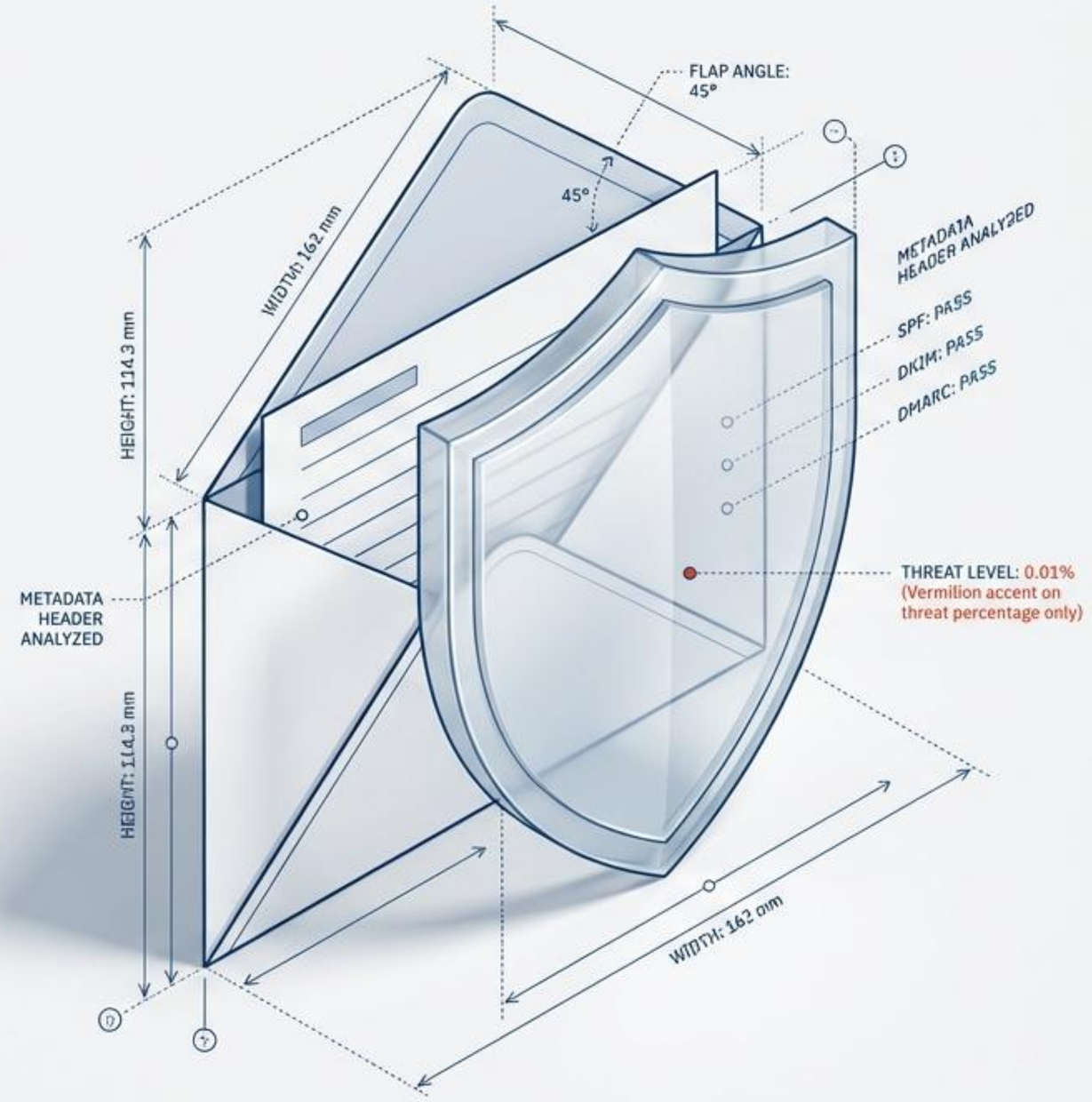
