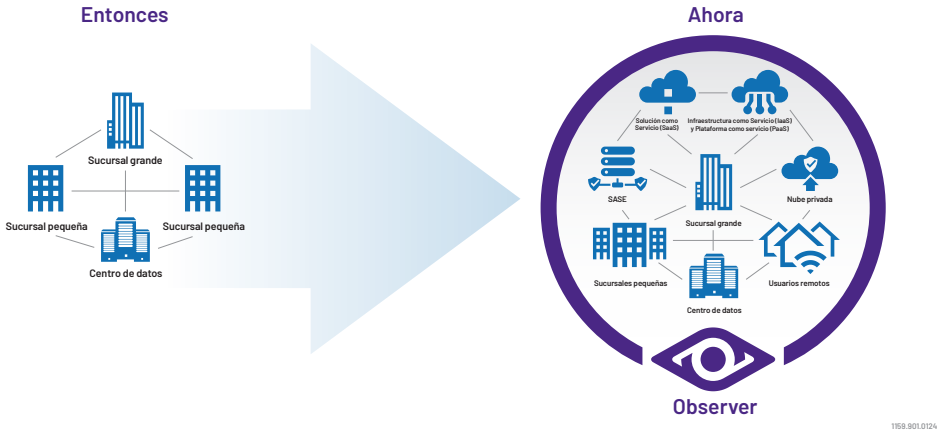
Observer Apex

Creado para los equipos de operaciones y seguridad de red: más visibilidad y una resolución más rápida.
Proporcionamos una visibilidad completa de la red y la seguridad a través de análisis avanzados.

LA RED ESTÁ EN TODAS PARTES

Aplicaciones multicapa complejas alojadas en las instalaciones o en recursos basados en la nube, incluidos SaaS, IaaS, PaaS y SASE: la nueva norma es que los usuarios accedan a las aplicaciones desde cualquier lugar. Las redes de hoy no conocen fronteras, pero cada servicio de TI depende de ella.

Si cualquier componente de la arquitectura del servicio o la red falla, la entrega de las aplicaciones puede degradarse rápidamente, lo que resultaría en un cliente insatisfecho y una menor rentabilidad del negocio. Para evitarlo, la capacidad de observación del servicio completo es primordial.



Observer Apex ofrece visibilidad donde más lo necesita, y es la primera solución de gestión del desempeño que genera una puntuación de la experiencia del usuario (EUE) en cada transacción. Apex ofrece adaptabilidad y visibilidad a través de diversas fuentes de datos: paquetes, metadatos y flujos enriquecidos. Las organizaciones pueden seleccionar las fuentes que mejor se ajusten a sus presupuestos.

Apex permite conocer el estado del servicio de TI global, en línea con su compromiso de ofrecer una visibilidad completa. Cuando surgen anomalías en el servicio o se detectan posibles fallos de seguridad, los eficientes flujos de trabajo permiten a los grupos de NetOps, DevOps y SecOps descubrir la causa raíz y solucionarla de forma rápida.

CENTRO DE COMANDOS PARA LOS EQUIPOS DE OPERACIONES Y SEGURIDAD DE RED

- Con aprendizaje automático la puntuación de Experiencia de Usuario (EUE) automatizada, convierte múltiples métricas (KPI's) en una única puntuación fácil de comprender, y contiene las deducciones de puntuación detalladas que aíslan automáticamente los dominios del problema y proporcionan la información necesaria para priorizar una solución rápida.
- Las opciones flexibles de fuentes de datos, incluidos paquetes, metadatos y flujos enriquecidos, ofrecen la vista adecuada para cada parte interesada, desde el ingeniero de redes hasta el propietario de la línea de negocio.
- Los paneles personalizables para inteligencia operativa global con flujos de trabajo eficientes permiten una rápida identificación y resolución de problemas a equipos de NetOps, SecOps y DevOps.
- El mapeo de dependencias de aplicaciones bajo demanda permite una visibilidad precisa de las aplicaciones multicapa sin necesidad de configuración alguna.
- Gestión integrada del desempeño y análisis forense para una rápida respuesta ante anomalías de servicio y violaciones de ciberseguridad.

