Fortkern

CIBERSEGURIDAD GENERAL Y AUTÓNOMA

Que nada crítico ocurra sin prueba.



Defensa con inteligencia artificial, a velocidad de máquina, para gobiernos, banca, infraestructura crítica, empresas, sitios web, personas, la inteligencia artificial y el mundo cripto.

Diseñada para estar entre los sistemas de defensa más avanzados del mundo. El objetivo es que una llave, una sesión o una credencial robadas dejen de bastar para causar daño.

CONFIDENCIAL

Hoy una falla se explota antes de que exista el parche.

Ventana de exposición entre la primera explotación y la instalación del parche. La escala muestra plazos orientativos.

–7 días

Ya se está explotando.

Día 0

La falla se hace pública.

+30 a 60 días

Parche instalado.

<24 h

Entre el descubrimiento de una falla y su explotación activa, con la IA acelerando al atacante, según Microsoft Digital Defense Report 2026.

–7 días

Tiempo medio hasta la explotación según Mandiant, M-Trends 2026. El ataque llega antes que el parche.

2.760

Víctimas de ransomware en un solo trimestre de 2026. Récord histórico según GuidePoint GRIT.

Objetivo de Fortkern: protección activa en horas, sin esperar al parche, e investigación propia de fallas. Fuentes citadas en la diapositiva 40.

Las defensas actuales miran el síntoma desde fuera.

Fortkern busca impedir que nazca la operación maliciosa, que se ejecute el malware o que una llave robada baste para firmar.

Defensa tradicional · sistema protegido

Vigila desde fuera. Alerta cuando el daño ya empezó y espera a que una persona actúe.

Fortkern · sistema protegido

Por diseño, actúa desde dentro para neutralizar el ataque en el punto donde nace.

Talento escaso

Las defensas dependen de especialistas. El material de referencia cifra el déficit mundial en millones.

Ataques que cambian

Las defensas estáticas se enfrentan a atacantes que cambian en tiempo real con IA.

El punto donde nace el daño

El equipo que firma, valida u opera necesita protección.

Un sistema de defensa que actúa, aprende y se recupera solo.

Una suite integral de ciberseguridad autónoma concebida para proteger, desde un solo sistema, todo lo que una institución no puede permitirse perder.

- **Actúa** — En segundos, sin esperar a un analista.
- **Aprende** — De cada ataque. El diseño prevé compartir esa inmunidad con toda la red de clientes, sin exponer sus datos.
- **Se recupera** — Y se autosana.

Ámbitos previstos: gobierno, banca, infraestructura crítica, empresas, servidores, redes, sitios web y APIs, inteligencia artificial, industria, pymes, personas y cripto.



Seis capacidades de diseño en un solo sistema.

Fortkern está diseñado para estar entre los sistemas de defensa más avanzados. La comparación con otras plataformas requiere métricas publicadas y evaluaciones independientes.

01

Prueba antes de actuar

Dieciséis aplicaciones de un mismo principio. Firmar, pagar, administrar, cambiar una red vital o un registro, o dispensar efectivo exige un origen íntegro demostrado.

02

IA con garantías matemáticas

Un ejército de agentes que propone y un núcleo verificable que decide. El objetivo es comprobar las contramedidas antes de activarlas.

03

Diseñado para la red en crisis

Operar aislado durante semanas, reconstruirse desde cero con tiempos de recuperación demostrables y proteger la hora y los registros.

04

Defensa en todas las capas

Del firmware a la web, de la identidad a la IA, del equipo industrial a la billetera personal, con un mismo núcleo.

05

Velocidad de máquina

Reflejo en milisegundos, contramedidas en horas sin esperar al parche y freno activo a los atacantes que son agentes de IA.

06

Inmunidad colectiva soberana

Que lo aprendido en un cliente proteja a todos en minutos sin exponer datos, y que el sistema pueda funcionar entero dentro de un país.

Objetivos de diseño. El prototipo de laboratorio cubre el motor de reglas con eventos simulados y la lógica del Guardián.

Lo que hace, explicado por resultados.

Resultados previstos para la suite completa.

01

Defensa autónoma en el equipo

Detectar y neutralizar ataques donde ocurren, en segundos, sin intervención humana.

02

Contramedidas antes del parche

Proteger frente a una falla nueva en horas, sin reiniciar ni detener el servicio. Investigar fallas para anticipar la protección.

03

Antimalware de dos velocidades

Bloqueo en milisegundos y análisis e inmunización de toda la flota en segundos, incluido el malware dirigido por IA.

04

Firma con Prueba de Integridad

Impedir que una llave robada baste para mover fondos o autorizar operaciones críticas. La lógica del Guardián se demuestra en software.

05

Inmunidad colectiva

Cuando un cliente sufra un ataque nuevo, proteger a los demás en minutos sin compartir datos privados.

06

Recuperación y autosanación

Investigar automáticamente, revertir el daño y guiar la recuperación desde el propio sistema.

Firma con Prueba de Integridad

El diseño exige dos comprobaciones antes de firmar: la integridad del equipo y el cumplimiento de las reglas de la operación. Así, una llave robada dejaría de ser suficiente para mover fondos.

Operación legítima

Sistema íntegro, dentro de las reglas.

Atacante con la llave robada

Intenta firmar una operación.

Guardián de Fortkern

Prueba de integridad: ¿el sistema que firma está íntegro?

Reglas de la operación: ¿la operación respeta las reglas?

Sin ambas pruebas no hay firma

Operación firmada

Procede con normalidad.

Firma denegada

Los fondos no se mueven.

Primera de dieciséis aplicaciones. En la demo, el Guardián verifica una declaración de integridad firmada en software y firma operaciones de prueba. La medición en hardware y la integración con custodia están previstas.

Una sola idea para proteger fondos, pagos, actos de gobierno, redes vitales, registros, la hora y la web.

Prueba de Integridad. El origen demuestra que está íntegro en ese instante. Dieciséis aplicaciones propuestas y un solo principio.

Firma	Fondos y operaciones críticas.
Credencial	Accesos de máquinas y agentes.
Pago	Órdenes bancarias y reservas.
Acto	Acciones privilegiadas de Estado.
Mando	Equipos industriales y médicos.
Cambio	Redes vitales: nada de golpe.
Carga	Logística y transporte.
Contratación	Personal remoto verificado.



Código	Scripts de terceros en la web.
Interfaz	La página que ve el usuario.
Dirección	Direcciones de cobro.
Dato	Lo robado no se puede leer.
Registro	Registros oficiales y saldos.
Tiempo	La hora de bancos y redes.
Dispensa	Cajeros automáticos.
Baja	Accesos cerrados al salir.

