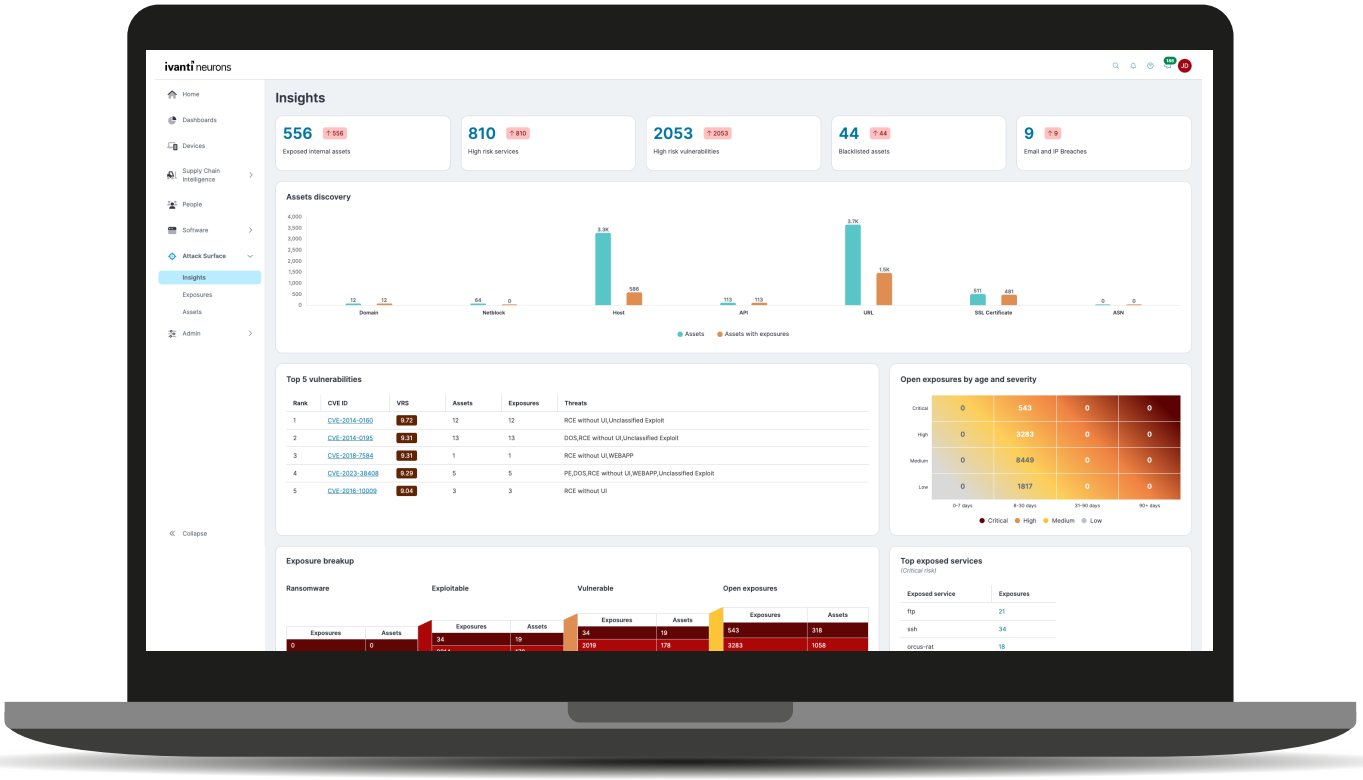
Ivanti Neurons for EASM

Combate la expansión de la superficie de ataque con una visibilidad completa de los activos externos e inteligencia procesable sobre las exposiciones.

El aumento de la prevalencia del Everywhere Work y la incesante transformación digital han provocado una expansión incontrolada de la superficie de ataque. Ivanti Neurons for External Attack Surface Management (EASM) proporciona una vista completa y continua de tu superficie de ataque y de las expocisiones asociadas para los activos orientados a Internet. Gracias a esta tecnología, podrás eliminar las exposiciones de alto riesgo y protegerte de forma proactiva contra los ciberataques.



