CYREBRO + SentinelOne™

Managed Endpoint Detection & Response

SentinelOne Endpoint Detection and Response

EDRs are a core component in the detection and response capability stack. A recent CYREBRO study uncovered that 78% of critical incidents derived from a lack of EDR tools to monitor endpoints. Endpoint protection is key to preventing intrusion at one of the most common entry points.

SentinelOne is a world-class EDR that delivers a robust approach to endpoint protection, according to the MITRE ATT&CK Evaluation. Through deep insight into endpoints and leveraging behavioral AI, SentinelOne rapidly stops malware and other files attack.

Benefits of a CYREBRO Managed EDR

Interactive Platform

The EDR is connected to the interactive SOC Platform where you can see investigations

Threat Intelligence

Identify susceptibilities and neutralize threats before they penetrate systems

Complete EDR Management

Management and investigation by CYREBRO's best of class SOC team that is adept not only in EDR, but all alert types

Threat Hunting

Proactive search through your endpoints, networks, and datasets

A Second Layer of Protection

Protection beyond the EDR provided by CYREBRO's custom rules

Expert Support

Around the clock support for questions and system assistance

Managed SentinelOne® EDR Solution

CYREBRO's SOC & Managed SentinelOne EDR is managed, maintained, and configured by CYREBRO, and accessible through the SOC Platform.

Your CYREBRO + SentinelOne solution includes the following:

Deliverable	Description
Threat Intelligence	Both manual and automated processes of threat intelligence covering countless sources and knowledge bases including CYREBRO's intelligence of the crowd aggregation.
24x7x365 Monitoring & Response	Real-time monitoring and active threat hunting to detect and respond to security incidents.
Forensic Investigation & Malware Analysis	In-depth analysis of security incidents to track an attack's origin and methods and identify the specific type of malware used.
Fleet Management	Easy management and monitoring of the entire fleet of endpoints, including the ability to deploy, configure, and update agents and perform remote actions to contain and remediate security incidents.
Policy Management	Configuration and enforcement of security policies across the entire fleet of endpoints, including creating and managing custom policies, assigning different policies to different groups of endpoints, and monitoring compliance in real time.
Users & Roles Management	Management and monitoring network access, including creating and managing custom roles, assigning different roles to different users, and monitoring user activity in real time.
Agent High-level Troubleshooting	Diagnosis and resolution of issues with agents, including the ability to review agent logs, troubleshoot common issues and perform remote actions to resolve issues.
Allow / Block List Management	Management and monitoring network access, including creating and managing custom allow/block lists, assigning different lists to different groups of endpoints, and monitoring compliance in real time.
Device Control	Ability to set USB rules to control which devices can access the network, including the ability to block or allow specific devices based on their type and set rules for different groups of endpoint.
Version Updates	Automatic deployment of updates and patches to all endpoints, ensuring that the organization's endpoints are always protected against the latest threats.
Support	Access to a dedicated support team that can answer any questions and provide assistance with any issues that may arise, as well as a comprehensive knowledge base and documentation.

Contact us
www.cyrebro.io
info@cyrebro.io

New York Office: 38 High Avenue. 4th Floor. Nyack, NY, 10960
Israel Office: 52 Menachem Begin street, Tel Aviv