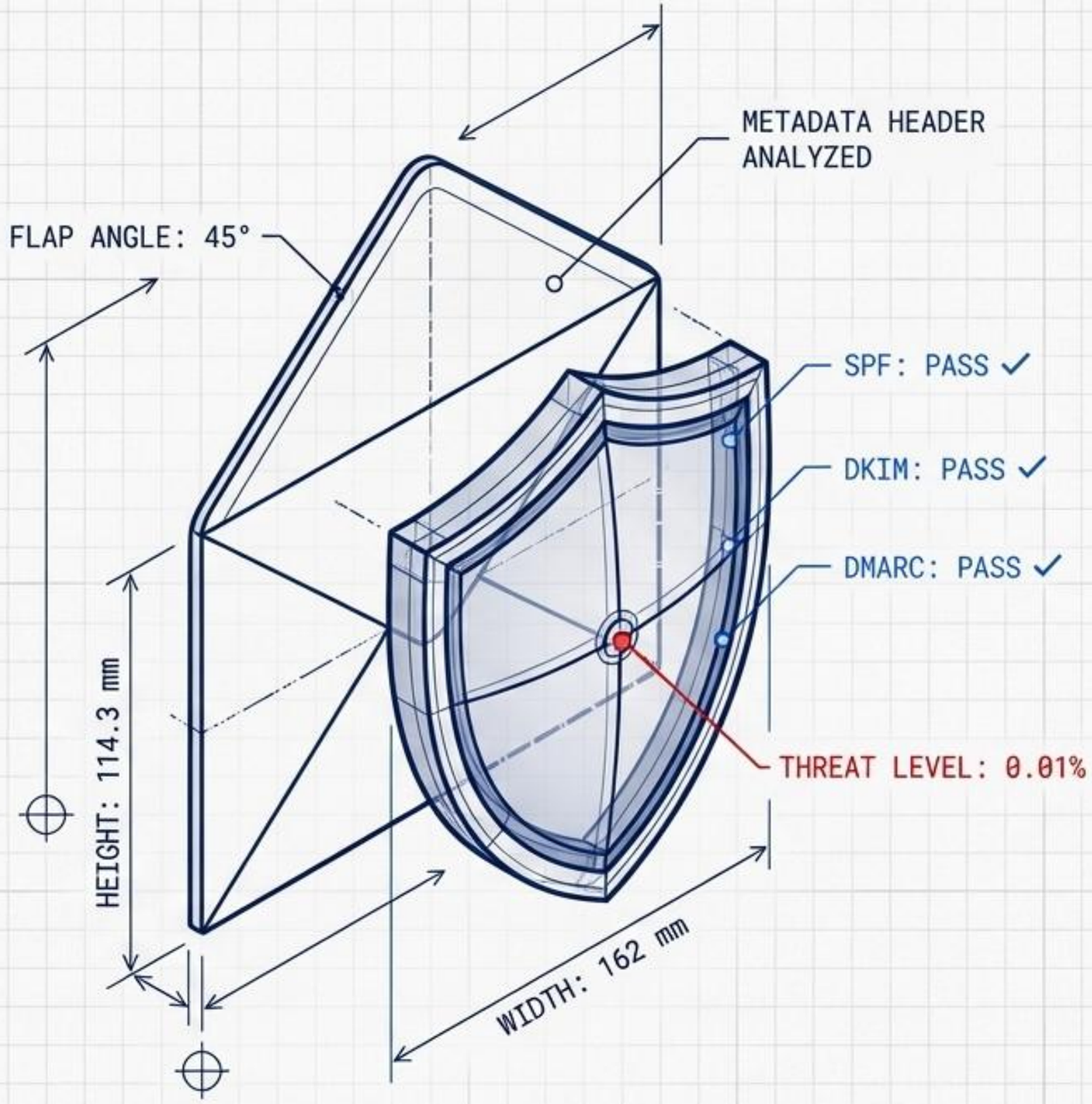
CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

