

Securing KYC Data

Protecting Organizations from Untrusted Data & Zero-Day Malware

A Partnership for Success

The main challenge of identity verification and KYC processes is managing data safely.

Sensitive documents are shared, reviewed, and stored, making them a prime target for cyber threats. Attackers can embed malware or hidden exploits within files, slipping past traditional security measures.

Additionally, organizations that operate globally must find ways to comply with various compliance regulations and laws.

Challenges in Securing Data

- Receiving data from untrusted sources
- Defending against zero-day and unknown threats
- Working to comply with compliance laws and global regulations

Know Your Customer (KYC) and identity verification processes are essential across financial services, government agencies, and highly regulated industries. These processes help prevent fraud, money laundering, identity theft, and other security risks while working to comply with regulatory frameworks.

To achieve this, organizations must collect and process vast amounts of sensitive data—often from **untrusted sources**—including identity documents, financial statements, and other personally identifiable information (PII).

This influx of unverified data creates a prime attack vector for cybercriminals. Threat actors embed malware, hidden exploits, and fraudulent identities within submitted files and images, which can often bypass traditional detection-based cybersecurity measures.

The challenge those working in these industries face is twofold: Protecting the integrity of incoming data while working to prevent cyber threats from compromising systems. In fact, **64% of organizations** surveyed in the [CYBER360 Report](#) cited **that leveraging threat prevention solutions will ultimately reduce the likelihood of costly data breaches and operational disruptions.**

With financial institutions, government departments, & critical infrastructure sectors being top targets for cybercriminals, a new approach is needed—one that reduces risks from untrusted data sources & works to neutralize zero-day threats before they reach critical systems.

Enhancing KYC Security with Everfox CDR

Unlike traditional anti-malware or sandboxing solutions, Everfox CDR doesn't rely on detecting known threats. Instead, it works to disarm all potentially malicious data at the source, meaning that none of the original data—including any potential malware—enters the network.



Safe documents, images, and files – Stopping malicious code from infiltrating systems while preserving the integrity of customer-submitted data.



Easily integrates with existing infrastructure



Defends against zero-day threats and advanced persistent threats (APTs) that traditional detection-based cybersecurity solutions may fail to stop.



Delivers brand new, verified data in near real-time, maintaining operational efficiency.



Security that goes beyond detection-based methods, proactively securing against threats.

Complete Protection for KYC and Identity Verification Data

By integrating Everfox CDR, organizations can help keep incoming data secure from cyber threats, comply with regulations and maintain operational efficiency.

- **Malware-Free Data** – Helps stop zero-day exploits, hidden malware, and embedded threats in submitted documents.
- **Integrate with Ease** – Everfox CDR within existing workflows to sanitize files before they enter back end systems.
- **Regulatory Compliance** – Helps users comply with Anti Money Laundering (AML) laws, data protection, and national security regulations.



How Everfox CDR Works

01

File Received

A document, image, email or other supported file type is received.



02

Analysis & Recipe Creation

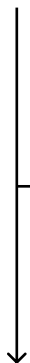
Everfox CDR examines the file's legitimate content and creates a set of instructions (a recipe) for creating a new file with the same content but without including any of the original data.



03

Original File Discarded

The original file is either discarded or stored securely, complete with any malware, in your forensic suite for later analysis.



04

Recipe Verification

The generated recipe is verified to confirm it is complete, consistent and not carrying anything extra.



