Seguridad y Gestión de Riesgos

SPARK Matrix™: Protección Digital contra Riesgos (DRP), 2022

Perspectivas del mercado, evaluación competitiva y clasificación de proveedores Rankings

Junio 2022

TABLA DE CONTENIDOS

Resumen Ejecutivo

Este servicio de investigación incluye un análisis detallado de la dinámica del mercado global, la solución de protección contra riesgos digitales (DRP), las principales tendencias, el panorama de los proveedores y el análisis de posicionamiento competitivo. El estudio proporciona análisis de la competencia y clasificación de los principales proveedores de DRP en forma de SPARK Matrix. Esta investigación proporciona información estratégica para que los proveedores de tecnología comprendan mejor el mercado que respalda sus estrategias de crecimiento y para que los usuarios evalúen las capacidades de los diferentes proveedores, la diferenciación competitiva y su posición en el mercado.

Dinámica del mercado y visión general

Quadrant Knowledge Solutions define el DRP como la solución Digital Risk Protection (DRP) que protege a las organizaciones de las amenazas cibernéticas al identificar y eliminar ataques en tiempo real en los activos digitales de las organizaciones, incluidos los canales de redes sociales, los dispositivos IoT e incluso los proveedores externos expuestos a diversas formas de amenazas digitales.

Una solución DRP proporciona visibilidad de la superficie, la dark web y deep webprofunda para identificar amenazas potenciales. Protege todos los activos externos, como sitios web, transacciones de terceros, intercambio de datos, aplicaciones móviles, panorama en la nube, canales de redes sociales, dispositivos de Internet de las cosas (IoT) e incluso proveedores de terceros de amenazas cibernéticas. La solución detecta, previene y responde a varios tipos de amenazas cibernéticas asignando una puntuación de riesgo a cada vulnerabilidad identificada para que las más críticas puedan abordarse y remediarse con prioridad. Una solución DRP ofrece información procesable e inteligente sobre varios activos digitales que son propensos a los riesgos y, por lo tanto, permite a las organizaciones desarrollar soluciones sólidas para mitigar las amenazas y ofrecer una mejor protección. Una plataforma DRP avanzada aprovecha las tecnologías de AI/ML, como la detección basada en tecnología neural, la inteligencia de estafas, la puntuación autoajustable y otras para detectar el uso ilegítimo de activos digitales en una amplia gama de recursos. Estos recursos incluyen nombres de dominio, tiendas de aplicaciones móviles, redes sociales, mensajeros, deep & dark web, bases de datos de phishing y más.

Las soluciones DRP tienen como objetivo contrarrestar las amenazas digitales calculando la puntuación de riesgo para cada vulnerabilidad y luego decidiendo el nivel de riesgo para cada una de ellas. Las soluciones identifican varios tipos de riesgos digitales, como amenazas cibernéticas, daños a la marca, amenazas internas y cumplimiento, y luego asignan una puntuación de riesgo para abordar cada vulnerabilidad para su corrección. Las soluciones DRP se centran en detectar, prevenir y responder a las amenazas cibernéticas mediante el monitoreo de fugas de datos (intencionales y no intencionales), compromiso de marca (derechos de autor, marcas comerciales, productos duplicados), adquisiciones de cuentas (suplantaciones de cuentas), campañas de fraude: phishing y daños a la reputación, entre otros.

Antes de DRP, los firewalls y los sistemas de autenticación eran los métodos tradicionales para encontrar riesgos. Sin embargo, estos enfoques tradicionales eran inadecuados para identificar, evaluar y gestionar el riesgo. Estos métodos convencionales se enfrentan a muchos desafíos durante el rápido cambio de las empresas hacia la digitalización, ya que su cobertura no puede extenderse a los canales de comunicación digital y las plataformas de redes sociales. Además, estos controles de seguridad tradicionales se basan en patrones,

firmas y reglas empíricas. Esto da como resultado un lapso de tiempo entre el descubrimiento y la corrección de nuevos ataques. Este tiempo transcurrido hace que sea más fácil para los ciberdelincuentes hackear el sistema.

La efectividad de los métodos tradicionales se ha visto desafiada aún más por el aumento sin precedentes de las amenazas cibernéticas, impulsadas por la digitalización de las empresas, el trabajo remoto, el aumento de la actividad en línea y la mayor adopción de BYOD. Los avances tecnológicos están haciendo posible que los ciberdelincuentes encuentren formas innovadoras de lanzar nuevos ataques de creciente sofisticación. Por lo tanto, para evitar estos desafíos, incluido el retraso en la detección a través de métodos tradicionales y la corrección, las organizaciones están adoptando tecnologías sofisticadas como DRP para una visibilidad más rápida y una temprana detección y eliminación de amenazas y vulnerabilidades para garantizar una mayor seguridad necesaria para operar sin problemas en entornos desafiantes.

La solución DRP va más allá de la detección de amenazas para proteger continuamente los activos digitales a través de un proceso cíclico de detección y remediación. Se compromete a mejorar la postura de seguridad continua de todos los activos digitales y las redes de proveedores en todos los canales en línea, como los canales sociales, móviles, de la deep y dark web. Al mejorar la seguridad y aumentar la confianza, las soluciones DRP están ganando popularidad entre las organizaciones en todas las verticales.

La solución de gestión de riesgos digitales tiene la capacidad de integrar y gestionar los riesgos derivados de la transformación y los impactos digitales extendidos en toda la organización. Las siguientes son las capacidades clave de una solución DRP:

- **Ingesta de datos: :** Las soluciones DRP recopilan grandes cantidades de datos a través de la superficie web, la deep web, la dark web, las redes sociales, los blogs, las fuentes de datos públicas y privadas y otras fuentes de terceros para obtener una amplia visibilidad de las amenazas externas en línea. Los datos se recopilan y procesan mediante técnicas como el análisis, el rastreo, la lucha contra la evasión y el pivote. La capacidad de ingesta de datos aprovecha la inteligencia integral utilizando modelos avanzados de aprendizaje automático impulsados por IA que derivan automáticamente información sobre los datos que se ingieren para su posterior procesamiento e impulsar una amplia gama de propósitos de inteligencia.

- **Mapeo de activos:** El mapeo de activos es la capacidad clave de las soluciones DRP. Esta capacidad identifica vulnerabilidades en constante evolución y crecimiento al pensar más allá del firewall para comprender dónde y cómo se pueden atacar los activos y

mapear todos los activos digitales y físicos de caras externas. Implica identificar varios puntos de entrada potenciales de ataques en el ecosistema, mantener un inventario de todos los activos y mapear los rastros digitales para comprender mejor los tipos de amenazas y la acción requerida para mitigarlas. El seguimiento de los rastros digitales en constante crecimiento sigue siendo un desafío y, por lo tanto, el mapeo de rastros digitales identifica todos los activos orientados a Internet, incluidas las integraciones de terceros en la infraestructura. El mapeo del rastro digital permite a las soluciones DRP identificar el riesgo de ciberseguridad, las fugas de datos, el riesgo de terceros y el riesgo operativo en todo el ecosistema digital.