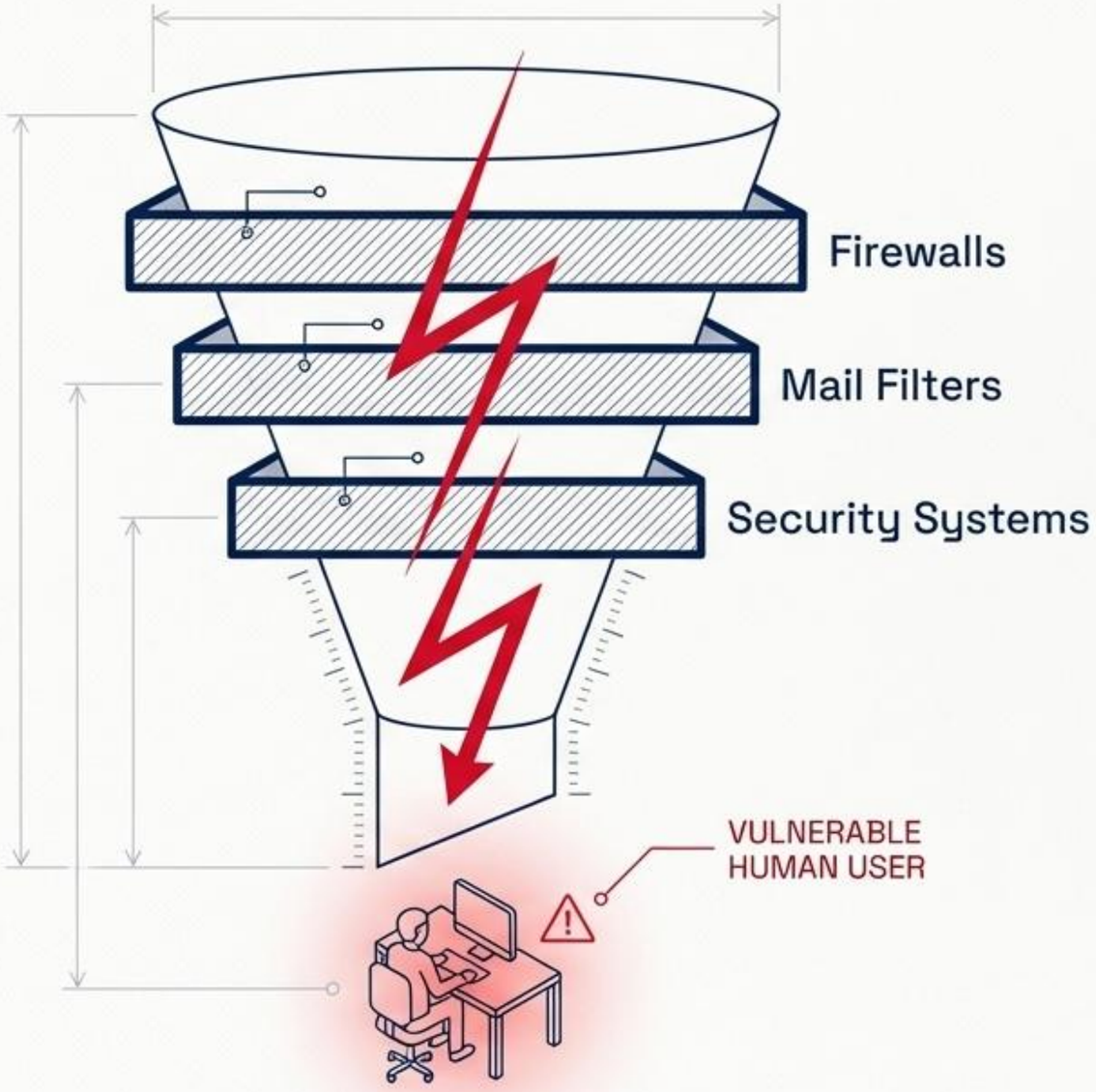


Cyber Zones MailGuard

Email Reliability Analysis Tool

The final line of defense against phishing.

CYBER ZONES
Innovation & Research Division



Targeting the Human Element: The Vulnerability that Bypasses Traditional Systems

Modern phishing attacks no longer rely exclusively on malware; instead, they focus on hacking the user's decision.

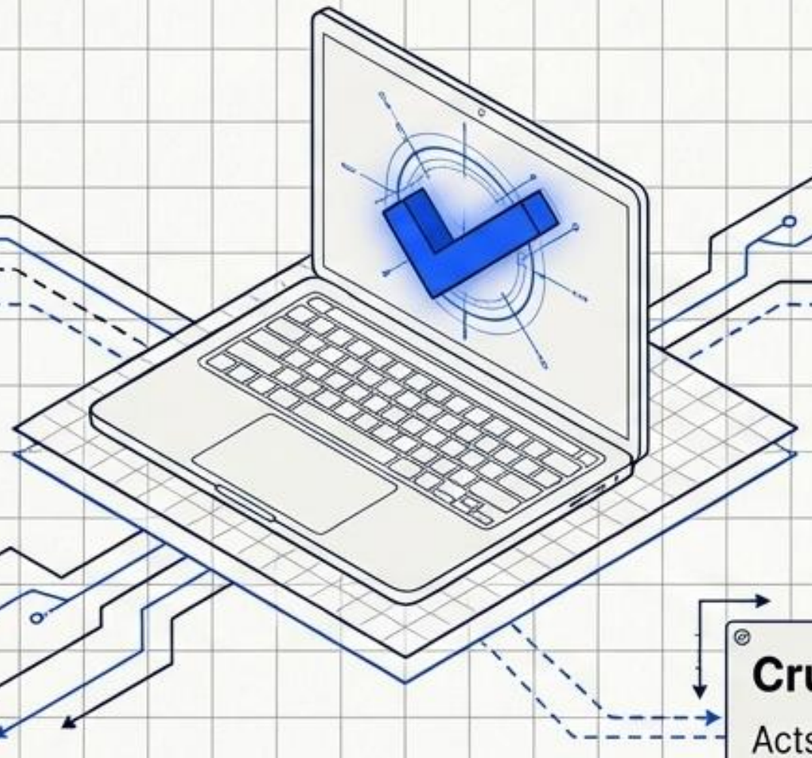
The employee today is the starting point of any successful breach.

Ransomware attacks or corporate breaches begin with a forged corporate email that successfully bypassed technical systems, targeting the user's decision and trust directly.

CYBER ZONES MailGuard
Cyber Zones lightweight protection tool

Cyber Zones MailGuard: Empowering the User to Make the Right Decision

Developed entirely by the Innovation & Research Department at Cyber Zones.



On-Premise Local Analysis Tool

Works directly on the end-user's device.

