cybrilliance

Empower Your Business with Cyber Resilience

Forensic Auditing

Actifile stands as a cutting-edge data security platform, designed to assist forensic auditors and investigators. It effectively diminishes the time and resources necessary for comprehensive analysis during data incidents within organizations.

Reveal the hidden

The Actifile tool facilitates the discovery of sensitive and private data, providing insights into data usage patterns within the organization.

Remarkably, Actifile can be utilized both proactively, prior to any incident, and re-actively, following an unanticipated event.

Actifile provides critical functions for auditors and forensic investigators:

- **Discovery:** Actifile aids in locating and cataloging data within files. It can discover sensitive data types (such as Personally Identifiable Information (PII), credit card data (PCI), etc.) and can be customized to search for any specific data type. The tool provides a record count for each type of data found within each file.
- **Monitoring:** Actifile observes data file usage patterns, tracking data entry and exit, user interactions with local and web-based applications, and identifying which applications are used in conjunction with sensitive data.
- **Sensitive data** - being used on a device with applications deemed as shadow-IT are fully discoverable.
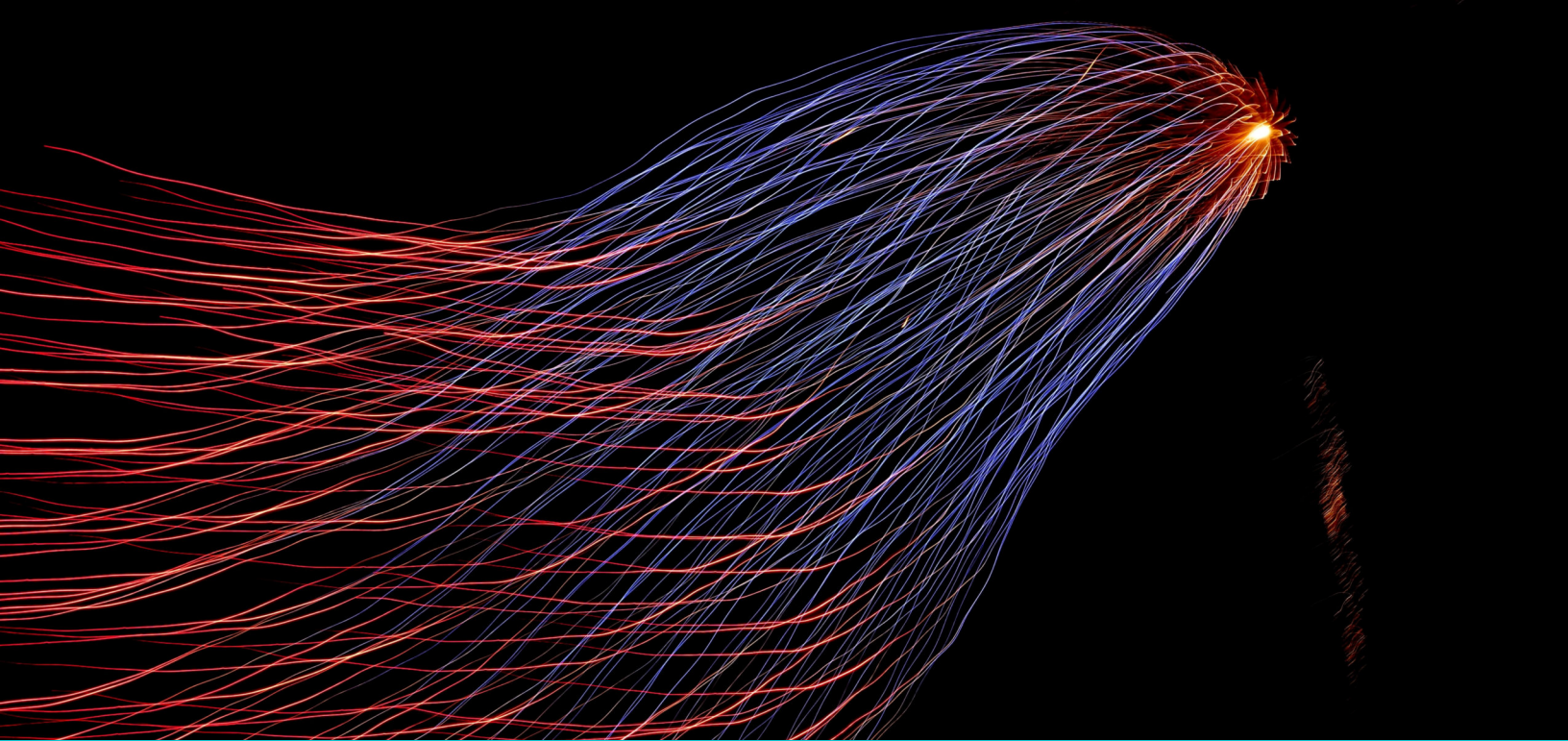
Summarizing Data Risk

actifile

Deploying Actifile agents to all devices, or selectively to affected devices, is a straightforward process. They immediately commence scanning for PII or other sensitive data, with the discovery phase duration varying from minutes to hours depending on data volume. The progress of this phase can be tracked from the Installed Devices page.