- **Evaluación digital de riesgos:** Un sistema DRP puede identificar automáticamente amenazas y violaciones más allá del perímetro de la red de la organización. Proporciona evaluaciones de riesgos digitales automatizadas continuas de los activos de la organización. La evaluación digital de riesgos permite la intervención manual y automática, dependiendo del tipo, la escala y la gravedad del riesgo. Aborda los problemas de seguridad mediante el uso de inteligencia de amenazas para monitorear, recopilar y analizar eventos de amenazas en canales web, sociales y móviles y utiliza análisis incorporados para evaluar el riesgo asociado. Proporciona indicadores como quién está atacando, cuáles son sus motivaciones y capacidades, y dónde buscar qué áreas están comprometidas en los sistemas, lo cual ayuda a tomar decisiones informadas.

- **Puntuación de amenazas:** las soluciones de protección de riesgos digitales pueden utilizar indexación avanzada de datos, análisis predictivo, inteligencia artificial y aprendizaje profundo para identificar el uso y las violaciones de activos ilegítimos en línea. Las soluciones DRP identifican y clasifican las amenazas y proporcionan puntuaciones basadas en el contexto y la gravedad de los riesgos digitales. Los puntajes de amenaza se calculan mediante algoritmos de IA en función de las especificaciones proporcionadas por la empresa. La puntuación ayuda a priorizar los eventos de riesgo y remediar primero los eventos de alto riesgo.

- **Respuesta y remediación:** Las soluciones de protección de riesgos digitales protegen a las organizaciones de diversas amenazas en línea al ofrecer respuesta y corrección en tiempo real. Una solución DRP proporciona detección en tiempo real y corrección automatizada, que podría incluir la eliminación de la infraestructura del atacante para prevenir futuros ataques. Una solución DRP también genera informes detallados de todas las campañas de mitigación de riesgos para informar sobre la inteligencia procesable.

- **Panel y visualización:** Una solución DRP permite la gestión de riesgos al proporcionar capacidades de visualización a través de un panel digital personalizable que representa gráficamente los riesgos en tiempo real. Esta representación visual facilita a los gestores de riesgos la comprensión del nivel de amenazas y la aplicación del conjunto adecuado de controles para mitigarlas, lo que permite una identificación, prevención o predicción más rápida de los incidentes. Recopila y recopila datos de diferentes fuentes y los coloca en una sola presentación gráfica para que sea fácil de entender y analizar. Esta visualización ayuda a dar sentido a los datos complejos al notar patrones, eliminando el tiempo dedicado al análisis de datos, reduciendo el riesgo de pasar por alto información importante y permitiendo a las partes interesadas tomar medidas rápidas.

Panorama competitivo y análisis

Quadrant Knowledge Solutions realizó un análisis en profundidad de los principales proveedores de protección contra riesgos digitales (DRP) mediante la evaluación de sus productos, presencia en el mercado y propuesta de valor para el cliente. La evaluación se basa en la investigación primaria con entrevistas a expertos, el análisis de casos de uso y el análisis interno del mercado general que realiza Quadrant. Este estudio incluye un análisis de proveedores clave, incluidos Appgate, Axur, Blueliv, Crisp, CTM360, Cyberint, CybelAngel, DigitalStakeout, Digital Shadows, Flashpoint, FraudWatch, IntSights, Phishlabs, Proofpoint, Recorded Future, RiskIQ, SafeGuard Cyber y ZeroFox.

Appgate, CTM360, CybelAngel, CyberInt, Digital Shadows, Flashpoint, IntSights, Recorded Future y ZeroFox son los líderes tecnológicos y de mejor rendimiento en el mercado global de DRP. Estas compañías proporcionan una plataforma tecnológica de protección de riesgos digitales sofisticada e integral para abordar una variedad de casos de uso de DRP.

Digital Shadows y ZeroFox se posicionan como los líderes. **Digital Shadows** ofrece capacidades de DRP a través de su plataforma SearchLight, que proporciona visibilidad del panorama de riesgos digitales de las organizaciones de los clientes mediante la gestión y mitigación de amenazas de ciberseguridad, exposiciones y violaciones de datos, amenazas de marca y riesgos de terceros. La plataforma ofrece libros de jugadas automatizados incorporados basados en el marco NIST, lo que reduce el tiempo de clasificación al recomendar un plan claro paso a paso para la respuesta y, en algunos casos de uso, se puede configurar para desencadenar la acción automática. La plataforma también ofrece integraciones con XSOAR y Splunk Phantom para permitir la utilidad del cliente y reducir la fricción dentro del ecosistema de tecnología de seguridad.

ZeroFox ofrece una plataforma que aprovecha una amplia gama de fuentes de datos y análisis basados en IA para proteger a las organizaciones de ataques dirigidos, compromisos de marca, exposiciones de credenciales y explotación de datos. La plataforma ofrece soluciones de interrupción del adversario y eliminaciones integrales para abordar las amenazas al proporcionar características como ocultar, bloquear y eliminar contenido malicioso u ofensivo, eliminar cuentas y sitios de redes sociales falsos, hacer cumplir los términos del servicio y prohibir aún más a los atacantes al deshabilitar su infraestructura con la ayuda de la red de interrupción global de la compañía.

Appgate proporciona una solución de protección contra amenazas digitales que ofrece visibilidad de amenazas y capacidades de gestión de riesgos para monitorear y detectar datos comprometidos y proporcionar información

detallada y procesable. La solución se centra en minimizar el impacto del fraude y los incidentes de seguridad, y proporcionar mitigación de amenazas y protección a las empresas seguras. La solución incluye la función Victim Insights, que ofrece un enfoque de remediación específico y proactivo, detección de documentación expuesta y código fuente filtrado en repositorios de código público. La solución también proporciona una función de malware instantáneo que permite a las organizaciones mejorar la precisión de la detección mediante la captura inmediata de páginas inyectadas de malware.

Recorded Future aprovecha la recopilación y el análisis automatizados de datos con inteligencia humana para proporcionar visibilidad en tiempo real de adversarios, infraestructura y objetivos. También proporciona información procesable que permite a las organizaciones tomar medidas preventivas. La compañía ofrece una herramienta patentada titulada gráfico de inteligencia que combina el aprendizaje automático y la inteligencia humana para generar inteligencia procesable a través del descubrimiento, categorización y conexión de entidades en tiempo real.

