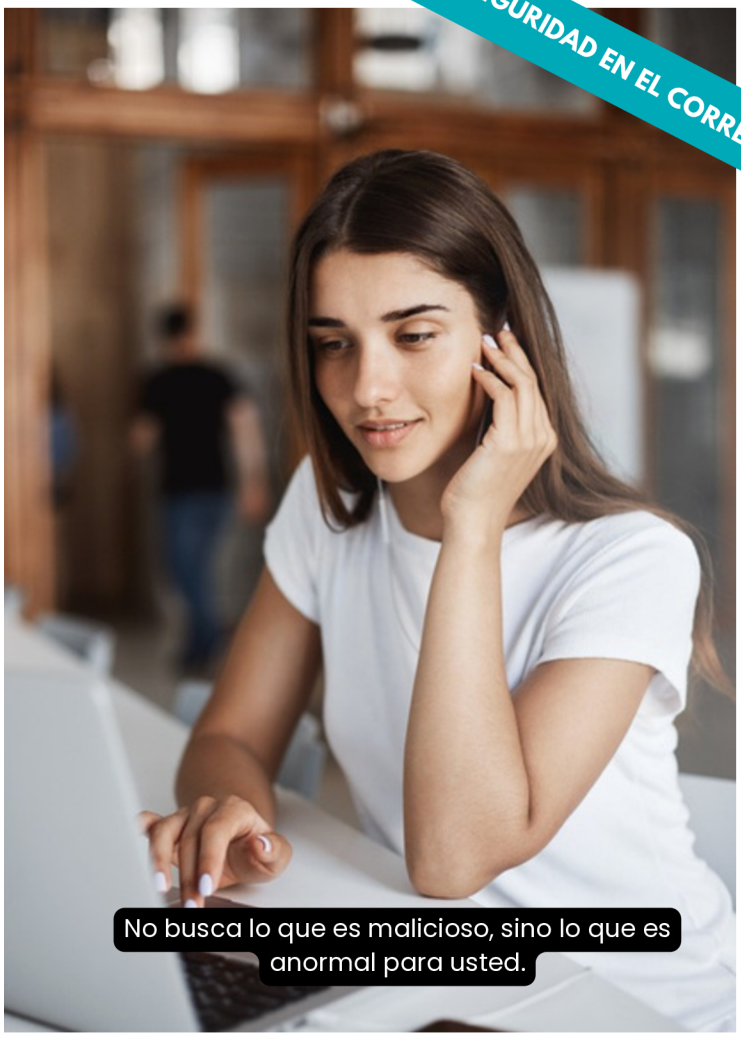
SEGURIDAD EN EL CORREO

Abnormal

Protección del Correo Electrónico Impulsada por Inteligencia Artificial

Abnormal Security es una solución de ciberseguridad que se especializa en la detección automática de ataques de día cero. Mientras las soluciones convencionales se basan en listas negras y firmas conocidas, Abnormal utiliza un enfoque revolucionario:

- **Modelo de Comportamiento Basado en IA**:
  1. Identidad Digital. Crea un modelo único para cada persona en su organización, analizando miles de puntos de datos
  2. Comportamiento normal: Estilo de escritura, patrones de comunicación, horarios, relaciones con colegas y proveedores.
  3. Contexto de la identidad: Jerarquía en la empresa, permisos, departamento, etc.



- **Análisis en Tiempo Real:** Cada email entrante es comparado contra estos modelos de comportamiento. Cualquier desviación o anomalía es detectada instantáneamente, incluso si el ataque es nuevo y nunca antes visto.

- **Protección Integral:** La plataforma identifica y bloquea automáticamente amenazas que otros sistemas pasan por alto, deteniendo el ataque antes de que llegue a la bandeja de entrada.

Abnormal AI Nombrado “Lider” en The Forrester Wave : Enterprise Email Security, Q2 2025

Estadísticas que Demuestran su Eficacia

- +90% de detección de ataques de BEC que otras soluciones pasan por alto.
- Miles de millones de dólares en pérdidas potenciales prevenidas para sus clientes.
- Reducción del >90% en el tiempo de investigación y respuesta a incidentes de correo.
- Minutos para implementar la solución, frente a horas o días de otras plataformas.

Abnormal

¿Cómo Funciona Abnormal AI?

1. Integración API Nativa

- Se conecta directamente a Microsoft 365 o Google Workspace via API
- Sin redirección de correo (sin cambios en MX records)
- Implementación en minutos sin afectar el flujo de email