Robar la llave, la credencial o el acceso debe dejar de ser suficiente. Solo la aplicación de firma cuenta hoy con código de laboratorio.

Un ejército de agentes con autoridad limitada.

La inteligencia propone. Un núcleo verificable decide. En esta arquitectura prevista, aunque engañen a un agente, su propuesta debe superar controles independientes.

Agentes de IA

Vigilan, analizan y proponen contramedidas.

Núcleo verificable

Comprueba la autoridad del agente y la política legítima antes de cada acción.

Una persona decide lo irreversible

La autorización humana precede a una acción irreversible.

Acción autorizada

Se ejecuta y queda un registro inviolable y explicable.

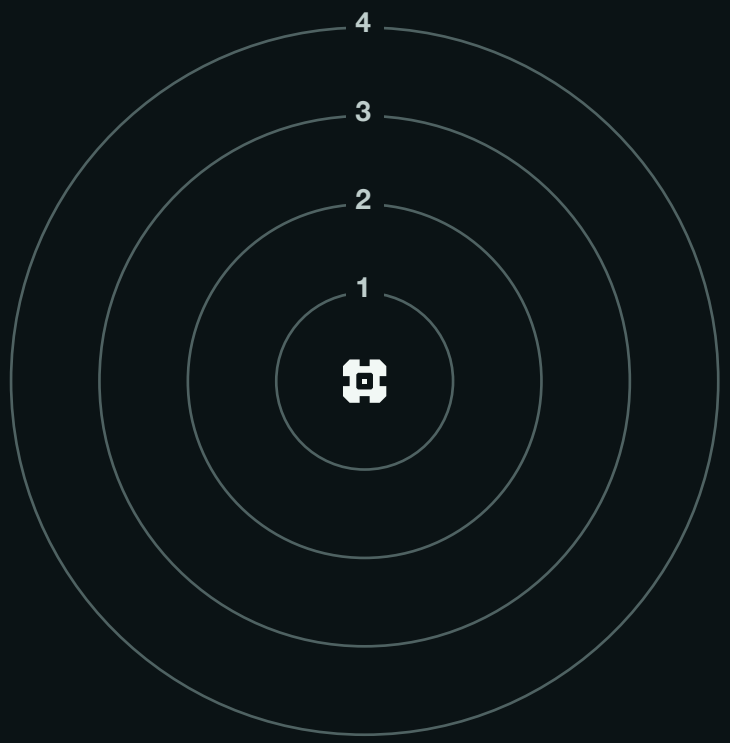
Propuesta descartada

El agente se aísla si no puede demostrar su integridad.

El peor escenario de un sistema autónomo es que un atacante lo secuestre. El diseño de Fortkern busca mantener a cada agente dentro de su autoridad.

Un defensor que también se defiende a sí mismo.

Quien comprometa al guardián compromete todo lo que protege. Fortkern se trata a sí mismo como el activo más crítico de la red. Cuatro anillos de protección previstos.



ANILLO 1

El agente

No puede ser detenido ni alterado sin autorización legítima. Se verifica y se restaura solo.

ANILLO 2

La entrega

Ninguna actualización ni licencia sale con una sola aprobación.

ANILLO 3

La inteligencia

Modelos protegidos contra el robo y contra la manipulación de lo que aprenden.

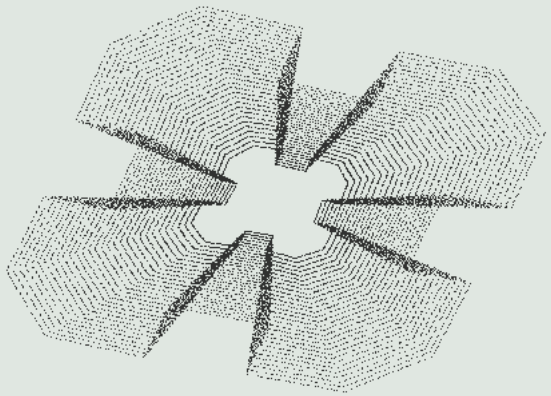
ANILLO 4

El silencio es alarma

Si Fortkern calla en un equipo, el resto lo trata como un ataque en curso.

Defensa en todas las capas y en todo el ciclo.

Un atacante necesita una sola capa sin vigilar. Fortkern está diseñado para cubrirlas desde un único sistema que comparte lo que ve entre todas.

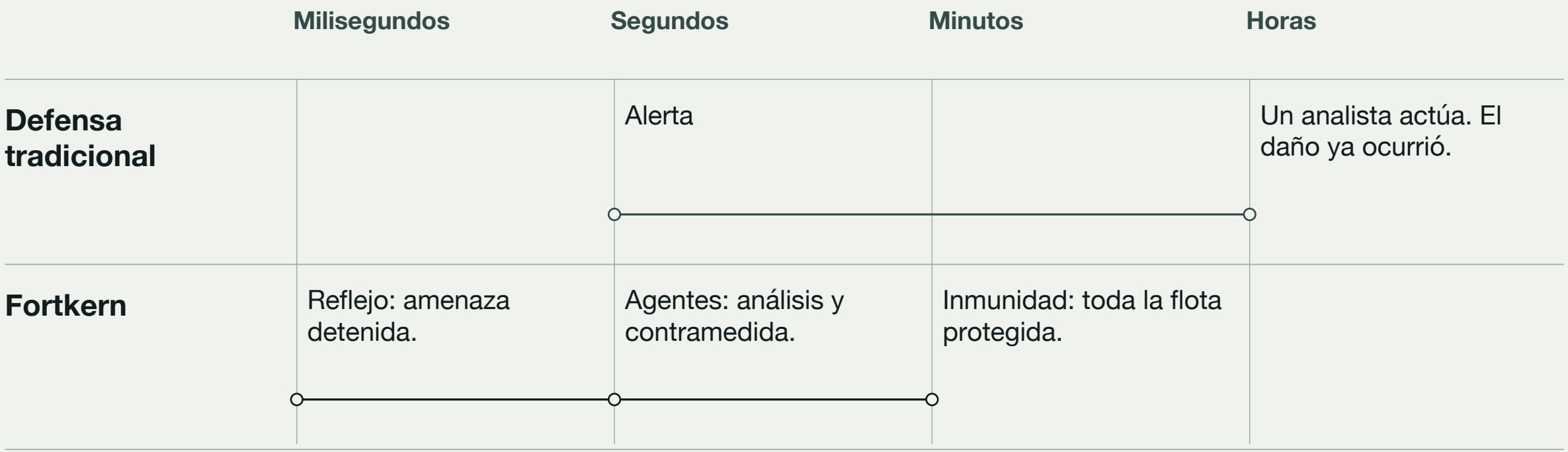


Humana	Ingeniería social, suplantación y deepfakes.
Identidad	Credenciales de personas y de máquinas.
Web y APIs	Scripts de terceros, bots, dominio y datos.
Red	Secuestro de rutas, aislamiento y conectividad.
Equipo	Malware, fallas nuevas, firmware y arranque.
Datos	Registros, saldos, la hora y lo robado.
IA	Modelos, agentes y fuga de datos.

