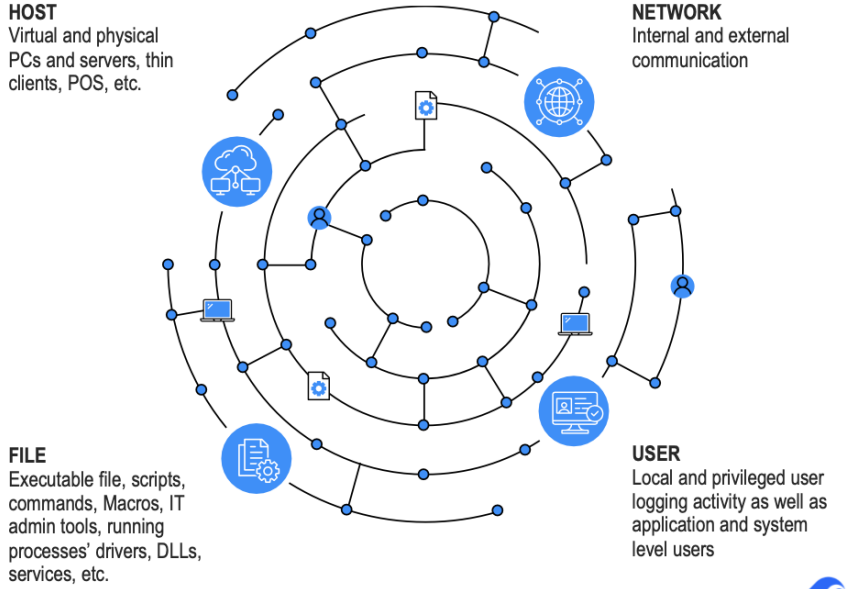
Cynet's in-house team of threat analysts and security experts, CyOps, operates a 24/7 SOC to help protect all client environments. CyOps continuously monitors and prioritizes alerts, informing customers in real-time of critical security events and guiding them through the response process.

Automatically detect and respond to threats when your team is offline.

Cynet Incident Response Methodology



CyOps monitors your environment 24x7 and is always available for on-demand support.



cynet

Thank You

www.cynet.com