IntSights ofrece una plataforma de inteligencia de amenazas y se especializa en servicios automatizados de eliminación interna. La compañía ofrece una solución emblemática, Threat Command, que convierte señales complejas en inteligencia contextual de superficie de ataque, lo que facilita a las organizaciones remediar sus amenazas más críticas.

La plataforma de protección de riesgos externos de **CybelAngel** aprovecha las capacidades de IA y ML para descubrir, monitorear y resolver amenazas externas en varias fuentes de datos y proteger los activos críticos y la reputación de la marca. La plataforma ayuda a las organizaciones a minimizar los falsos positivos al aprovechar una combinación de algoritmos de modelos de ML y analistas humanos.

Flashpoint ofrece una plataforma de Inteligencia Flashpoint que combina información y conocimientos para identificar y mitigar el riesgo y combatir las amenazas cibernéticas y los fraudes. La compañía ofrece un motor de cobros que permite a los analistas rastrear varios tipos de comunidades en línea, una canalización de datos para almacenar, analizar y normalizar datos diversos y en tiempo real en múltiples tipos de comunidades en línea, y un motor de análisis que aprovecha las tecnologías de análisis patentadas para ofrecer entrega y priorización de datos relevantes.

Cyberint ofrece Argos Edge para la plataforma DRP que está equipada con inteligencia de amenazas y capacidades de gestión de superficie de ataque para proporcionar a las organizaciones visibilidad de la exposición a riesgos externos y la capacidad de mitigarlos. La plataforma ofrece una fusión nativa de una combinación de descubrimiento y gestión de superficies de ataque, inteligencia de amenazas y

protección de marca para permitir alertas precisas y enfocadas, probabilidades reducidas de elementos faltantes debido a la configuración incorrecta de los activos e identificación automática de activos.

CTM360 ofrece tres plataformas de protección de riesgos digitales (DRP), Hackerview, CyberBlindspot y ThreatCover, que identifican vulnerabilidades y detectan, administran y responden a amenazas en la superficie, la dark web y la deep web a través de una pila DRP consolidada. La compañía ofrece una función de eliminación ++ que permite a las organizaciones ir más allá de las eliminaciones convencionales al proporcionar respuestas a incidentes en la nube que neutralizan las amenazas en una etapa temprana.

RiskIQ, Proofpoint, Crisp y Axur se posicionan como retadores. **RiskIQ** ofrece inteligencia de amenazas a través de su producto titulado Illuminate, que proporciona un contexto instantáneo en torno a las amenazas relacionadas con la superficie de ataque única. El producto, con su capacidad de descubrimiento automatizado, aprovecha el descubrimiento continuo y sin contacto para mantenerse al tanto de los cambios, ya que rastrea y monitorea continuamente los ataques externos, detecta automáticamente los cambios y califica los riesgos en observaciones en tiempo real de amenazas externas. La solución de protección de riesgos digitales de Proofpoint proporciona defensas holísticas para todos los canales digitales para proteger la marca y los clientes de la organización contra riesgos digitales como las redes sociales, los dominios web y la deep y dark web. Escanea continuamente las redes sociales para encontrar cuentas asociadas con la marca de la organización y nuevas cuentas que intentan copiar la marca para uso malicioso y envía alertas automatizadas a las partes interesadas cuando se detectan cuentas riesgosas.

Crisp ofrece protección de marca a las organizaciones a través de su solución de Inteligencia de Riesgos Corporativos mediante el monitoreo de sitios de Internet relevantes, incluidas las páginas de redes sociales de la marca, en tiempo real para detectar cualquier problema o incidente temprano que pueda representar un riesgo para la marca. Identifica y bloquea a los malos actores de publicar contenido potencialmente dañino en las propias páginas de redes sociales de la organización. La solución de protección de riesgos digitales de Axur ofrece una rápida identificación de amenazas al encontrar y analizar automáticamente los componentes de la marca de la organización en la web. La plataforma muestra un registro completo de todas las infracciones en detalle para permitir a los equipos de seguridad analizar cada caso de manera fácil y rápida y para respaldar la toma de decisiones. La plataforma también ofrece un proceso de eliminación transparente con la opción de solicitar la eliminación de infracciones con un solo clic u obtener lo mismo automáticamente, basado en disparadores inteligentes previamente configurados.

PhishLabs, Blueliv y SafeGuard Cyber se posicionan entre los desafíos emergentes. **PhishLabs** ofrece una solución de protección de riesgos digitales que recopila datos de la deep y dark web, fuentes de redes sociales, fuentes de datos privadas y públicas, y a través de la integración con fuentes de terceros. Estos datos se procesan mediante técnicas de análisis automatizado, tecnología de rastreo, anti-evasión y procesos de pivote para generar inteligencia enriquecida por los expertos internos para ajustar la plataforma para ofrecer inteligencia procesable. La plataforma también ofrece una estrategia de mitigación completa al proporcionar una red global de eliminación y bloquear navegadores e integraciones automatizadas con controles de seguridad internos. La plataforma de protección de riesgos digitales de SafeGuard Cyber está diseñada para la colaboración, el chat móvil y varias aplicaciones de redes sociales. La defensa basada en la nube de la plataforma proporciona detección y respuesta a aplicaciones en la nube seguras centradas en el negocio de ransomware, ingeniería social, riesgos de terceros y amenazas internas. El producto estrella de Blueliv, titulado Threat Compass, utiliza tecnología adaptativa, modular, multi inquilino y basada en suscripción, que ayuda a detectar amenazas externas y analizarlas más a fondo utilizando inteligencia de amenazas dirigida, precisa y procesable. El producto está respaldado por modelos avanzados de aprendizaje automático para ofrecer cero falsos positivos y orquestar y remediar más rápido mediante la eliminación de sitios web ilegítimos, aplicaciones móviles, menciones en redes sociales y más.

FraudWatch y DigitalStakeout se posicionan como aspirantes en el espacio DRP. La solución **FraudWatch** ofrece un servicio totalmente administrado, que incluye búsqueda de amenazas, inteligencia, detección y eliminación de amenazas. La solución aprovecha las herramientas patentadas internas para detectar amenazas externas a la organización en combinación con el apoyo de expertos en riesgos digitales para ayudar a una toma de decisiones más rápida. **DigitalStakeout** ofrece protección contra el riesgo digital a través de su producto estrella denominado plataforma Scout. La plataforma permite un acceso más amplio a la presencia digital para obtener una visibilidad esencial del rastro digital de la organización. La plataforma aprovecha aún más la tecnología de aprendizaje automático y la inteligencia artificial para detectar amenazas externas a la organización y ofrece el mejor soporte de su clase de expertos en riesgos digitales para proporcionar valor para la inversión, ya que ayuda a una toma de decisiones más rápida.