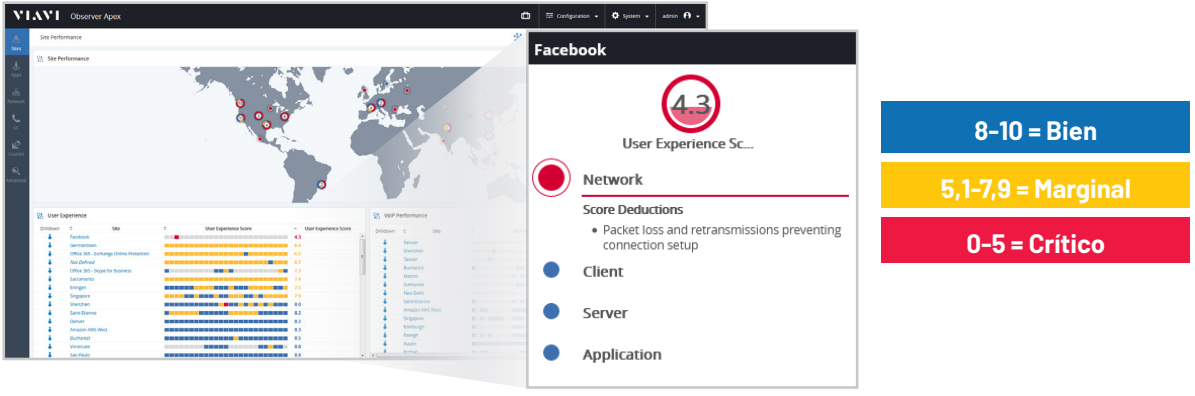
- Las funciones de inspección profunda de paquetes (DPI) abordan el desafío de comprender la composición del tráfico de red y determinar si el tráfico no crítico está impactando negativamente a los usuarios finales y los servicios comerciales clave.
- Los análisis forenses de Observer con inteligencia de amenazas y tecnología CrowdStrike® combinan información a nivel de paquetes con contexto de adversarios integrado para enriquecer las investigaciones, con una clasificación más rápida, una validación de máxima confianza y una visibilidad de amenazas procesable en entornos híbridos.
- El análisis de certificados digitales identifica los certificados que han caducado, o están a punto de caducar, y destaca los protocolos obsoletos, lo que ayuda a garantizar el cumplimiento y servicio ininterrumpido para los usuarios.
- Los flujos de trabajo de comunicaciones unificadas (UC) guían a los expertos en UC con resúmenes globales y vistas específicas del sitio hasta detalles de llamadas interactivas. Los datos de paquetes y flujos se integran a la perfección para visualizar la ruta de una llamada punto a punto o una llamada compleja multi punto a través de la infraestructura de red.
- Los análisis y la introducción de registros de flujos en la nube proporcionan la visibilidad necesaria del tráfico en la nube, lo que ayuda en la detección de amenazas de seguridad, la identificación de anomalías y cumplimiento de normas para entornos basados en la nube, como Amazon Web Services (AWS) y Microsoft Azure.
- Las flexibles opciones de implementación, desde equipos físicos para el centro de datos hasta imágenes de máquinas virtuales, para una simple, eficiente instalación en la nube.

GESTIÓN DEL DESEMPEÑO

Puntuación de la experiencia del usuario

Apex elimina las conjeturas al evaluar la satisfacción de los usuarios con análisis patentados equipados con aprendizaje automático para analizar y evaluar con precisión todas las conversaciones. Cada una recibe una puntuación de entre 0 y 10 mediante una codificación de colores y una clasificación que representa el desempeño desde la perspectiva del usuario, teniendo en cuenta el comportamiento único del entorno y de la aplicación para eliminar los falsos positivos.