Prevenir: contramedidas antes del parche y antes de ejecutar la operación. Detener: bloqueo autónomo en segundos con niveles de intervención configurables. Recuperar: investigación, reversión del daño y autosanación.

Cuando el atacante es un algoritmo, la defensa debe ser más rápida.

Secuencia ilustrativa. Los tiempos de Fortkern son objetivos de diseño.



Velocidad uno, milisegundos: el reflejo detendría el proceso al detectar un comportamiento amenazante, sin depender de firmas conocidas.
Velocidad dos, segundos: los agentes analizarían, aislarían y fabricarían una contramedida para proteger a la flota de toda esa familia de malware.

La misma idea, llevada a toda credencial.

Según SpyCloud 2026, las credenciales de máquina comprometidas fueron la principal vía de entrada en el 31 % de las organizaciones, casi el doble que el phishing. Incluyen claves de servicios, accesos automáticos y credenciales de agentes de IA.

95 % Cree tenerlas bajo control.

36 % Las vigila.

Credencial con Prueba de Integridad

Acceso concedido
Usada desde un equipo íntegro.

Acceso denegado
Robada y usada desde otro lugar: no sirve.

Diseño previsto: inventario completo, cada identidad con responsable. Las credenciales expuestas se detectarían y se renovarían solas.

No intentamos reconocer la cara falsa. Exigimos la prueba verdadera.

El material de referencia describe la clonación de una voz con tres segundos de audio y la posibilidad de una videollamada enteramente sintética. Detectar la falsificación es una carrera que se pierde. Fortkern propone proteger la orden.

Directivo real

Da la orden por llamada.

Suplantador con voz clonada

La imitación puede ser perfecta.

→

Orden con prueba

Identidad verificada desde su propio equipo íntegro.

Segundo canal con aprobación independiente.

→

La orden se ejecuta

Pago o cambio autorizado.

La orden no pasa

El dinero no sale.

No se juzga la cara. Se exige la prueba. Flujo previsto en el diseño.

Cuando el proveedor de confianza sirve el código malicioso, confiar en el dominio ya no basta.

Según el caso recogido en la presentación original, el 16 de noviembre de 2026 llegó código malicioso a los visitantes de 178 organizaciones de primer nivel a través de un proveedor legítimo. Fortkern está diseñado para que solo se ejecute el código aprobado y para proteger el dominio, las cuentas y cada dato detrás de las APIs.



Dominio	Guardia de dominio y del registrador.
Página y scripts	Código con Prueba. Solo versiones aprobadas.
Inicio de sesión	Cuentas y bots, agentes de IA verificados.
APIs y datos	Cada dato, solo para su dueño.

Para el visitante y en crisis · Interfaz con Prueba · Inmunidad colectiva de terceros · Modo estático de emergencia

Adoptar inteligencia artificial sin filtrar datos ni incumplir la ley.

Diseño para salud, finanzas y sector público. Bloqueo y evidencia en un mismo sistema, dentro de la red de la institución.

Personas y agentes de la institución

Origen de las interacciones.

→

Fortkern IA

Descubre toda la IA en uso. Filtra los datos sensibles. Comprueba cada acción sensible. Registro inviolable con evidencia lista para el auditor y el regulador.

→

Modelos y servicios de IA internos y externos

Solo lo permitido. Datos sensibles bloqueados.

39,7 %

de las interacciones con IA incluyen datos sensibles.

1 de 5

organizaciones sufrió una brecha por IA no autorizada.

63 %

de las organizaciones afectadas carecía de una política de gobierno de IA.

Fuentes citadas: Cyberhaven e IBM, Cost of a Data Breach 2025.

Debajo del sistema operativo y más allá de la oficina.

Firmware y arranque

Comprueba que cada equipo arrancó con el firmware aprobado y vigila los controladores de gestión remota de los servidores. Un equipo que no lo demuestra pierde la confianza para firmar, pagar o administrar.

Equipos conectados y energía

Refrigeración, climatización, inversores solares, cargadores y drones. Un valor físicamente peligroso se rechaza aunque llegue por el portal oficial, y una orden a miles de equipos exige varias aprobaciones.

Fábricas de IA

Verifica que el modelo en ejecución es la versión aprobada y protege los clústeres de cómputo frente al robo de modelos, la manipulación y el uso no autorizado.

1,3 M

de decodificadores certificados con una puerta trasera de fábrica.

9

países con supermercados cuyos equipos de frío se alteraron a distancia.

100 %

de las víctimas de un bootkit de 2026 tenía Windows actualizado. El bootkit eludió el arranque seguro.

Casos citados: Google, SecurityWeek e Infosecurity Magazine, y Kaspersky vía BleepingComputer (2026).

La protección que hoy solo tienen las instituciones, en el bolsillo de cualquiera.

01

Escudo anti-estafas

Avisa si alguien te hace instalar un acceso remoto durante una llamada y detecta falsas inversiones y falsos bancos o gobiernos.

02

Guardia de número

Si alguien traslada tu número a otra SIM, las transferencias y recuperaciones de cuenta esperan.

03

Modo protector

Para personas mayores, una persona de confianza recibe aviso antes de un pago inusual.

04

Guardián personal

Una segunda firma para tu billetera que solo se da si el teléfono o la laptop están íntegros.

05

Firma en lenguaje llano

«Vas a dar permiso a un desconocido para llevarse todos tus fondos». Antes de firmar.

06

Escudo de tokens

Antes de comprar, ¿se puede vender?, ¿quién lo creó?, ¿puede retirar la liquidez?

Según el informe 2025 del FBI IC3, solo en Estados Unidos se perdieron 8.600 millones de dólares en fraudes de inversión en 2025. El diseño incluye un botón de pánico para coordinar la congelación con los exchanges en minutos.

Seguridad de nivel institucional para el negocio que no tiene a nadie de sistemas.

01

Lista en minutos

Instalación guiada, sin consola técnica. En la primera hora revisa contraseñas, doble factor, copias y actualizaciones.

02

Asistente en lenguaje llano

Hace de responsable de seguridad. Explica cada aviso y propone una sola decisión.

