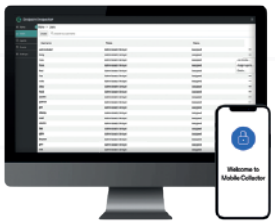
ATIPAX

CONTRAINTELIGENCIA CORPORATIVA

KAYMERA

CELULARES ENCRIPTADOS GRADO MILITAR

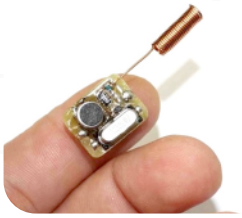
Nº 1 en el Mundo



Cellebrite ENDPOINT INSPECTOR

INTELIGENCIA E INVESTIGACIÓN ANTICORRUPCIÓN

Nº1 en el Mundo



DETECCIÓN DE DISPOSITIVOS ESPÍA

Incluye GPS de rastreo

CONSULTORÍAS EN SEGURIDAD DIGITAL

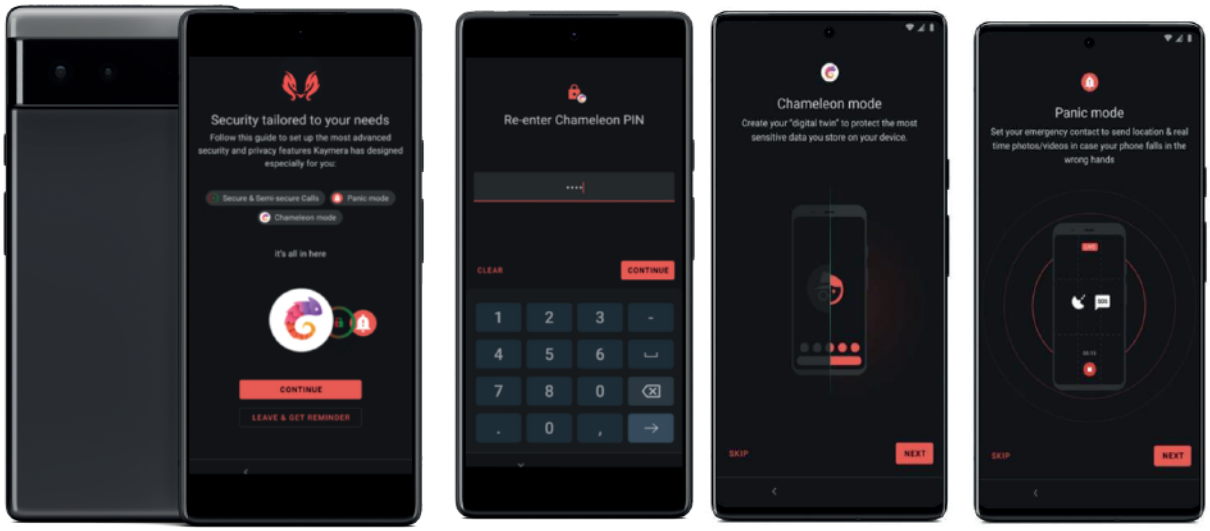
Modelos Integrales

EQUIPAMIENTO Y SOLUCIONES PARA CONTRAINTELIGENCIA Y SEGURIDAD DIGITAL

KAYMERA

CELULAR TOTALMENTE ENCRIPTADO

Desarrollado por Kaymera, el dispositivo se basa en el SO Kaymera, un sistema operativo altamente seguro, construido desde la base para maximizar la protección del dispositivo con los más altos estándares de usabilidad que proporciona la plataforma Android de serie.



Kaymera es una empresa de ciberseguridad, centrada en la seguridad del ecosistema Android a través del sistema operativo, las herramientas para desarrolladores y las aplicaciones. Creada para gobiernos, empresas y particulares.

Las amenazas a la seguridad en cifras

+21M
Muestras de malware para móviles en 2021

< 41%
Violaciones de datos causadas por dispositivos robados y perdidos

$32M
Costo medio de la filtración de datos en las empresas

206 d
Promedio de días para identificar una filtración

Privacidad e integridad de los datos

El dispositivo proporciona seguridad por capas frente a todos los vectores de ataque conocidos, entre ellos:

Interceptación de red: VPN encriptada siempre activa protege todas las comunicaciones de voz, SMS e Internet.

WIFI: protegido contra interceptación, manipulación de datos e infección.

Caballos de Troya (APTs) y ataques de Malware: política de control de permisos total sobre SO reforzado.

Ataques de hombre en el medio: sólido mecanismo de cifrado impide que terceros intercepten las llamadas a través de LTE o WIFI.

