cybereason | PRODUCT BRIEF

CYBEREASON EDR

Mitigate threats before they become breaches

KEY BENEFITS

- Understand the entire attack in seconds
- Control your environment with full visibility and integrated remediation tools
- Remediate threats with a single click
- Enhance your existing security team
- Build detection rules across Windows, macOS, Linux, Android, and iOS

Detection in seconds – Remediation in minutes

As attackers develop more sophisticated methods of attack, it's becoming harder to confidently address threats. During an incident, every second counts. Security and IT teams are often slowed down from a lack of context from alerts, excessive manual work required to investigate, limited automation, and a lengthy effort to remediate. These challenges often result in added uncertainty and outright fatigue.

Cybereason EDR consolidates all intelligence about each attack into a single visual representation called a Malop (malicious operation). Each Malop organizes the relevant attack data into an easy-to-read, interactive graphical interface, providing a complete timeline of the attack, the flow of malware across processes and users, and all incoming and outgoing communications for affected machines. Remediation actions can be automated or accomplished remotely with a click.

Respond instantly to remediate at scale

The Cybereason Defense Platform empowers analysts of all skill levels to quickly dig into the details of an attack without crafting complicated queries and easily pivot directly from investigating a Malop to remediating affected machines. With Cybereason EDR, analysts can execute a full suite of remediation actions from machine isolation and process killing to removing persistence mechanisms, all from within an intuitive point and click interface.

Hunt threats proactively

Cybereason EDR allows proactive, automated threat hunting to uncover IOCs and IOBs (indicators of compromise and behavior) hidden within the environment. Our advanced threat hunting platform turns unfiltered endpoint data into actionable intelligence and provides an intuitive user interface for syntax-free investigations, enabling L1/L2 analysts to perform like L3s - a true force multiplier.

Detect Advanced Attacks

The Cybereason Defense Platform collects data from all endpoints across all operating systems. It uses behavioral analysis and data correlation across all devices to give a complete picture of activity in your environment. The real-time correlation of data across all machines allows you to take into account the most critical information about an attack with fewer false positives. This results in detailed, correlated, and enriched data from every endpoint to reduce the potential for gaps in detection.

A full suite of remediation actions

With the Cybereason Defense Platform's remediation tools, analysts can execute a full suite of remediation actions—from machine isolation to killing processes to removing persistence - all from the console using a point-and-click interface. The Cybereason Defense Platform empowers users of every skill set to act. Analysts can pivot directly from investigating an attack to remediating all affected machines through a single click of a button, saving time and creating a more efficient workstream for your team.

About Cybereason

Cybereason is the champion for today's cyber defenders with future-ready attack protection that extends from the endpoint, to the enterprise, to everywhere. The Cybereason Defense Platform combines the industry's top-rated detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a malicious operation (Malop). The result: defenders can end cyber attacks from endpoints to everywhere.

Security for all

With Cybereason EDR, there are no special skills required. New team members can investigate and remediate without calling on senior team members, and advanced teams can leverage intuitive investigation and remediation tools to pivot from one attack to another and spend more time hunting and less time triaging. The intuitive UI of Cybereason EDR was designed to increase SOC efficiency by automating common tasks and empowering any member of the SOC to quickly understand the scope and impact of threats so that they can act immediately.

Prefered operating systems for version 20.1 of the Cybereason Platform Endpoint Sensor

WINDOWS:

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

MACOS

- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

LINUX

- CentOS 8
- CentOS 6 and 7
- Red Hat Enterprise Linux 8
- RedHat Enterprise Linux 6 and 7
- Oracle Linux 6 and 7
- Ubuntu 14 LTS and 16 LTS
- Debian 8 and 9
- Amazon Linux AMI 2017.03

ANDROID

- Android 7
- Android 8
- Android 9
- Android 10

iOS

- iOS 11
- iOS 12
- iOS 13

For a full list of supported operating systems, including older operating systems such as Windows XP, please reach out to sales@cybereason.com