SALT

inception
Un evento de TrustDimension 2026

Su negocio funciona con APIs: nosotros las protegemos

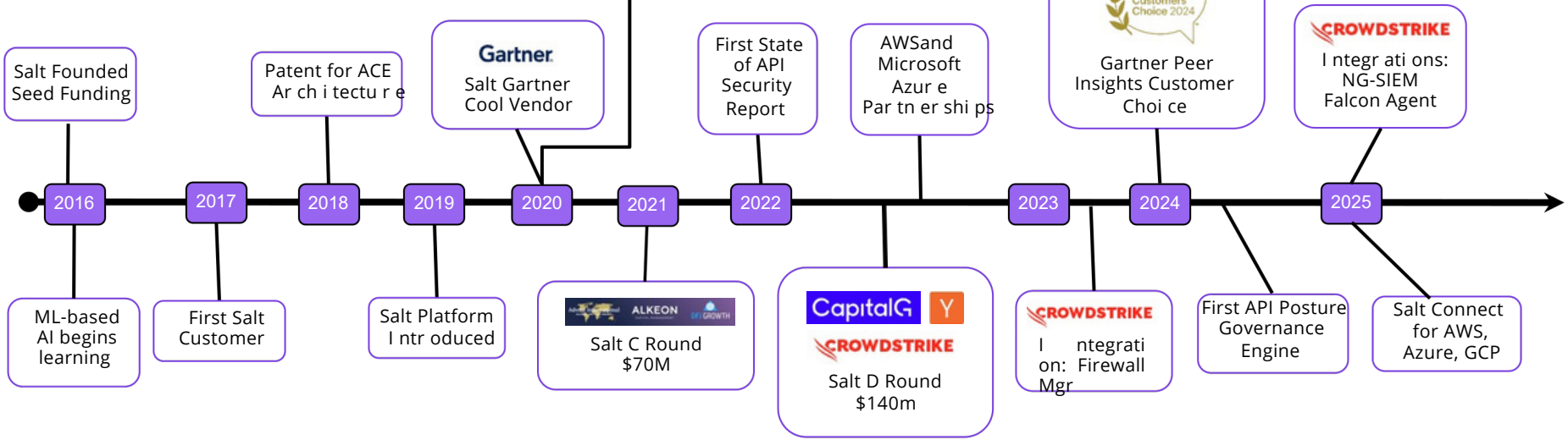
Descubra, gobierne y proteja sus APIsen toda su empresa

Salt Created the API Security Category

SALT

HQ: Palo Alto, CA
200+ Employees
$260m In Funding

Salt A Round $20M
Salt B Round $30M



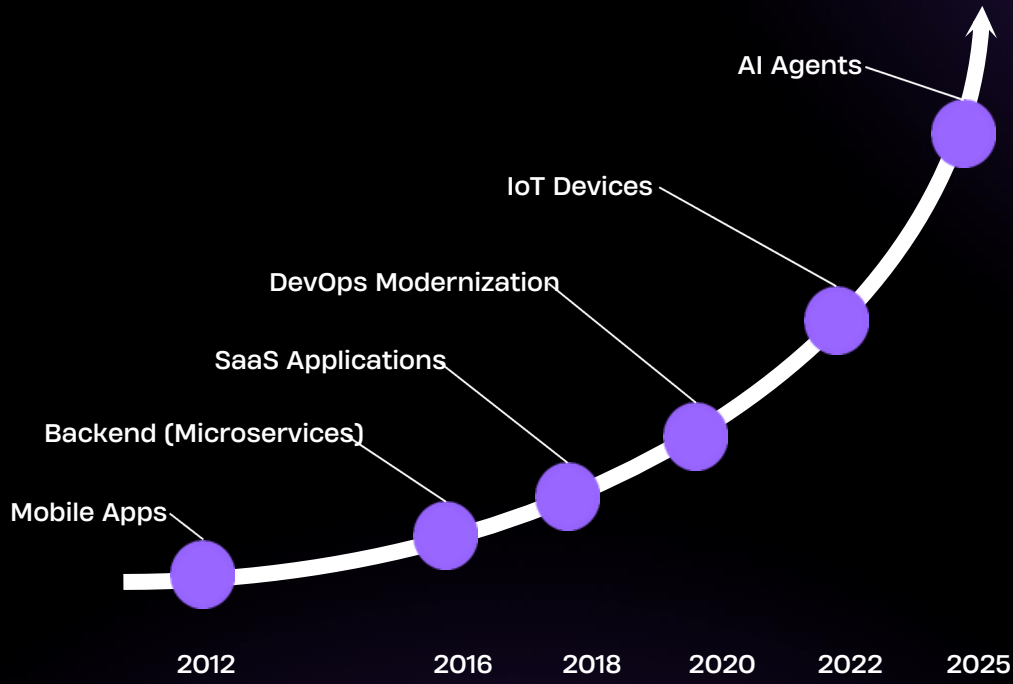
Su fábrica de APIs crece a cada dia.