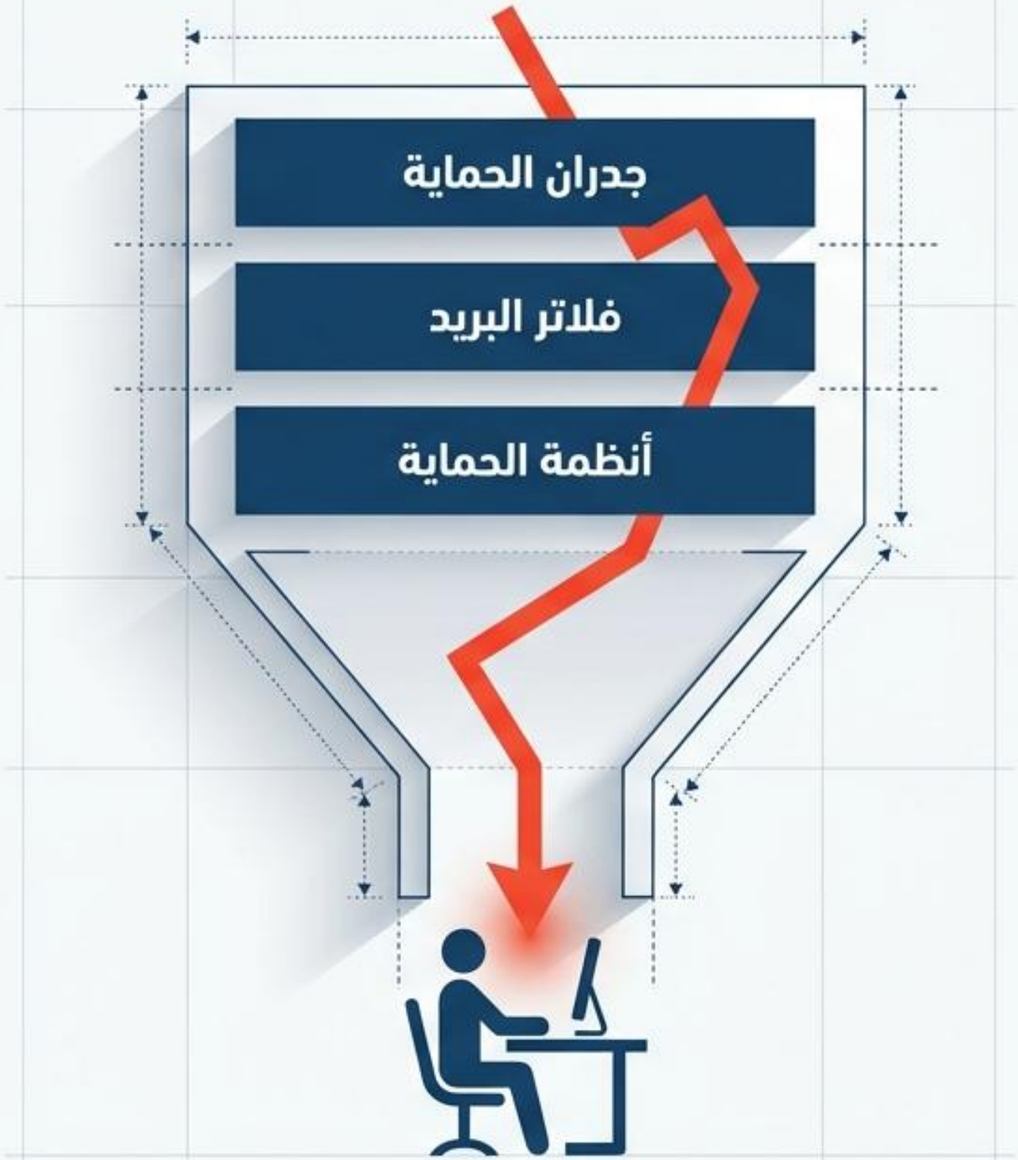