Ataques al cargador de arranque: El cargador de arranque seguro defiende de los ataques contra el cargador de arranque o las primeras fases del proceso decarga del SO.

Extracción de datos físicos: La tecnología de templado de puertos / USB supervisa los puertos físicos del teléfono, interviene en los eventos de E/S y notifica al usuario si se realiza una operación sensible (no de carga).

Protección contra la Interceptación de la Cámara y el Micrófono: Los detectores y sensores de E/S proporcionan protección en tiempo real para impedir que cualquier forma de malware se ejecute en el dispositivo.

VAULT - GESTIÓN DE DISPOSITIVOS MÓVILES (MDM) KAYMERA

La Vault Kaymera permite al equipo de TI y de Seguridad tener un control total sobre el entorno móvil del usuario final con fines de seguridad móvil. El objetivo principal de la Vault es mantener el control, la visibilidad y mitigar el riesgo de error humano mediante la vigilancia y la aplicación de las políticas de Configuración, Aplicación y Seguridad que se utilizan en el conjunto de dispositivos.

Dashboard - Vista de la organización

Dispositivos - Gestiona y visualiza todos los dispositivos de la organización

Políticas - Crea y gestiona políticas de configuración

OTA - Carga una nueva versión de firmware y gestiona las versiones

Aplicaciones - Crear y gestionar políticas de perfil de aplicación (permisos)

Grupos de mensajes - Crea y gestiona los mensajes del grupo Admin

SKRYPT- PLATAFORMA DE MENSAJERÍA DIGITAL

Nuestro sistema de mensajería cuenta con el cifrado de grado militar de Kaymera y características de seguridad integradas para permitir comunicaciones seguras de mensajería instantánea y VoIP a través de Internet público.

Crea normas de comunicación seguras para tu organización:

Autenticación segura de usuarios con certificados TLS

Cifrado de extremo a extremo para llamadas de audio y video con ZRTP

Cifrado de extremo a extremo para mensajes instantáneos en conversaciones individuales y grupales

Desplegable en varios servidores para escalabilidad y alta disponibilidad

En sitio o en la nube

Integrado con sistemas de notificaciones push para no perder ninguna llamada en iOS o Android

Servicios de instalación y soporte disponibles

Plataforma de Seguridad Móvil 360°

Protección total

El potente motor de detección y prevención de amenazas móviles equipa a las organizaciones con una solución de seguridad a prueba de balas para proteger todos los puntos potenciales de ataque: dispositivos, aplicaciones, transferencia de datos y más.

Excelente usabilidad

Proporcionamos confidencialidad personal y protección de los datos empresariales a todos los puntos finales móviles de tu organización, permitiendo a los empleados trabajar de la manera que deseen sin que la experiencia del usuario se vea afectada.

Visibilidad total del riesgo

Identifica los riesgos no deseados y haz frente a las amenazas a medida que surgen. Nuestro motor de aprendizaje automático devuelve a tus manos el control sobre tu postura de seguridad. Mantente informado, gestiona los usuarios, las licencias, los dispositivos y haz frente a las amenazas.

Integración perfecta

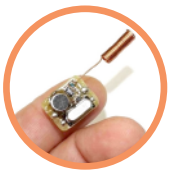
La avanzada tecnología de seguridad móvil incorporada en todos los módulos de Kaymera se integra de forma nativa con aplicaciones de software especializadas: desde soluciones de Dev hasta HelpDesk. Fácil de configurar, mantener y gestionar.

LIMPIEZA ELECTRÓNICA

La limpieza electrónica es la contramedida de seguridad más importante para las insitituciones. Este método se utiliza para la detección de micrófonos ocultos y escuchas, detección de cámaras ocultas, y localización de todo tipo de dispositivos para el espionaje de instituciones y sus funcionarios.

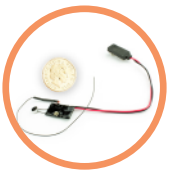
El procedimiento se realiza en oficinas, salas de directorio, vehículos, domicilio, etc. Además de la inspección con aparatos electrónicos, es necesario e imprescindible una inspección manual y ocular pormenorizada de toda la zona.

¿Qué se detecta con una Limpieza Electrónica?



Micrófonos Ocultos
Micrófonos activos, pasivos y desactivados

Cámaras Ocultas
Cámaras espía y microcámaras



Transmisores Telefónicos
Escuchas telefónicas en teléfonos y líneas fijas

Micrófonos Digitales
Frecuencias Bluetooth, Wifi, FHSS, Burst, etc.