User Empowerment

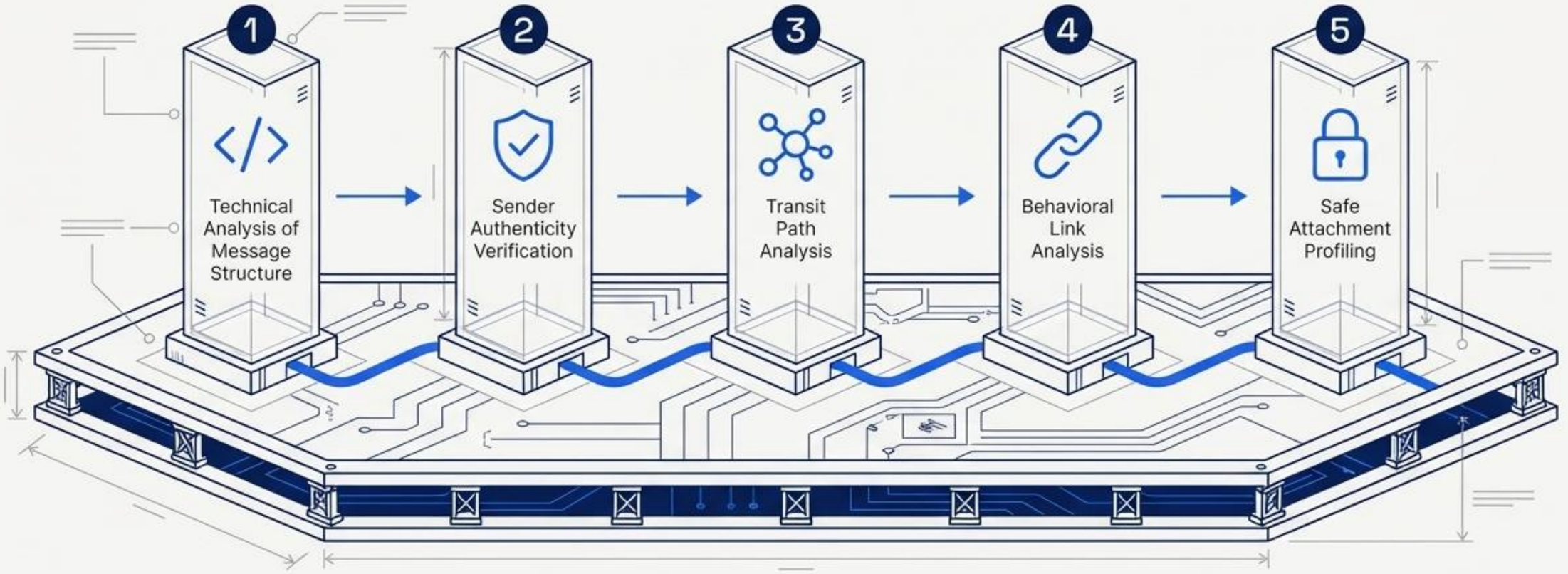
Enables the user to inspect messages technically and behaviorally before interacting.

Crucial Verification Layer

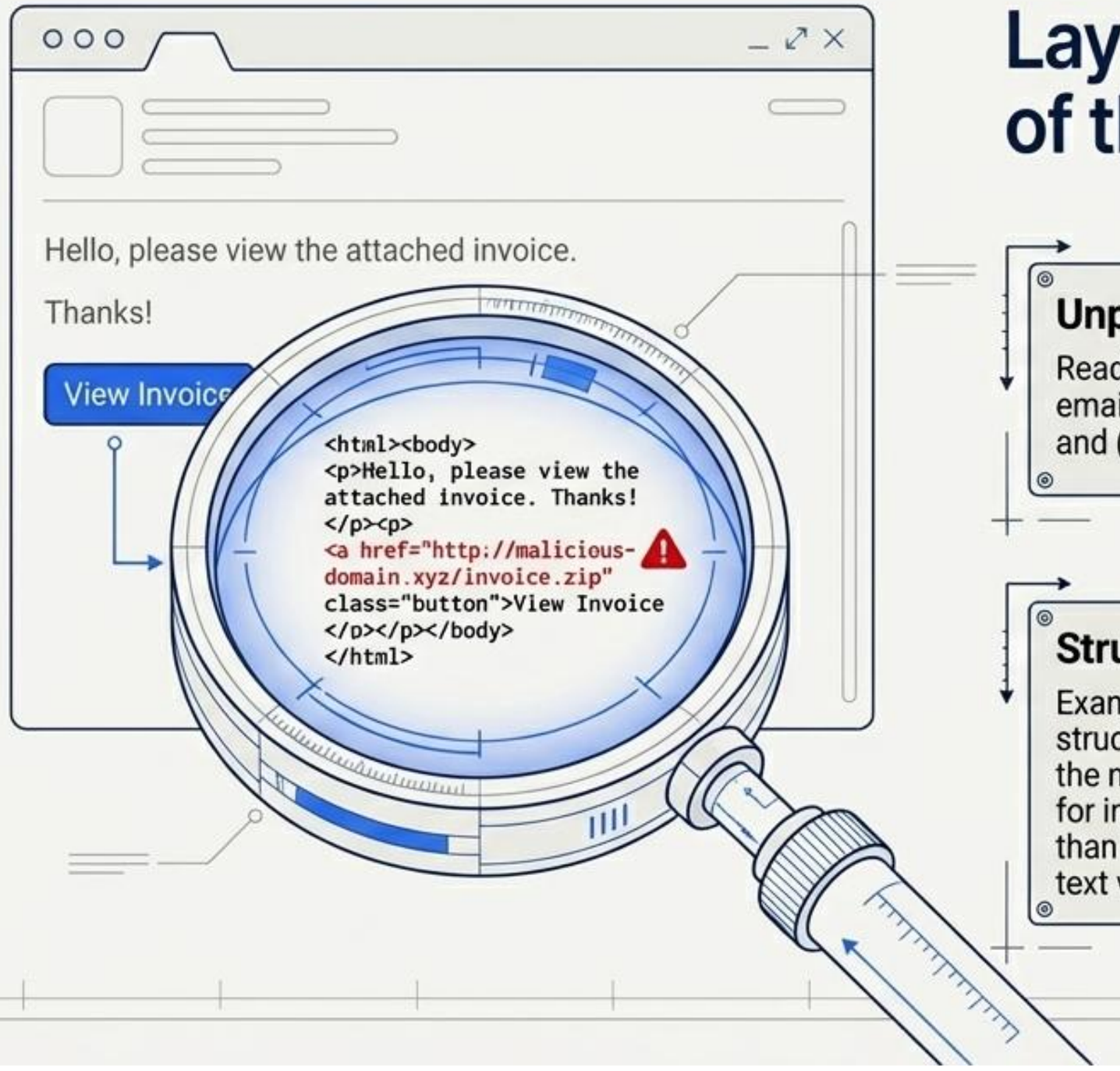
Acts as an additional verification layer without replacing corporate security systems.