Las puntuaciones brindan visibilidad de la experiencia de un solo usuario o puede expandirse a la vista de un sitio, un servicio o una empresa global. Apex va más allá en este paso y aísla el dominio del problema en la red, en el cliente, en el servidor o en el aplicativo con descripciones del problema fáciles de comprender.



Paneles personalizados a nivel empresarial

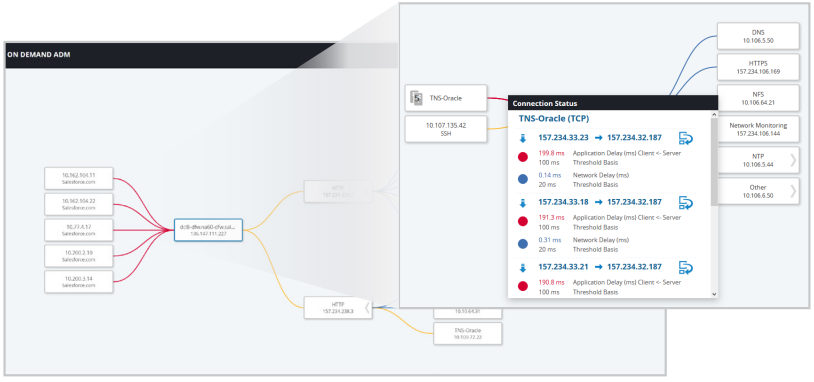
Los paneles definidos por el usuario y basados en geolocalización permiten, de forma integrada, conocer la situación de toda la empresa en cuanto al estado de la prestación del servicio.

Flujos de trabajo para solución de problemas

Los flujos de trabajo orientados a sitios y servicios, al integrarse con la puntuación de la experiencia del usuario, permiten a los equipos de TI conocer al instante la situación global en cuanto a todos los recursos y, entonces, llegar a un usuario específico para solucionar rápidamente el problema.

Inteligencia de aplicaciones multicapa bajo demanda

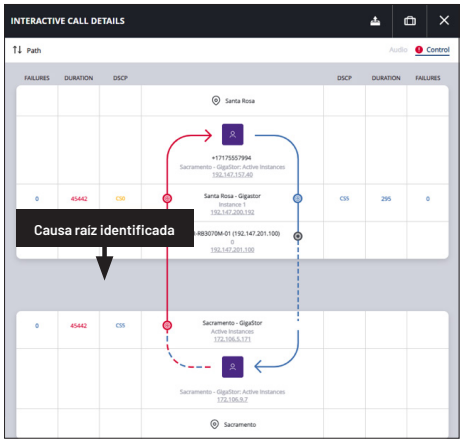
El mapeo de dependencias de aplicaciones bajo demanda permite el conocimiento del servicio multicapa, una detección rápida de las interdependencias de las aplicaciones y una presentación ad hoc de mapas donde se visualizan estas complejas relaciones con claridad. Con un solo clic del ratón, Apex genera el mapa completo, y automáticamente señala y resalta las peores conexiones para que los usuarios puedan asignar rápidamente la prioridad para la solución de problemas.



Mapas automatizados de dependencias de aplicaciones con puntuación de la experiencia del usuario integrada

Comunicaciones unificadas (UC)

Los paneles de Comunicaciones Unificadas (UC) y flujos de trabajo de Apex ofrecen una guía eficaz a los expertos en VoIP y UC con resúmenes globales y vistas específicas de los sitios, así como visualizaciones únicas e interactivas de detalles de llamadas. Solo Observer combina a la perfección datos de paquetes y flujos para visualizar la ruta de una sola llamada de punto a punto o una llamada multipunto a través de la infraestructura de red, identificando los orígenes de la degradación de calidad y, ofreciendo acceso con un solo clic a los datos de paquetes relevantes cuando sea necesario.



Las visualizaciones interactivas de los detalles de las llamadas identifican las causas raíz de las degradaciones de calidad.