03

Anti-ransomware con copias incluidas

Aísla el equipo infectado y recupera el negocio en un clic.

04

Pagos verificados

Ningún cambio de cuenta de un proveedor pedido por correo se paga sin comprobación por otro canal.

05

Cuentas del negocio

Mensajería de empresa, redes sociales y tienda en línea protegidas contra el robo de cuenta.

06

Punto de venta

Protección de la caja y del terminal de cobro.

El diseño incluye un nivel Micro para negocios de uno a cinco equipos, con el objetivo de costar una fracción del precio de un servicio gestionado.

Diseñado para quien no puede permitirse fallar.

Soberanía total

El diseño prevé el despliegue dentro de la red de la institución, con inteligencia artificial que corre en sus propios servidores. Ningún dato sale.

Supervisión humana integrada

Niveles de autonomía configurables. Lo irreversible siempre pasa por una persona. El sistema puede interrumpirse en cualquier momento.

Auditoría inviolable

Cada decisión queda registrada, explicada y verificable de forma independiente, lista para reguladores y auditores.

Alineado con la regulación

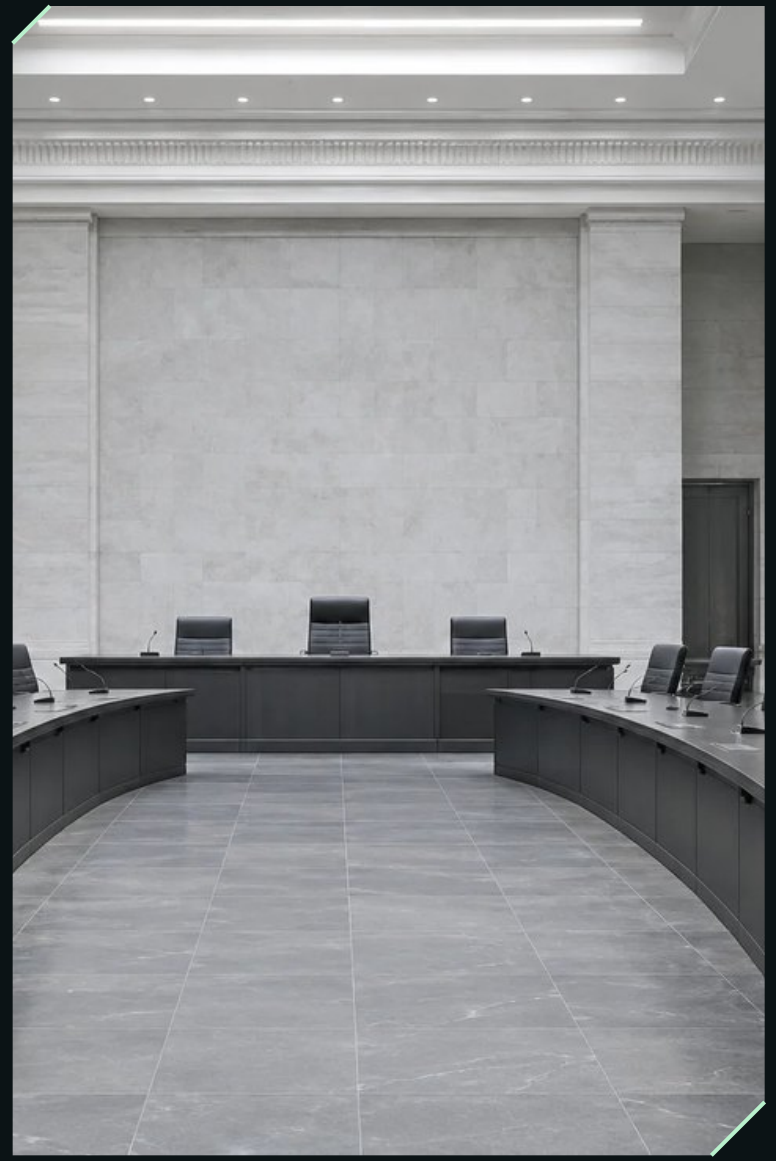
Concebido para las exigencias del AI Act europeo, NIS2 y DORA, incluida la supervisión humana y el reporte de incidentes.

Defensa post-cuántica

Comunicaciones y firmas diseñadas para resistir la computación cuántica, frente al riesgo de «cosechar hoy, descifrar mañana».

Resistencia operativa

Si una parte del sistema cae o es atacada, el diseño prevé que se recupere sola sin interrumpir la protección.



Capacidades previstas en el diseño institucional.

Al intruso que espera en silencio no hace falta encontrarlo: se le deja sin suelo.

El ataque más grave contra un Estado no roba ni cifra. Entra con cuentas válidas, se queda quieto y espera a una crisis. La presentación cita casos de más de cinco años. Ante la ausencia de anomalías que detectar, el diseño de Fortkern invierte la carga de la prueba.

Acto con Prueba

Equipo íntegro · Persona verificada · Orden vigente.

Administrador legítimo

Con orden vigente, se ejecuta. El acceso legítimo se renueva con prueba.

Intruso con cuenta válida

Sin orden ni equipo íntegro, no ejecuta nada.

Caducidad de la persistencia

El acceso durmiente del intruso no puede volver a probarse. Se extingue solo.

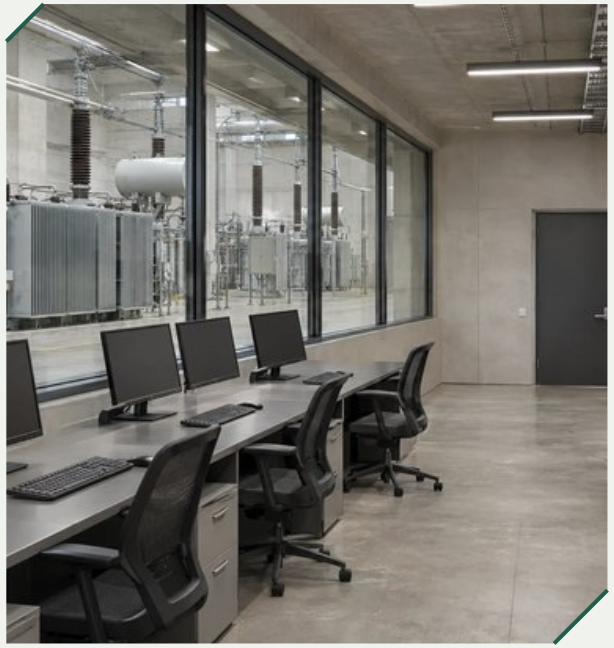
Interruptor de crisis

Ante una alerta nacional, permisos al mínimo, regeneración inmediata y redes de control separadas.