The Analytical Engine: Merging Technical Inspection with Behavioral Analysis

The tool dissects message components across 5 simultaneous layers:



Layer One: Technical Analysis of the Message Structure



Unpacking Files:
Reading and dissecting email files in both (.msg) and (.eml) formats.

Header Extraction:
Extracting message Headers and analyzing the true, hidden transit path.

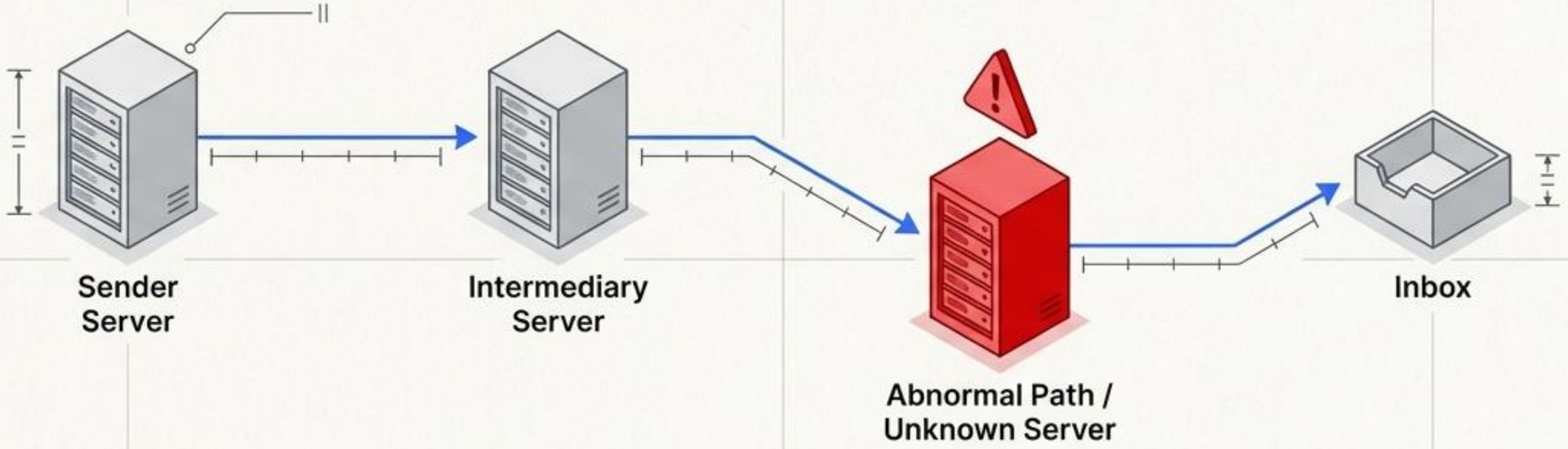
Structural Integrity:
Examining the actual structural composition of the message and searching for inconsistencies, rather than relying solely on the text visible to the user.

Safe Environment:
Analyzing links and attachments within a secure environment without executing them.

Layer Two: Detecting Spoofing and Sender Authenticity

- **Standard Protocols**: Reviewing standard authentication protocols (SPF / DKIM / DMARC).
- **Domain Contradictions**: Detecting glaring contradictions between domains (.From, Reply-To, Return-Path).
- **Impersonation**: Monitoring the use of known company names combined with fake domains.
- **Visual Similarity**: Discovering visually similar and recently created domains.
- **Deobfuscation**: Deconstructing hidden or obfuscated links that rely on social engineering.

Layer Three: Message Transit Path Analysis



Untrusted Infrastructure: Monitoring the use of untrusted sending infrastructure or unknown source servers before the message arrives.

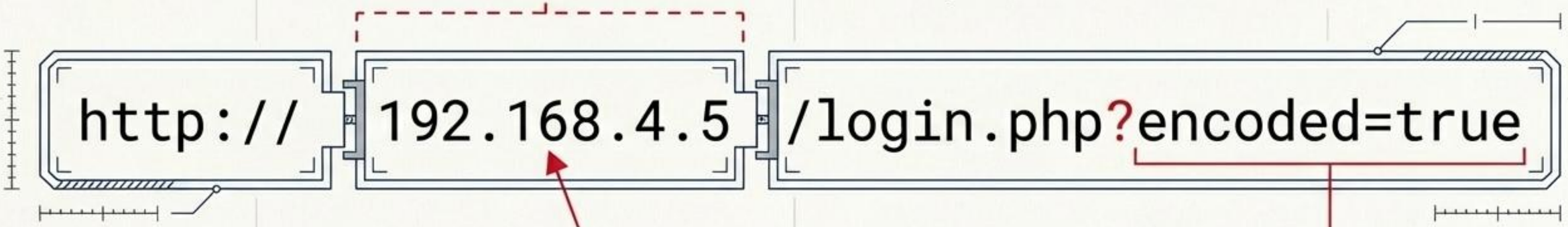
Geographic Anomalies: Discovering abnormal geographic or technical paths for message transit.

