CY4DATA LABS MAKES EVERY CYBERSECURITY THREAT OBSOLETE.

WITH CY4SECURE™, YOUR DATA IS ALWAYS ENCRYPTED, SO EVEN WHEN IT'S STOLEN, IT'S NEVER AT RISK.

THE CYBERSECURITY LANDSCAPE

Cybersecurity has advanced dramatically in two decades, **yet breaches keep rising in frequency and cost**. The Splunk Top 50 Cybersecurity Threats report shows most cyberattacks still exploit the same 50 common threats. Well-funded industries are struggling to keep pace with increasingly sophisticated attackers.

Two of the most damaging and persistent data breach attack vectors are:

- **Insider Threats** – Authorized users, whether malicious or careless, who misuse legitimate access.
- **Loss or Theft of Credentials** – Compromised usernames, passwords, API keys, or tokens that give attackers legitimate-looking access.

Both scenarios bypass perimeter defenses and encryption, often evading detection until it's too late. With valid credentials or malicious insiders, attackers can access sensitive data in plain text despite network or storage security.

TODAY'S STANDARD PROTECTIONS ARE LIMITED

Most organizations rely on a familiar trio of safeguards: data masking, data-at-rest encryption, and data-in-motion encryption. These are important, but each only addresses a narrow slice of risk, and none fully prevents the most damaging breaches.

DATA MASKING

STRENGTH	Masks sensitive information and commonly used data in test environments.
WEAKNESS	Remains natively in the clear in the database and requires an intermediary proxy slowing performance while increasing the attack surface.
RESULT	Effective against low-skill threats, but ineffective against skilled insiders or stolen credentials.

DATA-AT-REST ENCRYPTION

STRENGTH	Protects files, drives, and storage arrays against physical media theft and direct access.
WEAKNESS	Data is always decrypted and exposed when used by applications.
RESULT	Stops a thief from reading a stolen drive, but not from exploiting a logged-in application.

DATA-IN-MOTION ENCRYPTION

STRENGTH	Secures communication traffic between systems.
WEAKNESS	Only protects data in transit; once it arrives, it's decrypted and exposed.
RESULT	Prevents eavesdropping but not theft at the endpoint.

THE BLIND SPOT: When data is actively in use, being processed, queried, or viewed, it is often completely unprotected.

THE MISSING ELEMENT: DATA-IN-USE PROTECTION

Data in use, information being processed, viewed, or held in memory, is when insiders and credential thieves can cause the most damage, and where traditional encryption fails.

Without ***in-use protection***, it only takes:

- An insider downloading sensitive records to an external drive.
- A compromised application, user or admin accounts leads to a database dump.
- Malware scraping unencrypted data from memory, logs or snapshots.

THIS GAP IS WHY INSIDER THREATS AND CREDENTIAL THEFT REMAIN LEADING CAUSES OF BREACHES YEAR AFTER YEAR.

THE BRINKS ANALOGY, MAKING THE GAP VISIBLE

Think of sensitive data as cash:

- **Using TDE – Data at Rest**

  This is like keeping your money in a high-security safe. If someone steals the safe, they can't get to the cash without the combination. It's great protection while the money is stored.

- **Using TLS – Data in Motion**

  This is like hiring a Brinks truck to transport the money. It's secure while it's on the road, armed and protected from interception. But once the truck arrives and unloads at either an intermediatory or final destination, the money is again at risk.

The Overlooked Moment, When the Money Is in Use

What about the moment the money is counted, exchanged, or handed over for legitimate use? What if someone "forgets" and leaves the safe door open? Or the Brinks truck is left unlocked, or when the guard is carrying the money to and from the truck? In those moments, all the previous security becomes irrelevant, because the money is vulnerable to theft.

The Login Dilemma: Application logins are like checking the ID of the person collecting the money. But IDs (credentials) can be stolen. An attacker with stolen credentials can walk straight into the vault. In most systems, once logged in, they have full access to clear-text data, no questions asked.

HOW CY4DATA LABS SOLVES IT

Using the money analogy, Cy4Data Labs takes a different approach. Instead of protecting only the safe and the truck, **we eliminate the security gaps and protect down to every single bill individually**. This means, each data element can be encrypted with its own encryption key, and keys are only provided to the authorized user at the right moment.

Put simply:

- Even if the safe is open, the data is still encrypted.
- Even if the Brinks truck is unlocked, the data is still encrypted.
- Even if a bag of money is dropped or falls off the truck, the data remains encrypted.
- Even if credentials are stolen, the data is still encrypted, because possession of a password isn't enough to get keys to all the data.

Bottom Line: With Cy4Secure, you must be the right person, using the right application, at the right time, not just someone holding a valid password.