Cyber Zones MailGuard

أداة تحليل موثوقية البريد الإلكتروني

خط الدفاع الأخير ضد التصيّد الاحتيالي الإلكتروني

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool



استهداف العنصر البشري: الثغرة التي تتجاوز الأنظمة التقليدية

هجمات التصيّد الاحتيالي (Phishing) الحديثة لم تعد تعتمد حصرياً على البرمجيات الخبيثة، بل تركز على اختراق قرار المستخدم.

الموظف اليوم هو نقطة البداية لأي اختراق ناجح.

تبدأ هجمات الفدية أو الاختراقات المؤسسية برسالة بريد إلكتروني مزورة نجحت في تجاوز الأنظمة التقنية، لتستهدف قرار المستخدم وثقته مباشرة.

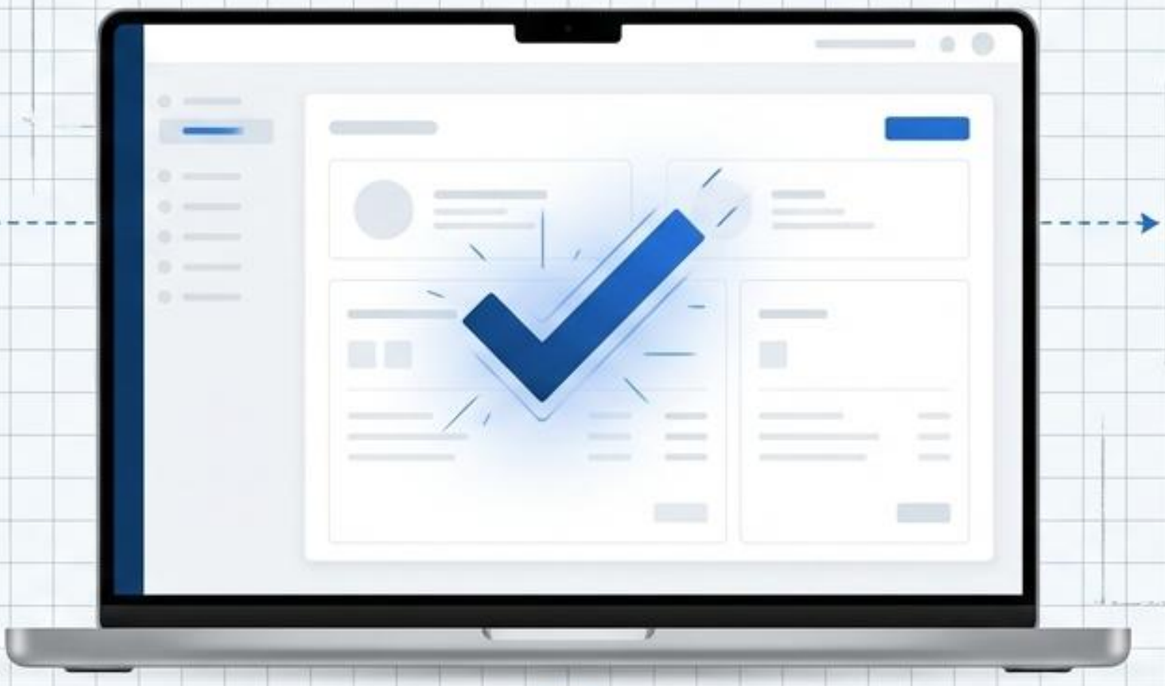
تمكين المستخدم للقرار الصحيح: Cyber Zones MailGuard

مُطورة بالكامل داخل قسم الابتكار والبحث في شركة سايبرزون.

CYBER ZONES MailGuard
Cyber Zones lightweight protection tool

أداة تحليل محلية (On-Premise)

تعمل مباشرة على جهاز المستخدم النهائي.



تمكين المستخدم

من فحص الرسائل تقنياً وسلوكياً قبل التفاعل.

تعمل كطبقة تحقق إضافية حاسمة

دون استبدال أنظمة الحماية المؤسسية.

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

المحرك التحليلي: دمج الفحص التقني بالتحليل السلوكي

تقوم الأداة بتشريح مكونات الرسالة عبر 5 طبقات متزامنة:

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

الطبقة الأولى: التحليل التقني لبنية الرسالة

- استخراج رؤوس الرسالة (Headers) وتحليل وتحليل مسار الإرسال الحقيقي المخفي.
- قراءة وتفكيك ملفات البريد بصيغتي (.eml) و (.msg).
- فحص التركيبة الفعلية للرسالة والبحث عن التناقضات، وليس فقط الاعتماد على النص الظاهر للمستخدم.
- تحليل الروابط والمرفقات في بيئة آمنة دون تشغيلها.