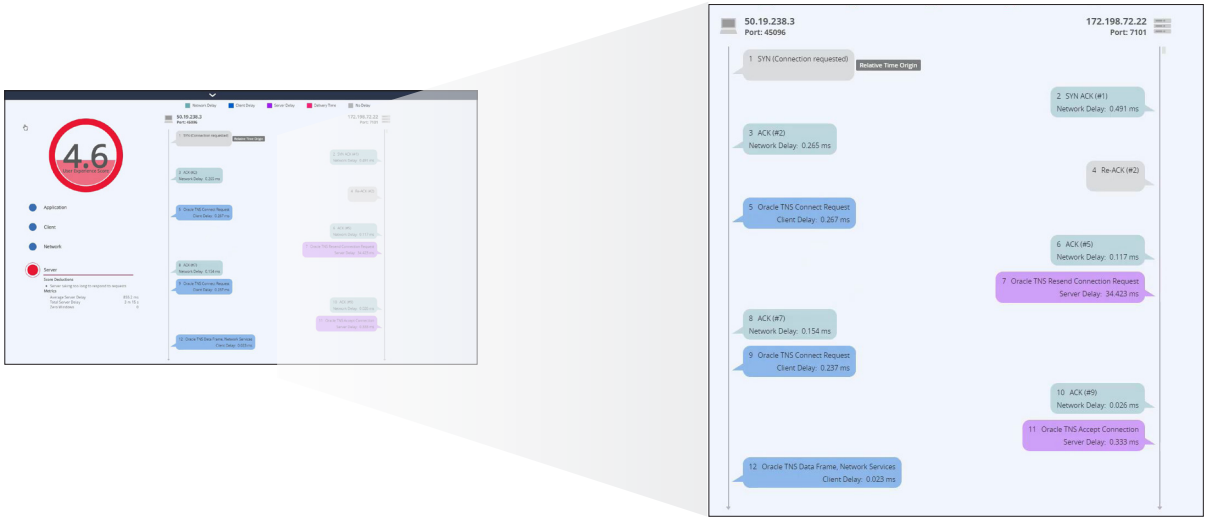
Los beneficios clave incluyen:

- **Mapeo Visual del Recorrido:** transformación de datos de paquetes y flujos en visualizaciones intuitivas de las rutas de las llamadas
- **Resolución rápida del problema:** reducción significativa del tiempo medio de reparación (MTTR) con una identificación sencilla de la causa raíz de los problemas de desempeño de las Comunicaciones Unificadas (UC)
- **Interfaz Amigable:** interfaz fácil de usar y comprender que le permite empoderar al personal no experto con descripciones simplificadas de llamadas de Comunicaciones Unificadas (UC) complejas multipunto o de punto a punto

ANÁLISIS DE SEGURIDAD Y RED

Observer y su Análisis forense de red integra dos fuentes de datos, paquetes y flujos enriquecidos, con la capacidad de retener estos datos durante períodos de tiempo prolongados. Las opciones de implementación de imágenes de máquinas virtuales permiten la recopilación y el análisis de flujos enriquecidos y paquetes de aplicaciones alojadas en la nube. Para llegar hasta la causa raíz de numerosos problemas de desempeño y fallos de ciberseguridad comienza con metadatos y paneles intuitivos, pero se suele recurrir al final a flujos de trabajo lógicos que permiten visualizar los datos subyacentes, a veces, días después del evento. Es por eso que Observer sigue brindando los detalles durante períodos de tiempo más largos.

Como se ha descrito anteriormente, muchas anomalías del desempeño se aíslan rápidamente con la puntuación de la experiencia del usuario. Sin embargo, cuando se requieran detalles de mayor fidelidad, podrá acceder a los datos en un instante.