Received Chain: Exact and precise tracking of the receipt chain.

Layer Four: Advanced Behavioral Link Analysis

The tool does not simply rely on blocklists; it analyzes the behavior of the link itself.

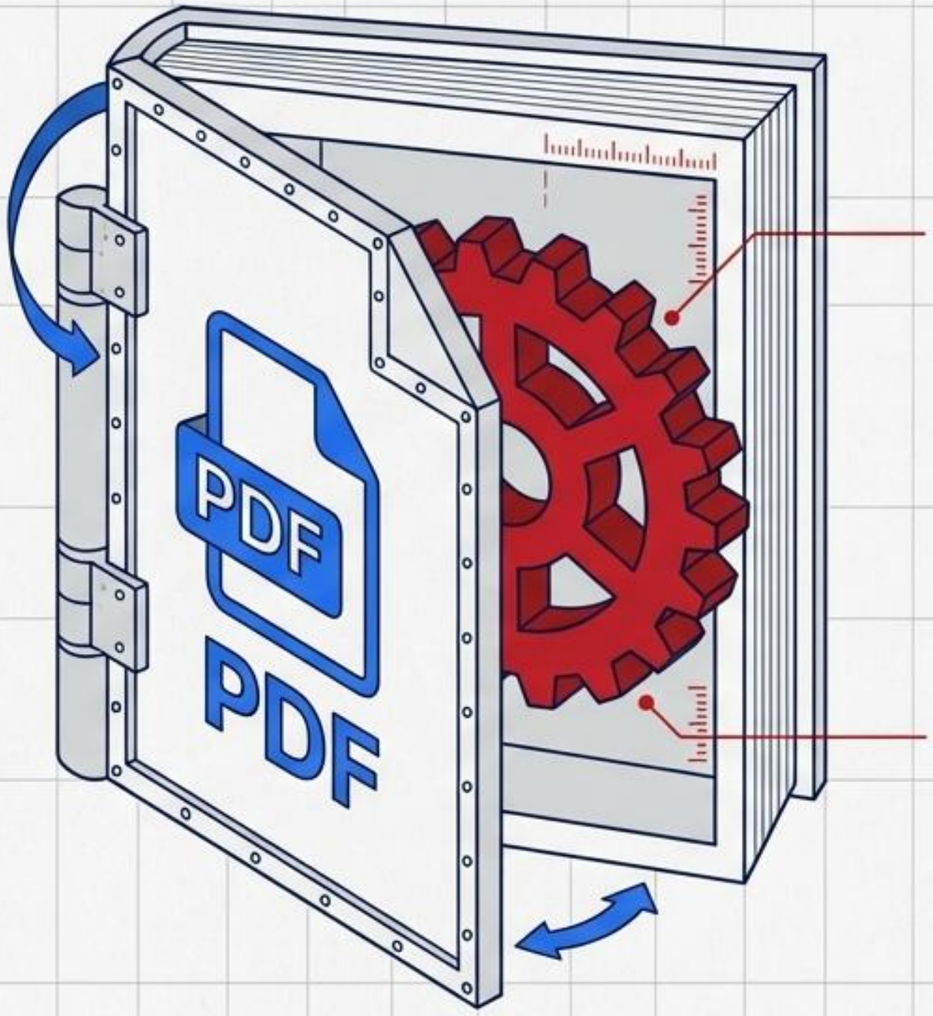
Infrastructure Evaluation:
Real-time assessment of domain age.
Domain Age: 1 Day



Shortener Abuse:
Uncovering URL shorteners used exclusively to hide the final destination.

Direct IP Routing:
Monitoring links built directly on IP addresses.

Obfuscation Detection:
Discovering encoding and obfuscation techniques hidden inside the link structure.



