CrowdStrike, Okta y Zscaler: Unificando la seguridad con protección entre dominios para mejorar la ciberresiliencia en la era de la IA

Desafíos

Los adversarios se mueven más rápido que nunca, con el tiempo promedio observado de fuga de eCrime en un mínimo histórico de 48 minutos en 2024, y el más rápido en solo 51 segundos[1]. Al mismo tiempo, el 79% de los ataques estaban libres de malware, aprovechando la explotación de identidad, la ingeniería social y las configuraciones incorrectas de la nube para evadir la detección[1]. Las estrategias de seguridad tradicionales y reactivas ya no pueden contrarrestar las tácticas cambiantes de los adversarios modernos. Los actores de amenazas utilizan métodos cada vez más sofisticados, incluyendo la automatización impulsada por IA y las tácticas de sigilo, para infiltrarse y moverse sin ser detectados en los entornos. Para superar estos desafíos, las organizaciones deben ir más allá de las soluciones de seguridad fragmentadas y puntuales, un enfoque que aumenta la complejidad, retrasa la respuesta y, en última instancia, debilita la seguridad general.

¿Qué necesita?

Es el momento de replantearnos cómo abordamos la seguridad y utilizar el poder de la IA para brindar velocidad y escala. Las organizaciones necesitan plataformas de seguridad avanzadas que funcionen juntas sin problemas para brindar protección en capas, reduciendo la complejidad e impulsando la eficiencia operativa.

Solución

Para abordar las amenazas en constante evolución intensificadas por la IA, CrowdStrike, Okta y Zscaler ofrecen una solución de seguridad multidominio totalmente integrada diseñada para eliminar los puntos ciegos, mejorar la visibilidad y acelerar los tiempos de respuesta para mitigación robusta de amenazas. Este enfoque combinado protege y autentica las identidades y permite una gestión dinámica controles de acceso Zero Trust conscientes del contexto y protege puntos finales distribuidos mientras se aprovecha el SIEM de próxima generación para detección y respuesta a amenazas en tiempo real.

Al correlacionar las señales de riesgo en las capas de identidad, puntos finales, nube, red y más allá, los equipos de seguridad obtienen una visión unificada del movimiento del adversario, lo que les permite detectar, contener y neutralizar las amenazas antes de que causen daños. Con automatización impulsada por IA, intercambio de inteligencia sobre amenazas bidireccional y acciones de respuesta coordinadas, la solución conjunta no solo detecta amenazas, sino que las detiene antes de que escalen.

Los equipos de seguridad pueden anticipar las tácticas de los adversarios, automatizar las acciones de respuesta y moverse a la velocidad de la máquina para contener los ataques antes de que los adversarios se presenten.

A medida que las amenazas cibernéticas se vuelven más rápidas y sofisticadas, las organizaciones deben adoptar una defensa proactiva impulsada por IA que opere a la velocidad del adversario, garantizando que las amenazas se neutralicen antes de que afecten al negocio.

Seguridad que funciona como una sola: protección unificada para una nueva era

Para las organizaciones que se embarcan en un viaje Zero Trust o diseñan una solución Zero Trust que maximiza las inversiones actuales, las alianzas sólidas y la experiencia comprobada las integraciones de los líderes del mercado

1. Informe de amenazas globales de CrowdStrike 2025, https://www.crowdstrike.com/en-us/global-threat-report/

CROWDSTRIKE | okta | zscaler

CrowdStrike, Okta y Zscaler proporcionan un modelo para una solución Zero Trust de extremo a extremo, desde los usuarios hasta los puntos finales y las aplicaciones.

Estas integraciones proporcionan a los administradores información en tiempo real visibilidad del panorama de amenazas y la postura de seguridad de los puntos finales y las aplicaciones. El acceso a aplicaciones críticas se puede cambiar según el usuario, el punto final y las políticas de acceso. Si ocurre un ataque, se activa rápidamente una solución multiplataforma. Las defensas son más amplias fortalecido con políticas de prevención aplicadas en todo el país integraciones para ayudar a frustrar ataques similares en el futuro.

El resultado neto es un sistema dinámico, nativo de la nube y de primera clase. Solución Zero Trust basada en el contexto que ayuda a los equipos a mantenerse por delante de las amenazas modernas impulsadas por IA con un riesgo reducido y una implementación simplificada, eliminando la complejidad de los enfoques "hágalo usted mismo".

