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

Problemas

Los ciberdelincuentes se mueven más rápido que nunca: en 2024, el tiempo medio de ataque observado se redujo a un mínimo histórico de 48 minutos, y el más rápido se produjo en tan solo 51 segundos[1]. Al mismo tiempo, el 79 % de los ataques no contenían malware, sino que aprovechaban la explotación de identidades, la ingeniería social y las configuraciones erróneas de la nube para eludir la detección[1]. Las estrategias de seguridad tradicionales y reactivas ya no pueden contrarrestar las tácticas cambiantes de los adversarios modernos. Los actores malintencionados utilizan métodos cada vez más sofisticados, como la automatización basada en IA y las tácticas de ocultación, para infiltrarse y moverse sin ser detectados por los entornos. Para superar estos retos, las organizaciones deben ir más allá de las soluciones de seguridad puntuales y fragmentadas, un enfoque que aumenta la complejidad, retrasa la respuesta y, en última instancia, debilita la seguridad general.

Lo que necesita

Ha llegado el momento de replantearnos cómo enfocamos la seguridad y utilizar el poder de la IA para proporcionar velocidad y escala. Las organizaciones necesitan plataformas de seguridad avanzadas que funcionen juntas de manera fluida para ofrecer protección por capas, reduciendo la complejidad e impulsando la eficacia operativa.

Solución

Para hacer frente a las amenazas en evolución intensificadas or la IA, CrowdStrike, Okta y Zscaler proporcionan una solución de seguridad multidominio totalmente integrada, diseñada para eliminar los puntos ciegos, mejorar la visibilidad y acelerar los tiempos de respuesta para una mitigación sólida de las amenazas. Este enfoque combinado protege y autentica identidades, permite controles de acceso dinámicos Zero Trust sensibles al contexto y protege los puntos finales distribuidos, al tiempo que aprovecha la tecnología SIEM de última generación para la detección y respuesta a amenazas en tiempo real.

Al correlacionar las señales de riesgo entre las capas de identidad, puntos finales, nube, red y más, los equipos de seguridad obtienen una visión unificada de los movimientos de los adversarios, lo que les permite detectar, contener y neutralizar las amenazas antes de que causen daños. Gracias a la automatización impulsada por IA, el intercambio bidireccional de inteligencia sobre amenazas y las acciones de respuesta coordinadas, la solución conjunta no solo detecta las amenazas, sino que las detiene antes de que se intensifiquen.

Los equipos de seguridad pueden anticipar las tácticas de los adversarios, automatizar las acciones de respuesta y actuar a la velocidad de una máquina para contener los ataques antes de que los adversarios logren escapar.

A medida que las amenazas cibernéticas se vuelven más rápidas y sofisticadas, las organizaciones deben adoptar una defensa proactiva impulsada por la inteligencia artificial que opere a la velocidad de los adversarios, garantizando que las amenazas se neutralicen antes de que afecten a la empresa.

Seguridad unificada: protección integrada para una nueva era

Para las organizaciones que inician su transformación al modelo Zero Trust o que diseñan una solución Zero Trust

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

que maximiza las inversiones actuales, las alianzas sólidas y las integraciones probadas de los líderes del mercado CrowdStrike, Okta y Zscaler proporcionan un modelo para una solución Zero Trust integral, desde los usuarios hasta los puntos finales y las aplicaciones.

Estas integraciones proporcionan a los administradores visibilidad en tiempo real del panorama de amenazas y del estado de seguridad de los puntos finales y las aplicaciones. El acceso a aplicaciones críticas se puede modificar en función del usuario, el punto final y las políticas de acceso.

Si se produce un ataque, se activa rápidamente la remediación multiplataforma. Las defensas se refuerzan aún más con políticas de prevención aplicadas en todas las integraciones para ayudar a frustrar ataques similares en el futuro.

El resultado final es una solución Zero Trust dinámica, basada en el contexto, nativa de la nube y de primera categoría que ayuda a los equipos a anticiparse a las amenazas modernas impulsadas por la inteligencia artificial con un riesgo reducido y una implementación simplificada, eliminando la complejidad de los enfoques autogestionados.

Puntos destacados de la solución

Acceso adaptativo de Zero Trust:

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

Detección de amenazas y respuesta unificadas entre dominios:

CrowdStrike ofrece una visibilidad completa y respuestas coordinadas y automatizadas 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, evitando el movimiento lateral.

Detección de amenazas de identidad y puntos finales:

CrowdStrike detecta y mitiga las amenazas dirigidas a usuarios y puntos finales compartiendo las señales de Zscaler Deception con Okta ITP para respuestas adaptativas, mientras que la telemetría de CrowdStrike proporciona un contexto enriquecido para impulsar la detección de amenazas.

Gestión automatizada del ciclo de vida de las identidades:

Okta agiliza el aprovisionamiento y la eliminación de usuarios mediante la integración con Okta SCIM, lo que permite actualizaciones en tiempo real basadas en roles y reduce la carga de trabajo manual.

Visibilidad de riesgos unificada:

Zscaler Risk360 y Data Fabric ingieren registros de identidad de Okta y señales de punto final de CrowdStrike.