Top Cybersecurity Threats

Cybersecurity Threat	Cy4Secure Solves	TDE Solves	TLS Solves	Cy4Secure Advantage or (comment)
Account Takeover	**Yes**	No	No	Governed access and MFA verification
Advanced Persistence	**Yes**	No	No	Access monitoring limits or stops access
AWS (S3) Attacks	**Yes**	N/A	No	(Classic At-Rest case)
App Access Token (OAuth)	**Yes**	No	No	Only encrypted data passes through the App
Brute Force Attack (Password)	**Yes**	No	No	Data remains protected once in the network
Command & Control Attack	**Yes**	No	No	The compromised App server has no key access
Compromised/Lost Credentials	**Yes**	No	No	Single system per user invokes MFA
Credential Dumping	**Yes**	No	No	ML detection governs access; forces MFA
Credential Reuse Attack	**Yes**	No	No	ML detection governs access; forces MFA
Cross-Site Scripting	**Yes**	No	No	Governed access and MFA verification
DNS Hijacking	**Yes**	No	No	Access monitoring limits or stops access
Drive-by Download Attack	**Yes**	No	No	(Classic At-Rest case)
Insider (bad actors)	**Yes**	No	No	Only encrypted data passes through the App
IoT Devices Compromised	**Yes**	Yes/No	No	Data remains protected once in the network
Macro Viruses	**Yes**	No	No	ML detection governs unusual access patterns
Malicious PowerShell	**Yes**	No	No	Single system per user invokes MFA
Malware	**Yes**	No	No	ML detection governs access; forces MFA
Man-in-the-Middle Attack	**Yes**	No	Yes/No	ML detection governs access; forces MFA
Masquerade Attack	**Yes**	No	No	Similar to phishing attacks
Meltdown/Spectre Attack	**Yes**	No	No	DB server only operates on encrypted data
Network Sniffing	**Yes**	No	**Yes**	Data is always/remains encrypted
Pass the Hash Attack	**Yes**	No	No	ML detection governs access; forces MFA
Phishing/Payload/Spear/Whale	**Yes**	No	No	Similar to compromised/lost credentials
Privileged User Compromised	**Yes**	No	No	Monitoring limits/stops key access to decrypt
Quantum Resistant	**Yes**	**Yes**	No	Uses proven symmetric key encryption
Ransomware	**Yes**	No	No/PQC	Cybercriminals can't query DB's contents nor read files
Router & Infrastructure Attack	**Yes**	N/A	**Yes**	Data In-Flight is always encrypted
Shadow IT and Admins	**Yes**	No	No	IT/Admins don't have/need key access
Social Engineering Attacks	**Yes**	No	No	Similar to compromised/lost credentials
Spyware	**Yes**	No	No	Similar to compromised/lost credentials
SQL Injection Attacks	**Yes**	No	No	Data remains encrypted through the App server
Supply Chain Attacks	**Yes**	No	No	Data and Keys are separated with no connection between key locations, data, and users

DETECTING AND STOPPING BAD ACTORS IN REAL-TIME

Cy4Secure does more than secure data, it monitors every key request, instantly detecting and blocking any unauthorized access.

WHY THIS MATTERS:

- **Insider Threats:** An employee tries to access an unusually large amount of the customer database. Cy4Secure spots the abnormal request pattern and stops it.
- **Stolen Credentials:** An attacker logs in and queries sensitive data. Cy4Secure blocks it because the context doesn't match authorized use.
- **Automated Attacks:** Malware attempts to scrape memory or sniff traffic on applications or endpoint devices. Cy4Secure protected data remains encrypted in-memory and in-use rendering any hijacked data useless.

HOW CY4DATA LABS CLOSES THE GAP

Cy4Secure delivers what other solutions ignore, persistent encryption for data at rest, in motion, and in use.

Key Advantages:

- Persistent Encryption: Data stays encrypted across its entire lifecycle.
- Element-Level Security: Each field of a record can have a unique key.
- No Performance Hit: Databases operate natively on encrypted data, without decryption.
- Always Encrypted: Decrypted in milliseconds when displayed on the end-point device..
- Real-Time Access Control: Keys are only issued to authorized users/applications.
- Insider Threat Visibility: Detects and stops abnormal access patterns instantly.
- 100% Brownfield Deployments: Works with existing data application systems.

BUSINESS IMPACT, TURNING SECURITY INTO A COMPETITIVE ADVANTAGE

By securing personal information and personal health information at the data level, organizations can:

- Reduce Breach Impact: Stolen PI/PHI data is useless without access to the keys.
- Enable Safe Data Sharing: Share across teams or partners without exposing clear-text.
- Simplify Compliance: Persistent encryption helps meet GDPR, CCPA, HIPAA, and more.
- Protect AI & Analytics: Data stays protected even during training and inference.

Cy4Data Labs eliminates this problem by making data useless without the right keys, no matter where or how it's accessed. This isn't just compliance, it is active defense, ensuring your most valuable assets are **always encrypted and never at risk.**