Okta, CrowdStrike y Zscaler ofrecen la mejor solución Zero Trust integrada que proporciona seguridad entre dominios y basada en el contexto.

Desafíos

Proteger a sus usuarios, puntos finales y aplicaciones es un desafío mientras a la vez trabaja para implementar iniciativas de transformación digital y respaldar a su fuerza laboral distribuida. Este desafío se ve exacerbado por un panorama de amenazas en evolución.

Las identidades de usuario, los puntos finales, las aplicaciones y las redes son vectores de ataque principales que amplían la superficie de ataque y aumentan el riesgo. Las soluciones de seguridad puntuales que abordan un área, pero no se integran bien con otras soluciones le dan una falsa sensación de seguridad. Este enfoque deja lagunas en la cobertura de seguridad y expone a las organizaciones a riesgos cibernéticos y costosas soluciones. Esto explica por qué estamos viendo un aumento en el número de ciberataques a pesar de las inversiones adicionales en soluciones de ciberseguridad.

¿Qué necesita?

Durante años, las organizaciones han intentado ir por delante de sus adversarios incorporando soluciones de seguridad puntuales para cerrar cualquier brecha en su arquitectura de seguridad. Ahora hemos llegado a un punto de rendimientos decrecientes y agregar productos adicionales está agregando más complejidad, aumentando los tiempos de respuesta y, en última instancia, haciendo que estemos menos seguros. Es el momento de replantearnos cómo abordamos la seguridad y utilizar el poder de la IA para brindar velocidad y escala. Tener soluciones de seguridad avanzadas adecuadas que trabajen juntas a la perfección ofrece un enfoque de seguridad por capas muy necesario, ayudar a impulsar la eficiencia operativa y reducir la complejidad.

Solución

El compromiso con un enfoque Zero Trust, que se basa en la verificación continua en tiempo real y basada en riesgos de la identidad del usuario, el contexto del punto final y la política comercial, llevará a un nivel superior a la seguridad de las organizaciones. Este enfoque proporciona mayor simplicidad, mejor seguridad y mayor agilidad empresarial que las soluciones puntuales de seguridad heredadas y aisladas para hacer posible una transformación digital exitosa.

La seguridad integrada es poderosa

Una arquitectura Zero Trust tiene tres pilares fundamentales:

Identidades **Puntos finales** **Aplicaciones**

Para las organizaciones que se embarcan en un viaje hacia el Zero Trust o que diseñan una solución Zero Trust que maximiza las inversiones actuales, las sólidas asociaciones e integraciones probadas previamente de los líderes del mercado Okta, CrowdStrike y Zscaler brindan un modelo para una solución Zero Trust de extremo a extremo: desde los usuarios hasta los puntos finales y las aplicaciones.

Estas integraciones garantizan que los administradores vean en tiempo real el panorama de amenazas y la postura de seguridad de sus puntos finales y aplicaciones.

El acceso a las aplicaciones críticas se puede cambiar dinámicamente según el contexto del usuario, el punto final y las políticas de acceso. Y si hay algún ataque, se toman rápidamente medidas de remediación entre plataformas. Las defensas se fortalecen aún más con políticas de prevención que se agregan a todas las integraciones para frustrar ataques similares en el futuro.

El resultado final es la mejor solución Zero Trust nativa de la nube y basada en el contexto que simplifica la implementación al eliminar la complejidad de las soluciones de seguridad que tiene que gestionar usted y, al mismo tiempo, reduce el riesgo.

Resultados comerciales clave

Prevención

Reduzca la superficie de ataque y evite compromisos a través de la información sobre amenazas y el uso compartido de telemetría entre dominios para impulsar decisiones de control de acceso Zero Trust y verificación continua.