CYBER ZONES

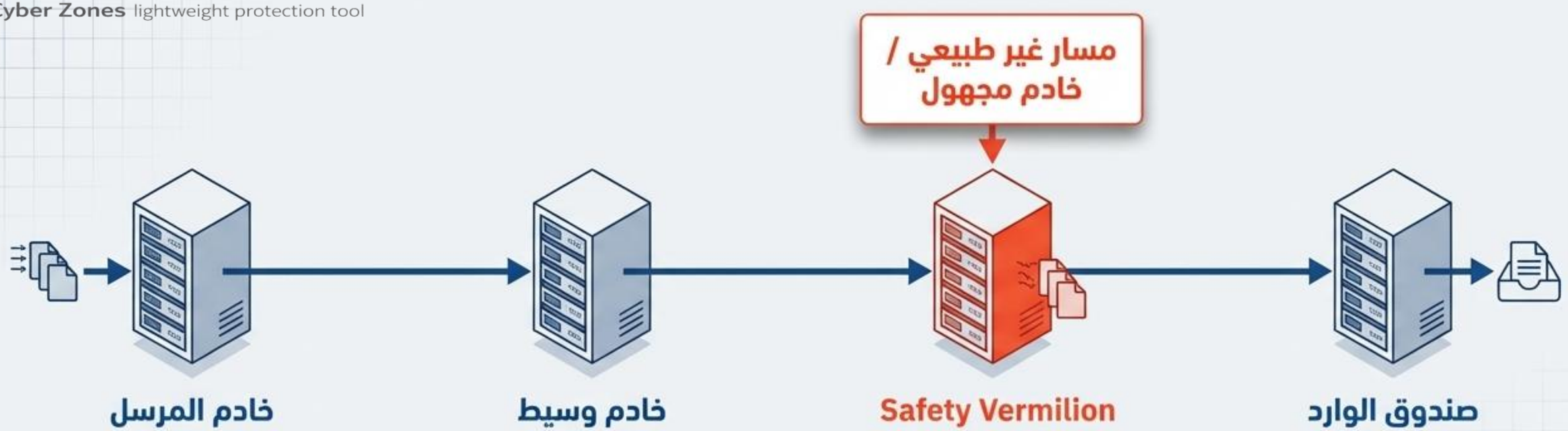
CYBER ZONES MailGuard
Cyber Zones lightweight protection tool

الطبقة الثانية: كشف انتحال الهوية ومصداقية الإرسال

- مراجعة بروتوكولات المصادقة القياسية: SPF / DKIM / DMARC.
- كشف التناقض الصارخ بين نطاقات: From, Reply-To, Return-Path.
- رصد استخدام أسماء شركات معروفة مع نطاقات مزيفة (Impersonation).
- اكتشاف النطاقات المتشابهة بصرياً والنطاقات المُنشأة حديثاً.
- تفكيك الروابط المخفية أو المموهة التي تعتمد على الهندسة الاجتماعية.

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

الطبقة الثالثة: تحليل مسار انتقال الرسالة



- تتبع دقيق لسلسلة خوادم الاستلام (Received Chain).

- اكتشاف المسارات الجغرافية أو التقنية غير الطبيعية لانتقال الرسالة.

- رصد استخدام بنية إرسال غير موثوقة أو خوادم مجهولة المصدر قبل وصول الرسالة.

