

Zscaler y CrowdStrike

Ampliar Zero Trust para modernizar el centro de operaciones de seguridad (SOC)

Resumen de la solución

© 2024 Zscaler, Inc. Todos los derechos reservados.

Puntos clave

- Zscaler recopila y analiza las señales de incidentes de seguridad activos que se producen en el punto final desde la plataforma CrowdStrike Falcon, agregando una rica capa de contexto a su motor de políticas de control de acceso adaptable y haciendo que el control de acceso Zero Trust impulsado por la postura del dispositivo sea aún más sólido.
- El servicio Zscaler Risk360 se integra con CrowdStrike para brindar información sobre los factores que contribuyen al riesgo dentro de su organización, los clasifica en categorías de etapa de ataque de Risk360 y cuantifica cada factor de riesgo según su ponderación de riesgo.
- Data Fabric for Security de Zscaler enriquece y correlaciona los datos CVE de CrowdStrike con flujos de datos concurrentes para proporcionar información contextualizada y en tiempo real sobre vulnerabilidades y exposiciones en todo su entorno de TI.
- Desarrollada de manera nativa por CrowdStrike, la aplicación Falcon Foundry de Zscaler sirve de base para la integración de Zscaler con la plataforma de gestión de incidentes y eventos de seguridad de nueva generación (NG-SIEM) de CrowdStrike. La oferta prediseñada automatiza y orquesta el intercambio de información sobre amenazas y permite acciones políticas coordinadas para una respuesta rápida y efectiva a las amenazas a la seguridad.

El desafío

El trabajo híbrido ha disuelto el perímetro y continúa reinventando el panorama empresarial, dejando a las organizaciones con la compleja tarea de habilitar de manera segura una fuerza de trabajo distribuida desde cualquier ubicación y en cualquier dispositivo mientras protegen su empresa de los ciberataques.

El cambio de paradigma en la manera de realizar el trabajo ha llevado a un crecimiento exponencial en el número de dispositivos conectados a las redes corporativas actuales. Cada dispositivo conectado representa un punto de entrada potencial para ciberataques, lo que complica aún más los esfuerzos de seguridad.

En medio de los desafíos de la industria, los equipos de TI y de seguridad se esfuerzan por mantener un acceso seguro a las aplicaciones a través de diversos entornos multinube y panoramas de amenazas fluctuantes. Necesitan visibilidad y control para escalar la seguridad en todo el vasto ecosistema de puntos finales y aplicaciones para proteger todas las superficies de ataque potenciales.

Los equipos de operaciones de seguridad enfrentan sus propios desafíos únicos. Al tener la responsabilidad de detectar amenazas avanzadas y controlar los riesgos a partir de grandes volúmenes de datos inconexos, se espera de ellos que respondan a los incidentes de seguridad en el menor tiempo posible. Todo ello mientras se coordinan de manera superlativa las estrategias de respuesta a través de múltiples herramientas y plataformas. Estos desafíos se ven agravados por la brecha entre la seguridad de TI y las operaciones de seguridad, que a menudo retrasa la resolución de incidentes, debilitando la postura de seguridad general de la organización.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Zscaler y CrowdStrike: un enfoque de defensa en profundidad inigualable

Zscaler y CrowdStrike ofrecen una solución de seguridad Zero Trust integrada que simplifica la seguridad desde los puntos finales hasta las aplicaciones en un mundo híbrido. Al ampliar las capacidades básicas de Zero Trust, la solución ofrece un conjunto de nuevas y potentes integraciones que transforman el centro de operaciones de seguridad (SOC).

La plataforma Zscaler Zero Trust Exchange™ distribuida en la nube de Zscaler sirve como centralita inteligente que conecta de manera segura a millones de usuarios, dispositivos y aplicaciones a través de cualquier red y ubicación. Zscaler ha ampliado aún más el poder de su plataforma con nuevas capacidades de cuantificación de riesgos y contextualización de datos para ayudar a resolver las dificultades diarias que enfrentan las operaciones de seguridad para detectar y responder a las amenazas.