Aspectos destacados de la solución

Acceso adaptativo Zero Trust:

Zscaler aplica un acceso con privilegios mínimos en función de la identidad del usuario, la postura del dispositivo y el contexto de riesgo, y Zscaler Zero Trust Exchange (ZTE) integra Identity Threat Protection con Okta AI (ITP) y puntuaciones CrowdStrike Falcon® ZTA para implementar políticas de acceso basadas en riesgos en tiempo real.

Gestión automatizada del ciclo de vida de la identidad:

Okta optimiza el aprovisionamiento y desaprovisionamiento de usuarios a través de la integración de Okta SCIM, lo que permite actualizaciones basadas en roles en tiempo real y reduce la carga de trabajo manual.

Identidad y detección de amenazas en endpoints:

CrowdStrike detecta y mitiga las amenazas dirigidas a los usuarios y los endpoints al compartir señales de Zscaler Deception con Okta ITP para obtener respuestas adaptativas, mientras que la telemetría de CrowdStrike proporciona un contexto enriquecido para impulsar la detección de amenazas.

Autenticación continua y acceso basado en riesgos:

Zscaler aplica políticas de acceso dinámicas y Okta activa una autenticación incremental en función del comportamiento anómalo detectado por Zscaler o CrowdStrike.

Visibilidad de riesgo unificada:

Zscaler Risk360 y Data Fabric ingieren registros de identidad de Okta y señales de puntos finales de CrowdStrike.

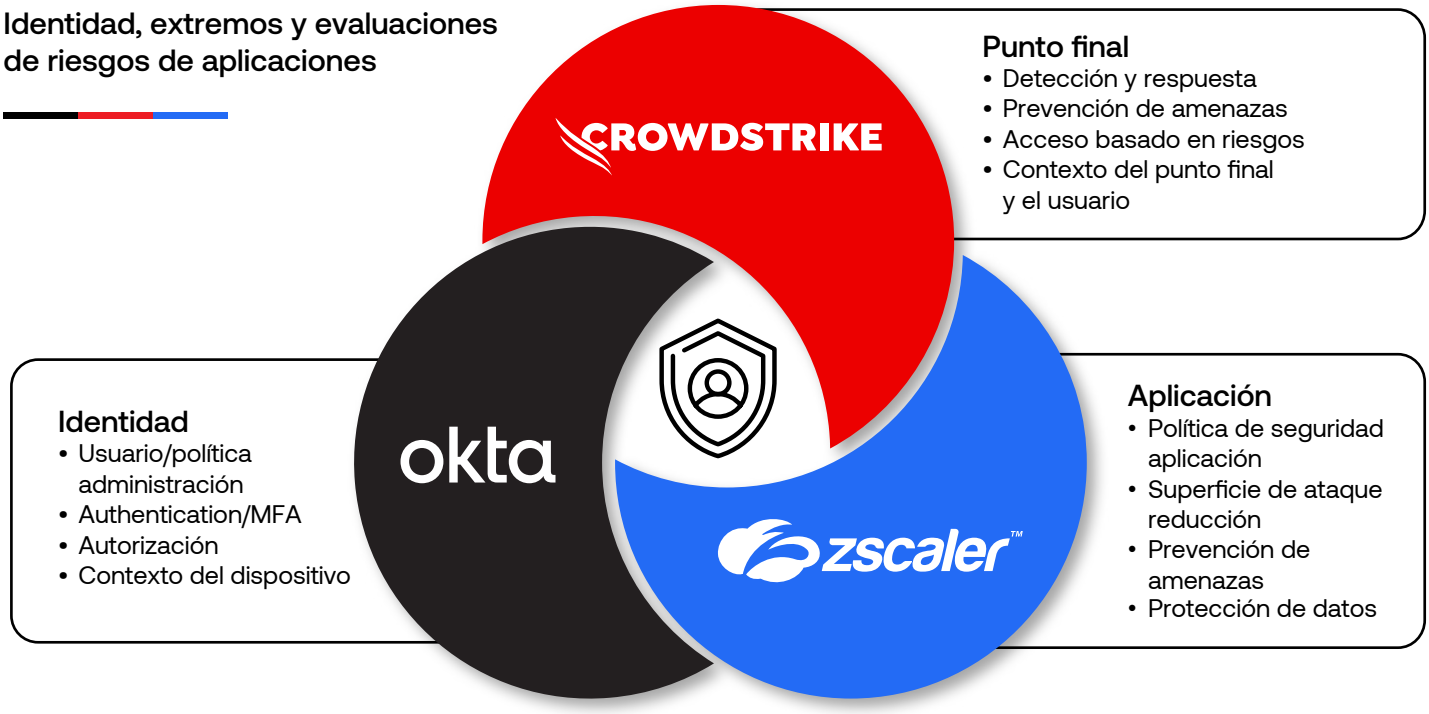
Intercambio de inteligencia sobre amenazas entre plataformas:

Zscaler comparte telemetría unificada para acelerar la detección y la respuesta, y CrowdStrike mejora las listas de bloqueo personalizadas de Zscaler para una protección proactiva.