El diseño prevé un parte de limpieza comprobable por un tercero y evidencia apta para la atribución.

Las defensas actuales suponen una red conectada y en paz. Fortkern está diseñado para la red en crisis.

Las agencias de Estados Unidos y Australia ya piden a la infraestructura crítica que pueda aislar sus sistemas vitales y operar así semanas o meses. En Europa, el riesgo cibernético para el sistema financiero se elevó a «grave» en 2026.



Crisis o ataque	Aislar los sistemas vitales con una orden de quórum.
Isla Operativa	El servicio esencial sigue semanas sin internet.
Recuperación desde cero	Imágenes limpias firmadas y tiempos de recuperación que deberán demostrarse.
Desalojo verificado	Certificado de limpieza comprobable por un tercero.

Capacidades transversales · Tiempo con Prueba · Registro con Prueba · Sala de crisis soberana. Para todo un país, Fortkern Nación prevé proteger municipios, escuelas y hospitales desde una sola consola, con un asistente para equipos no expertos.

Un solo cambio detuvo el espacio aéreo de un país. Un atacante podría hacerlo a propósito.

Según la FAA y AFP, el 13 de noviembre de 2026 un equipo nuevo inundó la red del control aéreo de EE. UU. con más de 1.000 intentos de conexión cada pocos segundos. Afectó a 17 de 22 centros y se suspendieron todos los despegues. Otros operadores de telecomunicaciones cayeron por ataques deliberados contra el núcleo de su red.



Cambio propuesto	Firma desde equipo íntegro y aval del operador.
Réplica de la red	Alcance simulado antes de tocar nada.
Un solo equipo	Barreras de salud automáticas.
Toda la red, por oleadas	Vuelta atrás automática.

Si algo falla · Contención de tormentas en segundos · ¿Ataque o falla? en minutos · Imagen dorada para reconstruir. Cambio con Prueba está diseñado para impedir que un error o un atacante lleve un cambio a toda la red de golpe, con vigilancia de extremo a extremo del servicio vital, red de gestión fuera de banda y ruta de reserva con varias constelaciones. Los tiempos son objetivos.

Una semana de caídas en cadena. Casi ninguna fue un ciberataque.

EVENTO	QUÉ PASÓ, SEGÚN LA PRESENTACIÓN ORIGINAL	RESPUESTA DE FORTKERN, POR DISEÑO
Microsoft 365	Casi 24 horas caído por un defecto en un arreglo propio, más carga de una conmutación automática. No fue un ataque.	Prueba bajo carga y conmutación con capacidad comprobada.
Red de la NSA	Parches urgentes que no volvieron a arrancar.	Parche sin prisa. Escudo al instante y parche ensayado.
JPMorgan Chase	Un error tras una actualización retrasó operaciones con otros bancos.	Cortacircuitos de contraparte y modo degradado de pagos.
Apple	Una actualización interna. La página de estado seguía en verde.	Cambio con Prueba y estado con verdad independiente.
Avisos falsos	A las pocas horas, correos masivos de «restaurar mensajes» con el número real del incidente.	Escudo de confusión durante caídas públicas.
Equinor	El único ciberataque confirmado. Sistemas de oficina afectados, producción intacta.	Separación oficina-planta comprobada y desalojo verificado.

Un cambio sin prueba y una dependencia compartida pueden hacer tanto daño como un atacante. Fortkern no evita la falla interna de un proveedor ajeno. Está diseñado para que el cliente siga protegido y operando mientras dura, y para saber en minutos si es un ataque, una falla o un farol.

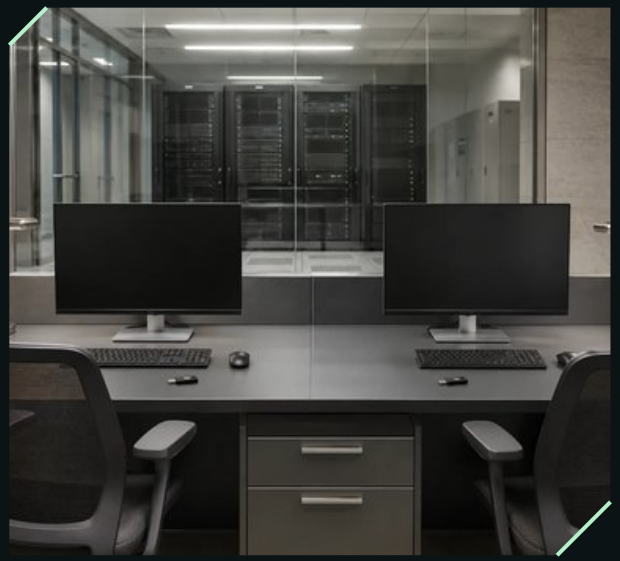
Cada dolor real de estos sectores tiene una respuesta concreta.

SECTOR	DOLOR REAL (2026)	RESPUESTA DE FORTKERN, EN DISEÑO
Gobierno	Solo el 22 % de los responsables de seguridad estatales confía en proteger los datos públicos. Presupuestos a la baja y falta de especialistas.	Fortkern Nación. Un país protegido desde una consola, con asistente para equipos no expertos.
Gobierno	Intrusos que esperan hasta cinco años dentro de las redes y borran sus huellas.	Retro-caza, registros imborrables y desalojo verificado.
Banca	Riesgo sistémico elevado a «grave». Dependencia de pocos proveedores tecnológicos comunes.	Modo degradado de pagos y recuperación desde cero verificada.
Banca	Unos 700 ataques con malware a cajeros en 2025 y más de 20 millones de dólares perdidos.	Dispensa con Prueba.
Infraestructura	Solo el 37 % ve todos sus equipos industriales. Windows antiguo sin parches en planta.	Fortkern Frontera y escudo para sistemas antiguos.
Infraestructura	Exigencia de operar aislados durante semanas. Hora por satélite falsificable.	Isla Operativa con Prueba y Tiempo con Prueba.

Referencias citadas: NASCIO-Deloitte, CISA, ESRB, FBI IC3 y Palo Alto Networks. Relación de fuentes en la diapositiva 40.

Los robos a bancos ya no rompen cajas fuertes: ordenan pagos desde dentro.

En los grandes casos recientes citados en la presentación, nadie rompió la criptografía ni robó a clientes. Se abusó de un sistema autorizado para ordenar pagos a través de un proveedor. Este blindaje está diseñado para proteger la orden en todo su recorrido.



Orden de pago	Pago con Prueba de Integridad.
Proveedor de conexión	El tercero no puede ordenar pagos por sí solo.
Sistema de pagos	Freno previo en pagos instantáneos.
Destino	Congelación coordinada si el dinero sale hacia cripto.

