CYBERHAVEN

ENDPOINT SENSOR

OVERVIEW

Through the use of a lightweight endpoint sensor, Cyberhaven provides unified visibility and protection of unstructured data across endpoints, network shares, and SaaS applications. Additionally, Cyberhaven provides deep SaaS application support via API integration into Microsoft 365, G Suite, Box, and Salesforce.

Cyberhaven sensors track all data origins and paths and transform every user data action into an auditable event, automatically building a dataset to provide a contextual history and digital chain of custody.

Cyberhaven delivers forensic-class attestation of your company's data journey while minimizing endpoint impact and maximizing user productivity.

OS Support: Windows, macOS, and Virtual Desktop Infrastructure.

User space architecture

Unlike other endpoint agents, Cyberhaven sensors are designed to run in user space on both Mac and Windows. This approach allows Cyberhaven to a) see processes as the user sees them (e.g., we see data before it gets encrypted) and b) avoid problems caused by applications running in the kernel, such as machine and application crashes and tricky incompatibility issues.

Event collection and stitching

Sensors capture and analyze granular data activity from hundreds of thousands of logs and application events to track files across all data silos and processes — network share to endpoint, endpoint to cloud through VPN. The Cyberhaven cloud service analyzes and connects events in our scalable graph database, then uses data science to stitch files and events back together without tagging, modifying documents, or comparing hashes.

What events are captured?

Upload and download, open and create, modify and delete, move and copy, and emailing of documents and files.

Ingress of documents, files, and emails into the enterprise.

Sending of emails and attachments to domains inside the enterprise and to external domains.

Transformation of data by converting it to other formats, by splitting, merging, archiving, or encrypting it, or by obfuscating it using steganography tools.

Cutting and pasting of content snippets between emails, files, documents, and instant messages.

Export of data and reports from databases and applications.

Uploading of documents and files to external websites and copying to removable media on servers and endpoints.

What information is captured?

Cyberhaven does not store files or file content, only metadata about:

- **file size and hash**
- **file system path and hostname**
- **application path, command line, name**
- **browser URL, domain**
- **user (Access Directory username, group membership, SID list)**
- **software installed on endpoint**
- **hardware connected to endpoint**
- **users connected to endpoint**

Additional telemetry is sent to the Cyberhaven backend from the endpoint that includes software version and performance measurements of the agents.

Where is this captured from?

- **application events and accessibility logs**
- **network domain registrar of shares**
- **agent polls group membership**
- **conditional group membership checking from the endpoint**
- **poll local AD from the endpoint — analyze token to see current groups**
- **system resolves network**

What's not captured?

Cyberhaven is noninvasive and privacy-friendly:

No keystroke capture

No message monitoring

No website monitoring

No screen recording

No webcam recording

How is content inspection performed?

Cyberhaven can perform content inspection and "discover" documents, files, emails, and other objects that contain names, account and customer numbers, insurance codes, and many other types of personal information, as well as patterns specified by each enterprise. The discovery process is automated and completely transparent to end users.

Content inspection is performed server-side and only scans for content when a file is moved out of the company (browser, email, or USB), avoiding slowdown or resource consumption on the endpoint. The file is sent once for analysis, the system stores relevant metadata attributes, and then it forensically purges the file and its contents. The next time content inspection is needed, the sensor (endpoint or API) sends a hash of the file and checks if we have cached results for that content.

Content is continually tracked using OS and application logs even if files are renamed, copied, or zipped, or content is copy/pasted into other apps and documents.

Performance

Cyberhaven data tracking is asynchronous, only processing events as they happen, and performs content scanning on a file once. It only stores metadata, making the entire process extremely efficient and causing no user experience issues while maintaining low performance requirements — typically less than 0.1% of CPU capacity.

Management

Cyberhaven's agent is designed with ease of use in mind. Deployment is via automated endpoint solutions (SCCM, JAMF, etc), agent health monitoring, and self-managed updates.