Expansión descontrolada de la superficie de ataque

La transición al *Everywhere Work* y el avance de la transformación digital han acelerado el uso de las TI oculta y las herramientas basadas en la nube. Al mismo tiempo, las organizaciones están experimentando una mayor adopción de dispositivos IoT y cadenas de suministro más interconectadas.

Como resultado, los equipos de seguridad están luchando por obtener visibilidad de los activos externos en toda su superficie de ataque. También carecen de visibilidad en las exposiciones asociadas con esos activos.

Los activos desconocidos, no verificados, no gestionados y no parcheados exponen a las organizaciones a riesgos de violaciones de datos, multas y tiempos de inactividad. Los equipos de seguridad necesitan una visibilidad continua de toda la superficie de ataque, para proteger adecuadamente a sus organizaciones.

Presentación de Ivanti Neurons for EASM

Obtén y mantén la visibilidad de cada activo externo por toda la superficie de ataque de tu organización con Ivanti Neurons for EASM. Aprovecha de la inteligencia procesable basada en los riesgos sobre las exposiciones que afectan a esos activos, para protegerte de forma proactiva contra las violaciones de datos, las multas y el tiempo de inactividad.

ivanti

Funciones principales

Llega a la visibilidad completa

Desbloquea la visibilidad de todos los activos orientados a Internet y de la exposición asociada en toda la superficie de ataque de tu organización. El monitoreo sin agentes descubre activos que las herramientas de detección tradicionales no detectan, así como aquellos que los equipos de seguridad no suelen supervisar: por ejemplo, los buckets de Amazon S3 mal configurados, los entornos de desarrollo y control de calidad pasados por alto, los sitios web de marketing olvidados y las aplicaciones Java que se ejecutan en servidores que todos consideraban fuera de servicio.

Tipos de activos descubiertos por EASM	Vectores de exposición descubiertos por EASM
■ API ■ Dominio ■ Host ■ Netblock ■ Certificado SSL ■ URL	■ Seguridad de las aplicaciones ■ Fugas de datos ■ Salud del DNS ■ Seguridad del correo electrónico ■ Seguridad de la red ■ Cadencia de aplicación de parches ■ Ingeniería social

El monitoreo continuo garantiza una visibilidad de estos activos casi en tiempo real, para que sepas inmediatamente cuándo se expongan los activos existentes, o se implementen otros nuevos y puedas responder en consecuencia.

La función de espacio de trabajo permite agrupar los activos y las exposiciones por categorías, como departamentos y filiales. También resulta útil cuando se utiliza Ivanti Neurons for EASM para monitorear las superficies de ataque externas de organizaciones de terceros, como los socios de la cadena de suministro.

Prioriza las exposiciones de alto riesgo

Aprovecha la inteligencia procesable sobre las exposiciones en toda tu superficie de ataque externa para determinar dónde dirigir los esfuerzos de remediación. La inteligencia incluye una Puntuación de Riesgo de Vulnerabilidad (VRS, Vulnerability Risk Score) para cada CVE que Ivanti Neurons for EASM encuentra.

El VRS facilita la toma de decisiones informadas al permitir que los equipos de seguridad cuantifiquen el riesgo que representa una vulnerabilidad y comprendan su contexto de amenaza. Considera las puntuaciones CVSS de la Base Nacional de Datos de Vulnerabilidades (NVD) más una serie de otros atributos que reflejan el impacto de una vulnerabilidad en un entorno determinado.

