Visit us to learn more: www.indexengines.com/cybersense

CyberSense®
Powered by Index Engines

10 Questions to Ask About Cyber Resiliency

Question to Ask	Why it's Important	The CyberSense Approach
Question 1 Are the corruption detection methods based on full-content analysis of ALL data?	If cyber resiliency tools fail to conduct thorough forensic analysis by inspecting the content of ALL files, databases, and core infrastructure, hidden corruption can easily remain undetected.	CyberSense scans the data in files, databases, and backup files in a single pass. By offering this level of insight into data integrity, CyberSense can detect more advanced ransomware variants that bypass metadata-level, threshold and entropy changes.
Question 2 When ransomware partially encrypts inside a database page, is this detected? Can you report on the individual pages that were impacted?	Most solutions do not check the integrity of databases for corruption. Some claim to check databases, but are not checking the content, only the container.	CyberSense ensures the integrity of databases by conducting a thorough validation of both the database and individual page structures. CyberSense scrutinizes these structures for any signs of suspicious activity, such as encryption or corruption.
Question 3 If an attack does not change file-level metadata, does not significantly change entropy (partial encryption) and avoids exceeding thresholds, will the corruption be detected? How?	Modern variants are designed to conceal their tracks effectively. They may avoid altering metadata properties to evade detection by metadata analysis tools or employ slow corruption techniques to bypass threshold analysis tools.	CyberSense uses ML and over 200 content-based analytics, empowering it to detect a wide range of malicious changes in data. These analytics identify even subtle alterations that may indicate a ransomware attack or data corruption.
Question 4 Entropy is a common approach used by vendors to check for signs of corruption. At what level is the entropy being measured: backup image or file content?"	Significant changes in file entropy can indicate encryption of the file's contents. However, it is important to note that some vendors claim to use entropy but instead measure the compression rate of the backup.	CyberSense calculates entropy at the file level and analyzes how entropy changes across all the files within a backup. This analysis, combined with numerous other content-based statistics, allows CyberSense to adopt a highly precise approach.
Question 5 Do your algorithms detect partial encryption technologies that minimize or avoid significant entropy changes?	New variants including LockFile and BianLian employ encryption algorithms that partially corrupt files, enough to make them unavailable but not enough to trigger an increase in entropy. Relying on significant entropy changes is not enough.	CyberSense successfully detects partial encryption or encryption methods that do not alter entropy significantly. This is accomplished by looking beyond just entropy and inspecting the content to uncover this hidden corruption.

CyberSense®
Powered by Index Engines

10 Questions to Ask About Cyber Resiliency

Question to Ask	Why it's Important	The CyberSense Approach
Question 6 How does the solution differentiate between user-based & malware activity? For example, if a user adds thousands of files to a compressed zip folder, vs ransomware that encrypts thousands of files?	This example where files are encrypted by a user will trigger a high change in entropy which may trigger an alert based on lower backup compression or exceed file change threshold rates. This results in a false positive and waste of resources.	While the addition of many encrypted files will be detected by CyberSense, it is not flagged as an alert since this behavior alone is not indicative of typical cyber corruption. CyberSense's approach minimizes false positives and false negatives.
Question 7 Do they use machine learning (ML) to detect signs of ransomware corruption? If so, how are they training and updating the ML models? If not, why are you considering them?	Bad actors in the cybersecurity landscape are constantly evolving their methods of corrupting data, making it critical for organizations to stay updated and adaptive in their approach to maintaining cyber resiliency.	CyberSense trains its ML on over 6,500 variants, adding an average of 80 new viruses a month. CyberSense employs various sources, including platforms like virustotal.com, to identify new ransomware variants and observe how ransomware changes data. No signature needed.
Question 8 Are the data corruption detection processes done on-premises or does it rely on data being sent to the cloud?	More advanced content-based corruption detection tools require more resources than what is available on premise. As a result, they are required to send data, including sensitive files, to a common cloud platform to be analyzed.	CyberSense is a self-contained application designed to run on-premises. It provides users with the flexibility to deploy and manage the solution within their own infrastructure. However, there is a version of CyberSense that can be deployed in the cloud.
Question 9 What are the limits of the detection capabilities? Can ransomware corruption be detected on data/backups, unstructured files, virtual images, databases, critical infrastructure, Active Directory, DNS servers?	Bad actors do not want organizations to recover quickly. They will corrupt all classes of data to accomplish this goal. If your cyber resiliency strategy does not support all classes of data and infrastructure you will be left vulnerable.	CyberSense stands out as the only solution that delivers comprehensive analysis of all data at a full-content level including backup files, virtual images, user files, databases, and core infrastructure components.
Question 10 Is the workflow automated? Or does it require scripts, API calls or other manual processes?	Organizations do not have the resources to manage systems using manual processes. Running these processes every day becomes prone to neglect and error. Automated systems are critical to maintain accuracy and reliability.	CyberSense is integrated into the workflow and provides fully automated validation of data integrity. No additional scripts or APIs need to be managed by the user in order to access all the product features.