



Data Security Platform

Product Q&A

info@actifile.com

www.actifile.com

Mar 2024



There are lots of features, but I'd like to focus on the following statement. Please let us know if I am incorrect. Summary:

We will be able to create policies to encrypt data automatically on Desktops, Servers, and Microsoft (SharePoint, OneDrive, Teams) to prevent sensitive information from “getting out into the wild” via data exfiltration or the inadvertent sharing of information.

Answer:

- Clarifying question: If a file is on a user's computer, and it is encrypted via an Actifile policy, and they email that file outside the organization, it will stay encrypted?

Answer: Yes. it will stay encrypted per our file level encryption

- If they do need to “unencrypt” the file to upload into a “web portal”. We have a specific use case where a Healthcare customer has to upload PDFs and Word Docs to a partner organization for “authorizations”.?

Answer: Yes, we have several ways to share encrypted files with external partners, and one of them is the above scenario.

- Clarifying question: If a file is on a user's computer, and it is encrypted via an Actifile policy, and they email that file *INSIDE* the organization, if the employee has access/permissions, will they be able to view the contents of the file?

Answer: Yes, using our transparent decryption, anyone who has Actifile on their machine can open encrypted files seamlessly (no user, password needed and w/o any latency)

- If not, will the EU be able to do something to enable that? We are not saying this is the proper way to do it, but I know we will be asked.

Answer: No need to as stated above.

Exfiltrated Data: Will Actifile show the same level of logging on file data that doesn't have a “policy applied”. Let's say that we have a marketing file share, and we don't want to encrypt the data on there. Assume we are hacked, and encrypted and non-encrypted Marketing Data is stolen. Will the logging identify the exfiltration of the encrypted as well as the non-encrypted data?

Answer: Files do not need to be encrypted in order for Actifile to log their activities. Actifile can log activities based on one of the file classifications: content (aka PII), file type (any type), or location (Folder). If you want to track and audit certain files, they must belong to a classification, for instance, a certain content of the file (that identifies it as marketing content) or certain file type.



would probably charge 8-10 hours as there would be client interviews (we create a worksheet for customers to fill out to guide our onboarding), a little PM, create the tenant, package the app, roll out, audit, and set a follow up meeting with the customer to do a proof of value review. Does that “2 hours” also include the configuration and integration with Office365/Azure?

Answer: The 2 hours refer to only the limited initial deployment phase. Your plan to charge 8 -10 hours for the broader scope of what we can “Data Risk Assessment” makes sense, and includes the items you included, ending in a meeting with the customer in which you explain their data risks and the potential remediation paths. We call it Data Risk Assessment, because it actually provides a details at rest and in motion analysis of their landscape, and not just the POV. This can be repeated on a monthly or over QBR, to enrich your meeting with the changes that happened over time in the data risks, alerts that crossed the threshold and how the Managed Encryption helped with external and internal threats.

Licensing and Site questions:

- Can you run the Data Risk Assessment and Managed Encryption on the same site? Use Case example: a client has a bunch of computer Kiosks, and there is almost zero risk to having corporate sensitive data on those systems. Can you run the Managed Encryption on 80% of the devices, and the Data Risk Assessment on the remaining 20%?

Answer: Yes you can from a licensing perspective, but keep in mind that if the Managed Encryption is on in that organization, the Kiosks stations will not be able to open up encrypted files. That is of course also an advantage, as it might be what you are looking for to happen at the Kiosks.

- Take the above example a bit further: You have 40 office workers and 60 computers on a manufacturing floor. The client wants the Managed Encryption on the 40 office PCs but doesn’t want anything on the 60 PCs on the floor. Obviously, they miss out on the core offering, but I’d like to make sure there aren’t any big gotchas.

Answer: See the answer above. The 60 PCs on the floor will not be able to open encrypted files with our Managed Encryption, as they are not licensed for it.

For the \$195 per month:

- That looks to be our base and it includes 100 NFR Data Risk Assessment licenses, correct?

Answer: It includes an NFR (for internal usage at your MSP), 100 Data Risk Assessment licenses for use at your customers, and the setup of your partner portal.

- Does it include any “Managed Encryption” Licenses to use either internally or for demo?

Answer: The base package NFR (for MSP internal usage only) includes both the Data Risk Assessment and Managed Encryption. The NFR is not licensed for demo purposes at customers.



Answer: In addition. The Data Risk Assessment is the base (Tier 1) license and the Managed Encryption is on top of that.

- Do you have pricing recommendations? We generally like to look at 40-60% GP depending on how much overhead the product takes.

License Management:

- How are we billed, for the number of active agents (both user PCs, and Servers)?

Answer: Yes, on top of the base package.

- How is it billed for Office365? There could be 40 agents installed, but 100 Office365 users (4.b. example above).
- How are agents decommissioned?

Answer: Through an Actifile procedure in the Partner Portal. More details here <https://support.actifile.com/docs/deactivating-and-activating-actifile-at-a-client-site/>

- Do we have to manually remove?

Answer: No, there is a procedure you can use from the Partner Portal.

- Or is there a policy, i.e. if it is offline for 30 days or more, the user is removed, and the license is freed up?

Answer: There is no automated procedure like that as of now, but we can definitely add it to the roadmap.

- If we onboard a customer with 100 seats, and they leave us, are we able to “go down” in usage, i.e. 400 one month and 300 the following?

Answer: Yes.