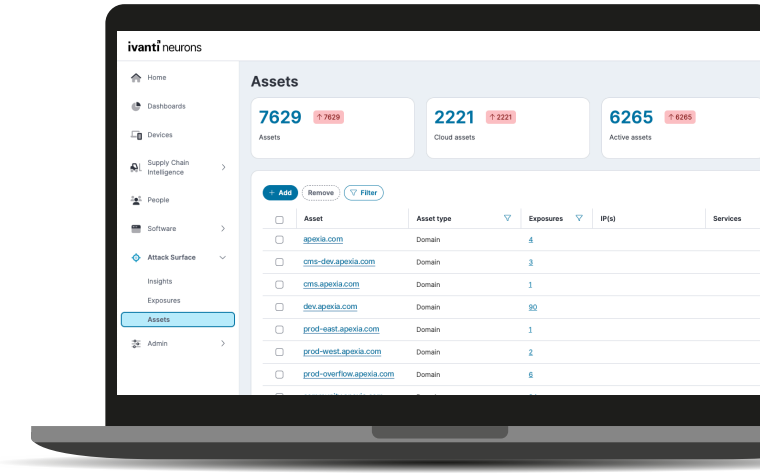
Reportar sobre el riesgo

Responde a los requisitos de elaboración de informes de los responsables de seguridad de alto nivel y ayuda a la diligencia debida sobre posibles adquisiciones, socios y proveedores con informes en PDF. Estos informes exportables proporcionan un resumen detallado de las exposiciones asociadas a la superficie de ataque externa de una organización.

Colma las lagunas de tu superficie de ataque

Aprovecha el valor de Ivanti Neurons para cerrar las brechas críticas en la superficie de ataque descubiertas por Ivanti Neurons for EASM. Combina Ivanti Neurons for EASM con los siguientes productos para obtener una respuesta más rápida a los problemas que afectan a los activos externos:

- Ivanti Neurons for ITSM: organiza la respuesta a los problemas en todos los equipos.
- Ivanti Neurons for UEM: gestiona y protege los endpoints.
- Ivanti Neurons for Patch Management: corrige las vulnerabilidades.



ivanti

Amplios casos de uso de EASM

El EASM aborda una serie de retos a los que se enfrentan las empresas modernas.

- **Detectar e inventariar activos digitales:** detectar y catalogar los activos orientados a Internet desde sitios web, direcciones IP, nombres de dominio, certificados SSL y servicios en cloud, TI, IoT y OT.
- **Analizar y priorizar las exposiciones:** priorizar la remediación de las exposiciones que afectan a los activos externos, desde vulnerabilidades no parcheadas, hasta configuraciones incorrectas y puertos abiertos.
- **Controlar dispersion en la nube y la TI oculta:** identificar los activos públicos en todos los proveedores de servicios en la nube, incluidas las instancias creadas por empleados fuera de los canales adecuados.
- **Detectar la fuga de datos:** controlar la fuga de datos o la exposición de datos sensibles a través de herramientas de colaboración y aplicaciones en la nube utilizadas internamente y por terceros.
- **Realizar evaluaciones de riesgos en filiales, terceros y objetivos de adquisición:** ejecutar controles de seguridad exhaustivos antes de integrar sistemas con otras entidades.
- **Reducir los ataques de phishing e ingeniería social:** monitorear los dominios de phishing, identificar los sitios web falsos y detectar posibles ataques de ingeniería social dirigidos a empleados y clientes.
- **Adherir a los requisitos de cumplimiento normativo:** cumplir con las normativas, incluidas GDPR, HIPAA y PCI DSS, que requieren el descubrimiento y el inventario de activos.

Acerca de Ivanti

Ivanti mejora y asegura el «Everywhere Work» para que las personas y las empresas puedan prosperar. Logramos que la tecnología trabaje para las personas, no al revés. Los empleados actuales utilizan una amplia gama de dispositivos corporativos y personales para acceder a aplicaciones y datos de TI a través de múltiples redes para mantenerese productivos donde y como quieran trabajar. Ivanti es una de las pocas empresas de tecnología que encuentra, gestiona y protege cada activo de TI y terminales de una empresa. Más de 40.000 clientes, incluidos 88 de las 100 empresas de Fortune, confían en Ivanti para que les ofrezca una excelente experiencia digital a sus empleados y mejorar la productividad y eficiencia de los equipos de TI y seguridad. En Ivanti, nos esforzamos por crear un entorno en el que se escuchen, respeten y valoren todas las perspectivas, y estamos comprometidos con un futuro más sostenible para nuestros clientes, socios, empleados y el planeta. Para más información, visita ivanti.com.

ivanti

Para más información o para contactar con Ivanti, visita ivanti.com.

1. Forrester, "The External Attack Surface Management Landscape, Q1 2023," 9 de enero de 2023