Layer Five: Safe Attachment Profiling

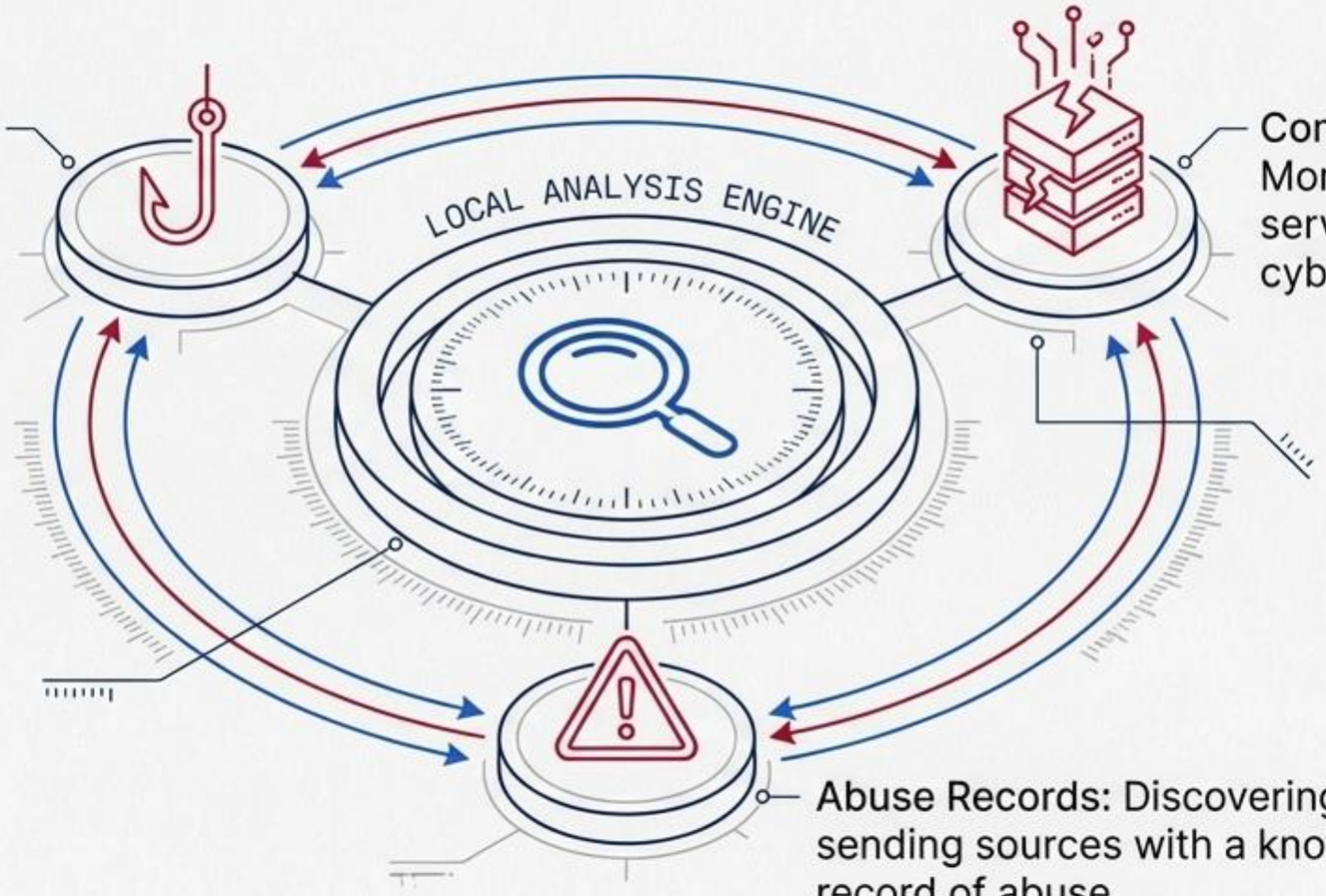
True File Verification: Verifying the true file type through its digital signature and structure, regardless of the visible extension.

Hidden Executables: Precise identification of hidden executable files inside seemingly safe attachments.

Macro Detection: Detecting malicious Macros embedded within Office files.

Matching with Global Threat Intelligence (OSINT)

Discovered local indicators are immediately compared with public threat databases:



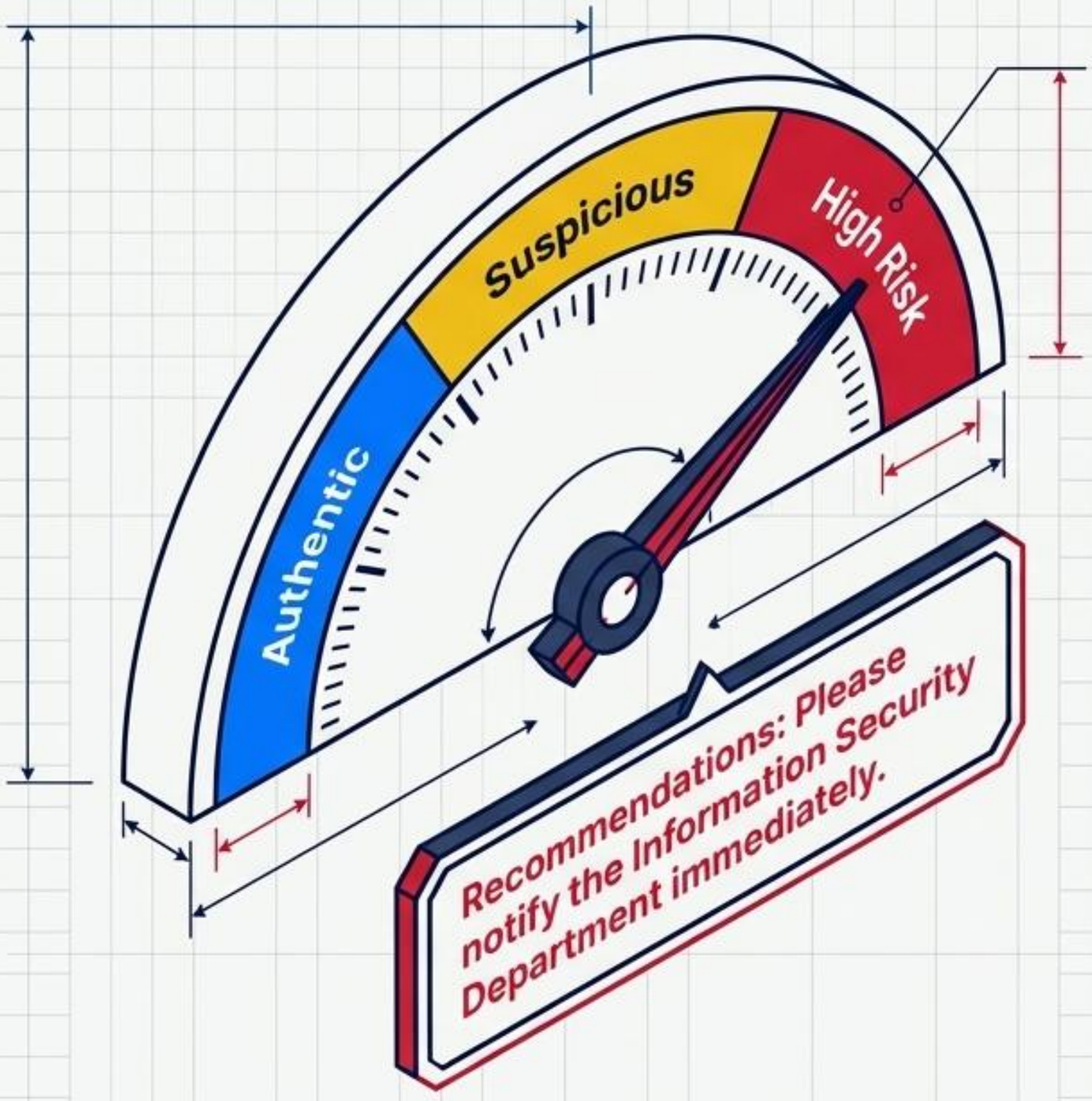
Active Campaigns: Identifying links tied to known and active phishing campaigns.