SALT

•Más de 80% del tráfico de la Internet

fluye por APIs —40% hace diez años

•Agentes de IA deben motivar el crecimiento del tráfico de APIs en 100x



A diferencia de los activos de TI físicos, no puedes ver tu Fábrica de APIs.

Y es mucho más grande de lo que piensas…

- Una organización tiene **miles de APIs**,

  interconectadas con riesgos variados de exposición

- La mayor parte de las organizaciones subestima la cantidad de API en **70-80%**

- **75%** de las APIs son actualizadas semanalmente

- Riesgo real de impacto financiero con exfiltración de datos.

Exposición de APIsy multas.

SALT

"...en promedio, la violación de API genera al menos 10 veces más datos exfiltrados que cualquier otra violación de seguridad".

Gartner

Meta

Incidente: En 2018, los atacantes explotaron una vulnerabilidad en la función "Ver como" de Facebook, que interactuaba con las API de la plataforma, comprometiendo los tokens de acceso y exponiendo los datos personales de aproximadamente 29 millones de usuarios.

Multa:€251,000,000

PayPal

Incidente: A fines de 2022, los ciberdelincuentes explotaron debilidades en los sistemas de PayPal, que potencialmente involucraban vulnerabilidades de API, lo que llevó a un acceso no autorizado a la información personal de los clientes, incluidos los números de Seguro Social.

Multa:$2,000,000

AT&T

Incidente: En enero de 2023, una filtración de datos afectó a 8,9 millones de clientes de AT&T Wireless. La filtración involucró a un proveedor de servicios en la nube, y si bien no se revelaron detalles específicos sobre la participación de la API, estas filtraciones suelen implicar fallos de seguridad de la API.

Multa: $13,000,000

Soluciones tradicionales son insuficientes.

SALT

Problemas	Salt Security	CNAPP / CSPM	EdgeSecurity (CDN/WAAP)
Cobertura APIsencualquier ambiente o tecnología -nube, on prem o encriptado.	Coberturatotal	Parcial en nube apenas	Edgeonly
Postura de Gobernanza ¿Cómo puedovalidar la postura de mis APIs frente a las mejores prácticas y regulaciones?	Sí	No	Inspección básica
Protección de los datos ¿Será que mis datos en movimiento están protegidos?	Sí	Limitado	No ve el payload
Seguridad ¿ Cómopuedo reducir el riesgo de ataques lógicos?	Sí, con el uso de IA	No o basado en Firma /Schema	Basado en Firma /Schema

Casos de uso críticospara Seguridad API.

SALT

"Hasta el 2028, más del 50% de las exfiltraciones de datos generadas por abusos en APIs serán relacionados con IA."
- Gartner

Reducción de la Superfície de Ataques

Mapee rápidamente toda su superficie de ataque de API y reduzca el riesgo identificando y eliminando APIs fraudulentas, obsoletas y ocultas en todos los entornos.

Creación de un Inventario unificado

Obtenga visibilidad completa en minutos y elimine los puntos ciegos para descubrir automáticamente la estructura de API en su organización: API internas, externas, ocultas y de terceros.

Posturade Gobernanzay Compliance

Evalúe el riesgo de las APIsen todos los entornos.
Aplique sus políticas de seguridad y logre el cumplimiento normativo detectando errores de configuración y otras vulnerabilidades de manera proactiva.

Protección de Datos en APIs

Monitorea los datos confidenciales en movimiento a través de las API para descubrir riesgos de exposición que DSPM no detecta. Aplica políticas en el punto de acceso para prevenir fugas y cumplir con los requisitos de PCI, HIPAA y GDPR.