Factores competitivos clave y diferenciadores tecnológicos

Impulsados por la creciente demanda de soluciones DRP, especialmente entre las pequeñas y medianas empresas que atraviesan la transformación digital y necesitan reducir la carga sobre sus recursos financieros, los proveedores se están centrando en sólidas capacidades de detección y remediación. Los proveedores de soluciones DRP están tratando de diferenciarse al proporcionar una solución holística todo en uno para monitorear y mitigar la exposición al riesgo en línea. Impulsados por la creciente competencia, los proveedores buscan cada vez más mejorar sus capacidades tecnológicas y su propuesta de valor general para seguir siendo competitivos. Algunos de los factores competitivos clave y diferenciadores para la evaluación de los proveedores de DRP son los siguientes:

Gestión de la superficie de ataque mediante capacidades de visualización: las organizaciones modernas se enfrentan a desafíos para lograr una visibilidad completa en toda la superficie de ataque, lo que hace que los activos se vean comprometidos. Para identificar todos los posibles activos comprometidos, los usuarios deben buscar proveedores con sólidas capacidades de administración de superficies de ataque. Esta capacidad, respaldada con sólidas características de visualización, puede proporcionar una visibilidad completa del riesgo a los equipos de administración de vulnerabilidades. Los proveedores también ofrecen escáneres de vulnerabilidades que asignan puntuaciones específicas de los activos y están integrando capacidades de visualización para proporcionar a los usuarios información adicional sobre la tipología y los controles.

Al seleccionar una solución para la protección de riesgos digitales, los usuarios deben buscar proveedores que ofrezcan opciones de visibilidad en profundidad y una amplia gama de funciones de corrección. Además, los usuarios deben buscar proveedores que ofrezcan capacidades para ver datos integrados de varias soluciones de seguridad y señales de exposiciones de riesgo priorizadas y contextualizadas.

Uso de Zero Trust para reducir el riesgo: Factores como el aumento inducido por la pandemia de COVID-19 en el trabajo remoto, junto con un aumento en los métodos de transformación empresarial digital, como las implementaciones híbridas y multinube, y un enfoque tradicional de seguridad de red basado en el perímetro ya no es una opción segura. Por lo tanto, las organizaciones están optando por Zero Trust Security que puede ayudarlas a mejorar su due dilligence y gestionar los riesgos de escenarios comerciales desconectados. Los proveedores incluyen soluciones de detección de amenazas, gestión de acceso a identidades (IAM), protección de puntos de llegada y datos, y servicios de seguridad administrados que funcionan con Zero Trust.

Al elegir el enfoque correcto para la gestión de riesgos digitales, los usuarios deben buscar proveedores que incorporen confianza cero en su solución DRP. Además, los usuarios deben evaluar a los proveedores en función de sus ofertas clave, como las políticas de acceso a datos específicas para cada individuo o activo, la infraestructura de clave pública (PKI) que autentica los certificados emitidos contra la autoridad de certificación global, la información de seguridad y los sistemas de administración de eventos (SIEM) entre otros. Con Zero Trust, los usuarios pueden lograr un mejor gobierno y madurez de la gestión de riesgos dentro del marco de cumplimiento.

Monitoreo e informes de la dark web: el anonimato proporcionado por la dark web la ha convertido en un destino principal para los malos actores que buscan vender datos confidenciales obtenidos a través de medios maliciosos. Los crecientes casos de datos robados que llegan a la dark web están haciendo que las organizaciones busquen un sistema robusto de monitoreo de la dark web.

Los usuarios deben buscar proveedores que ofrezcan capacidades de monitoreo de la dark web para ser notificados de cualquier amenaza potencial relacionada con la dark web. Los proveedores están ofreciendo servicios de escaneo de la dark web que escanean toda la dark web y alertan a los usuarios si se encuentra algún dato expuesto, y también proporcionan información procesable. Los usuarios pueden tomar medidas preventivas como cambiar sus credenciales, monitorear estados de cuenta de transacciones, congelar cuentas de crédito, entre otros.

Protección de la marca digital: las organizaciones corren el riesgo de comprometer su marca digital, ya que continúan utilizando el enfoque omnicanal para atraer a sus clientes. Las organizaciones necesitan una solución robusta de protección de marca digital que descubra los componentes del compromiso de la marca y proteja la marca en general. Los proveedores ahora ofrecen soluciones de automatización personalizadas junto con conectores de datos y libros de jugadas para ayudar a los usuarios a detectar amenazas más rápido y reducir los falsos positivos.

Los usuarios deben buscar proveedores que ofrezcan características como el monitoreo continuo de dominios sospechosos y alertas de alta prioridad en tiempo real con respecto a casos de compromiso de marca, campañas de phishing, riesgos recurrentes, así como eliminaciones realizadas por un equipo de expertos. Además, los usuarios deben evaluar a los proveedores en función de la exhaustividad de la solución de protección de marca digital, con características como la seguridad contra las adquisiciones de cuentas, la protección contra el fraude de marca al permitir la eliminación de cuentas falsas y aplicaciones móviles, y la protección contra el secuestro de la marca contra los malos actores que hacen un mal uso de los componentes de la marca digital.

Amplia cobertura de fuentes de recopilación de datos y casos de uso: los usuarios deben buscar proveedores que proporcionen un mayor grado de automatización en los procesos de recopilación de datos. Los usuarios deben seleccionar proveedores que ofrezcan una gama de fuentes de recopilación de datos que incluyan páginas TOR, páginas I2P (Invisible Internet Project), foros criminales, mercados de la dark web, sitios de pegado y repositorios de código, en una amplia gama de casos de uso como protección de marca, monitoreo de dominios, protección de redes sociales, prevención de adquisición de cuentas, protección de fugas de datos y protección ejecutiva.

Monitoreo basado en activos: las organizaciones necesitan soluciones sólidas de monitoreo basadas en activos, ya que mantener y asegurar los activos puede ser un gran desafío, pues si tales activos fallan o no están disponibles pueden resultar en operaciones retrasadas, pérdidas financieras y un servicio al cliente deficiente. Los proveedores que ofrecen soluciones de monitoreo basadas en activos ayudan a los usuarios a mapear la superficie de ataque organizacional al identificar activos desconocidos, cercanos y distantes y convertirlos en activos administrados al aprovechar un amplio espectro de metodologías basadas en OSINT, reconocimiento de red y conjuntos de big data. A continuación, la solución identifica las amenazas comunes en estos activos para priorizar los parches y las eliminaciones. Los proveedores ofrecen capacidades de mapeo de superficies de ataque que se fusionan de forma nativa con la inteligencia de amenazas y proporcionan un descubrimiento continuo de activos para dominios, subdominios, direcciones IP y activos en la nube. Los proveedores también se integran de forma nativa con las funciones de administración de la nube para la recopilación de datos de activos adicionales basados en la nube.