Compromised Infrastructure: Monitoring infrastructure and servers previously used in cyberattacks.

Abuse Records: Discovering sending sources with a known record of abuse.

CYBER ZONES MailGuard

Cyber Zones lightweight protection tool



Outputs: Supporting the User's Decision, Not Replacing It

Immediate Results: The tool displays a clear, final, executable result directly to the user with specific risk levels: **Authentic | Suspicious | High Risk.**

Simplified Explanations: A simplified technical explanation clarifies the reason for the evaluation without confusing the employee.

Actionable Guidance: Practical, clear recommendations for the correct action to take.

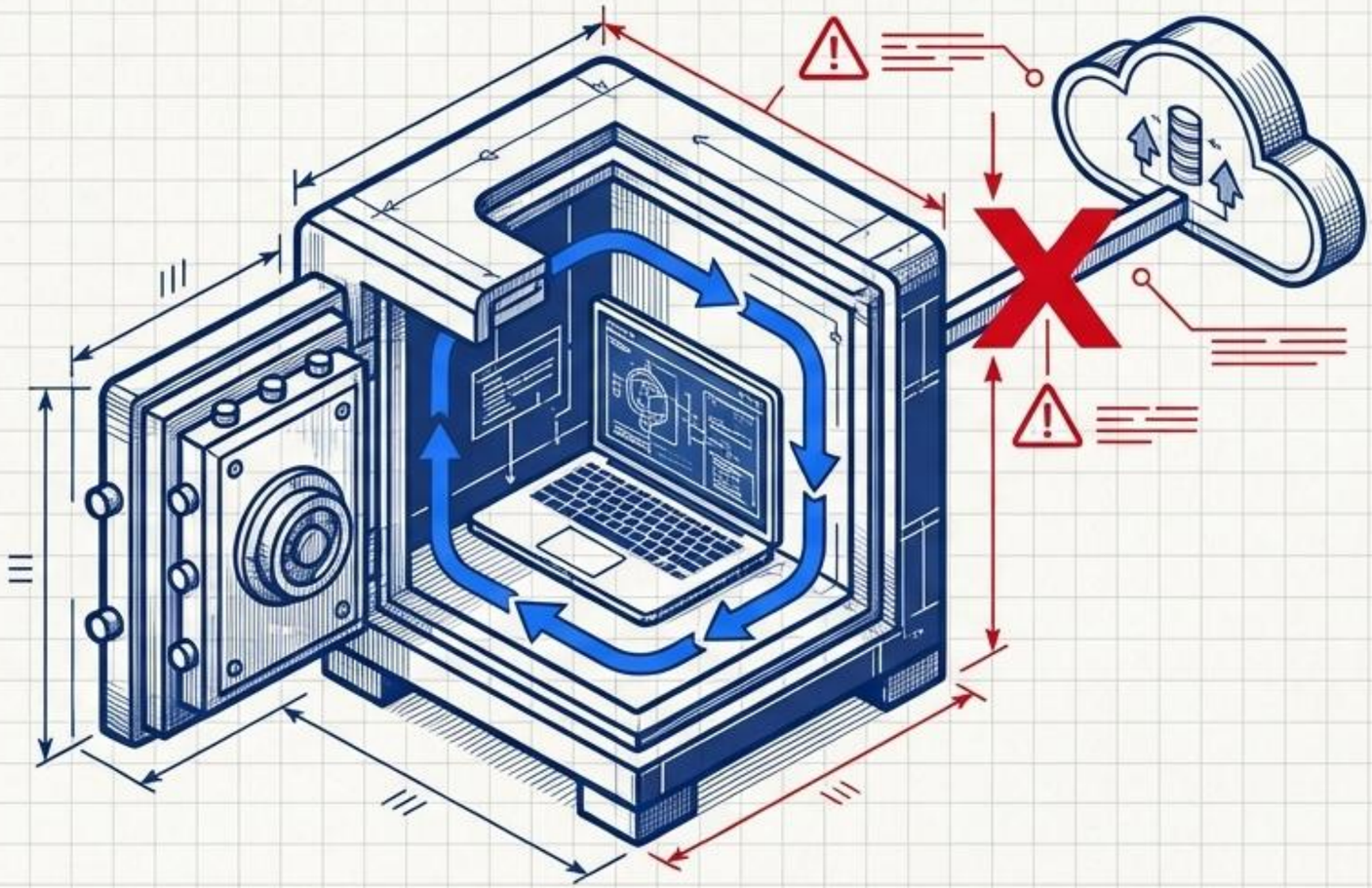
CYBER ZONES MailGuard
Cyber Zones lightweight protection tool

Absolute Privacy | Complete Data Sovereignty

The tool is designed to operate entirely within the isolated corporate environment, making it perfectly suited for highly sensitive entities.

