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

Problemas

Proteger a sus usuarios, puntos finales y aplicaciones es todo un desafío cuando trabaja para poner en marcha iniciativas de transformación digital y dar soporte a su fuerza de trabajo 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. Un enfoque de este tipo deja lagunas en la cobertura de seguridad y expone a las organizaciones al riesgo cibernético y a costosas medidas correctivas. Esto explica por qué estamos viendo un aumento en el número de ciberataques a pesar de las inversiones adicionales en soluciones de ciberseguridad.

Lo que necesita

Durante años, las organizaciones han intentado superar a sus adversarios añadiendo más soluciones de seguridad puntuales para tapar las deficiencias de su arquitectura de seguridad. Ahora hemos llegado a un punto de rendimientos decrecientes en donde añadir productos adicionales significa añadir más complejidad, aumentar los tiempos de respuesta y, en última instancia, hacernos más vulnerables. Ha llegado el momento de replantearnos cómo enfocamos la seguridad y utilizar el poder de la IA para proporcionar velocidad y escala. Disponer de las soluciones de seguridad avanzadas adecuadas que funcionen juntas a la perfección puede ofrecer un enfoque por capas muy necesario para la seguridad, ayudar a impulsar la eficacia operativa y reducir la complejidad.

Solución

El compromiso con un enfoque de Zero Trust que se basa en la verificación continua en tiempo real y en función de los riesgos de la identidad del usuario, el contexto del punto final y la política empresarial, mejorará la seguridad de las organizaciones. Este enfoque proporciona una mayor simplicidad, una seguridad mejorada y más agilidad empresarial que las soluciones de seguridad heredadas puntuales y en silos para permitir el éxito de la transformación digital.

La seguridad integrada significa seguridad de máximo nivel

Hay tres pilares fundamentales de una arquitectura Zero Trust:

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

Para las organizaciones que emprenden un viaje hacia Zero Trust o que estén diseñando una solución Zero Trust que maximice las inversiones actuales, las asociaciones sólidas y las integraciones previamente verificadas de los líderes del mercado Okta, Crowdstrike 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 garantizan que los administradores tengan una visión en tiempo real del panorama de amenazas y de la postura de seguridad de sus puntos finales y aplicaciones.

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

El resultado final es una solución Zero Trust de primera clase, nativa de la nube y basada en el contexto, que simplifica la implementación eliminando la complejidad de las soluciones de seguridad manuales, al tiempo que reduce el riesgo.

Resultados empresariales clave

Prevención

Reduzca la superficie de ataque y evite el compromiso mediante el intercambio de información sobre amenazas y telemetría entre dominios para impulsar las decisiones de control de acceso Zero Trust y la verificación continua.

Contención

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

Respuesta

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

Evaluaciones de riesgos de identidad, puntos finales y aplicaciones

Punto final
- Detección y respuesta
- Prevención de amenazas
- Acceso basado en riesgos
- Punto final y contexto del usuario

Identidad
- Gestión de usuarios/ políticas
- Autenticación/MFA
- Autorización
- Contexto del dispositivo

Aplicación
- Aplicación de políticas de seguridad
- Reducción de la superficie de ataque
- Prevención de amenazas
- Protección de datos

Telemetría compartida e inteligencia sobre amenazas

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