Los usuarios deben buscar proveedores que ofrezcan capacidades integrales de monitoreo basadas en activos, como monitoreo automatizado de activos digitales, ajustes continuos y cumplimientos por parte de analistas. Los usuarios deben seleccionar proveedores que proporcionen un alto grado de automatización en las funciones de supervisión basadas en activos. Los usuarios también deben evaluar a los proveedores en función de las características diferenciadas, como la ponderación de activos para sopesar los activos críticos y, en consecuencia, asignar puntajes de riesgo y un equipo de expertos para manejar el mapeo y la configuración manual de activos.

Playbooks automatizados integrados en SOAR: los playbooks basados en la tecnología SOAR impulsan los procesos de seguridad al automatizar los flujos de trabajo. Estos libros de jugadas proporcionan características para respuestas automatizadas a incidentes para diferentes tipos de amenazas. Por lo tanto, los proveedores se están centrando en mejorar sus ofertas de libros de jugadas integrados en SOAR. También se están enfocando en mejorar la racionalización de los procesos de seguridad para manejar alertas, crear respuestas automatizadas y lograr una remediación más rápida.

Los usuarios deben buscar proveedores que ofrezcan características diferenciadas que faciliten la integración de las decisiones humanas con la automatización para manejar escenarios críticos de seguridad. Los usuarios deben seleccionar proveedores que ofrezcan libros de jugadas SOAR, ya que facilitan las investigaciones automatizadas de incidentes, el enriquecimiento de inteligencia de amenazas, las respuestas a incidentes procesables y los datos de amenazas automatizados que alimentan herramientas de seguridad como SIEM, firewalls, plataformas de respuesta a incidentes y otros. Por último, con los libros de jugadas automatizados, los usuarios pueden aumentar su productividad y eficiencia en varias operaciones de seguridad.

Inteligencia de amenazas y fuentes de inteligencia de amenazas: los datos de código abierto carecen del contexto que los equipos de seguridad requieren para que sean útiles. Sin embargo, los marcos de inteligencia de amenazas permiten a las organizaciones atribuir la información a grupos de amenazas específicos, agregando así una capa adicional a la postura de seguridad de las organizaciones. Los usuarios deben buscar proveedores que aprovechen la inteligencia de amenazas para proporcionar información rica en contexto sobre indicadores de compromiso (IoC) y tácticas, técnicas y procedimientos (TTP) de los actores de amenazas. Adicionalmente, aunque las organizaciones están tratando de incorporar fuentes de datos de amenazas para obtener información técnica que se centre en un solo tipo de indicador de amenazas, requerirán herramientas de inteligencia de amenazas para descifrar esta información y aprovechar los conocimientos procesables proporcionados por las soluciones de inteligencia de amenazas cibernéticas.

Los usuarios deben seleccionar proveedores que ofrezcan herramientas de inteligencia de amenazas extensibles y basadas en datos que se centren en los servicios de la API para que las fuentes de inteligencia de amenazas se puedan integrar en las aplicaciones de seguridad internas. Por último, los usuarios deben buscar herramientas de inteligencia contra amenazas que proporcionen cobertura de extremo a extremo en todos los activos, facilidad de integración con los sistemas de seguridad internos y fuentes de recopilación de datos en una gama más amplia de fuentes de datos.

Modelo de amenazas robusto y priorización de riesgos: los usuarios deben buscar proveedores que utilicen un modelo de amenazas que combine la ciencia de datos, los algoritmos de aprendizaje automático de propiedad y la inteligencia humana para reducir significativamente los falsos positivos.

Capacidades integrales de interrupción y una eliminación interna del dominio: para hacer frente a los actores de amenazas responsables de amenazas públicas como suplantaciones de marca, explotación de la lealtad y confianza del cliente y phishing de los datos de los empleados, los proveedores ofrecen funcionalidades que permiten eliminaciones e interrupciones para fortalecer la postura de seguridad de las organizaciones. Los usuarios deben seleccionar proveedores que ofrezcan una combinación de capacidades de interrupción y eliminación para automatizar los procesos de corrección y liberar los recursos para utilizar en otros esfuerzos de seguridad.

OSINT & Web Intelligence: OSINT & Web Intelligence: las organizaciones aprovechan los datos de código abierto para analizar el panorama de amenazas y hacer frente a los riesgos conocidos dentro de la infraestructura de TI.

Los proveedores están ofreciendo marcos estratégicos de OSINT que definen las fuentes de la amplia gama de fuentes de datos de código abierto disponibles. Los usuarios deben buscar proveedores que ofrezcan el marco OSINT, ya que les ayuda a mejorar la postura de seguridad existente, establecer un rastro digital de amenazas conocidas y recopilar toda la inteligencia disponible sobre el TTP de un actor de amenazas. Los usuarios deben evaluar a los proveedores en función de la madurez de su tecnología de IA y ML, ya que puede mejorar la capacidad de una herramienta OSINT para almacenar volúmenes de datos.

La sofisticación de las capacidades tecnológicas: el creciente volumen, la sofisticación y las complejidades en los fraudes en línea están elevando constantemente la exposición al riesgo de las IF y las empresas. En los últimos años, las organizaciones globales en todas las regiones geográficas han observado un aumento en las amenazas en línea de varios canales, incluida la web superficial, la deep web, la dark web, las tiendas de aplicaciones y las redes sociales, lo que impulsa la necesidad de una solución DRP robusta. Por lo tanto, los usuarios deben evaluar una solución DRP que ofrezca capacidades integrales, incluida la detección de amenazas en los rastros digitales, el monitoreo y la respuesta a las amenazas, la mitigación del riesgo con intervención manual y automática, y el mantenimiento de la protección en todos los activos digitales. Además, la propuesta de valor del cliente de los proveedores puede diferir en términos de facilidad de implementación, facilidad de uso, relación precio/rendimiento, soporte para una amplia gama de casos de uso, servicio de soporte global y otros. La mayoría de los proveedores ofrecen estas funcionalidades y continúan invirtiendo fuertemente en mejorar aún más sus plataformas con IA, ML y análisis de riesgos para la detección en tiempo real y la remediación automatizada de amenazas digitales.