Al integrar la seguridad Zero Trust líder del sector de Zscaler y la gestión de riesgos impulsada por la IA con la protección avanzada de puntos finales, la inteligencia de amenazas y las capacidades SIEM de próxima generación de CrowdStrike, la solución integrada agiliza todo el ciclo de vida de gestión de riesgos, detección y respuesta, cerrando eficazmente el bucle entre la seguridad de TI y las operaciones de seguridad.

La integración de Zscaler y CrowdStrike es multicapa y admite múltiples casos de uso:

- **Acceso adaptativo Zero Trust:** Zscaler aprovecha las puntuaciones de dispositivos y las señales de incidentes de seguridad de CrowdStrike Falcon Zero Trust Assessment (ZTA) para habilitar controles de acceso adaptables, garantizando que solo los dispositivos seguros accedan a las aplicaciones.
- **Intercambio de inteligencia sobre amenazas:** los indicadores de compromiso (Iocs) de CrowdStrike alimentan el motor de inteligencia de amenazas de Zscaler, mejorando sus listas de bloqueo personalizadas para la prevención proactiva de amenazas.
- **Detección y cuarentena avanzadas de amenazas de día cero:** Zscaler Cloud Sandbox se integra con la telemetría CrowdStrike Falcon para detectar malware de día cero y facilitar acciones rápidas de cuarentena en los puntos finales afectados.
- **Señuelos para inteligencia temprana de amenazas:** Zscaler Deception implementa señuelos en puntos finales, redes, nube y sistemas de identidad para proporcionar alertas de alta fidelidad sobre indicadores tempranos de ataque (IOA) y compartir esta información sobre amenazas de alta confianza con CrowdStrike.
- **Visibilidad integral del ciberriesgo, evaluación y gestión del riesgo:** Zscaler Risk360 y Data Fabric for Security ingieren factores de riesgo únicos a lo largo de la cadena de ataque y datos CVE respectivamente de CrowdStrike para cuantificar el riesgo y priorizar las vulnerabilidades críticas en flujos de trabajo de remediación automatizados.
- **Intercambio y correlación de telemetría entre plataformas:** Zscaler se integra con CrowdStrike para compartir registros relevantes de Zscaler para mejorar la visibilidad de extremo a extremo con telemetría de puntos finales, redes y aplicaciones en la nube para maximizar la eficacia entre plataformas para acelerar las investigaciones.
- **Detección y respuesta multiplataforma:** CrowdStrike Falcon Next-Gen SIEM ahora se integra con Zscaler a través de la aplicación Falcon Foundry para Zscaler y proporciona una remediación de circuito cerrado completo entre el entorno aislado avanzado de ZIA, el SIEM de próxima generación de CrowdStrike y el motor de cumplimiento de políticas de ZIA.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Las últimas integraciones de Zscaler y CrowdStrike admiten los siguientes nuevos casos de uso:

Caso de uso 1

Aplicación de políticas de acceso adaptativo según el contexto

Al ampliar el alcance de las capacidades de acceso adaptativo, Zscaler ahora aprovecha el contexto en tiempo real de CrowdStrike, lo que permite una evaluación de riesgos superior y la toma de decisiones de aplicación de políticas. La nueva integración va más allá de aplicar la política de control de acceso basada en los puntajes de estado del dispositivo Falcon ZTA y ahora incorpora datos detallados de incidentes de seguridad de CrowdStrike para evaluar los riesgos en tiempo real.

Zscaler recopila y analiza señales de incidentes de seguridad activos que ocurren en el punto final de CrowdStrike, agregando una rica capa de contexto a su motor de políticas de control de acceso adaptativo y haciendo que el control de acceso Zero Trust impulsado por la postura del dispositivo sea aún más sólido.

El flujo continuo de datos de incidentes de seguridad de CrowdStrike proporciona una postura de seguridad dinámica y receptiva desde el punto final hasta la aplicación, ampliando significativamente las capacidades de acceso adaptativo de Zscaler y permitiendo controles de acceso más granulares y conscientes del contexto.