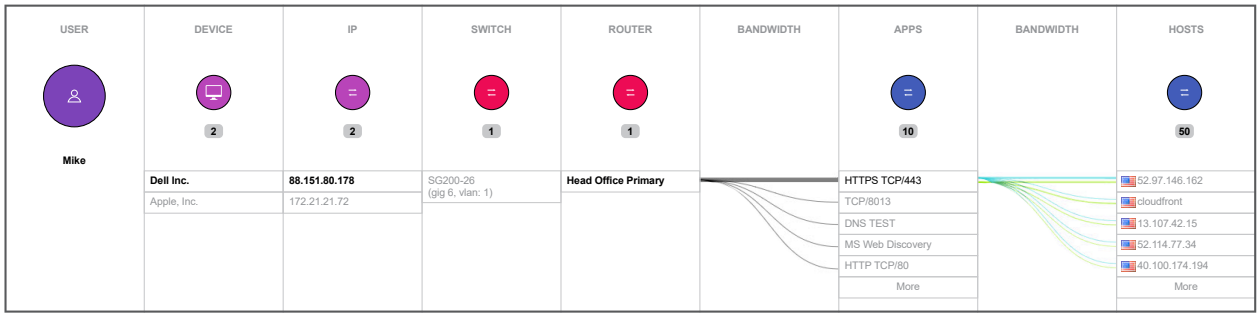
Puntuación de la experiencia del usuario final con conexión asociada y un desglose dinámico de la conversación

Conversación Forense

Con los datos de paquetes que captura por Observer, cada transacción, desde el principio hasta el fin, está disponible para su revisión, así como para fines de investigación. Los flujos de trabajo eficientes guían a los usuarios, desde los paneles globales hasta paquetes individuales, cuando sea necesario y en solo unos pocos pasos.

Con la visibilidad adicional proporcionada por la identificación de aplicaciones basadas en Inspección de Paquetes (DPI), Observer proporciona información avanzada de tráfico de red. Esta capacidad permite a los ingenieros de red identificar fácilmente el tráfico que se produce en puertos no estándar, cuantificar el tráfico no crítico, y analizar con mayor detalle los protocolos HTTP y HTTPS. Las capacidades de Inspección de Paquetes (DPI) de Observer le permiten identificar más de 4300 aplicaciones, lo que permite saber con claridad y de inmediato si una conversación se trata de una transacción comercial u otra operación.

Análisis Forense de flujos enriquecidos



El Observer GigaFlow y su visor de dirección IP permite la visibilidad de la actividad del usuario en la infraestructura de red para cada conversación

Al recopilar información de las capas 2 y 3 en un solo registro de flujos enriquecidos, Observer puede producir visualizaciones interactivas únicas donde se ilustran las relaciones entre usuario, dirección IP, dirección MAC y utilización de las aplicaciones en la red. Los usuarios solo tienen que introducir un nombre o identificación de usuario, o una dirección IP para encontrar de inmediato todos los dispositivos, interfaces y aplicaciones asociadas. Descubrir qué está conectado y quién se está comunicando a través de la red nunca había sido tan fácil.

Gestión de Certificados Digitales

Observer monitorea los protocolos de enlace SSL/TLS mientras analiza el tráfico de red, identifica certificados digitales que han caducado, o están a punto de hacerlo, y proporciona notificaciones proactivas. Identifica servidores que publican sesiones no seguras, resalta protocolos obsoletos, valida el cumplimiento normativo y ayuda a garantizar un servicio ininterrumpido a los usuarios.

El panel de análisis de certificados proporciona la versión TLS, el estado de caducidad de certificados y las distribuciones de la suite de cifrado.

Para los administradores y los ingenieros de red, garantizar la actividad y la satisfacción de los clientes es esencial a la hora de prestar servicios basados en web. La transición de métodos de informes manuales, como las hojas de cálculo, a un enfoque proactivo de análisis de certificados simplifica el proceso y protege a la empresa frente a posibles interrupciones de servicio relacionadas con certificados.

Entre las ventajas clave, se incluyen las siguientes:

Monitoreo proactivo: análisis en tiempo real, reportes y notificaciones que le mantienen un paso por delante del vencimiento de los certificados.

Información de seguridad mejorada: obtenga una visión clara de las versiones de SSL o TLS operativas, lo que permite una retirada rápida de los protocolos obsoletos o que no son seguros.

Servicio ininterrumpido: al identificar y solucionar problemas relacionados con los certificados, se evitan posibles interrupciones del servicio, lo que garantiza una experiencia del usuario perfecta.