The Privacy Guarantee

- Messages are absolutely never uploaded to any external or cloud server.
- No message data or logs are stored whatsoever.
- The content of the user's device is never shared in any form.



CYBER ZONES MailGuard
Cyber Zones lightweight protection tool

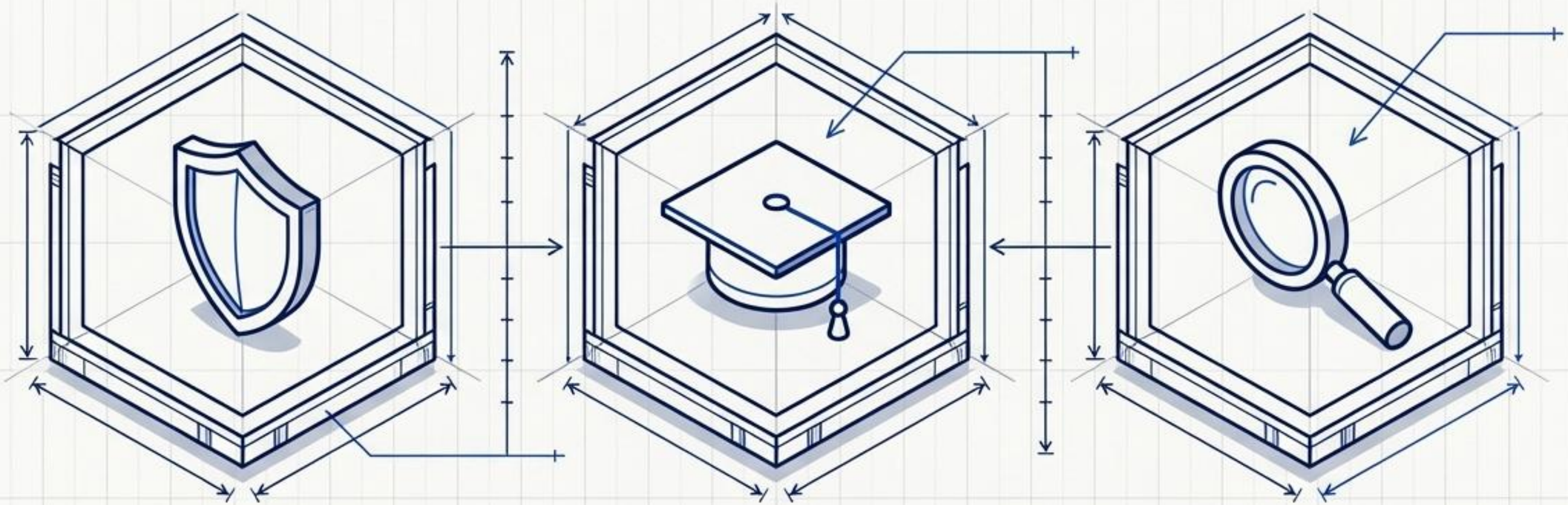
Operational Positioning: What does Cyber Zones MailGuard represent?

Is Not	But Rather
✗ An automated blocking or filtering tool.	✓ An independent verification layer that enhances user decision-making.
✗ An alternative email system.	✓ A support tool utilized prior to direct interaction with a message.
✗ An alternative to corporate security systems.	✓ The final line of defense and a means to reduce human-factor risks.

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

The Corporate Impact: Why is MailGuard an absolute necessity today?

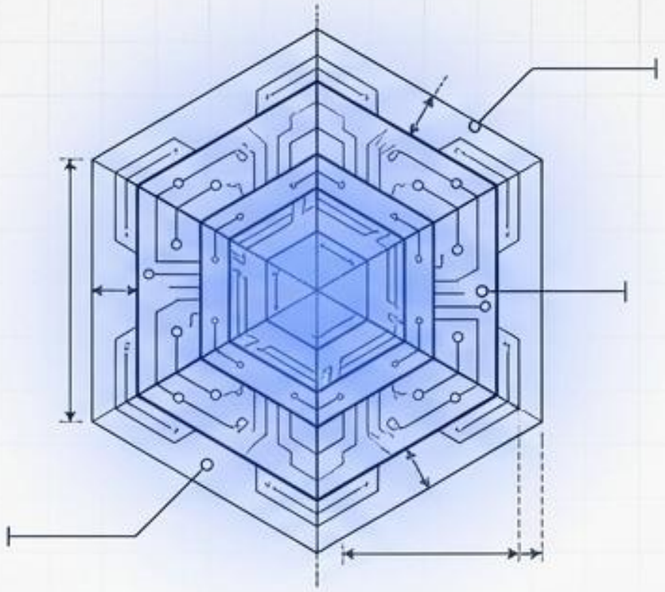
Attacks have successfully bypassed system stages and reached the user clicking a link. MailGuard intervenes specifically here:



The Final Line of Defense: Preventing the cyber incident before it occurs and actively reducing human risk.

Effective & Practical Security Awareness: Training the employee daily through hands-on practice, not just theoretical lectures.

Pre-Verification Tool: Empowering inspection before any involvement or interaction with suspicious content.



CYBER ZONES
MailGuard

Cyber Zones lightweight protection tool

Cyber Zones Vision for Strategic Innovation

Enhancing Open-Source Intelligence (OSINT).

Reducing overall exposure to digital attacks.

Building practical security awareness integrated directly into the defense ecosystem.

We recommend including MailGuard in your operational environment to enhance your digital sovereignty and transform your employees into the definitive first line of defense.

To trial the tool and explore the Innovation & Research Department's platforms, contact us: info@cyber-zones.com