Con esta nueva capacidad, los administradores de Zscaler ahora pueden establecer umbrales de incidentes de seguridad y otorgar acceso a aplicaciones a puntos finales que cumplan con los criterios de conformidad de Falcon ZTA y los umbrales de incidentes de seguridad especificados.

La integración de CrowdStrike con Zscaler comparte inteligencia sobre amenazas y permite flujos de trabajo automáticos bidireccionales para ayudar a las organizaciones a reducir la cantidad de incidentes de seguridad y, si ocurre un incidente, ofrece un tiempo rápido de detección y remediación.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Caso de uso 2

Cuantificación y visualización integral del ciberriesgo

Zscaler Risk360 es un potente marco de cuantificación y visualización de riesgos para remediar los riesgos de ciberseguridad. Recopila datos reales de fuentes externas, el entorno Zscaler del cliente e investigaciones de seguridad de ThreatLabz para generar un perfil detallado de la postura de riesgo de la organización. El marco abarca las cuatro etapas del ataque, es decir, la superficie de ataque externa, el compromiso, la propagación lateral y la pérdida de datos, y todas las entidades de su entorno, incluidos los activos, las aplicaciones, los usuarios y terceros.

El servicio Risk360 se integra con CrowdStrike para brindar información sobre los factores que contribuyen al riesgo dentro de su organización. Una vez configurado, Zscaler extrae información relacionada con el riesgo de la plataforma Falcon, la clasifica en categorías de etapa de ataque de Risk360 y cuantifica cada factor de riesgo según su ponderación de riesgo.

Esta integración permite a los clientes tomar medidas sobre las políticas para actualizarlas o modificarlas. También incluye flujos de trabajo de investigación guiados que permiten realizar análisis más profundos para investigar problemas específicos.

Caso de uso 3

Contextualización de datos de seguridad y gestión unificada de vulnerabilidades

Actualmente, los equipos de seguridad aprovechan una gran variedad de tecnologías y soluciones para proteger sus empresas de una superficie de ataque en expansión. Cada una de estas herramientas produce cantidades masivas de datos valiosos. Sin embargo, estos datos suelen estar aislados y duplicados en distintas herramientas. Como resultado, los equipos de seguridad se enfrentan a una sobrecarga de información, flujos de trabajo opacos y una creciente dificultad para defender su postura de ciberseguridad.

Data Fabric for Security de Zscaler agrega datos de distintas herramientas, haciéndolos más prácticos y útiles. Transforma la manera en que las operaciones de seguridad gestionan y responden a las amenazas de seguridad al agregar fácilmente datos de más de 150 fuentes, incluidas las vulnerabilidades y exposiciones comunes (CVE) detectadas en el punto final por CrowdStrike. Data Fabric enriquece y correlaciona los datos CVE de CrowdStrike con flujos de datos simultáneos para proporcionar información contextualizada y en tiempo real sobre vulnerabilidades y exposiciones en todo su entorno de TI.

Con este conocimiento, los analistas de seguridad pueden conectar dinámicamente los puntos entre vulnerabilidades, amenazas, hallazgos, incidentes, activos, componentes de software y usuarios, y apoyarse en inteligencia procesable y cruzada para priorizar y abordar de manera eficiente primero las vulnerabilidades y riesgos más críticos.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Caso de uso 4

Intercambio coordinado de información sobre amenazas, detección y respuesta

Desarrollada de manera nativa por CrowdStrike, la aplicación Falcon Foundry Zscaler sirve de base para la integración de Zscaler con CrowdStrike Falcon Next-Gen SIEM. La aplicación preconstruida automatiza y orquesta el intercambio de información sobre amenazas y permite coordinar las acciones a nivel de política para responder de manera rápida y eficaz a las amenazas contra la seguridad.

