Autonomous Exposure Management

Cómo la IA está cerrando la brecha entre saber y actuar

Hugo Origel · Head of Sales, NoLA · Tanium

✦ Impulsado por Anthropic AI

TANIUM

Lo que cubriremos hoy

30 minutos · Diseñado para CISOs y líderes de seguridad

01	**El Reto** Por qué los equipos de seguridad están perdiendo terreno — y por qué las herramientas tradicionales no bastan	5 min
02	**Nuevo Paradigma** Qué es Autonomous Exposure Management y por qué la IA lo cambia todo	8 min
03	**El Framework** IDENTIFY → PRIORITIZE → VALIDATE → REMEDIATE: cómo funciona en la práctica	12 min
04	**Prueba y Próximos Pasos** Resultados de negocio respaldados por Forrester y casos reales de clientes	5 min

TANIUM

SECCIÓN 01 — EL RETO

Los Equipos de Seguridad Pelean la Batalla de Ayer

Las herramientas no han evolucionado al ritmo de las amenazas.

Procesos Complejos

- Datos puntuales, sin visibilidad en tiempo real
- Falsos positivos que abruman a los analistas
- Múltiples transferencias que ralentizan la respuesta

Herramientas Fragmentadas

- Herramientas en silos que no se comunican entre sí
- Datos duplicados e inconsistentes
- Mayor costo total de propiedad y operación

Remediación Manual

- Semanas entre detección y remediación
- Resiliencia operacional debilitada
- IT Ops y Seguridad trabajando en conflicto

Las herramientas de ayer impiden que Seguridad y IT Ops den lo mejor de sí.

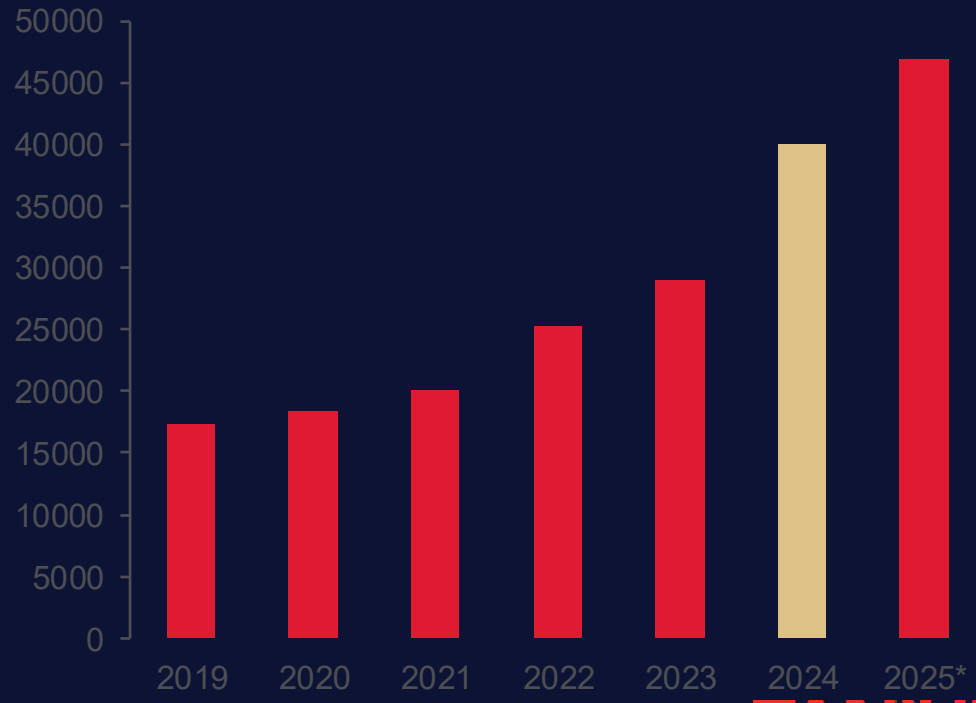
SECCIÓN 01 — EL RETO

La Superficie de Ataque Está Explotando

2X

en 2 años

Crecimiento en CVEs publicados (Fuente: cve.org, enero 2025)



La Brecha de Exposición a Remediación es Donde Vive el Riesgo

SABES DEL RIESGO

- Escaneo de vulnerabilidades completado
- CVEs identificados en endpoints
- Inventario de activos actualizado

LA BRECHA

- Semanas de triaje manual
- Prioridades en conflicto entre equipos
- Fatiga de alertas y ruido
- Ciclos de parchado inconsistentes
- Sin vista unificada del riesgo

ACTÚAS SOBRE EL RIESGO

- Parche desplegado en endpoints afectados
- Riesgo validado y cerrado
- Cumplimiento confirmado

La mayoría de las organizaciones mantienen esta brecha abierta por semanas — a veces meses. Ahí es donde ocurren las brechas de seguridad.

