Enterprise Strategy Group

SHOWCASE

OCTOBER 2025

Busting the Database Security Myth With Index Engines CyberSense

Database Integrity Validation Is Key to Database Resiliency

Stephen Catanzano, Senior Analyst

Abstract: For decades, databases have been the beating heart of enterprise IT. From financial transactions to healthcare records, they contain the mission-critical data that organizations rely on every second of every day. As cyberthreats grow more advanced, databases are increasingly targeted, but often overlooked, in resiliency strategies. Many leaders assume their databases are fully protected because backups exist or because surface-level scans show no anomalies. Yet this confidence is misplaced. Modern AI-driven attacks can silently corrupt individual database pages, indexes, or transaction logs, leaving organizations exposed while giving the illusion of security.

Recent Enterprise Strategy Group research highlighted the challenge, showing that 49% of organizations cited data security as one of their most significant database management-related concerns,[1] yet organizations often rely on surface-level protection that misses subtle, slow-moving threats. The result is a dangerous myth of database safety. Index Engines' CyberSense platform applies AI-driven full-content indexing to detect database integrity challenges that others miss.

49% of organizations cited data security as one of their most significant challenges in terms of managing and securing their database systems.

Databases in the Crosshairs of Modern Attacks

Databases have always been high-value assets. They house the structured data that powers critical applications, drives customer experiences, and supports real-time decision-making. But as ransomware and AI-driven attacks evolve, they have become a prime target. Unlike file shares or endpoints, database corruption is especially dangerous because even small changes at the table or index level can cascade into application failures, reporting errors, or compliance gaps. Even partial compromise can erode trust in data integrity, disrupt operations, and create long-term exposure.

74% of organizations cited that database technology is evolving faster than their ability to implement new innovations.

According to Enterprise Strategy Group research, 74% of organizations cited that database technology is evolving faster than their ability to implement new innovations, highlighting how organizations often lag behind sophisticated database attackers. Database administrators (DBAs) and IT infrastructure leaders frequently assume that existing tools, such as backup software, storage snapshots, or metadata-based anomaly

[1] Source: Enterprise Strategy Group Research Report, *Rethinking Database Requirements in the Age of AI*, February 2025. All Enterprise Strategy Group research references in this Showcase are from this report unless otherwise noted.

detection, provide sufficient protection. Unfortunately, these measures typically operate at too high a level, failing to spot page-level changes, such as altered allocation maps, damaged B-trees, or partial record encryption, that modern ransomware introduces. Cyberattackers understand the high leverage of disrupting structured data. Databases require specialized protection.

The Myth of Database Security

A common belief in IT organizations is that databases are inherently protected simply because they are backed up or monitored for availability and that databases and the data within them are not targets. Vendors claim that databases fall under broader cyber-resilience frameworks, which reinforces this myth. In reality, most solutions only check metadata or high-level file system indicators. They miss corruption within the content itself, particularly when ransomware encrypts portions of a database without taking it offline.

Other misconceptions compound the risks. For example, some believe that encrypted databases cannot be protected. In practice, CyberSense can distinguish between legitimate application-based encryption and malicious encryption. Others assume that hardware encryption blocks content-level inspection. In reality, hardware-encrypted storage decrypts on read operations, which still allows CyberSense to analyze the data.

Metadata-only inspection is insufficient, as it fails to spot page-level changes that cause inconsistency within the page allocation maps. Assuming database immunity creates hidden risks. Real-world scenarios such as slow query performance, isolated account issues, or partial transaction corruption illustrate how attacks can remain undetected for months. Database security is not binary; it requires going deeper than surface-level checks. A new trend began in 2025 in which ransomware began corrupted or introducing erroneous data into databases rather than encrypting the data, causing disruption and trust issues. Many Index Engines competitors don't validate the integrity of database files, and the ones that do only validated metadata or a high-level sampling of a very small number of rows, such as 1% or the first 1,000, and make assumptions from there.

The Reality of Modern Attacks on Databases

AI-driven attacks have become increasingly sophisticated. Attackers recognize that disrupting databases delivers maximum leverage, yet full encryption of an entire database is rarely necessary. Instead, intermittent or partial encryption can achieve the same goal of creating uncertainty and distrust in the integrity of data. A single corrupted table foreign key relationship or authentication record can ripple across systems, creating outages or compliance issues that are hard to trace back to the root cause. This is a particularly critical concern in healthcare environments where massive databases and complex infrastructure such as Epic EHR systems manage sensitive patient data across multiple interconnected modules.

This trend is exacerbated by AI-enhanced attack techniques. Adversaries now use AI to accelerate ransomware development, uncover passwords and authentication methods, disable security tools, and create convincing phishing campaigns.

Skill gaps further compound the challenge. Nearly half of organizations (46%) admitted they require additional expertise to manage new database technologies, while 38% also ranked security and compliance capabilities as top criteria when evaluating and selecting database technologies.

46% of organizations admitted they require additional expertise to manage new database technologies, while 38% also ranked security and compliance capabilities as a top database criterion.