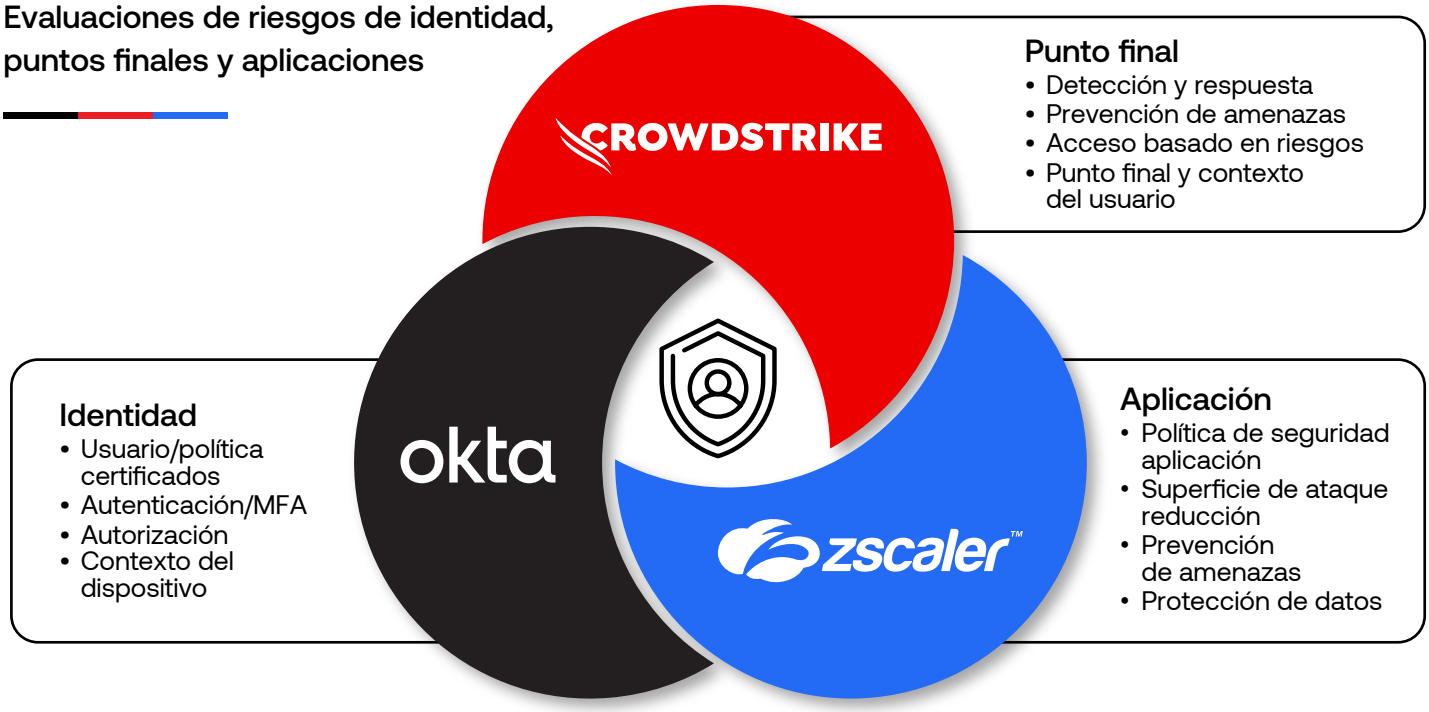
Autenticación continua y acceso basado en riesgos:

Zscaler aplica políticas de acceso dinámicas con Okta activando la autenticación escalonada basada en comportamientos anómalos detectados por Zscaler o CrowdStrike.

Intercambio de inteligencia sobre amenazas entre plataformas:

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

Evaluaciones de riesgos de identidad, puntos finales y aplicaciones



Telemetría compartida e inteligencia sobre amenazas

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

1. Acceso de zero trust mejorado:
El acceso de zero trust evita el movimiento lateral de amenazas con la aplicación de políticas de acceso adaptativas basadas en la identidad del usuario, la postura del dispositivo y el contexto de amenazas en tiempo real.

2. Detección y corrección automatizadas de amenazas:
La detección en tiempo real y la inteligencia sobre amenazas desencadenan respuestas inmediatas y coordinadas, incluida la aplicación de políticas y el cierre de sesión universal.

3. Visibilidad unificada de riesgos:
Zscaler Risk360 se integra con registros de CrowdStrike y Okta para proporcionar telemetría contextualizada y perspectivas de riesgo integrales, acelerando la investigación y la remediación.

4. Investigación y respuesta rápidas:
La investigación y respuesta aceleradas mediante la integración con la SIEM de nueva generación de CrowdStrike Falcon proporciona visibilidad unificada, detección potenciada por IA y flujos de trabajo automatizados para contener rápidamente las amenazas entre dominios.

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

6. Experiencia de usuario mejorada:
El acceso ininterrumpido habilitado por Okta SSO, MFA y las políticas adaptables 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 de la actualidad.

Juntos, proporcionan a las organizaciones una defensa Zero Trust que simplifica el acceso basado en la identidad y refuerza la detección de amenazas entre dominios. Esta potente alianza ayuda a las organizaciones a reforzar de forma proactiva su postura de ciberseguridad y a 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 en la nube más avanzada del mundo para proteger las áreas críticas de riesgo empresarial: puntos finales y cargas de trabajo en la nube, identidad y datos. Creada específicamente en la nube con una única arquitectura de agente ligero, la plataforma Falcon ofrece una implantación rápida y escalable, una protección y un rendimiento superiores, una complejidad reducida y una rentabilidad inmediata.

Acerca de Okta

Okta, Inc. es la empresa de identidad del mundo (The World's Identity Company™). Aseguramos la identidad para que todos sean libres de usar cualquier tecnología de forma segura. Nuestras soluciones para clientes y personal permiten a empresas y desarrolladores utilizar el poder de la identidad para impulsar la seguridad, la eficacia y el éxito, protegiendo al mismo tiempo 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, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos al conectar de forma segura a los usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos a nivel mundial, Zero Trust Exchange basado en SASE es la plataforma de seguridad en la nube en línea más grande del mundo.

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