Cuando se trata de ciberseguridad, la mejor protección contra las amenazas exige una estrategia triple de prevención, detección y respuesta.

Prevención		Detección	Respuesta
• Cortafuegos • Prevención de DDoS • Prevención de pérdidas de datos • Prevención de intrusiones • Prevención antivirus y antimalware	• Cifrado • Prevención correo no deseado y phishing • Controles de acceso • Seguridad de puntos finales	• Detección de intrusiones • Gestión de eventos de seguridad (SIEM) • Detección de puntos finales	• Análisis Forense de red • Gestión de eventos de seguridad (SIEM)

Para muchas organizaciones, el enfoque suele ser la prevención y la detección, hasta que una falla se confirma y el escenario donde el centro de guerra se vuelve urgente y hasta entonces se comienza a responder a la amenaza. En este punto, tener acceso inmediato a todas las actividades de la red que sucedieron en el pasado es crítico para limitar los daños y poder decir con confianza que "todo está bien".

Aquí es donde el análisis forense de la red es de un valor incalculable. Observer ofrece el poder combinado de tráfico forense y el análisis forense de flujos enriquecidos para poner su negocio en marcha respondiendo a las cuestiones clave de cada fallo de seguridad: cómo, quién, qué y dónde.

Análisis forense de tráfico

¿Cómo están o estaban conectados los dispositivos?

¿Quién se está o estaba comunicando?

Análisis Forense de flujos enriquecidos

¿Qué se está o estaba transmitiendo?

¿Hasta dónde llegaron las acciones cuestionables?

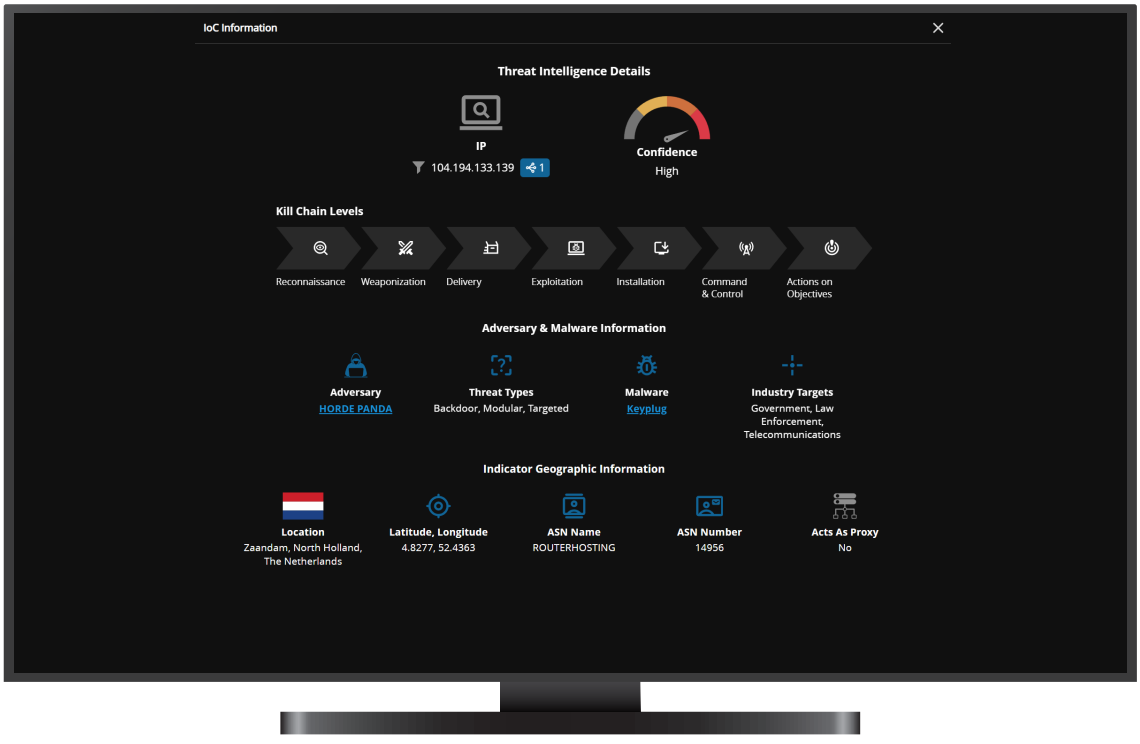
Al responder a estas preguntas, los equipos de TI pueden determinar rápidamente el "vector de ataque" (cómo el malhechor a burlado las medidas de prevención y detección para obtener acceso) y qué servicios de TI, dispositivos o datos confidenciales de clientes o empresas se han visto comprometidos. Una vez logrado esto, la contención es posible y se puede finalizar la evaluación de los daños.

