cybereason

The Endpoint Sensor

Cybereason is an advanced endpoint detection and response platform. The platform collects and analyzes millions of pieces of data every second and builds an ever-evolving picture of your environment. Cybereason gathers as much information as possible to detect and analyze complex threats while being as non-intrusive as possible, minimizing impact on the network and the endpoint.

THE CYBEREASON SENSOR ADVANTAGE

The Cybereason Endpoint Sensor uses unique capabilities to **run continuously in user space and still gain deep visibility into the kernel.** Cybereason has invested years of research into operating system mechanisms to develop a unique way of getting the same visibility into attacks as kernel level drivers. This minimizes the likelihood of impacting the user, but still allows access to the data needed to detect malicious activities.

- **No "blue screens"** The sensor runs in user mode, and cannot conflict with other software or OS operations. The sensor requires less integration testing before roll-out and system updates.
- **Uses no more than 5% of memory** The sensor also incorporates features to ensure that it does not consume a significant proportion of endpoint resources.
- **Does not interfere with user tasks** The sensor includes controls to de-prioritize sensor activity to ensure that it does not slow down tasks being executed by the user.

UNIQUE FEATURES OF THE ENDPOINT SENSORS

Runs in user space: Eliminates the risk of crashing the endpoint

Low overhead: Network traffic < 10MB per day, an average CPU load of 2-3% and 50MB of RAM

Supports entire response lifecycle: Execution prevention, network isolation, automated remediation of detected threats

PROPRIETARY COMMUNICATION PROTOCOL FOR ACTIVITY MONITORING

Getting true visibility into endpoint activity means gathering tens of thousands of endpoint events every day. In an environment with many thousands of endpoints this can create significant network overhead if not done properly. The same is true for an endpoint in a remote location where bandwidth may be limited.

- ✔ **Efficiently transmits endpoint data in real time** Cybereason has devised a proprietary, binary protocol to transmit this information as efficiently as possible. This protocol is designed to express changes in system state using as little data as possible, avoiding spikes in traffic while minimizing the impact on network performance.

- ✔ **Collects raw information on demand** When an incident occurs, responders can also use Cybereason to acquire raw file and memory data on demand. This allows malware and forensics analysts to understand the root cause of the incident and understand more about the attacker.

The net result is that the **Cybereason Endpoint Sensor causes network overhead of less than 10MB per day, an average CPU load of 2-3% and 50MB of RAM**. Even with this low overhead the system collects a large amount of data. Examples of this include:

- Process information, including parent/child processes, memory usage, network connections, start/end time
- Connections information, including local and remote IP address and port protocol, transmitted or received bytes, start/end time
- File information, including file attributes, versions, reputation information and file hash
- Auto-run and scheduled talk information, including registry and configuration information
- User information, including username, domain, password age and privileges

The Cybereason Endpoint Sensor collects system-level data that allows us to understand behaviors and detect malicious activities. The Sensors do not collect actual file content, network packet information or any user-sensitive information, unless otherwise instructed.

DISRUPTING ATTACKS: REMEDIATION, ISOLATION AND PREVENTION

In addition to threat detection, the Cybereason Endpoint Sensor automatically disrupts attacks through:

- **Network isolation of compromised machines** Cybereason can disrupt attacks and contain threats by preventing compromised machines from any network communication, restricting access to only your analysts for situations when a deeper examination is required.
- **Automatic remediation of detected threats** When Cybereason detects a threat, it can automate remediation activities like killing processes, quarantining files and deleting registry keys.
- **Behavioral ransomware detection and shutdown** Cybereason also examines file and network activity to watch for indications of ransomware attempting to perform the mass encryption of users' files. Cybereason also incorporates deception techniques to bait ransomware into attempting to damage worthless files, triggering our detection and prevention mechanisms, which prevent the ransomware from impacting the user.
- **Optional kernel level driver for prevention** Cybereason incorporates an optional kernel level driver that recognizes malware and can prevent it from executing. This adds a layer of protection that prevents attacks from propagating through the environment.

ENDPOINT MINIMUM REQUIREMENTS

CPU	Dual core 2Ghz core i3 and above
RAM	1 GB
Storage	100 MB
Operating System	Microsoft Windows XP SP3 and later
	OS X Maverick (version 10.9) and later
	Red Hat Enterprise Linux 6.5 and later, CentOS 7 and later
Network Connectivity	An IP-compatible network device

THE CYBEREASON DIFFERENCE

Cybereason is a company of elite former military cybersecurity experts with deep experience in cyber-offense operations. Cybereason's specialists have spent years understanding the adversary and how they operate, and have defended and analyzed some of the most advanced cyber-attacks ever executed.

Visit www.cybereason.com
and schedule a demonstration.

cybereason