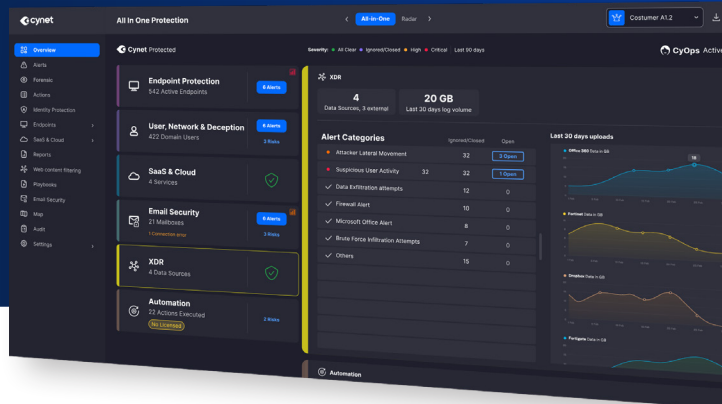


Cynet's Extended Detection & Response (XDR)

Clearer Insight. Stronger Protection. Faster Action.



Unify Your Defenses. Amplify Your Detection

Most organizations aren't losing ground because they lack security tools. They're losing ground because those tools don't talk to each other. Fragmented data creates blind spots, disconnected alerts create noise, and manual workflows create delay.

By natively unifying telemetry across more than seven data source categories into a single platform, CyAI correlates signals, maps attack paths, and triggers automated response in real time, delivering sub-5-minute detection and sub-10-minute response.



Endpoints

Seamlessly integrate with endpoint devices to collect and analyze critical data including process executions, file modifications, network connections, registry changes, and system events in real time. CyAI baselines normal endpoint behavior to detect anomalies, credential misuse, and lateral movement that signature-based tools miss.



Identity and Access Management (IAM) Systems

Monitor Active Directory and cloud identity systems for suspicious authentication events, privilege escalation, group membership changes, and administrative actions. Because identity data is processed alongside endpoint and network telemetry in a single platform, Cynet detects attack chains that span multiple domains simultaneously.



Real-Time Detection

Through continuous monitoring and real-time alerts, our platform enables organizations to detect security threats as they happen, minimizing the impact of cyber incidents on business operations.



Network Devices

Ingest data from firewalls, routers, switches, and IDS/IPS systems to enable comprehensive monitoring of network traffic, firewall logs, and lateral movement indicators. Network signals are correlated with endpoint and user telemetry natively, delivering detection accuracy that standalone NDR tools cannot match.



Advanced Correlation via CyAI

CyAI connects signals across sources simultaneously. The real-time attack path visualizations through Cynet's Attack Story feature automatically graph the root cause and lateral movement of an incident, giving analysts a complete picture in seconds rather than hours of manual investigation.



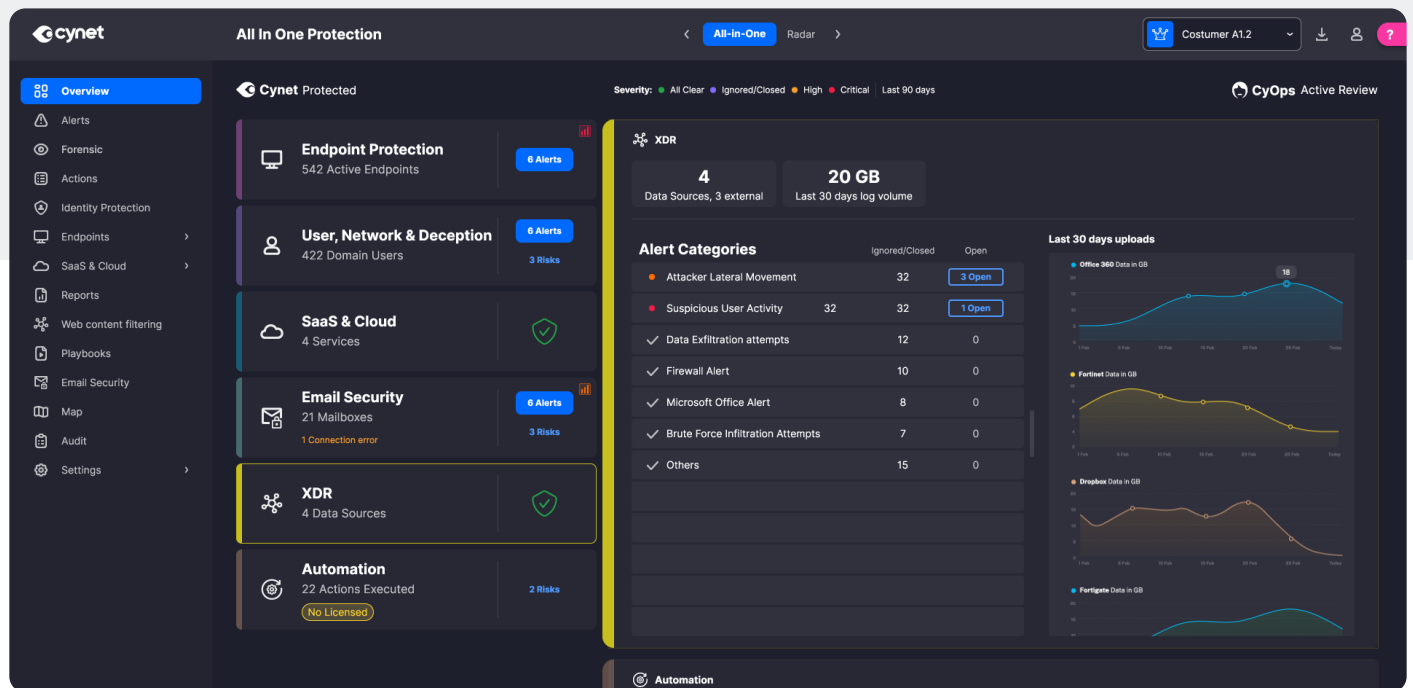
Cloud Environments

Monitor user activities, file access events, and configuration changes within cloud environments.

XDR that Proves Itself

When every second between detection and containment matters, a platform that requires manual correlation, tool switching, and analyst triage at every step is not a security solution, it's a liability. Cynet XDR was built natively unified from day one, so there is no integration debt to manage, no coverage gaps to close, and no delay between a threat appearing and CyAI acting on it.

Cynet empowers MSPs and security teams to scale and profitably deliver enterprise-grade cybersecurity with a unified, AI-powered platform covering endpoints, users, networks, identity, cloud, email and more. Backed 24x7 by CyOps MDR security experts, Cynet automates detection, response, and remediation so defenders can protect more clients, reduce overhead, and deliver stronger security outcomes with less effort.



About Cynet

Cynet's Unified, AI-Powered Cybersecurity Platform unifies a full suite of security capabilities on a single, simple solution, backed by 24x7 expert support. Cynet is purpose-built to enhance protection for small-to-medium enterprises and to maximize margins for MSPs.

Learn more at www.cynet.com