2. Modelado de Comportamiento Basado en IA

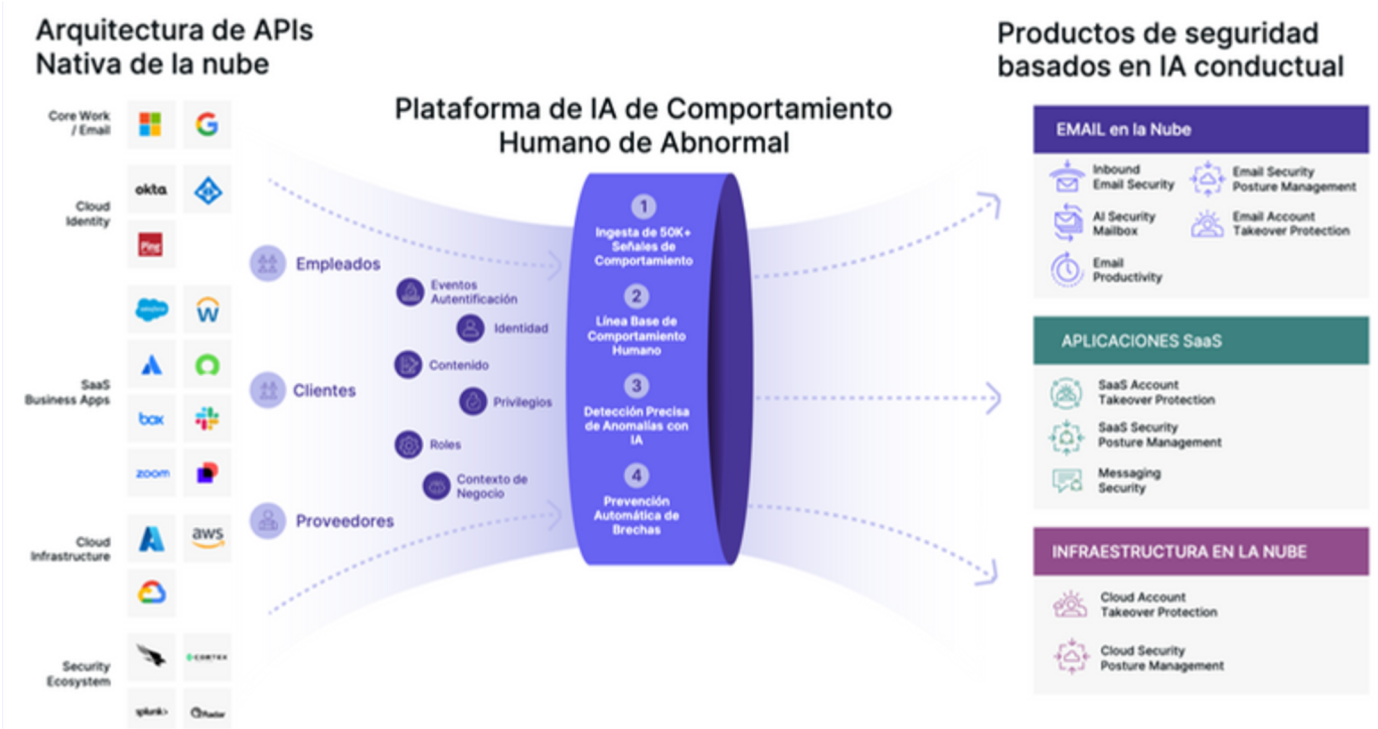
- Analiza +50,000 señales conductuales por usuario
- Crea una "Línea Base Conductual" entre Identidad, Comportamiento y Contexto:
  - Patrones de comunicación normales
  - Relaciones interdepartamentales típicas
  - Comportamiento histórico de correo
  - Dispositivos y ubicaciones habituales

3. Motor de Análisis en Tiempo Real

- Evalúa cada email contra el modelo de comportamiento establecido
- Aplica gráficos de relación entre entidades (empleados, proveedores, dominios)
- Analiza contexto organizacional y patrones transaccionales

4. Detección de Anomalías Multi-Capa

- Análisis de Identidad: Verifica desviaciones en el comportamiento del remitente
- Análisis de Relación: Detecta interacciones fuera de patrones establecidos
- Análisis de Contenido: Evalúa intención y contexto del mensaje
- Análisis de Dispositivo/Ubicación: Identifica acceso desde fuentes no habituales



5. Automatización de Respuesta

- Cuarentena automática de amenazas identificadas
- Recuperación automática de emails comprometidos
- Reversión de transacciones fraudulentas en casos de BEC

6. Plataforma Unificada de Protección

- Prevención de BEC (Business Email Compromise)
- Detección de suplantación de identidad
- Protección contra ataques a la cadena de suministro
- Defensa contra phishing y ransomware

Frente a las soluciones tradicionales, Abnormal IA correlaciona identidad, comportamiento y contexto para distinguir lo legítimo de lo malicioso

Beneficios Clave en Seguridad de Correo

- **Detecta lo Indetectable:** Detiene ataques de ingeniería social avanzada como el BEC (Business Email Compromise), suplantación de identidad de ejecutivos y ataques de cadena de suministro, que son la principal causa de pérdidas financieras.
- **Disminución de Falsos Positivos:** Al entender el comportamiento normal, prácticamente elimina los bloqueos de correos legítimos, mejorando la productividad y evitando que los equipos de TI pierdan tiempo revisando cuarentenas.
- **Automatización Total:** La IA no solo detecta, sino que responde automáticamente a los incidentes, como revertir transacciones fraudulentas en cuestión de minutos.
- **Protección Sin Configuración Compleja:** Al ser una solución basada en API, se integra en minutos con Microsoft 365 y Google Workspace, sin necesidad de cambiar flujos de correo o hardware.
- **Ahorro de Tiempo y Recursos:** Libera a los equipos de seguridad de la gestión manual de alertas, permitiéndoles enfocarse en estrategias más críticas.