Para reservas y bancos centrales · Varias aprobaciones con prueba · Retardo con derecho de veto · Operación soberana y aislada. Dispensa con Prueba en cajeros · Modo degradado de pagos · Guardia de infraestructura compartida · Tiempo con Prueba. Un incidente, todos los informes regulatorios.

Protección de extremo a extremo para quien custodia los fondos de millones.

Los grandes robos recientes a exchanges citados en la presentación no rompieron la criptografía. Abusaron de los sistemas internos que piden las firmas. Este blindaje está diseñado para proteger el recorrido completo de un retiro.

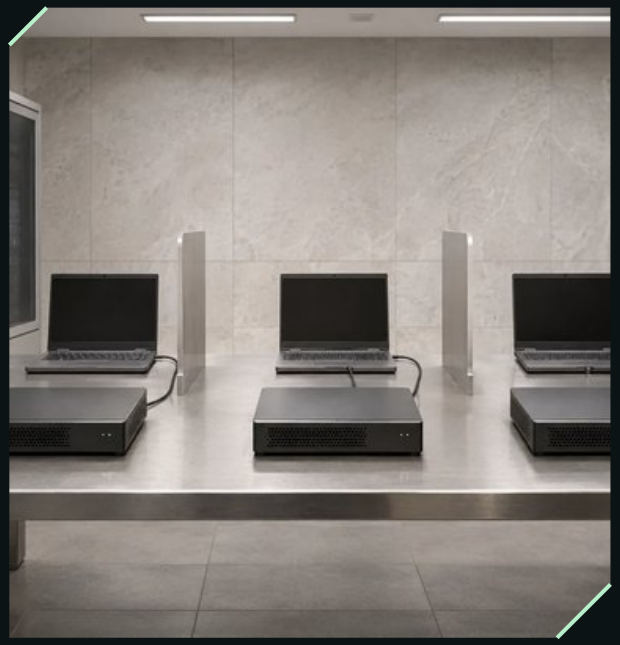
- **Solicitud de retiro** — Freno automático por velocidad, monto y destino.
- **Sistemas internos** — Accesos que solo sirven desde equipos íntegros.
- **Firmantes** — Cada firma, con prueba de integridad.
- **Red** — Señal de congelación coordinada entre plataformas.

Protección permanente de fondo · Reservas vigiladas · Equipo interno protegido · Réplica de ensayo permanente



Una entrevista de trabajo falsa precedió al robo de un gran exchange.

Según el comunicado del exchange citado en la presentación, en 2026 salieron unos 6.300 millones de dólares tras una entrevista falsa con una prueba de programación infectada y el abuso de una herramienta interna de IA. Fortkern está diseñado para cubrir el recorrido completo, de la llave al dinero ya robado.



Equipo del ingeniero	Código ajeno en caja aislada. IA sin suplantar.
Firma	Firmas defectuosas o sin prueba: no salen.
Robo detectado	Carrera de congelación: evidencia firmada en segundos, como objetivo.
Puentes y emisores	Retención breve de fondos marcados.

También en el diseño: validadores sin doble firma · claves de API sin retiro · contratación con Prueba.

Protección para los equipos donde no se puede instalar nada.

Controladores industriales, equipos médicos y sistemas heredados no siempre admiten un agente. El diseño sitúa Fortkern al lado y delante: escucha sin tocar y solo filtra las órdenes que cambian el proceso.

Puesto de ingeniería u operador

Emite la orden.

→

Pasarela Fortkern

¿El puesto que ordena está íntegro? ¿La orden cae en el rango seguro?

→

Controlador o equipo

Planta, hospital o red. La orden fuera de rango no pasaría.

Sensor pasivo

Escucha una copia del tráfico. Por diseño, queda fuera de la ruta de control del proceso y de los equipos vitales.

Las acciones con efecto físico requerirían siempre la aprobación de una persona. Los sistemas de seguridad del proceso quedarían intactos.

La carga ya no se roba solo forzando un camión: también se roba con una identidad falsa.

La presentación cifra el robo de carga por medios digitales en unos 725 millones de dólares en Estados Unidos y Canadá en 2025 y señala las cuentas robadas como un origen frecuente. Fortkern está diseñado para proteger el recorrido completo de un envío.



Oferta de carga	Cuentas que solo sirven desde equipos íntegros.
Asignación	Transportista con identidad verificada.
Recogida	Carga con Prueba de Integridad.
Entrega	Rastreo comprobado: posición plausible.

También en transporte: puertos y terminales · ferrocarril y marítimo · aviación (sistemas de tierra). Integridad de navegación prevista: avisar si la posición por satélite deja de ser fiable y detectar la falsificación, sin corregir la señal.

Un mismo núcleo, un paquete para cada sector.

Cobertura prevista en el diseño de los paquetes y las ediciones.



Finanzas y activos digitales

Exchanges · Protocolos y puentes · Banca · Reservas · Emisores regulados · Seguros · Usuarios



Estado e infraestructura

Gobierno · Elecciones · Defensa · Energía y agua · Salud · Telecomunicaciones · Transporte · Industria



Empresa y comercio

Tecnología y nube · Fábricas de IA · Comercio · Legal y consultoría · Educación · Farmacéutica · Medios · PyMEs

Edición PyME

Instalación en minutos, sin consola técnica: protección frente al ransomware, copias de seguridad incluidas y recuperación en un clic.

Todos los sistemas

Linux · Windows · macOS · Android · iOS · Nube · Contenedores · Firmware · Sitios web

Donde otras herramientas llegan tarde o no llegan, el mismo principio.

SECTOR	DOLOR DOCUMENTADO EN LA PRESENTACIÓN (2025–2026)	RESPUESTA DE FORTKERN POR DISEÑO
Inmobiliario	275,1 millones de dólares perdidos en 2025 (+58 %). Se suplanta a la empresa de cierre y se desvía el pago.	Cierre con Prueba y Registro con Prueba
Logística	Robo de carga habilitado por ciberataque: unos 725 millones de dólares, +60 % interanual.	Carga y Contratación con Prueba
Mercados	Voz clonada con IA contra grandes gestoras para colar órdenes.	Blindaje Mercados: orden y voz verificadas
Aviación	Un proveedor común de facturación cae y arrastra a muchos aeropuertos a la vez.	Guardia de proveedor compartido y ruta de reserva
Marítimo	Ataques a la tecnología operativa de a bordo (+150 %) y posición falsificada.	Tiempo y posición con Prueba
Datos e IA	Fallas en energía y climatización: un compromiso puede parecer un apagón.	Mando con Prueba y contención del radio de impacto

Otros sectores: nuclear · químicas · dispositivos médicos · genética · pensiones · cooperativas · recarga eléctrica · edificios inteligentes · robótica · BPO y mesas de ayuda · justicia · universidades · guarderías · casinos · deporte · eventos · semiconductores · videojuegos.