Balizas GPS
Localizadores de seguimiento

Micrófonos de Red
Tecnología móvil GSM, 3G, 4G y 5G

Si se pregunta cuándo es necesario realizar una limpieza electrónica, piense en la prevención, en la máxima confidencialidad de sus reuniones ante una posible intromisión.

Antes de una reunión delicada o cuando sospeche que sus comunicaciones están comprometidas, contáctenos y solicite un presupuesto para el servicio.

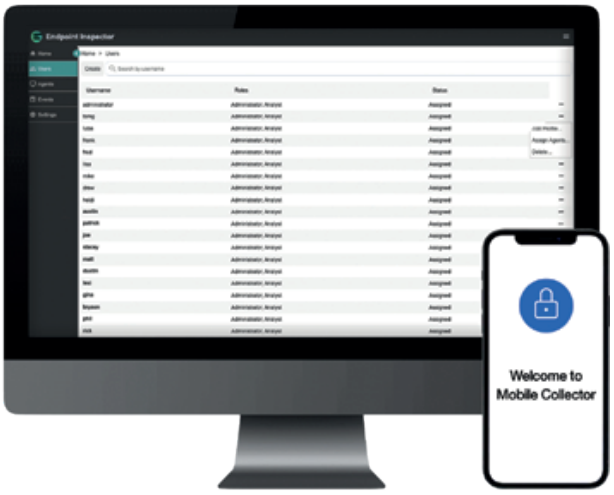
Cellebrite
ENDPOINT INSPECTOR

INTELIGENCIA E INVESTIGACIÓN CORPORATIVA

Esta solución líder en el mercado para el análisis rápido y exhaustivo de datos de dispositivos ayuda a los examinadores forenses y analistas a arrojar luz y obtener información sobre la actividad de un usuario. Busca, filtra y examina fácilmente grandes conjuntos de datos, que incluyen historial de internet, descargas, búsquedas recientes, sitios principales, ubicaciones, medios, mensajes y más.

Con Endpoint Inspector podrá acceder a los puntos finales (computadoras, tablets, celulares) de forma segura, en cualquier momento y en cualquier lugar: Endpoint Inspector permite la recopilación, análisis selectivo y remoto de datos de aplicaciones de iOS, Android, Mac, Windows y la nube a través de la red corporativa, para brindarle control de la información crítica. Haciéndolo posible desde el punto de vista legal al simplificar la recopilación de datos a información específica.

Funcionalidades



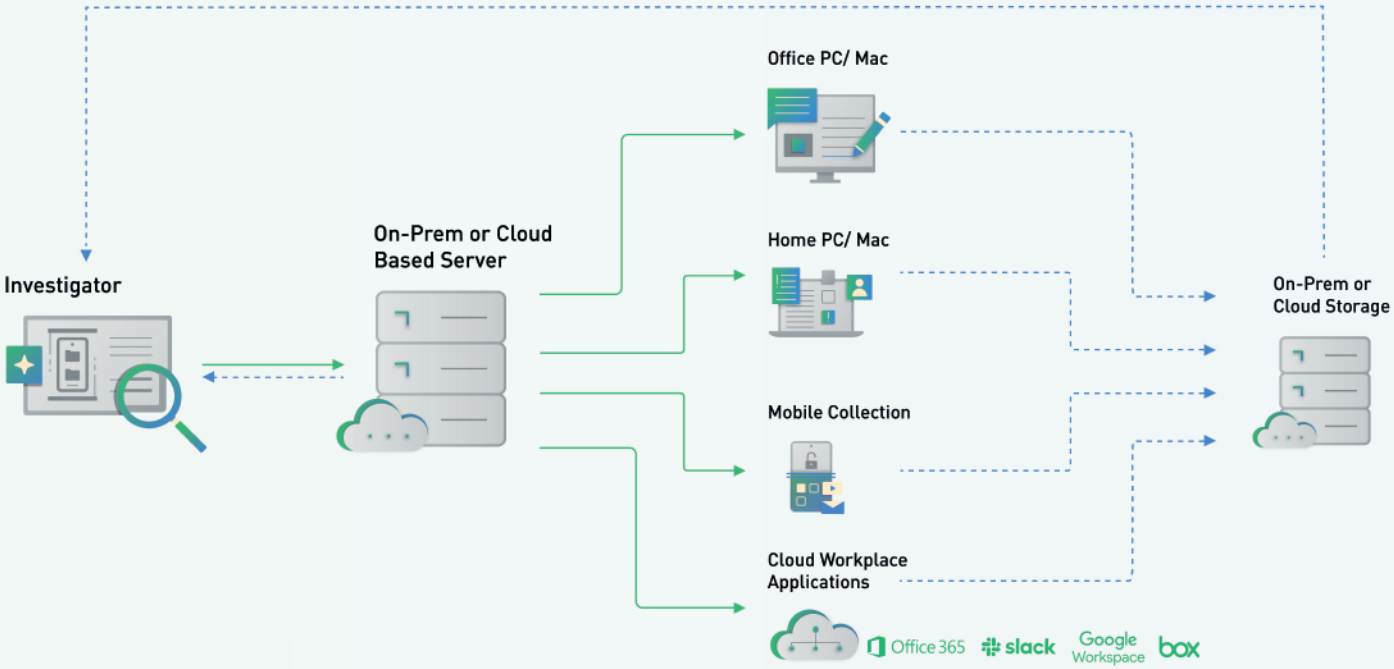
Crear y definir colecciones específicas de computadoras remotas, dispositivos móviles remotos y de aplicaciones de trabajo en la nube compatibles como Office365, Google Workspace, Slack y Box.