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

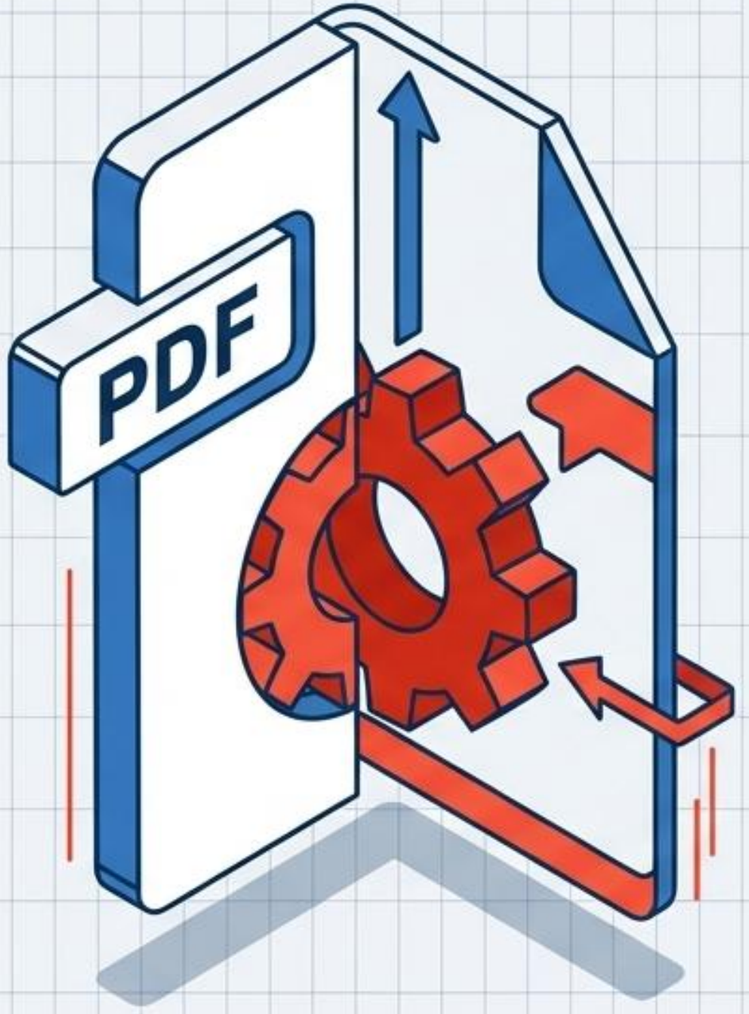
الطبقة الرابعة: التحليل السلوكي المتقدم للروابط

لا تكتفي الأداة بقوائم الحظر، بل تحلل سلوك الرابط ذاته:

- التقييم الفوري لعمر النطاق المرتبط لاكتشاف البنى التحتية المؤقتة.
- اكتشاف أساليب الترميز (Encoding) والإخفاء داخل بنية الرابط.
- رصد الروابط المبنية مباشرة على عناوين IP.
- كشف الروابط المختصرة المستخدمة حصرياً لإخفاء الوجهة النهائية.

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

الطبقة الخامسة: التوصيف الآمن للمرفقات



التحقق من نوع الملف الحقيقي من خلال **توقيعه الرقمي** وبنيته، بغض النظر عن الامتداد الظاهر (Extension).

التعرف الدقيق على **الملفات التنفيذية المخفية** داخل مرفقات تبدو آمنة.

كشف وجود **وحدات الماكرو (Macros)** الخبيثة المدمجة داخل ملفات Office.

مطابقة استخبارات التهديدات العالمية (OSINT)

تتم مقارنة المؤشرات المكتشفة محلياً مع قواعد بيانات التهديدات العامة فورياً:

رصد البنية التحتية والمخدمات التي استُخدمت سابقاً في هجمات سيبرانية.

تحديد الروابط المرتبطة بحملات تصيّد احتيالي معروفة ونشطة.

كشف مصادر الإرسال ذات السجل المعروف في إساءة الاستخدام.

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

المخرجات: دعم قرار المستخدم، وليس الاستبدال

- تعرض الأداة نتيجة نهائية واضحة وقابلة للتنفيذ مباشرة من قِبل المستخدم بمستويات خطورة خطورة محددة:
.Authentic | Suspicious | High Risk

- **شرح تقني مبسط** يوضح سبب التقييم دون إرباك الموظف.

- **توصيات عملية** وواضحة للتصرف الصحيح.