ANÁLISIS FORENSES DE AMENAZAS DE OBSERVER

Visibilidad de amenazas procesable para una respuesta con confianza

Los análisis forenses de amenazas de Observer añaden una nueva dimensión a los análisis forenses de la red, introduciendo pruebas a nivel de paquetes y de flujos enriquecidos con inteligencia de amenazas actualizada continuamente y equipada con la tecnología CrowdStrike®. Esto permite a los equipos de seguridad establecer una correlación entre el comportamiento de los adversarios y patrones de tráfico sospechosos y degradaciones del desempeño, todo ello en tiempo real.

Al integrar indicadores de compromiso (IOC), tácticas, técnicas y procedimientos de ataque, y otros detalles de los adversarios en el momento de la detección, Observer permite una validación de las amenazas inmediata y de gran confianza, sin una combinación manual de información ni un enriquecimiento retrasado.



Cada alerta, ya sea que se desencadene por una amenaza conocida o un comportamiento inesperado de patrones de tráfico de red, incluye un acceso adaptable a datos de paquetes sin procesar y metadatos de flujos enriquecidos para evaluar el impacto, investigar el ámbito, determinar la causa raíz y tomar medidas decisivas en entornos híbridos.

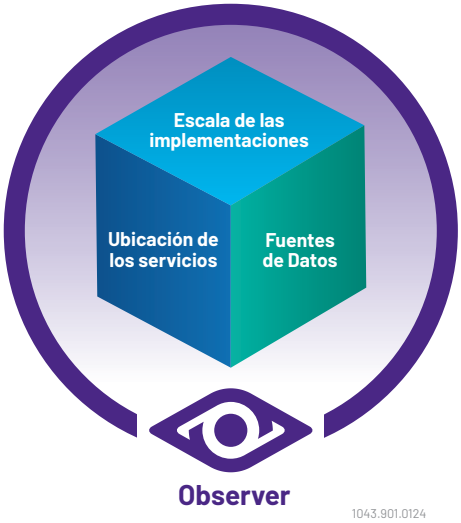
A diferencia de las soluciones tradicionales que normalmente dan comienzo desde el primer día, los análisis forenses de Observer ofrecen un análisis retrospectivo real, lo que permite a los equipos de seguridad realizar un seguimiento de las amenazas hasta el día cero. Con datos de total fidelidad conservados en el tiempo, los analistas pueden reconstruir la cronología completa del ataque, incluso antes de la detección inicial, para descubrir la causa raíz, los puntos de entrada y los movimientos laterales dentro de una fuente de verdad.

Los beneficios clave incluyen:

- **Correlación en tiempo real** entre el tráfico de red y la inteligencia de amenazas que reduce el tiempo medio de reparación (MTTR) y las conjeturas
- **Análisis retrospectivo** que proporciona visibilidad del día cero, lo que ofrece a los analistas de seguridad las pruebas forenses necesarias para investigar la actividad de amenazas antes de la detección inicial
- **Contexto de atacantes integrado** y tácticas, técnicas y procedimientos que permiten una clasificación y una investigación de confianza
- **Enlaces directos a las pruebas de paquetes** que permiten un desglose rápido para valorar el ámbito y el impacto
- **Visibilidad compartida** que impulsa la colaboración en los flujos de trabajo de NetOps y SecOps

Los análisis forenses de amenazas de Observer contribuyen a unificar las operaciones de red y seguridad con una vista compartida de alta fidelidad que establece una correlación entre el desempeño y la actividad de amenazas, lo que mejora las investigaciones y la confianza en los flujos de trabajo. Los metadatos y los flujos enriquecidos integrados proporcionan la granularidad y la retención necesarias para una clasificación en tiempo real y análisis forenses posteriores a las infracciones, de modo que se eliminen las conjeturas y se acelere la resolución.