SECCIÓN 02 — NUEVO PARADIGMA

Un Nuevo Enfoque: Autonomous Exposure Management

Cerrando el ciclo — automáticamente, continuamente, a escala.

Integrado

Gestión de exposición y endpoints en una única plataforma — eliminando silos entre seguridad y IT Ops.

Impulsado por IA

Análisis inteligente, priorización automatizada y Predictive confidence scores — impulsado por modelos de IA de vanguardia.

Continuo

Visibilidad y monitoreo permanentes con flujos de remediación automatizados que verifican el éxito y cierran el ciclo.

"*El Autonomous IT cierra el ciclo desde el insight hasta la acción. Con IA e inteligencia en tiempo real, los clientes reducen el riesgo más rápido mientras mejoran la eficiencia operacional.*" — **Forrester Research, 2026**

TANIUM

SECCIÓN 02 — NUEVO PARADIGMA

¿Por qué ahora? La IA de Vanguardia lo Cambia Todo

El momento Anthropic-Mythos: IA empresarial + inteligencia de endpoint en tiempo real.

Priorización Inteligente

Los modelos de IA separan la señal del ruido automáticamente, con contexto de amenazas en tiempo real. Sin más alertas sin fin.

Scoring Predictivo de Riesgo

La IA de vanguardia no solo reporta qué es vulnerable — predice qué exposiciones serán explotadas primero y cuándo.

Consultas en Lenguaje Natural

Haz preguntas a tus datos de seguridad en español. Obtén respuestas en segundos en lugar de esperar ciclos de reporte.

Anthropic AI · Tanium Mythos Platform

Los 4 Pilares del Autonomous Exposure Management

Un ciclo cerrado y continuo — no una fotografía puntual del riesgo.

01 IDENTIFY

Ver todo, en todo lugar

- Descubrimiento continuo y monitoreo
- Telemetría completa de endpoints
- Insights de riesgo proactivos

02 PRIORITIZE

Enfocarse en lo que importa

- Scoring dinámico de riesgo con IA
- Enriquecimiento de contexto por activo
- Priorización orientada al negocio

03 VALIDATE

Saber antes de actuar

- Inteligencia en tiempo real, no fotografías puntuales
- Correlación automatizada de exposición y endpoints
- Reducir falsos positivos a escala

04 REMEDIATE

Actuar a escala con confianza

- Zero-touch patching
- Predictive confidence scores
- Progressive ring deployment

See Everything, Everywhere — Continuoly

Descubrimiento Continuo

Telemetría de endpoint en tiempo real en cada dispositivo — on-prem, nube y remoto. Sin puntos ciegos.

Visibilidad Completa

Inventario de activos unificado y actualizado en tiempo real, no en lotes. Conoce tu entorno antes que los atacantes.

Insights Proactivos de Riesgo

Inteligencia de amenazas curada por expertos, mapeada a tu entorno real — no avisos genéricos.

El Reto del CISO

No puedes proteger lo que no puedes ver.

La mayoría de las organizaciones tienen una brecha del 30–40% entre lo que creen que tienen y su inventario real de activos.

TANIUM

La IA Corta el Ruido — Enfócate en lo que Importa

Priorización con IA

1. **Scoring Dinámico de Riesgo**

   Cada vulnerabilidad puntuada por explotabilidad, criticidad del activo y contexto de negocio — actualizada en tiempo real.

2. **Enriquecimiento de Contexto**

   La IA correlaciona datos de CVE, inteligencia de amenazas y tu entorno específico para identificar lo verdaderamente urgente.

3. **Priorización Orientada al Negocio**

   Alinea las prioridades de remediación con el impacto de negocio, no solo con CVSS scores. Tu CIO te lo agradecerá.

4. **Predictive Confidence Scores**

   Conoce cuán segura está la IA en cada recomendación antes de comprometer recursos a la remediación.