De la vigilancia a la inmunidad.

DIMENSIÓN	ENFOQUE REACTIVO DE REFERENCIA	FORTKERN, POR DISEÑO
Cuándo actúa	Detecta y alerta cuando el daño empezó.	Exigir prueba antes de cada acto crítico.
Qué hace al detectar	Alerta y espera a una persona.	Neutralizar en segundos (objetivo).
Fallas nuevas	Días o semanas hasta el parche.	Contramedida en horas, sin reiniciar (objetivo).
Llave o credencial robada	El atacante la usa.	Por sí sola no bastaría.
En una crisis	Presupone una red conectada y en paz.	Operar aislado y reconstruirse desde cero.
La hora y los registros	Se dan por buenos.	Comprobarlos.
Frente a atacantes de IA	Firmas estáticas.	Frenar y desviar a los agentes a velocidad de máquina.
Entre clientes	Cada uno aprende solo.	Inmunidad colectiva sin exponer datos.

Paridad con las plataformas líderes y diferencias de diseño

LO QUE OFRECEN LAS LÍDERES, SEGÚN LA PRESENTACIÓN	EL PASO MÁS DE FORTKERN, POR DISEÑO
Antiestafas con IA en correo, SMS, mensajería y web	Retener el pago a una cuenta nueva hasta verificar al destinatario.
Interrupción automática de ataques en curso	Explicar cada acción y revertirla automáticamente si afecta al servicio.
Agentes de IA que investigan y responden	Autoridad sellada: limitar las acciones a sus permisos aunque se engañe al agente.
Vigilancia de los agentes de IA de la empresa	Credencial con Prueba por agente e interruptor de apagado con prueba.
Centro de operaciones con lago de datos en su nube	Evidencia verificable y opción de operar por completo dentro del país.
Agentes de seguridad dentro del núcleo de Windows, en migración	Agente previsto en modo usuario para reducir el impacto de una actualización.
Adopción de la plataforma completa	Integración prevista con la protección que el cliente ya tiene.

Objetivo de paridad. Aún faltan resultados en pruebas independientes, escala de telemetría y vigilancia 24/7 propia. La calidad de detección no se compara hasta publicar resultados.

Un solo sistema. La licencia decide hasta dónde llega el blindaje.

01

Vigilancia

Detección y alertas.

02

Protección

Bloqueo en tiempo real y contramedidas.

03

Blindaje

Servidores, identidades y exposición continua.

04

Blindaje crítico

Firma con Prueba de Integridad y defensa de red.

05

Blindaje premium

Exchange, banca y reservas: licencia a medida.

06

Soberano

Instalación aislada en la institución. Ningún dato sale.

Modelo de entrega previsto: un instalador y una licencia de uso. Subir de nivel no exigiría reinstalar.

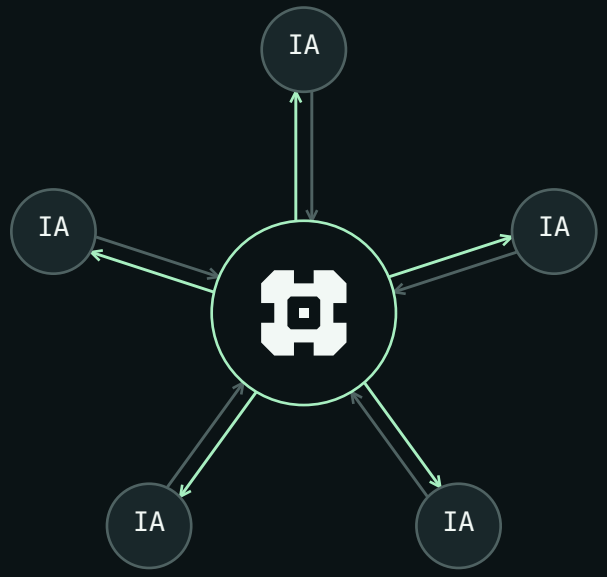
Desde una persona hasta un país, con el mismo núcleo.

PLAN	UNIDAD	MENSUAL	6 MESES	ANUAL
Personal	1 persona, hasta 5 equipos	5,99	31,99	56,99
Familia	Hasta 5 personas	11,99	64,99	114,99
Micro	Negocio de 1 a 5 equipos	14,99	80,99	143,99
Esencial	Por equipo	5,99	31,99	56,99
Pro	Por servidor	24,99	134,99	239,99
Fortkern IA	Por usuario	5,99	31,99	56,99
Web Básico / Web Pro	Por dominio	49 / 249	265 / 1.345	470 / 2.390
Crítico · Frontera · Blindaje Exchange y Banca · Soberano	A medida	—	Piloto	A cotización

Propuesta sin subida de precio al renovar. Precio regional un 35 % menor en Latinoamérica, África y Asia del Sur para Personal, Familia, Micro y Esencial. Precios de referencia sujetos a validación con futuros pilotos.

Una inteligencia de defensa que comparte lo que aprende.

IA Fortkern compartiría defensa comprobada con otras IA y verificaría lo que recibe.



IA Fortkern · Previsto

Un modelo propio especializado en defensa, que aprendería de ataques reales bloqueados, aportados de forma voluntaria y anónima.

Red entre inteligencias · Previsto

Compartir con otras IA conocimiento defensivo comprobado. Nunca nada que sirva para atacar.

Confianza medible · Previsto

Cada decisión se podría repetir y comprobar. Resultados publicados y sometidos a evaluación independiente.

