actifile
Data Security Made Simple

Cogent Data - Guiding Qualitative Digital Forensics

Summary

Actifile Data Security Platform can complement other Incident Response (IR) tools that provide digital forensics, and potentially help simplify the efforts needed to complete a digital forensics process. Actifile offers a way to supplement existing digital forensics tools, by preemptively securing sensitive and private data, so in the case of a data breach the attack surface for a criminal is much smaller.

Background

Digital evidence is used proactively and as part of the IR process, to detect that an event (breach, misuse of data, etc.) occurred, identify the root cause and internal/external actors, eradicate the threat, and mitigate future events, and provide evidence for legal teams and law enforcement authorities.

To enable digital forensics, organizations must centrally manage logs and other digital evidence, ensure they retain it for the appropriate duration, and protect event data from unlawful tampering, malicious access, or accidental loss.

Digital evidence can be used as supporting testimony in investigative and legal proceedings for several use cases, and Actifile can help with the data lifecycle, theft, and network events (breaches, misuse, etc.), assisting with the remediation of data security and privacy compliance risks. More specifically, it can help with computer-based forensics, where digital data needs to be examined for chain of custody and chain of events.

Actifile Value

Actifile Data Security Platform (DSP) has two components: Microsoft Azure based management portal (multi-tenant, centrally managed) and an agent deployed on endpoints, including Windows, MacOS and in Q2/2023 Linux. Actifile DSP is a unique solution that will identify and optionally automatically and transparently encrypt sensitive data across endpoints, file servers and cloud file repositories, all in real time.

At its core, Actifile focuses on data attributes with no reliance on events. A key capability of the Endpoint (EP) agent is application and user data behavior monitoring and tracking: The ability to capture the data lifecycle for all classifications (sensitive, personal, compliance, etc.) along with any associated application that executed the data action and the user and or device initiated the action. All the actions are captured in a comprehensive cloud-based audit log and can be analyzed at any given time.

Following deployment of the Actifile agent, immediate collection of data-behavioral meta data is stored in our schema for analysis via the management portal or loading into another central data analysis database. The forensic team analysis for proactive and reactive data analysis and contextualization prior or following an event becomes much simpler: Increased insights and productivity, eliminates the need to analyze system and application logs, trying to piece together the actual or hypothesized event lifecycle , Actifile provides:

-

- Mapping of all the lifecycle traits for all data types in an organization, including what the monetary data risk was as any given moment.
- What applications and users & devices (that initiated the operation) interacted with the data. To increase resource productivity, no integration is required for current or future applications, locally installed, cloud and SaaS apps, 3rd party portals, etc.
- Central repository, easily queried and well-integrated with other tools, of all data related events
- Do you have an API that can be used to supply or query data in your database?

All the above is accomplished with analysis performed only on the client side, with no file transfer to the cloud for analysis.

An additional client benefit is the value provided by Actifile to preemptively encrypt sensitive files per their data risk and avoid any external or internal threat to them by bad actors, in advance.