Another danger lies in "slow burn" corruption. Instead of dramatic, full-database takedowns, modern attacks might quietly compromise specific pages or objects. By the time

backup anomalies reveal the problem, it is often too late. CyberSense addresses this by tracking files over time, not just since the last backup, enabling it to catch slow-moving corruption that traditional defenses miss.

Levels of Detection: Why Going Deeper Matters

Not all detection methods are created equal. Today, most organizations operate at what can be considered "light," "moderate," or "advanced" levels of detection. At the light level, they rely on metadata analysis, scanning logs, and headers for anomalies. At the moderate level, they might detect when an entire database has been encrypted or corrupted, using methods like calculating the entropy of the file or the compression rate of the backup. While these methods provide some visibility, they fail to uncover the subtle, page-level corruption that defines modern threats.

True protection requires an advanced level of detection, with full-content inspection that validates database headers, page signatures, and structural integrity and analysis performed at network speeds. CyberSense achieves this by indexing data across multiple streams at line speeds, parsing and analyzing the actual structure and content of database files, including Oracle, SQL Server, SAP HANA, Epic, and more. The system first examines file headers to determine the database type, then employs specialized filters developed through engineering access of proprietary file formats to understand each database's unique page layouts and structures.

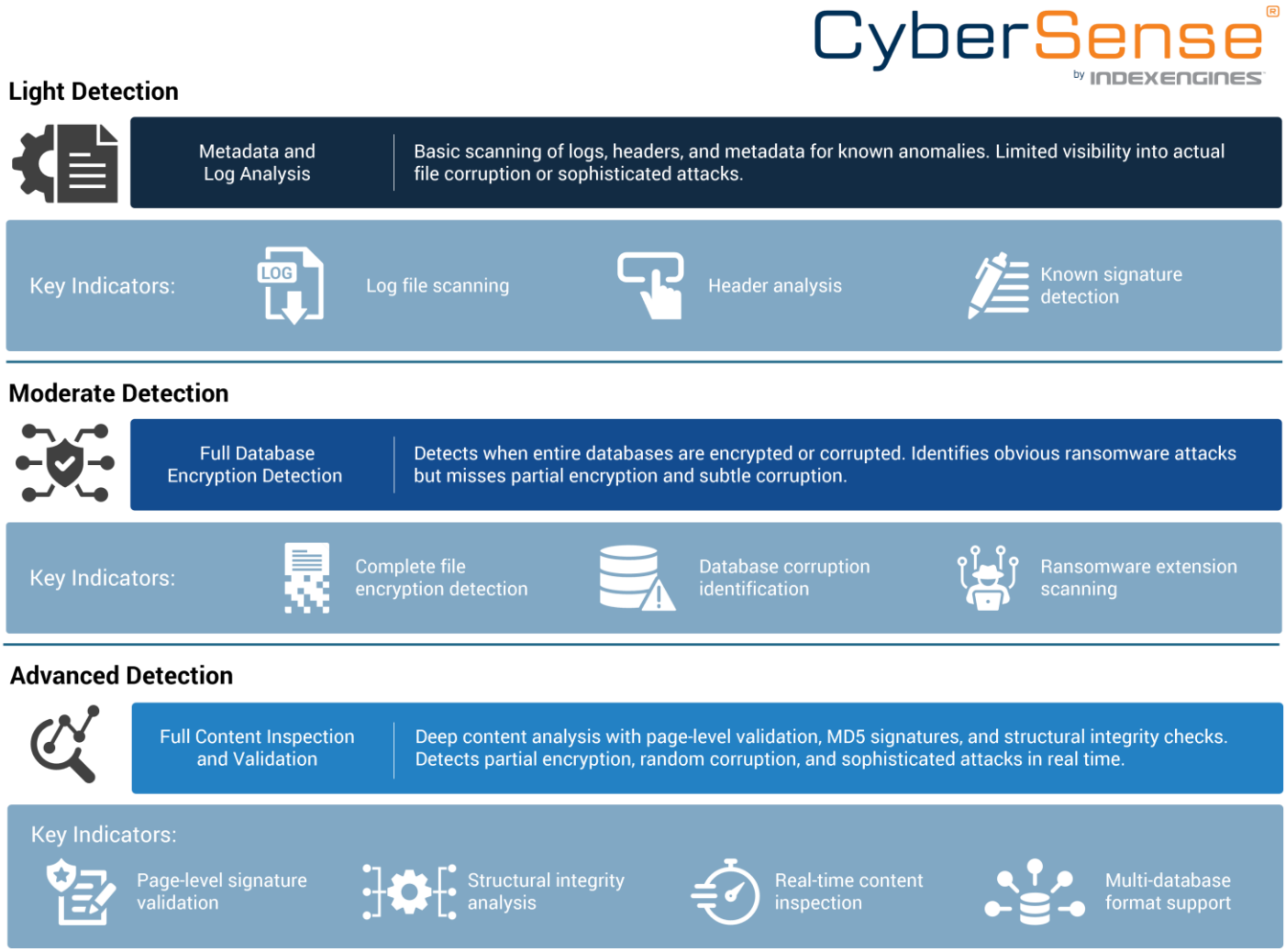
61% of organizations reported attack surface growth over the past two years. This included database environments.[2]

As CyberSense processes the file content, it performs a comprehensive validation by using the database format's proprietary checksum algorithm to verify the integrity of individual pages, validating each page's header structure, and confirming that each page is properly referenced within the database's allocation map. Additionally, the system chunks file bytes and performs entropy and similarity calculations for each chunk and the file as a whole. This deep analysis occurs for every database snapshot and tracks how data changes over time, enabling detection of partial encryption, full malicious encryption, random page corruption, and databases altered through malicious means.