Visión tecnológica y hoja de ruta: con la llegada del trabajo remoto, las redes privadas, los activos en línea y la rápida transformación digital, la superficie de ataque de las organizaciones ha sido testigo de una expansión considerable. Por lo tanto, es imperativo que los usuarios elijan el socio tecnológico adecuado según sus casos de uso específicos, las tendencias de riesgo en línea en evolución y su hoja de ruta de transformación digital. Los proveedores de DRP están constantemente mejorando e innovando su propuesta de valor tecnológica en términos de proporcionar una solución holística de evaluación de riesgos digitales con integración integral de datos, análisis de riesgos, puntuación y remediación impulsada por análisis avanzados, IA y ML, herramientas de visualización avanzadas, incorporación de flujos de trabajo automatizados y otros. Las organizaciones deben evaluar cuidadosamente las capacidades tecnológicas existentes del proveedor junto con su visión tecnológica y hoja de ruta para mejorar la satisfacción general y la experiencia de propiedad del cliente para el éxito a largo plazo.

Experiencia del proveedor y conocimiento del dominio: las organizaciones deben realizar una evaluación exhaustiva de numerosas soluciones DRP y proveedores antes de tomar una decisión final. Las organizaciones deben evaluar la experiencia de los proveedores y el conocimiento del dominio para comprender sus problemas comerciales únicos, casos de uso y requisitos específicos de la industria. Los usuarios también deben buscar la facilidad de uso, la exhaustividad de la oferta, la flexibilidad del software para adaptarse a los constantes cambios del mercado y los requisitos reglamentarios, minimizando el costo total de propiedad y la transparencia. Las organizaciones deben buscar soluciones que proporcionen una herramienta de análisis de riesgos unificada y efectiva que proporcione rápidamente información adecuada y vital para tomar las decisiones correctas. Los usuarios deben buscar soluciones integradas que ofrezcan una cobertura integral con una visión continua y holística de todos los activos organizacionales externos y los factores de riesgo. Las IF deben buscar soluciones DRP que admitan múltiples formas de IA y modelos de detección basados en reglas y deben tener el potencial de integración de datos de terceros. Los usuarios también deben buscar una solución con un historial de implementaciones exitosas a gran escala y analizar cuidadosamente los estudios de caso existentes de esas implementaciones. Esto debería formar la base para preparar las prácticas recomendadas para las implementaciones de plataformas DRP.

Protección digital contra riesgos utilizando IA, ML y análisis avanzados: IA, ML y análisis avanzado son tecnologías emergentes en el espacio DRP. Con ayuda de la IA, el ML y la analítica avanzada, una solución DRP proporciona un análisis mejorado de enormes conjuntos de datos, lo que aumenta la eficiencia de la solución. Potenciada por estas tecnologías emergentes, una solución DRP ofrece monitoreo continuo y detección de amenazas en tiempo real. La analítica avanzada proporciona una detección precisa de riesgos para todos los activos externos. La IA está relativamente extendida en el espacio DRP para procesar una enorme cantidad de datos para cualquier amenaza, ya que ayuda en la segmentación precisa y el análisis del comportamiento. Los proveedores utilizan cada vez más técnicas de análisis avanzadas como la analítica predictiva, la analítica de big data, la analítica de redes sociales, la analítica de gráficos, el PLN, los modelos de calificación de riesgo y otros para evaluar los datos de varios canales web y móviles. Los robustos modelos de calificación impulsados por la IA también ofrecen puntajes de riesgo en tiempo real basados en múltiples factores, y sus capacidades de detección mejoradas pueden atravesar canales, verticales y negocios.

Integración e interoperabilidad: la integración perfecta y la interoperabilidad con las tecnologías existentes de los proveedores se encuentran entre los factores cruciales que afectan la implementación de la tecnología y la experiencia de propiedad. Los proveedores están proporcionando soluciones DRP integrales que ofrecen una integración e interoperabilidad perfectas con múltiples soluciones de análisis de fraude, múltiples opciones para la recopilación de datos, alertas de riesgo de terceros y aplicaciones de seguridad móvil para garantizar un funcionamiento sin problemas, el intercambio de información y la flexibilidad de la implementación.

Adicionalmente, los proveedores ofrecen soluciones que respaldan la integración con los ecosistemas de tecnología de seguridad existentes como SIEM, SOAR y otras soluciones de inteligencia de amenazas. Los usuarios deben evaluar la capacidad del proveedor para proporcionar integración lista para usar con las mejores tecnologías y la integración personalizada con varios productos empresariales y de detección de fraude. Los usuarios también deben evaluar la plataforma DRP para ofrecer amplitud y profundidad de la capacidad de integración específica para sus herramientas e infraestructura existentes.

SPARK Matrix™: Evaluación estratégica del desempeño y posicionamiento

SPARK Matrix de Quadrant Knowledge Solutions proporciona una muestra del posicionamiento en el mercado de los participantes clave del mercado. SPARK Matrix proporciona una representación visual de los participantes del mercado y proporciona información estratégica sobre cómo cada proveedor se clasifica en relación con sus competidores, con respecto a varios parámetros de rendimiento basados en la categoría de excelencia tecnológica y el impacto en el cliente. El Análisis del Panorama Competitivo de Quadrant es una guía de planificación útil para la toma de decisiones estratégicas, como encontrar perspectivas de fusiones y adquisiciones, asociaciones, expansión geográfica, expansión de cartera y otros similares.

Cada participante del mercado es analizado en función de varios parámetros de excelencia tecnológica e impacto en el cliente. En cada uno de los parámetros (ver gráficos), se asigna un índice a cada proveedor de 1 (más bajo) a 10 (más alto). Estas calificaciones son designadas para cada participante del mercado en función de los hallazgos de la investigación. Sobre la base de las calificaciones de los participantes individuales, se calculan los valores de coordenadas tanto X como Y. Estas coordenadas finalmente se utilizan para hacer la SPARK Matrix. .

Excelencia en tecnología	Pesaje
Sofisticación de la tecnología	20%
Estrategia de diferenciación competitiva	20%
Diversidad de la aplicación	15%
Escalabilidad	15%
Integración e interoperabilidad	15%
Visión y hoja de ruta	15%

Impacto en el cliente	Pesaje
Estrategia de producto y desempeño	20%
Presencia en el mercado	20%
Registros comprobados	15%
Facilidad de implementación y uso	15%
Excelencia en el servicio al cliente	15%
Propuesta de valor única	15%

Criterios de evaluación: excelencia en tecnología

- **La sofisticación de la tecnología:** la capacidad de proporcionar capacidades funcionales integrales y características del producto, innovaciones tecnológicas, arquitectura de producto / plataforma y otros.
- **Estrategia de Diferenciación Competitiva:** la capacidad de diferenciarse de los competidores a través de capacidades funcionales y/o innovaciones y/o estrategia GTM, propuesta de valor del cliente, entre otros.