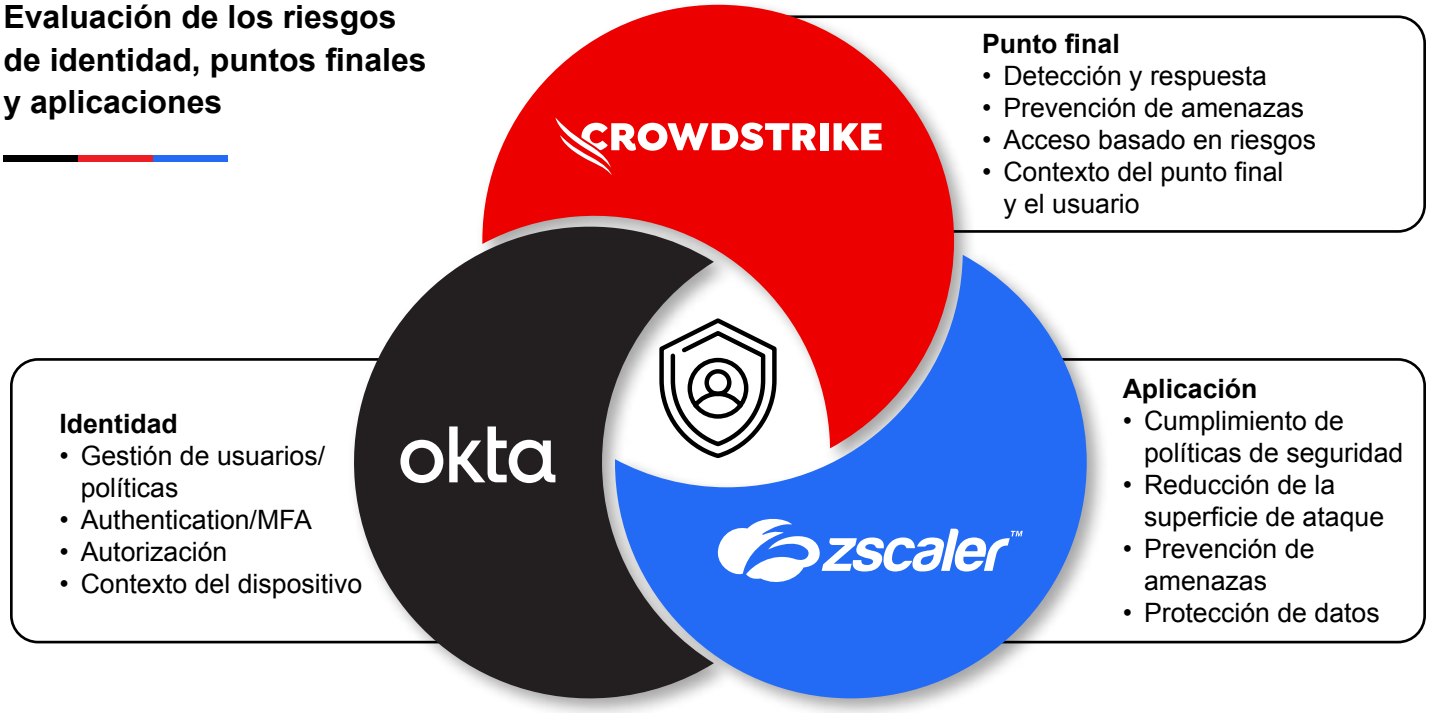
Contención

Proporcione contención de amenazas en tiempo real evitando el movimiento lateral con la detección de amenazas modernas, como el compromiso de credenciales, el malware de día cero, el ransomware o las amenazas internas, y permitiendo la aplicación de medidas entre dominios.

Respuesta

Acelere la detección y respuesta a amenazas multidominio a través del intercambio de telemetría contextual para descubrir, clasificar e investigar incidentes rápidamente, lo que lleva a una remediación más rápida y precisa.

Evaluación de los riesgos de identidad, puntos finales y aplicaciones



Telemetría e inteligencia sobre amenazas compartidas

Obtenga más información sobre nuestras soluciones en okta.com, crowdstrike.com y zscaler.es | ©2024