Unlocking Cyber Resilience With Actifile's Revolutionary Approach

Product Overview:

Actifile is a complete data security solution that is built to defend client data in today's cloud-based work environment. The post pandemic work force is highly mobile and spread out, giving more exposure to company networks and valuable data.

Traditional encryption tools protect the physical drive but do little to protect against ransomware and cyber-attack. In the event of a cyber-attack, a hacker would still be able to download data from an infected device. Actifile will ensure that if that data is lost, it is encrypted and useless to a hacker. Instead of blocking each option to exfiltrate sensitive files through any type of application, applying automatic encryption secures the file, and in the event of the file being stolen or leaked – it will not open without Actifile Sentry and the organization's decryption key.

The Actifile Sentry immediately starts scanning for sensitive data at rest, according to pre-templatized or customized patterns. Additionally, the Sentry tracks the flow of data throughout as well as in and out of the organization, without the need to integrate to any application. The Sentry then calculates the data risk in real-time, assigning each type of sensitive data risk in monetary value.

Actifile offers 3 levels of protection:

- Assessment-based on defined privacy regulations and PII definitions, Actifile will scan for sensitive data and will use an algorithm that multiplies every record by its total damage to assign a monetary value.
- Monitoring and Auditing-tracks and audits data-risk in real-time by continually monitoring incoming and outgoing sensitive data flows from and to the perimeter-less organization. Actifile will also locate and map sensitive data across all systems, devices and cloud.
- Remediation and Encryption-Automatically secure sensitive data across all endpoints, apps, 3rd party portals, and shadow IT.

While most cyber solutions are designed to protect an organization from an attack, Actifile will protect the organization when an attack occurs by encrypting data and logging which records have been compromised.

Contact:

The contact for cyber-security will be the decision maker for the organization. Cyber protection should be included in your proposal with your network solutions. Depending on the industry, there may be specific compliance officers that need to be involved as well.

Key Cyber Security Issues:

- Understand what are the key data points that need to be protected.

  - Employee records
  - Healthcare data
  - Customer data
  - Intellectual property

- Most MSPs and MSSPs inspect their customer's network for vulnerabilities but tend to overlook the data.

- Many industries have compliance rules and regulations that businesses must follow to protect employee, patient, and customer data.

- It is common for businesses to have specific requirements of their network that may be put in place by a vendor or customer. For example:

  - Government contractors and subcontractors
  - Certain auto manufacturers require dealers to comply with their network specifications.

General Approach:

- The first step in selling cyber security is to educate your customer on the realities of cyber-attack.

  - % of small businesses that are attacked
    - 95% of attacks are a result of human error.
    - % of businesses that go out of business after an attack

  - Ramifications of an attack
    - Recovery time
    - Downtime
    - Compliance issues and fines
    - Insurance and investigations

  - You must make the customer understand the value of their data and the risk to them if that data is compromised. In other words, they need to feel the pain.

  - Tip-Ask reflective questions such as
    - What would happen to your business if this data was stolen?

- Most successful MSSPs sell Actifile by starting with the Assessment Tool.
  - Run a scan of your client's devices and give them the monetary value of their data.

- Focus on Data Security as an add on service to your existing cyber security solution stack.

- Use real world data and specific examples of businesses that have suffered attack.

- Cyber security solutions should be a mandatory part of the service you provide. It should be included with every proposal you create.
  - If you allow your customers to opt out of cyber security solutions, you should have them sign a form acknowledging they have been educated on the risk involved and are absolving you of liability.

Common Objections/Questions:

- "Why should I spend money on cyber security, isn't that what I pay you to do?"

  - That is a great question, and my job is to protect your network and data. The service that I provide for you includes assessment and monitoring, as well as these necessary cyber security tools. I include comprehensive training and robust network equipment, however 95% of cyber-attacks are a result of human error. Tools, such as Actifile, will protect your organization from user errors such as opening infected files.

- "Why do I need Actifile, I already use 'encryption tool'."

  - Actifile is a powerful and easy to use encryption tool. Actifile offers preemptive encryption vs event driven encryption.

- "Do I need Actifile if I already use and XDR?"

  - Yes, Actifile will offer an additional layer of protection against cyberattack. An XDR monitors traffic on endpoints and is intended to prevent entry to the network. Actifile offers a unique solution that ensures that if/when a breach occurs, your customer's valuable data will be protected.

  - In addition, Actifile will keep audit logs to know exactly what data was exposed and show if it was encrypted.