OBSERVER DESCRIPCIÓN

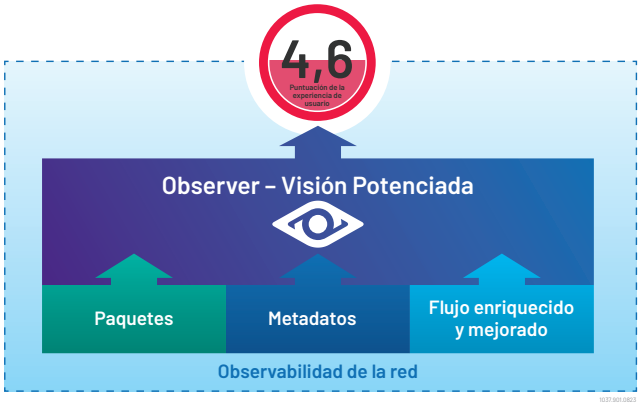


La plataforma Observer de VIAVI es una solución completa de gestión del desempeño y la seguridad que proporciona a los equipos de red, operaciones y seguridad información procesable en entornos híbridos. Observer Apex recopila metadatos de transacciones de diversas fuentes de datos para el cálculo de la puntuación de la experiencia del usuario (EUE). Integra detección e investigación de amenazas a nivel forense para proporcionar una visibilidad compartida y una sola fuente de verdad para los equipos de NetOps y SecOps.

Como panel integrado y recurso de informes, Apex sirve como punto de visibilidad global central y punto de lanzamiento para una resolución rápida de problemas con flujos de trabajo optimizados que ayudan a identificar la causa raíz utilizando paquetes, metadatos y flujos enriquecidos. Con contexto de amenazas integrado y acceso directo a los datos forenses, los equipos de seguridad pueden validar incidentes, evaluar el impacto y aislar rápidamente la causa raíz.

Observer ayuda a los equipos de TI de tres maneras esenciales:

- **Ubicación de los servicios:** Observer proporciona observabilidad en todos los entornos, ya sean de nube privada, usuarios remotos, en las sucursales remotas, en oficinas o en el centro de datos. No importa la ubicación, VIAVI Observer lo tiene cubierto.
- **Fuentes de datos:** Observer ofrece opciones flexibles de visibilidad mediante el uso de paquetes, flujos enriquecidos y metadatos. Este enfoque multicapa admite tanto la solución de problemas de desempeño como los análisis forenses posteriores a las infracciones. Con flujos de trabajo basados en roles y alertas con información de contexto, los equipos pueden investigar con confianza, desde anomalías del servicio hasta amenazas de seguridad, empleando los datos adecuados en el momento adecuado.
- **Escala de las implementaciones:** comience por implementaciones reducidas y amplíelas a medida que las exigencias operativas y de seguridad evolucionen. VIAVI ofrece modelos de implementación flexibles y precios de suscripción por niveles para adaptarse a sus necesidades de gastos operativos y de capital, lo que permite una visibilidad escalable y la convergencia entre los equipos de operaciones y seguridad de red sin sobrepasar el presupuesto ni los recursos.



Más información en viavisolutions.es/apex

viavisolutions.es
viavisolutions.com.mx

Contáctenos +34 91 383 9801 | +1 954 688 5660
Para localizar la oficina VIAVI más cercana, por favor visítenos en viavisolutions.es/contactenos

apex-br-ec-es
30194042 914 1025