- **Diversidad de aplicaciones:** la capacidad de demostrar la implementación de productos para una variedad de verticales de la industria y/o múltiples casos de uso.

- **Escalabilidad:** a capacidad de demostrar que la solución admite escalabilidad de nivel empresarial junto con ejemplos de casos de clientes.

- **Integración e interoperabilidad:** la capacidad de ofrecer una plataforma de productos y tecnología que admite la integración con múltiples tecnologías de primera clase proporciona integraciones prediseñadas listas para usar y soporte y servicios de API abiertos.

- **Visión y hoja de ruta:** evaluación de la estrategia y hoja de ruta del producto del proveedor con el análisis de las mejoras planificadas clave para ofrecer productos/tecnologías superiores y mejorar la experiencia de propiedad del cliente.

Criterios de evaluación: impacto en el cliente

- **Estrategia y rendimiento del producto:** evaluación de múltiples aspectos de la estrategia y el rendimiento del producto en términos de disponibilidad del producto, relación precio-rendimiento, excelencia en la estrategia GTM y otros parámetros específicos del producto.

- **Presencia en el mercado:** la capacidad de demostrar ingresos, base de clientes y crecimiento del mercado junto con una presencia en varias regiones geográficas y verticales de la industria.

- **Registro comprobado:** evaluación de la base de clientes existente de pymes, segmentos de medianas y grandes empresas, tasa de crecimiento y análisis de los estudios de casos de clientes.

- **Facilidad de implementación y uso:** la capacidad de proporcionar una experiencia de implementación superior a los clientes que admiten una implementación flexible o demostrar una experiencia superior de compra, implementación y uso. Además, los productos de los proveedores se analizan para ofrecer una interfaz de usuario fácil de usar y una experiencia de propiedad.

- **Excelencia en el servicio al cliente:** la capacidad de demostrar la capacidad de los proveedores para proporcionar una gama de servicios profesionales desde consultoría, capacitación y soporte. Adicionalmente, también se considera la estrategia del socio de servicio de la empresa o la capacidad de integración de sistemas en todas las regiones geográficas.

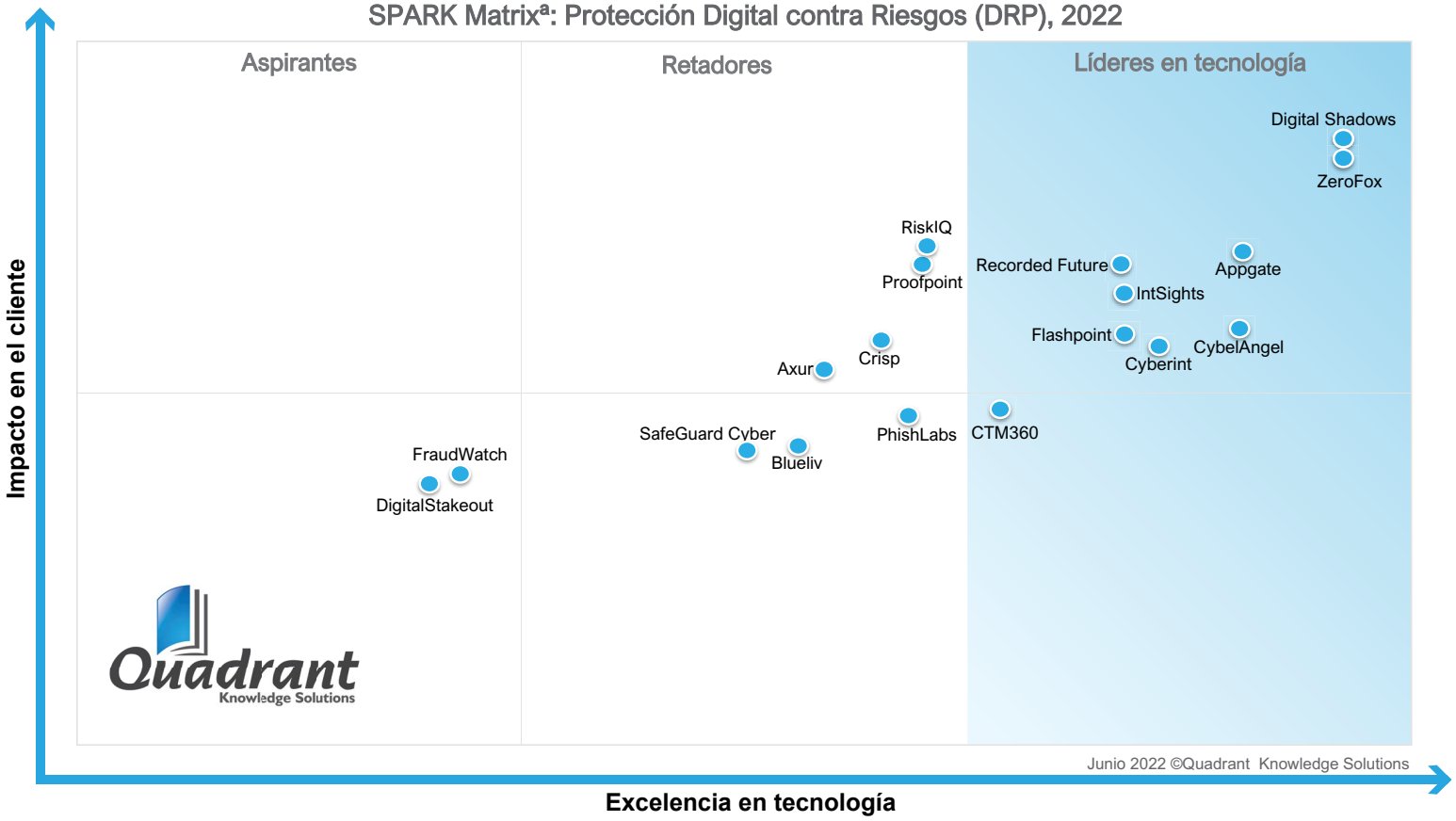
- **Propuesta de valor única:** la capacidad de demostrar diferenciadores únicos impulsados por las tendencias actuales de la industria, la convergencia de la industria, la innovación tecnológica, entre otros.

