cybereason

CYBEREASON EDR_

KEY BENEFITS

» Understand the entire attack in seconds

» Control your environment with full visibility and integrated remediation tools

» Respond to threats with a single click

» Enhance your existing security team

» Build detection rules across Windows, macOS, and Linux

ABOUT CYBEREASON

The Cybereason Defense Platform combines managed endpoint prevention, detection, and response in one lightweight agent. The platform leverages advanced techniques to prevent known and unknown threats. It also brings behavioral and deception techniques to prevent ransomware and fileless attacks. Combine the best platform on the market with expert implementation and support services from our security team for highly comprehensive defense against sophisticated cyber attacks.

CYBEREASON.COM/DEMO →

ASSESS IN SECONDS. ADDRESS IN MINUTES

As hackers 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 correlates the entire attack across all endpoints in your environment to give your team a single view of an attack in real time. With Cybereason EDR, your team can quickly examine an attack and respond immediately at scale. Teams can understand the scope of an attack in seconds and remediate issues and stop threats across all affected machines with a single click.

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 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.

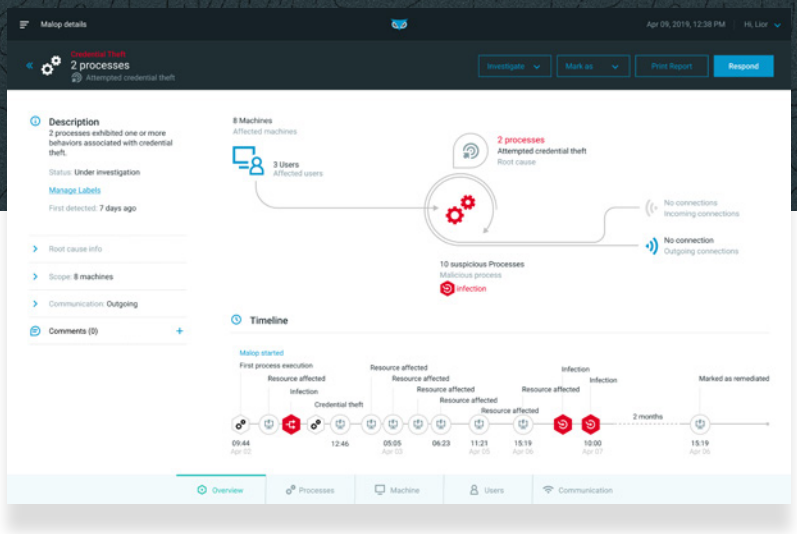
UNDERSTAND AN ATTACK IN SECONDS

Data collection is only half the battle. The Cybereason Defense Platform consolidates all relevant information for each attack into one view called a Malop (Malicious Operation). Malops facilitate a quick and intuitive understanding of malicious attacks.

In order to reduce manual investigation times and alert fatigue, each Malop organizes all relevant attack data into an easy-to-read, graphical interface. The interface gives your team a timeline of the attack, the flow of malware across processes and users, and all incoming and outgoing communications for affected machines.

Further investigation is "point and click," which eliminates the need for specialized expertise, reduces unnecessary manual work, and improves the team's ability to understand and respond to events.

SECURITY FOR EVERY ORGANIZATION_



RESPOND QUICKLY & REMEDIATE AT SCALE

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.

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. With Cybereason EDR, you can automate common tasks by setting up rules and lists. The intuitive UI was designed so that anyone could quickly understand the scope and impact of threats and immediately act as neededto increase SOC efficiency.

SUPPORTED VERSIONS

WINDOWS

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1, XP SP3
- Windows Vista Server 2003, Server 2003 R2
- Windows Vista Server 2008, Server 2008 R2

MACOS

- macOS 10.15 (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Yosemite (10.10)
- El Capitan (10.11)

LINUX

- CentOS 6 and 7
- RedHat Enterprise Linux 6 and 7
- Oracle Linux 6 and 7
- Ubuntu 14 LTS and 16 LTS
- Ubuntu 18.04
- SLES 12
- Debian 8 and 9
- Amazon Linux AMI 2017.03