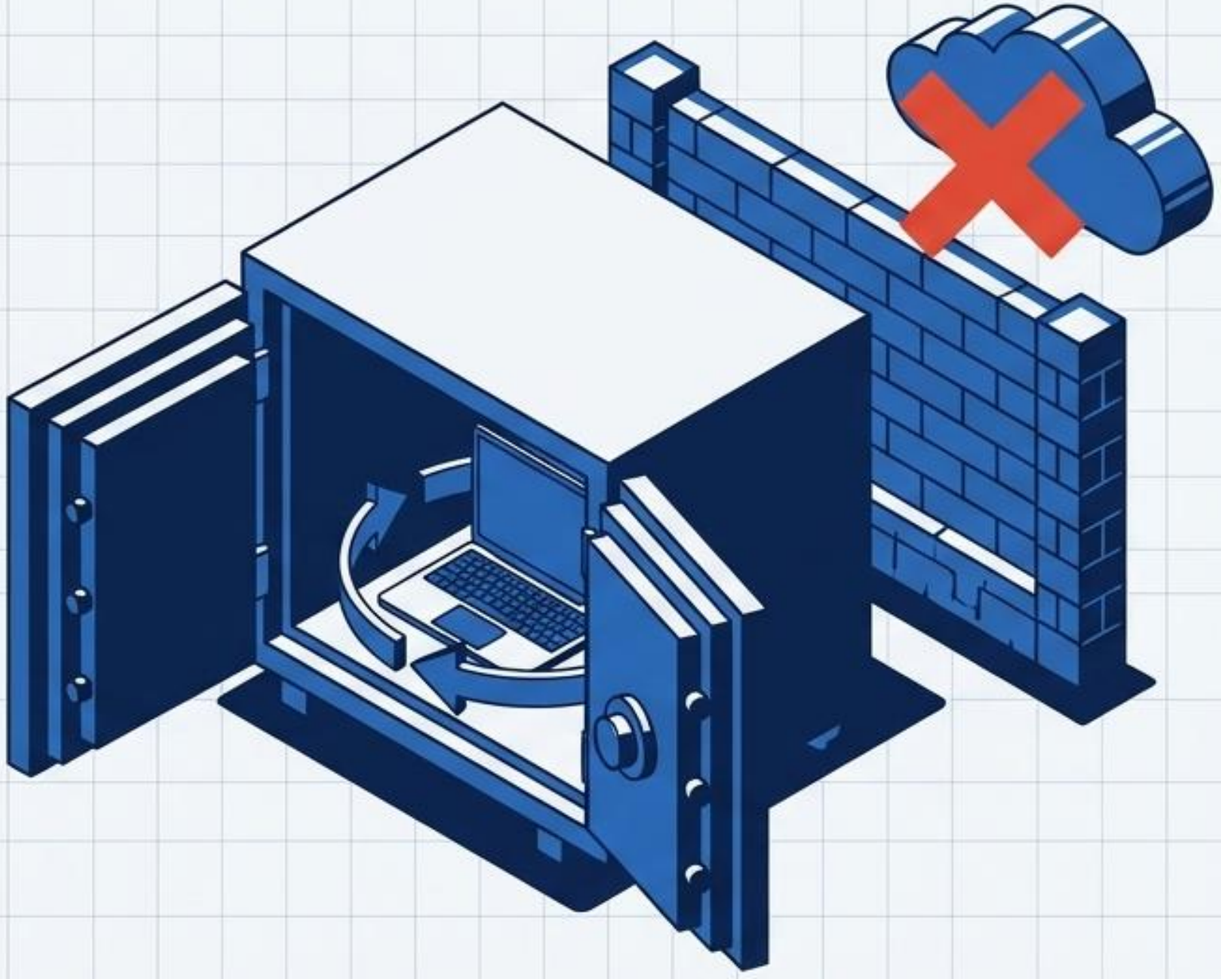
التوصيات: يرجى إبلاغ قسم أمن أمن المعلومات فوراً

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

خصوصية مطلقة | سيادة تامة على البيانات

صُممت الأداة لتعمل بالكامل داخل البيئة المعزولة للمؤسسة، وهي ملائمة تماماً للجهات الحساسة.

- لا يتم رفع الرسائل إلى أي خادم خارجي أو سحابي مطلقاً.
- لا يتم تخزين أي بيانات أو سجلات للرسائل.
- لا يتم مشاركة أي محتوى خارج جهاز المستخدم بأي شكل من الأشكال.



CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

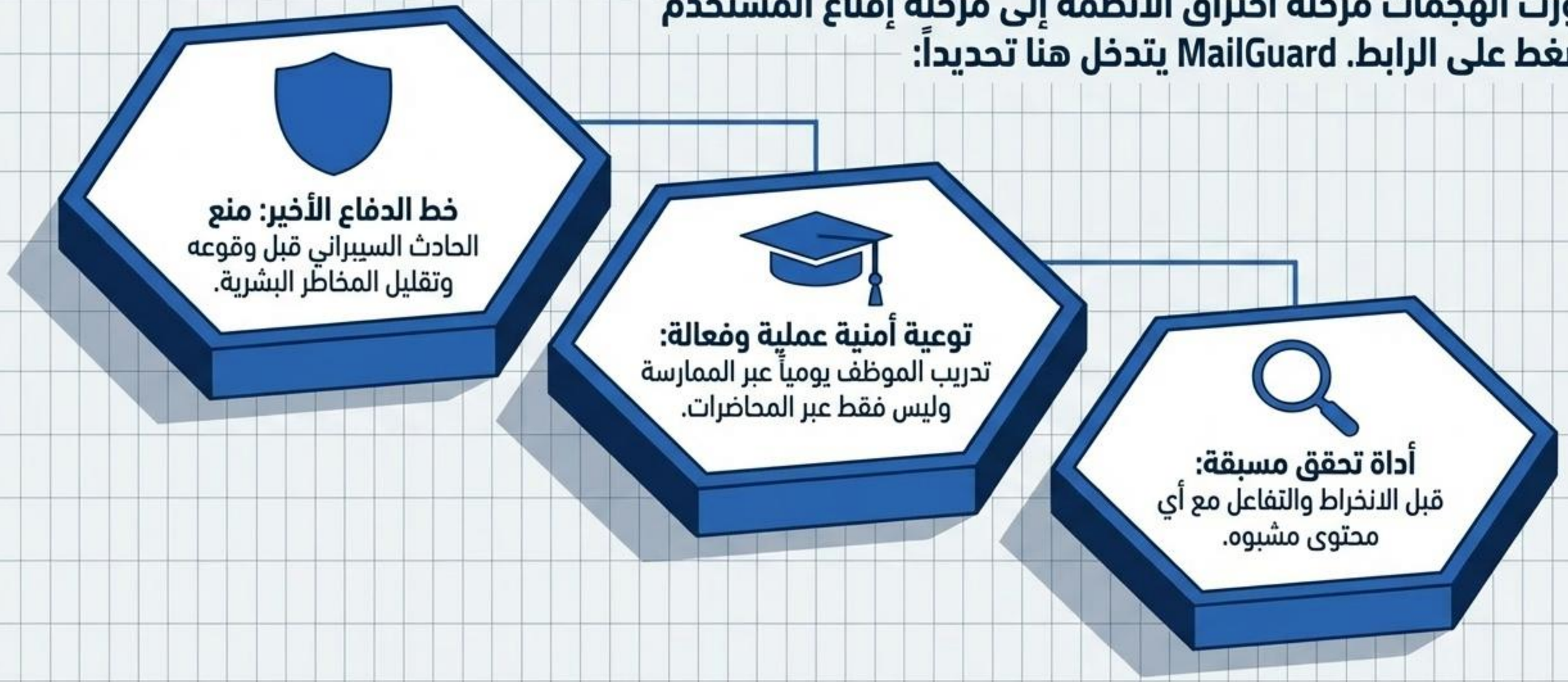
التموضع التشغيلي: ماذا تمثل أداة Cyber Zones MailGuard؟

ليس		بل	
أداة حظر أو فلترة تلقائية.	✗	طبقة تحقق مستقلة تعزز قرار المستخدم.	✓
نظام بريد إلكتروني بديل.	✗	أداة مساندة قبل التفاعل المباشر مع الرسالة.	✓
بديلاً لأنظمة الحماية المؤسسية.	✗	خط الدفاع الأخير ووسيلة لتقليل المخاطر الناتجة عن العامل البشري.	✓

CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

الأثر المؤسسي: لماذا MailGuard ضرورة حتمية اليوم؟

تجاوزت الهجمات مرحلة اختراق الأنظمة إلى مرحلة إقناع المستخدم بالضغط على الرابط. MailGuard يتدخل هنا تحديداً:



CYBER ZONES
MailGuard
Cyber Zones lightweight protection tool

رؤية سايبرزون للابتكار الاستراتيجي

تعزيز الاستخبارات المفتوحة (OSINT)	تقليل التعرض للهجمات الرقمية	بناء وعي أمني عملي يدمج الموظفين في منظومة الدفاع

ننصح بإدراج MailGuard ضمن بيئتكم التشغيلية لتعزيز سيادتكم على بياناتكم وجعل موظفيكم خط الدفاع الأول.

لتجربة الأداة واستكشاف منصات قسم الابتكار والبحث، تواصلوا معنا:
info@cyber-zones.com