Device Risk

Search

Device Name	User Name	Online	State	Risk Valuation	Files	Sensitive files	Shared Services	Outbound
\	SURFACE8-2TB\assaf	Offline	Active	$6,048,670	58576	47719		0
liat folder	SURFACE8-2TB\assaf	Offline	Active	$5,748,120	41214	31417		0
SURFACE8-2TB	SURFACE8-2TB\assaf	Online	Active	$3,707,803	8543	8040		1782
SURFACE8-2TB	SURFACE8-2TB\assaf	Offline	Active	$3,588,619	2962	2651		2043
ASSAF-DESKTOP	ASSAF-DESKTOP\yonat	Online	Active	$3,137,982	83885	77600		3282
SURFACE8	SURFACE8\assaf	Offline	Active	$632,560	1140	862		669

Identifying Sensitive Files per Device

Actifile presents a comprehensive summary of data per device, type of data, potential liability, and other crucial parameters, along with a full file list.

Device Name: **SURFACE8-2TB**

Status: Active
Last Activity Date: 08 Jun 2023 01:06 PM
Version: 2.0.98.0

Organization Unit: Assaf Litai
User: SURFACE8-2TB\assaf
Data Size: 11.60 GB

Actifile Data monitoring tools:
Activities Files Folders

Actifile Agent settings:
Enable Discovery   ON
Enable Data In Use Monitoring   ON
Enable Encryption   ON

Sensitive Files

Classification	Files	Records	Risk in USD	Encrypted Risk in USD	Countries	Regulation
US - Electronic Funds Transfer and Wire Information	27	1146839	$ 2,293,678	$ 2,293,428	United States of America	PII
US - SSN (hi-sensitivity)(New)	46	120078	$ 1,200,780	$ 1,200,710	United States of America	PII
Python Code	5090	5090	$ 101,800	$ 0		
All Office Documents	2635	2635	$ 52,700	$ 1,820		
Credit Card - American Express	5	111	$ 11,100	$ 0		PCI
CMMC - CUI	29	374	$ 7,480	$ 7,480	United States of America	
CMMC - FCI	40	332	$ 6,640	$ 6,640	United States of America	CMMC
CMMC - CUI (NOFORN)	11	208	$ 4,160	$ 4,160	United States of America	
CMMC - CUI (NOFORN)_Copy	11	208	$ 4,160	$ 4,160	United States of America	CMMC

Data and Application Risk per Device

The Actifile agent also supervises data usage on devices, revealing which user is accessing what data through which application. This feature can be particularly

useful if Actifile is in place prior to a data breach incident. However, given that most users tend to stick with their preferred applications and portals, they are likely to continue their patterns even post-breach. Hence, understanding user behaviors is simply a matter of deploying the agents and reviewing the dashboards over a week.

Conclusion

The Actifile Data Security Platform aids forensic analysts in focusing on devices containing significant data volumes and applications known to have vulnerabilities yet are still in use for data access within the organization.

The benefits Actifile brings to a forensic auditor or analyst during a data breach analysis include:

1. **Identifying the types of data present within the organization.**
2. **Revealing which devices store this data and in what volume.**
3. **Highlighting which applications are utilized in conjunction with the data.**
4. **Detailing how the breach occurred and whether the file was encrypted (If pre-installed before a breach).**

cybrilliance

Actifile

Data Security Platform

Actifile is different to legacy DLP systems that are based on an event-driven approach and require extensive ongoing rules management built for LAN perimeters.

Actifile is based on analyzing data risks, and applying preemptive encryption that handles both external threats and insider carelessness, all in the world of no security perimeters.

Data Discovery

Actifile discovery is an autonomous data guard that works like a silent watchdog. It constantly patrols your IT ecosystem, protecting against both internal and external threats. Sensitive data detection and automated data mapping operate 24/7.

Actifile automated data mapping locates sensitive data across all of your systems. You can see at a glance where all active and dormant data is located, exactly who has access to it, and the potential financial penalties for any leakage.

Forensics

Actifle's data lifecycle mapping provides full forensic analysis capability in the event of an incident and/or audit.

Data Encryption

The Actifile data encryption solution begins with a comprehensive data risk evaluation. Your data is located and
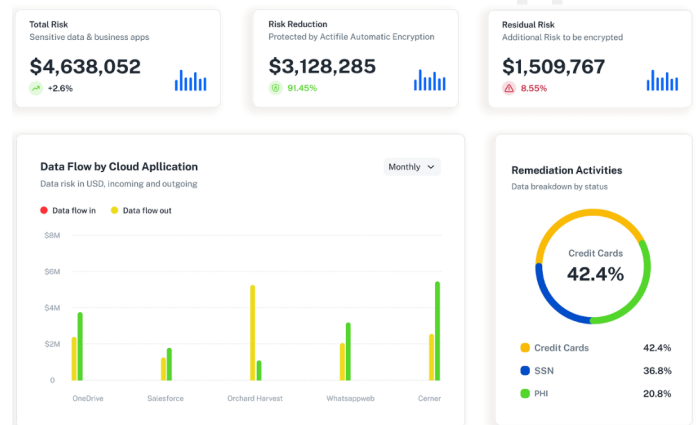
mapped and the fiscal penalties for data breaches are calculated in US dollars.

1-click encryption gives a choice of full immediate encryption or delayed encryption. File-level encryption is fully automated.

Actifile's preemptive data encryption delivers a level of protection that simply can't be matched by any event-driven data encryption solution.

Supported Platforms.
Windows, Linux, Unix and Mac

cybrilliance

Empower Your Business with Cyber Resilience

CyBrilliance is Cyber Resilience

For more information visit: https://www.cybrilliance.com

Contact@CyBrilliance.com

CyBrilliance HQ

Burlington,
Ontario,
L7L 4C4.
Canada.

CyBrilliance EMEA

Covent Garden,
London,
WC2H 9JQ.
United Kingdom.

CyBrilliance Asia

Ulsoor,
Bangalore,
560008.
India.