Recopilar fácilmente solo lo que se necesita de los dispositivos finales y las aplicaciones de trabajo en la nube sin que los empleados tengan que entregar su dispositivo, lo que ahorra tiempo y dinero valiosos a su organización.

Acceder a una única fuente para la recopilación de aplicaciones de trabajo en la nube sin tener que iniciar sesión en cada aplicación y extraer todos los datos de múltiples fuentes para cada empleado.

Autenticar el proceso de recopilación con un código QR en lugar de las credenciales del usuario para WhatsApp.

Un panel intuitivo proporciona una vista en tiempo real de los usuarios, el estado del agente, las tareas de recopilación de computadoras, dispositivos móviles, aplicaciones en la nube y aplicaciones de trabajo en la nube, y los eventos de aplicaciones.



Recopilación y análisis selectivos, de forma remota y segura, de datos de iOS, Android, Mac, Windows y aplicaciones de trabajo en la nube a través de la red de una organización, para brindarte los conocimientos críticos que necesitas.

Capacidades clave

• Recopile y analice archivos de iOS, Android, Mac, Windows y aplicaciones de trabajo en la nube de forma remota.

• Llevar a cabo varias investigaciones independientes a la vez.

• Recolecciones lógicas avanzadas incluyen datos de chat de terceros, SMS, mensajería instantánea, imágenes, videos, audio, datos del navegador, calendario, registros de llamadas y contactos.

• Recopile registros de aplicaciones para ver qué se instaló y cuándo se accedió.

• Los administradores pueden gestionar usuarios y autorizar fácilmente niveles específicos de permisos para gestionar colecciones de forma segura.

• Proporcione administración y permisos de usuarios, y realice auditorías a través de un servidor en línea.

• Obtenga una vista previa y evalúe los archivos en computadoras remotas en vivo para determinar la relevancia de los sistemas.

• Conéctese y recopile simultáneamente desde varias máquinas.

CONSULTORÍAS ESPECIALIZADAS EN SEGURIDAD Y PROTECCIÓN

Nuestras consultorías especializadas son parte de un Servicio Integral que permite a nuestros clientes tomar la decisión más adecuada.

Analizamos las vulnerabilidades y carencias que en materia de seguridad y prevención de amenazas digitales que pudiera tener una empresa o persona VIP en sus actividades, ya sea en el ámbito nacional como internacional.

Ayudamos al diseño de un adecuado Modelo de Prevención y Detección de Delitos; proporcionamos guías y características principales de medidas, para que la compañía o persona las pueda implementar.

Elementos de nuestro Modelo de Prevención:

- Mapa de riesgos, identificando actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.
- Protocolos de acción preventiva y reactiva frente a la detección de delitos.
- Asignación de recursos financieros.
- Sistema disciplinario de contramedidas, prevención y detección.

Trabajamos y comercializamos Bolsas Faraday para el bloqueo de señales de telefonía móvil, Wi-Fi, Bluetooth, GPS, RFID y frecuencias de radio.

ATIPAX

CONTRAINTELIGENCIA CORPORATIVA

WWW.ATIPAX-PERU.COM

VENTAS@ATIPAX-PERU.COM

997555758

987576068

EQUIPAMIENTO Y SOLUCIONES
PARA CONTRAINTELIGENCIA
Y SEGURIDAD DIGITAL