This approach works even with application-encrypted databases, where document headers, structure, and page headers remain unencrypted while only page contents are encrypted. Despite the high entropy of encrypted content, CyberSense can still validate database integrity through structural analysis. Competitors largely stop at metadata inspection, checking for known ransomware extensions or abnormal compression rates without examining actual file contents. By contrast, CyberSense processes multiple database files in parallel over high-throughput networks, delivering comprehensive protection through true content-level analysis.

[2] Source: Enterprise Strategy Group Complete Survey Results, *Midmarket and Small Enterprise Cybersecurity Program Development: A Work in Progress*, November 2024.

Figure 1. CyberSense Levels of Detection



Source: Enterprise Strategy Group, now part of Omdia

CyberSense: Trusted Data Through AI-driven Inspection

Index Engines developed CyberSense to address the gap left by conventional database protection. At its core, CyberSense is an AI-driven platform that performs high-speed, full-content indexing of unstructured files and databases and the files/databases contained in snapshots and backups. By leveraging more than 200 data points across files, including file-level metadata, file headers, content chunks, and entropy calculations, and leveraging AI/ML trained against real ransomware, CyberSense delivers forensic-level accuracy in detecting corruption.

The platform achieves 99.99% accuracy in detecting ransomware and advanced attack patterns, leveraging CyberSense Research Lab's patented methodology for detonating live ransomware variants in controlled environments. This proprietary process involves systematically detonating thousands of ransomware samples in a secure lab setting to observe and catalog the precise impact of malicious changes on transaction logs, page headers, allocation maps, and data files. By analyzing how different ransomware families alter database pages, encrypt content, and modify file headers, CyberSense builds comprehensive training and validation data sets that enable its ML models to distinguish between legitimate data changes and malicious modifications with exceptional accuracy.

Beyond this patented ransomware analysis approach, the platform's content indexing capabilities enable detection of changes, including malware signatures, inspection of executables using YARA rules, tracking changes between document versions, flagging abnormal modifications, and delivering threshold-based alerts for mission-critical files. This combination of AI/ML analysis trained on real-world ransomware behavior and comprehensive content inspection provides unparalleled protection against both known and emerging threats.

CyberSense is designed for practical deployment. It integrates seamlessly with leading backup and storage systems, including Dell Technologies, IBM, Hitachi Vantara, Infinidat, and others, and expands beyond backups into production environments. Its connector architecture supports flexible integration with various storage systems. Capacity-based pricing ensures scalability across enterprise deployments.

The approach delivers four key outcomes:

- **Detect data corruption:** Going beyond metadata to scan full database content.
- **Provide forensics:** Delivering detailed reports on what was affected, when, and how.
- **Enable confident recovery:** Identifying the last clean snapshot or backup for rapid restoration.
- **Integrate seamlessly:** Working with leading storage ecosystems to minimize operational friction.

By combining AI-driven inspection with forensic insights, CyberSense equips DBAs and CISOs with the tools they need to uncover hidden attacks, minimize downtime, and ensure resilience.

Positive Outcomes: Restoring Confidence in Databases

The ultimate goal of database protection is confidence, knowing that critical systems can be trusted and recovered when needed. With threats growing more complex and stealthier, that confidence cannot come from surface-level checks. It requires proof that data is uncompromised and a clear path to restoration if corruption is detected.

Enterprise Strategy Group found that 53% of organizations measured the ROI of database initiatives through improvements in data quality. In addition, 54% of organizations reported already using cloud databases, with 40% citing security and privacy as top challenges to managing these databases. CyberSense directly supports this by ensuring that clean, trusted copies of databases exist.

The business outcomes of adopting CyberSense are clear. Organizations benefit from trusted data, reduced downtime, and enhanced resilience. For executives, the impact extends beyond IT. By elevating database security from a technical concern to a boardroom priority, enterprises can align cyber resilience with broader business strategy.

Conclusion

Databases are too valuable to leave exposed. They contain organizations' critical infrastructure, health, and financial data. Yet many organizations still operate under the assumption that existing tools are enough. This false sense of security leaves organizations vulnerable to subtle corruption that can go undetected for months.

By embracing deeper inspection, organizations can break free from myths and gain real confidence in their database resilience. Index Engines' CyberSense platform provides full content indexing with highly accurate AI analysis needed to detect corruption at its earliest stages, deliver actionable forensics, and ensure fast, reliable recovery. For DBAs, architects, CIOs, and CISOs alike, the message is clear: Trusted data requires going deeper. Enterprise Strategy Group recommends that any organization looking to protect its critical databases should consider Index Engines.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com