CYREBRO + SentinelOne™

Managed Endpoint Detection & Response

B&H bgc walkme WIX monday.com DV DoubleVerify YOTPO WIND CREEK BETHLEHEM SWK TECHNOLOGIES

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. SentinelOne provides deep insight into endpoint activity through a single agent, and its comprehensive coverage of threats enables precise detection and analysis of malicious activity from endpoint devices.

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

Complete management of whitelists, blacklists, investigations, policies and more

Threat Hunting

Proactive search through your endpoints, networks, and datasets

Setup & Full Configuration

Fully guided installation and EDR configuration

Expert Support

Around the clock support for questions and system assistance

Managed SentinelOne® EDR Solutions

CYREBRO SOC + Managed SentinelOne EDR

Fully managed SOC and monitored EDR maintained and configured by CYREBRO, accessible through the SOC Platform.

This includes:

- ✓ 24 /7 Monitoring
- ✓ 24/ 7 Incident response
- ✓ I.R Monthly (up to 4 monthly hours)
- ✓ Threat intelligence
- ✓ Access to online platform
- ✓ Log types (unlimited)
- ✓ Multiply log-in sources

Managed SentinelOne EDR

Managed EDR that you access through the CYREBRO SOC Platform. This includes:

- ✓ 24 /7 Monitoring
- ✓ I.R Monthly (up to 4 monthly hours)
- ✓ Threat intelligence
- ✓ Access to online platform

FAQs:

Why is endpoint protection important?

Endpoint security is vital because end-user devices such as laptops, desktops, and mobile devices are often a landing point for an attacker looking to steal data or move laterally.

Does it replace a SIEM?

EDR and SIEM complement each other. A SIEM will consume data from EDR and feed it into an aggregated single-view of risk, acting as a centralized point of management.

Does CYREBRO setup and manage the EDR for me?

CYREBRO will guide you through installation and setup of the EDR, then will manage it entirely, from creating blacklists, running investigations, and managing policies.

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