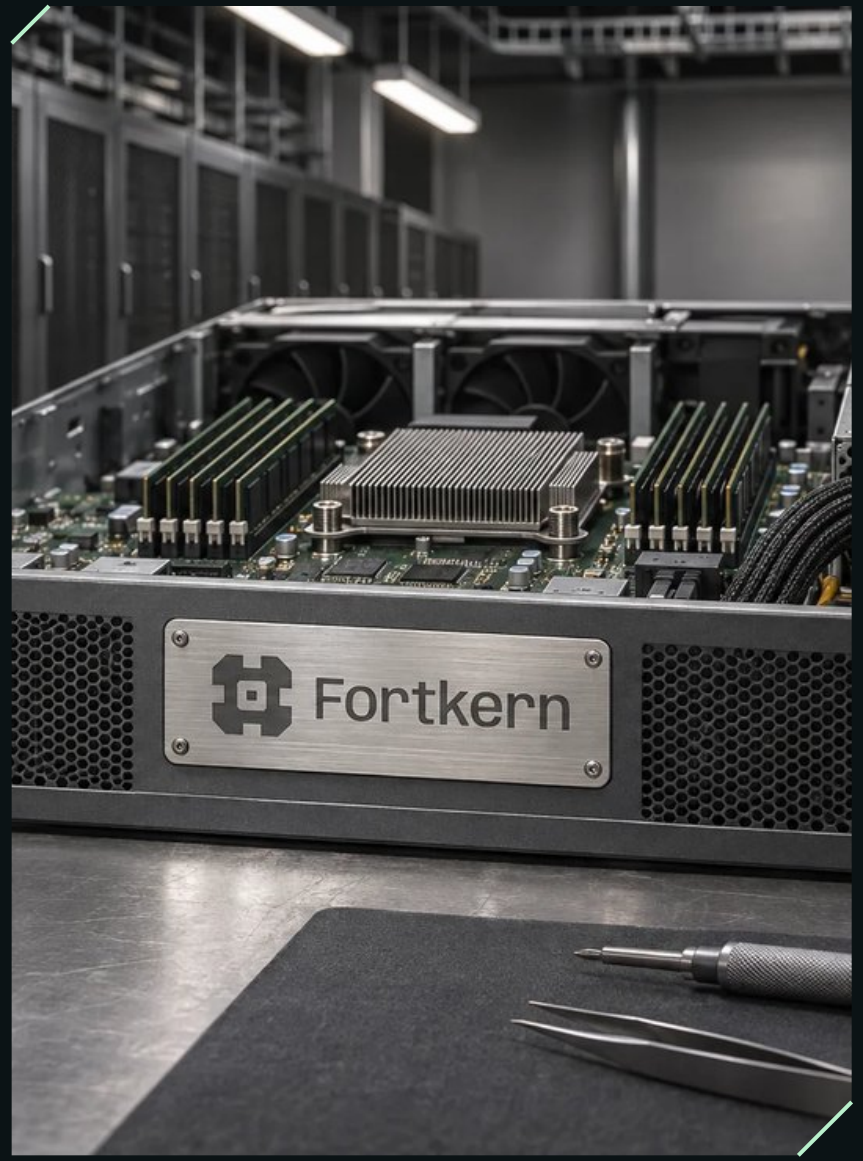
Un mundo más seguro se construye compartiendo la defensa y reservando el método.

Tres lenguajes de primer nivel, cada uno por una razón.

Ejército de agentes de inteligencia artificial previsto en la arquitectura.

Rust · Núcleo de laboratorio	Velocidad con seguridad de memoria.
Erlang · Diseño	Resistencia a fallos y recuperación sin detener el servicio.
Haskell · Diseño	Corrección demostrable en las decisiones sensibles.
Reservado	Lo que hace a Fortkern difícil de replicar.

Los agentes están diseñados para funcionar con modelos dentro de la red del cliente, sin depender de proveedores externos. Esta combinación es la base visible de la arquitectura. El resto permanece reservado.



Un núcleo de laboratorio que ya funciona y una ruta clara hacia la suite completa.

Estado del proyecto a 25 de noviembre de 2026.

HECHO	EN DESARROLLO	SIGUIENTE	PREVISTO	PREVISTO	PREVISTO
Núcleo de laboratorio	Caducidad y selección por versión	Sensor real y firma como servicio	Pilotos con socios	Suite por niveles	IA Fortkern y red entre IA

Demostrable hoy

El motor evalúa eventos simulados y registra decisiones. La demo valida reglas y distingue los modos observar y aplicar, sin bloqueo real. El Guardián verifica atestaciones de software y firma operaciones de prueba. Cinco de cinco pruebas internas superadas. Hoy la demostración se limita al laboratorio.

Alcance diseñado · 37 fases

Ejército de agentes, Fortkern Web e IA, Personal, Negocio, Frontera, Transporte, Escudo de Estado, resiliencia nacional, redes vitales, paquetes sectoriales y blindajes premium.

Modelo de servicio previsto

Un instalador y una licencia de uso por niveles. El software no se vende. La autonomía busca reducir el coste del trabajo manual repetido. Protección continua con opción soberana dentro de la institución.

La defensa del futuro no vigila: exige prueba, actúa y resiste la crisis.

Fortkern está diseñada para estar entre los sistemas de ciberseguridad más avanzados del mundo y proteger lo que una nación, una institución o una persona no puede permitirse perder. Invitamos a quienes compartan esa visión a conocer el proyecto en detalle.

Confidencialidad

Este documento describe capacidades y resultados, no implementación. Los métodos, la arquitectura y el código son propietarios y confidenciales. Compartido bajo reserva. Queda prohibida su divulgación, reproducción o uso para desarrollar un producto similar.

fortkern.com

Fuentes de los datos citados en la presentación original

Microsoft Digital Defense Report 2026 (explotación en menos de 24 h) · Mandiant, M-Trends 2026 (–7 días) · GuidePoint GRIT, tercer trimestre de 2026 (2.760 víctimas) · Report URI, noviembre de 2026 (178 organizaciones) · comunicado público del exchange afectado, 3 de noviembre de 2026 (6.300 millones) · Google, noviembre de 2026 (1,3 millones de decodificadores) · SecurityWeek e Infosecurity Magazine (equipos de frío, 9 países) · Kaspersky vía BleepingComputer, octubre de 2026 (bootkit) · FBI IC3, informe 2025 (8.600 millones) y aviso de febrero de 2026 (cajeros) · NASCIO-Deloitte 2026 (22 %) · ESRB, junio de 2026 (riesgo «grave») · Palo Alto Networks 2026 (37 %) CISA, CI Fortify 2026 · FAA y AFP, noviembre de 2026 (control aéreo, 17 de 22 centros) · Cyberhaven (39,7 %) · IBM, Cost of a Data Breach 2025 · SpyCloud 2026 (31 %, 95 %, 36 %) · FBI, robo de carga (725 millones) · CISA AA24-038A · Collins Aerospace, aeropuertos europeos (septiembre de 2026) · CloudSEK, tecnología operativa marítima (+150 %) · caso Kido, datos de 8.000 niños · Dragos 2026 (3.300 organizaciones industriales) · FBI IC3 2025 y FinCEN (fraude inmobiliario) · Data Center Knowledge, julio de 2026 · Microsoft, JPMorgan Chase, Apple, Equinor y CBS News (caídas del 12 al 18 de noviembre de 2026) · Plataforma de seguridad de Windows fuera del núcleo (noviembre de 2026).