Detención de ataques lógicos por analisis comportamental

Detenga las amenazas basadas en la lógica y el comportamiento, como BOLA, y el abuso de la funcionalidad legítima con detección basada en intenciones en tiempo real que va más allá de las reglas y las firmas.

Identificación de riesgos de usodeagentes de IA

.Descubra los activos de IA y monitoree a los agentes de IA que interactúan con sus API para garantizar un uso seguro y evitar la exposición no controlada.

Como Salt Security impulsa la seguridad de las API

SALT

① Salt Surface

- Comprende rápidamente la exposición detuAPI sin esfuerzo.
- Observa tu superficie de ataque externa desde la perspectiva de un adversario.

② Salt Connect

- Conéctese a sus entornos de nube y catalogeAPI en minutos.

Elimine las API no autorizadas, obsoletas y ocultas que aumentan su riesgo.

③ Salt Collect

- Analiceeltráfico deAPI paradescubrir API adicionales, uso de datos confidenciales, brechas de postura, configuraciones incorrectas y más.

④ Salt Protect

- Identifica el abuso intencional deAPI con IA, no con firmas.
- Detiene los ataques a la lógica de negocio que ignoran los WAF, las CDN y las puertas de enlace.

Reduzca la superficie de Ataqu

Crea un Inventario Unificado

Valide la Postura de Gobernanza y Compliance

Extienda la Protección de Datos para las APIs

Identifique riesgo de Agentes IA

Detenga ataques lógicos

Salt Surface.

SALT

Reduzca la superficie de ataques

- Obtengauna visiónexternadesusAPIexpuestas y tecnologías desoportedesdeunpuntode vista de un atacante.
- No requiere implementación. Simplemente introduzca sus dominios para iniciar el descubrimiento.
- Mapee automáticamente la huella de su API externa y las áreas de superficie de riesgo.
- A diferencia de las CNAPP y los escáneres de superficie de ataque tradicionales, Surface se centra en las API, no solo en recursos en la nube, hosts o dominios.

No teníamos ni idea de que tantas de nuestras API fueran visibles externamente ni del nivel de riesgo. Con Salt, capturamos esta información en menos de cinco minutos e implementamos medidas correctivas. -Importante banco estadounidense

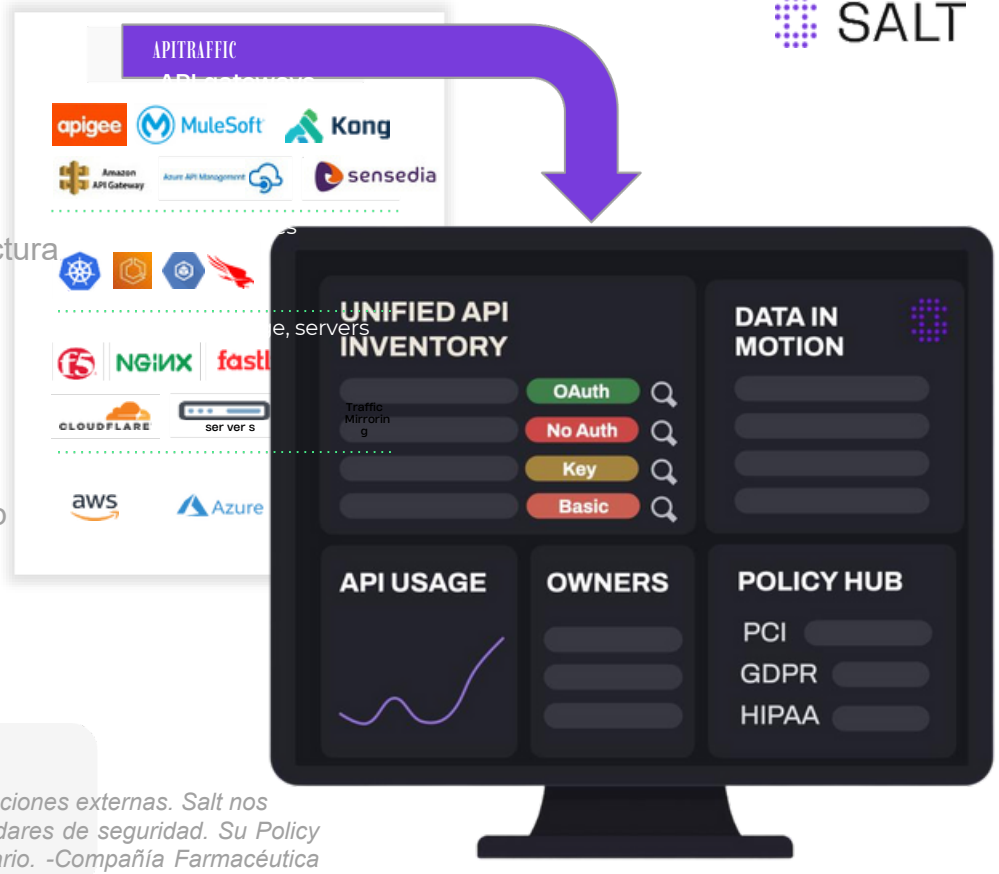
Salt Connect.