Sin IA

Los analistas dedican el 70% de su tiempo triando alertas que no son accionables.

Con IA

Los analistas se enfocan en el 3% de vulnerabilidades que representan riesgo real e inminente.

TANIUM

Confirmación en Tiempo Real — Saber Antes de Actuar

Inteligencia en Tiempo Real

A diferencia de los scanners puntuales, la telemetría continua da una imagen precisa del riesgo en todo momento.

Vista Unificada de Exposición y Endpoint

Datos de seguridad y TI en un solo lugar — sin reconciliar herramientas distintas para entender si hay exposición real.

Reportes Automatizados

Visibilidad de remediación y reportes de cumplimiento generados automáticamente para el consejo directivo.

TANIUM

Actuar a Escala — Con Confianza

Zero-Touch Patching

Despliegue automatizado de parches sin intervención manual. Menos trabajo operativo, más seguridad.

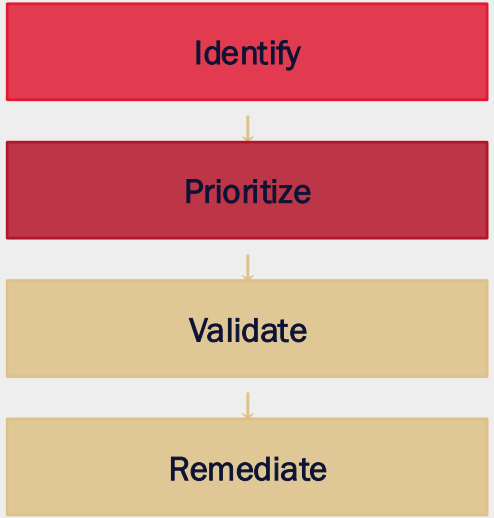
Predictive Confidence Scores

Acciones de remediación validadas por IA — conoce el resultado probable antes de desplegar. Menos rollbacks.

Ring-Based Progressive Deployment

Despliega primero a un grupo pequeño, valida el éxito y escala. Seguridad incorporada en cada paso.

Cerrando el Ciclo



TANIUM

SECCIÓN 04 — PRUEBA

El Caso de Negocio Está Claro

Resultados cuantificados — Forrester Total Economic Impact™, marzo 2026.

75%

Reducción en MTTR

para incidentes de endpoint que requieren remediación en el Año 3

95%

Eficiencia en Parchado

mejora para estaciones de trabajo en Año 3 (65% para servidores)

70%

Ganancia de Productividad

al unificar gestión de endpoints y seguridad en el Año 3

"Autonomous IT closes the loop from insight to action — reducing risk faster while improving operational efficiency."
— Forrester Research, Total Economic Impact of Tanium Autonomous IT, 2026

Organizaciones que ya Están Teniendo Éxito

4 de cada 5 clientes que evalúan este enfoque eligen adoptarlo.

Salud

Identificó +400,000 vulnerabilidades y las redujo un 80% en solo 2 semanas.

Automotriz

Ganó visibilidad total sobre vulnerabilidades Log4j en toda su flota global en menos de 5 minutos.

Gobierno

Parcheó +40,000 vulnerabilidades en más de 100 agencias locales con despliegue progresivo automatizado.

Servicios Financieros

Identificó y remedió endpoints sin parches críticos — reduciendo la ventana de exposición de semanas a horas.

Farmacéutica

Logró visibilidad de riesgo completa y remediación con un solo clic a escala global.

Bienes Raíces

Unificó gestión de endpoints y seguridad — parchado proactivo sin interrumpir operaciones.

Tres Preguntas para tu Equipo

Inicia la conversación correcta hoy.

1. ¿Tenemos visibilidad en tiempo real de todos los endpoints — o estamos trabajando con datos puntuales?
2. ¿Cuánto tiempo nos toma ir desde descubrir una vulnerabilidad crítica hasta confirmar que fue remediada?
3. ¿Nuestros equipos de Seguridad e IT Ops trabajan desde una plataforma unificada — o están reconciliando datos de herramientas distintas?

¿Listos para Cerrar la Brecha?

Hagamos una Evaluación de Exposure Management para tu entorno.

Reservar una Evaluación

hugo.origel@tanium.com

Tanium · 2026

TANIUM