Disponible en el Marketplace de CrowdStrike, la aplicación preconfigurada permite a los clientes mutuos con licencia mejorar su seguridad perimetral mediante supervisión avanzada y detección de amenazas, utilizando indicadores de compromiso (IoC) obtenidos de los repositorios de inteligencia de amenazas de CrowdStrike. Además, permite a los clientes desarrollar e implementar flujos de trabajo personalizados adaptados a casos de uso específicos de detección, investigación y respuesta a amenazas.

Al crear un bucle de retroalimentación continua y un mecanismo de respuesta coordinado entre el aislamiento de entornos de ZIA, Falcon Next-Gen SIEM y el motor de aplicación de políticas de ZIA, la aplicación lista para usar agiliza la automatización y orquestación del flujo de trabajo de seguridad para acelerar las operaciones de seguridad.

Beneficios de una mejor integración

- **Políticas de acceso adaptativas ricas en contexto:** mejore su postura de seguridad desde el punto final hasta la aplicación al establecer políticas Zero Trust que se adaptan dinámicamente a las condiciones cambiantes.
- **Visibilidad integral del panorama de ciberriesgos:** obtenga una visión precisa de la exposición al riesgo en las cuatro etapas del ataque y aproveche la puntuación de riesgo consolidada en múltiples fuentes para obtener una comprensión completa del ciberriesgo.
- **Datos de seguridad contextualizados para una mejor evaluación de riesgos:** agregue y contextualice los datos de seguridad para priorizar sus mayores riesgos y automatizar el flujo de trabajo para su remediación.
- **Integración SOAR lista para usar:** comience a trabajar con la aplicación Foundry prediseñada para Zscaler y comparta información sobre amenazas. Cree rápidamente flujos de trabajo personalizados de Falcon Fusion SOAR para automatizar la detección, la investigación y la respuesta de principio a fin.
- **Detección rápida y respuesta coordinada:** acelere el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR) con acciones coordinadas de respuesta y cumplimiento de políticas que reduzcan las brechas entre la seguridad de TI y las operaciones de seguridad.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Fortalezca las operaciones de seguridad con Zscaler y CrowdStrike

Zscaler y CrowdStrike tienen la misión de aumentar la aplicación de Zero Trust y fortalecer las operaciones de seguridad con potentes capacidades complementarias. Nuestras integraciones más recientes funcionan a la perfección para elevar sus operaciones de seguridad al siguiente nivel. Juntos, ampliamos la aplicación de Zero Trust más avanzada para dar paso a la era del SOC moderno.



CROWDSTRIKE

Acerca de CrowdStrike
CrowdStrike ha redefinido la seguridad con la plataforma nativa de la nube más avanzada del mundo, que protege y habilita a las personas, los procesos y las tecnologías que impulsan las empresas modernas. CrowdStrike protege las áreas de riesgo más críticas: puntos finales y cargas de trabajo en la nube, identidad y datos, para que los clientes estén un paso por delante de los adversarios de la actualidad y detengan las violaciones. Impulsada por CrowdStrike Security Cloud, la plataforma CrowdStrike Falcon® aprovecha indicadores de ataque en tiempo real, inteligencia de amenazas sobre la evolución de las técnicas de los adversarios y telemetría enriquecida de toda la empresa para ofrecer detecciones hiperprecisas, protección y remediación automatizadas, búsqueda de amenazas de élite y observación priorizada de vulnerabilidades, todo mediante un único agente ligero. Con CrowdStrike, los clientes se benefician de una protección superior, un mejor rendimiento, una menor complejidad y una rentabilización inmediata. Obtenga más información en crowdstrike.com.

OBTENGA MÁS INFORMACIÓN EN
zscaler.com/partners/crowdstrike

Descargue nuestra Guía de implementación de Zscaler + CrowdStrike

zscaler™ | Experience your world, secured.™

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, fuertes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo.
Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

© 2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas registradas listadas en **zscaler.com/mx/legal/trademarks son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y otros países. Cualquier otra marca comercial pertenece a sus respectivos propietarios.**

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134 zscaler.com.mx