Crea uninventario unificado

- DescubraAPIenAWS, Azure,GCP y otros entornos de nube.
- Analice configuraciones, metadatos y registros sin necesidad de tráfico.
- Identifique APIsno autorizadas, ocultas y zombi en todos los entornos.
- Comience el inventario y la evaluación de la postura en minutos sin necesidad de implementación.
- Complementa Salt Surface para una visión completa de dentro a fuera.

Al equipo le sorprendió la cantidad de APIsocultas que teníamos en nuestra organización. Salt nos ayudó a encontrarlas rápidamente y a buscar nuevas constantemente. La conexión a la nube fue fácil de implementar y nos proporcionó datos de inventario en menos de 5 minutos. –empresa de Aviación top 10

Salt Collect.



SALT

Enriquezca el inventario con inteligencia API

- Obtenga información del tráfico en tiempo real
- Descubra los tiposde autenticación,suusoysu estructura
- Genere documentación automáticamente
- Identifique los recursos delAenuso

Valide la Postura de Gobernanza y Compliance

- Implemente estándaresde seguridad yregulatorios
- Creación de políticas con un solo clic con PolicyHub
- Crea políticas personalizadas ilimitadas

Extienda la Protección de Datos para las APIs

- Identificar datos sensibles en movimiento
- Riesgosdeseguridaddedatossegúnlapuntuación de riesgo

Nuestra organización estásujeta anumerosos controles internos yregulaciones externas. Salt nos mostró de forma clara dónde teníamos deficiencias en nuestros estándares de seguridad. Su Policy Hub, una tienda de aplicaciones para políticas de API, es revolucionario. -Compañía Farmacéutica Global

Salt Protect.

SALT

Detenga ataques lógicos por analisis comportamental

- Detecte amenazas basadas en intención que los WAF, las puertas de enlace y lasCDN pasanpor alto.
- Reduzca el ruido con PepperAI: de miles de anomalías a unas pocas amenazas reales.
- PepperAI reduce las anomalías de miles a decenas.
- Enrute la inteligencia de ataques de alta fidelidad a SIEM y plataformas de seguridad como Splunk, Wizy CrowdStrike.Detect intent-based threats missed by WAFs, gateways, and CDNs

Nuestro equipo de SOC probó varios productos para la seguridad de API. Solo Salt logró determinar la intención del atacante y reducir nuestras alertas de miles a las decenas de ataques reales. Ahora somos más eficientes en nuestra investigación y podemos detener los ataques con mayor rapidez. - Empresa líder en SaaS

¿Por quélosclients elijenSalt?

SALT

Descubrimiento de API simple, rápido y completo

Descubrimiento panorámico unificado(externo,interno, deterceros,en lanube, tráfico).

Descubrimiento de inventario de API no intrusivo, rápido y continuo.

Gobernanzade postura personalizable

Marketplacede políticasdedatosy posturas flexible y ejecutable. Políticas predefinidas, tanto sectoriales como comunes, disponibles a través de un centro de políticas similar a una tienda de aplicaciones.

Arquitectura Escalable

Arquitectura escalable que prioriza la privacidad y garantiza el cumplimiento del RGPD (utiliza solo metadatos, no cargas útiles, y garantiza controles de privacidad).

Integración con su ecosistema de seguridad (CrowdStrike, Sentinel One, Splunk, JIRA, Wiz, HCL, etc.).

Demo

inception
Un evento de TrustDimension 2026

SALT

¡Gracias!