Detección y respuesta unificadas ante amenazas entre dominios:

CrowdStrike ofrece visibilidad integral y respuestas automatizadas y coordinadas en todos los puntos finales, identidades y aplicaciones a través de las integraciones de CrowdStrike Falcon® Next-Gen SIEM y CrowdStrike Falcon® Fusion SOAR con Okta y Zscaler para ver y detener rápidamente las amenazas entre dominios, lo que evita el movimiento lateral.

Identidad, extremos y evaluaciones de riesgos de aplicaciones



Telemetría e inteligencia sobre amenazas compartidas

Los beneficios de las sinergias combinadas para una ciberresiliencia de siguiente nivel

1. Acceso Zero Trust mejorado:
El acceso Zero Trust previene el movimiento lateral de amenazas gracias a la aplicación de políticas de acceso adaptativas basadas en la identidad del usuario, la postura del dispositivo y el contexto de la amenaza en tiempo real.

2. Detección y remediación automatizadas de amenazas:
La detección en tiempo real y la inteligencia de amenazas activan respuestas inmediatas y coordinadas, que incluyen la aplicación de políticas y el cierre de sesión universal.

3. Visibilidad unificada de riesgos:
Zscaler Risk360 se integra con los registros de CrowdStrike y Okta para proporcionar telemetría contextualizada e información completa sobre riesgos, lo que acelera la investigación y la remediación.

4. Investigación y respuesta rápidas:
Investigación y respuesta aceleradas mediante la integración con CrowdStrike Falcon Next-Gen SIEM que proporciona la unificación de visibilidad, detección impulsada por IA y flujos de trabajo automatizados para contener rápidamente amenazas entre dominios.

5. Gestión eficiente de la identidad:
El aprovisionamiento basado en SCIM de Okta garantiza la seguridad, el aprovisionamiento y el desaprovisionamiento automatizado de usuarios, permitiendo sólo el acceso autorizado.

6. Mejora de la experiencia del usuario:
Acceso sin inconvenientes habilitado por Okta SSO, MFA y las políticas adaptativas de Zscaler mejora la productividad sin comprometer la seguridad.

Conclusión

CrowdStrike, Okta y Zscaler ofrecen soluciones de seguridad integradas y simplificadas que mejoran la protección, reducen la complejidad y garantizan la escalabilidad para los ecosistemas digitales en evolución actual.

Juntos, empoderan a las organizaciones con una defensa Zero Trust que simplifica el acceso basado en identidad y fortalece la detección de amenazas entre dominios. Esta poderosa asociación ayuda a las organizaciones a fortalecer de manera proactiva su postura de ciberseguridad y desarrollar resiliencia para la era de la IA.

Acerca de CrowdStrike

CrowdStrike (NASDAQ: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa de la nube más avanzada del mundo para proteger áreas críticas de riesgo empresarial: puntos finales y cargas de trabajo en la nube, identidad y datos. La plataforma Falcon, diseñada específicamente en la nube con una única arquitectura de agente liviano, ofrece una implementación rápida y escalable, protección y rendimiento superiores, menor complejidad y tiempo inmediato para obtener valor.

Acerca de Okta

Okta, Inc. es la empresa de identidad del mundo™. Aseguramos la identidad para que todos sean libres de usar cualquier tecnología de forma segura. Nuestras soluciones para clientes y fuerza laboral permiten a las empresas y desarrolladores utilizar el poder de la identidad para impulsar la seguridad, la eficiencia y el éxito, todo ello mientras protegen a sus usuarios, empleados y socios. Descubra por qué las marcas líderes del mundo confían en Okta para la autenticación, autorización y más en okta.com.

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, sólidos y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de los usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la mayor plataforma de seguridad en línea en la nube del mundo.

Obtenga más información sobre nuestras soluciones en okta.com, crowdstrike.com, y zscaler.es |