05

File Reconstruction

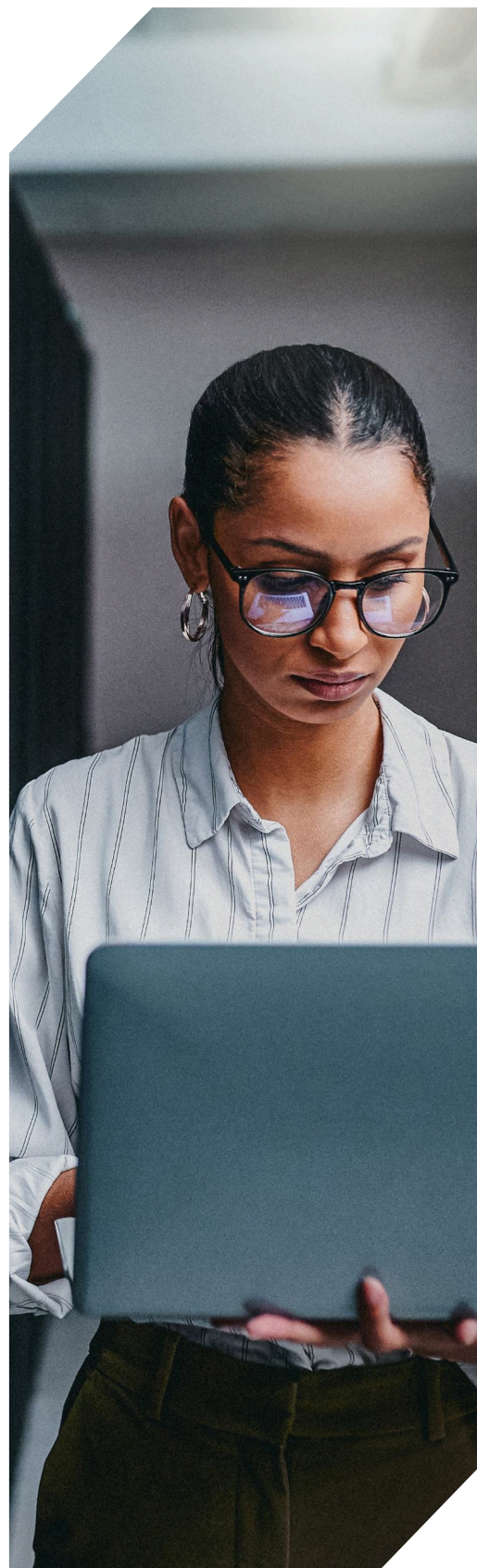
The recipe is followed to create a new, clean file, equivalent to the original content.



06

Secure Delivery

The newly built functional file is delivered to the user in near real-time.



Strengthening Cybersecurity in Identity Verification & KYC Compliance

Because financial institutions, government agencies, and other highly regulated industries must receive and process vast amounts of untrusted data, they have become prime targets for cybercriminals.

To mitigate these risks, organizations must adopt a proactive, multi-layered cybersecurity approach that safeguards sensitive data, assists with compliance, and streamlines operations.

1. Protecting Sensitive Data

Everfox CDR adds an essential layer of protection to identity verification and KYC processes by transforming and rebuilding customer-submitted documents and images before they enter the system—helping to keep hackers out and protecting critical data.

2. Meeting Regulatory Compliance

Everfox CDR helps organizations meet legal and regulatory requirements for protecting sensitive data across multiple industries and jurisdictions:


- Financial Services – GDPR, AML, KYC, and the USA PATRIOT Act mandate secure customer data handling.
- Government Agencies – National security and data protection laws require advanced cybersecurity for citizen and governmental records.
- Highly Regulated Industries – Compliance with healthcare, identity, and critical infrastructure regulations necessitates secure document processing.

3. Saving Time and Resources

By automating advanced threat protection, Everfox CDR allows security teams to focus on more critical tasks while avoiding lengthy delays caused by detection-based solutions like sandboxing.

4. Adapting to Global Needs

Highly regulated industries operate across multiple jurisdictions, each with unique regulatory requirements. The flexibility of Everfox CDR makes it an ideal solution for standardizing and securing identity verification workflows in regions such as the UK, UAE, USA, and beyond.



“70% of IT Risk Analysts believe detection technologies are flawed, particularly against zero-day threats.”

CYBER360 Report (2025)

Proactive Security for a Safer Digital Future

As financial institutions, government agencies, and critical industries face increasingly sophisticated cyber threats, securing KYC and identity verification data has become a critical priority. Relying solely on detection-based cybersecurity leaves organizations vulnerable to zero-day and unknown threats.

Everfox CDR provides a **game-changing approach** to securing identity verification and KYC workflows - reducing cyber risks from untrusted data sources before they can impact critical systems. This comprehensive security framework helps organizations protect sensitive data, maintain regulatory compliance, and operate with confidence in an increasingly hostile cyber landscape.

Secure Your Identity Verification & KYC Workflows with Everfox CDR

Don't let untrusted data put your organization at risk.

With Everfox CDR, you can automate document sanitization, defend against zero-day threats, and ensure compliance—without slowing down operations.

- Reduce malware risks in submitted documents and images
- Helps defend against zero-day and advanced persistent threats (APTs)
- High-quality, secure data processing

Protect your organization from untrusted data risks, learn more about [Everfox CDR](#)