SPARK Matrix™: Protección Digital contra Riesgos (DRP), 2022

Evaluación estratégica del desempeño y posicionamiento

Gráfica: SPARK Matrix™ 2022

(Evaluación y Clasificación del Desempeño Estratégico)
Mercado de la Protección de Riesgos Digitales (DRP)



Perfiles de los proveedores

A continuación, se presenta el perfil del proveedor líder en soluciones de protección contra riesgos digitales (DRP) con un impacto global. El siguiente perfil de proveedor se escribe en función de la información proporcionada por los ejecutivos del proveedor como parte del proceso de investigación. El equipo de investigación de Quadrant también se ha referido al sitio web de la compañía, los documentos técnicos, los blogs y otras fuentes para escribir el perfil. Un perfil detallado del proveedor y un análisis de todos los proveedores, junto con varios escenarios competitivos, están disponibles como un producto de investigación personalizado para nuestros clientes. Se aconseja a los usuarios que hablen directamente con los proveedores respectivos para una comprensión más completa de sus capacidades tecnológicas. Se recomienda a los usuarios que consulten Quadrant Knowledge Solutions antes de tomar cualquier decisión de compra, con respecto a conocer la tecnología de su cliente y la selección de proveedores en función de los hallazgos de la investigación incluidos en este servicio de investigación.

Appgate

URL : www.appgate.com

Fundada en 2020 y con sede en Florida, EE. UU., Appgate, una extensión de Cyxtera Technologies, ofrece soluciones y servicios de seguridad y análisis basados en la nube y en híbridos, que utilizan tecnología de Zero Trust. La compañía ofrece una cartera de soluciones y servicios que consiste en Appgate SDP, una solución de perímetro definido por software; el conjunto de acceso seguro del consumidor de autenticación basada en riesgos (RBA) y capacidades de protección contra amenazas digitales (DTP), junto con software orientado a la ofensa y servicios de simulación adversaria. La solución Digital Threat Protection de la compañía ofrece visibilidad de amenazas y gestión integral de riesgos para monitorear los datos expuestos y detectar datos comprometidos y proporcionar información detallada y procesable. La solución se centra en minimizar el impacto del fraude y los incidentes de seguridad y proporcionar mitigación de amenazas y protección a las empresas seguras. Las características y funcionalidades clave de la solución de protección contra amenazas digitales incluyen monitoreo de salud web, monitoreo de deep y dark web e inteligencia de marca.

La capacidad de monitoreo de la salud web de la compañía permite el monitoreo y la mitigación en tiempo real de diversas amenazas, incluidos el phishing, el pharming y la desfiguración, en varias fuentes, como sitios web, canales de redes sociales, cajas de abuso, weblogs de referencia y más. La capacidad ofrece una función de monitoreo y eliminación de phishing que permite un monitoreo proactivo continuo para sitios de phishing seguido de listas negras, eliminación e informes detallados. La función de supervisión de dominios similar proporciona visibilidad en el registro de dominios y ayuda a descubrir dominios similares vinculados con actividades sospechosas. Adicionalmente, la capacidad ofrece una función de información de las víctimas que proporciona información procesable sobre los sitios que causan daños junto con informes detallados de incidentes sobre los usuarios que han hecho clic en los sitios de phishing y su información comprometida.

La capacidad de monitoreo de la deep y dark web de la compañía protege a las organizaciones de las amenazas en la dark web. La capacidad permite a las organizaciones descubrir credenciales de clientes y empleados expuestas y detectar códigos fuente expuestos de forma maliciosa y accidental en repositorios de código público y documentación. Adicionalmente, esta capacidad les permite a las organizaciones descubrir sus nombres de dominio que son cibernéticos o errores. Adicionalmente, la capacidad les permite a las organizaciones detectar infracciones de marcas comerciales y cuentas sociales, dominios y sitios web, y marcas comerciales que intentan hacerse pasar por ellos.

La capacidad de inteligencia de marca de la solución protege el valor de la marca al monitorear y prevenir actividades fraudulentas en canales de phishing, sitios de redes sociales y tiendas de aplicaciones. La capacidad ofrece funciones de escaneo

de deep y dark web que permiten el monitoreo continuo de la deep y dark web, mercados subterráneos y foros de piratería, sitios web de pegado, redes sociales, IRC y varios canales, para descubrir fugas de datos, credenciales robadas y cuentas de redes sociales falsas, detectar sitios web fraudulentos que imitan marcas de clientes con fines ilícitos y otras entidades de fraude. Adicionalmente, la capacidad ofrece funciones de monitoreo de noticias y redes sociales que permiten a las organizaciones analizar las redes sociales y los registros de dominios para identificar perfiles sociales falsos y menciones maliciosas. Esta capacidad también proporciona características de protección de marca que permiten la detección y eliminación de aplicaciones no autorizadas, lo que reduce el riesgo de descargas de aplicaciones falsas. Esta función también ayuda a las organizaciones a eliminar sitios maliciosos al monitorear varios motores de búsqueda en busca de anuncios no autorizados y maliciosos que atraigan a los usuarios a dichos sitios.

Perspectiva del analista

A continuación, se muestra el análisis de las capacidades de Appgate en el mercado global de DRP:

- La solución de protección contra amenazas digitales de Appgate ofrece una gestión integral de riesgos digitales a través de canales externos que conforman el rastro digital de la organización. La solución proporciona información procesable sobre los diversos tipos de ataques y visibilidad continua de amenazas basada en el aprendizaje automático en todo el rastro digital y la dark web. La solución también proporciona facilidad de integración, implementación sin esfuerzo e invisibilidad completa para los usuarios finales.

- La solución proporciona informes de incidentes en profundidad de todos los incidentes en un solo lugar, actualizaciones en tiempo real sobre ataques, informes de incidentes personalizados y la capacidad de filtrar incidentes mientras se mantiene informados a los usuarios. La solución también ofrece soporte continuo en varios idiomas y un equipo de soporte dedicado para resolver consultas posteriores a la implementación.

- Algunas de las ofertas diferenciadas de la solución de protección contra amenazas digitales incluyen Victim Insights, que permite un enfoque de remediación dirigido y proactivo, detección de documentación expuesta y código fuente filtrado en repositorios de código público, credenciales de empleados comprometidas en bases de datos en toda la dark web con monitoreo e informes detallados, mitigación de los efectos de amenazas dirigidas al calificar el nivel de exposición al riesgo para garantizar una acción rápida contra los datos expuestos, y un completo portal de autoservicio para gestionar incidencias.

- La función de información de víctimas de la solución proporciona información y visibilidad de las credenciales que los usuarios ingresan al encontrarse con sitios web de phishing. Con esta información sobre los usuarios que han sido víctimas de ataques de phishing, las organizaciones pueden tomar las medidas de mitigación adecuadas de inmediato. La solución también proporciona una función de malware instantáneo que permite a las organizaciones mejorar la precisión de la detección mediante la captura inmediata de páginas inyectadas de malware. Además, esta característica también ayuda en las investigaciones forenses. Con esta característica, las organizaciones pueden identificar inmediatamente a los usuarios que han sido víctimas de los ataques de malware más recientes y responder a los riesgos emergentes en consecuencia.

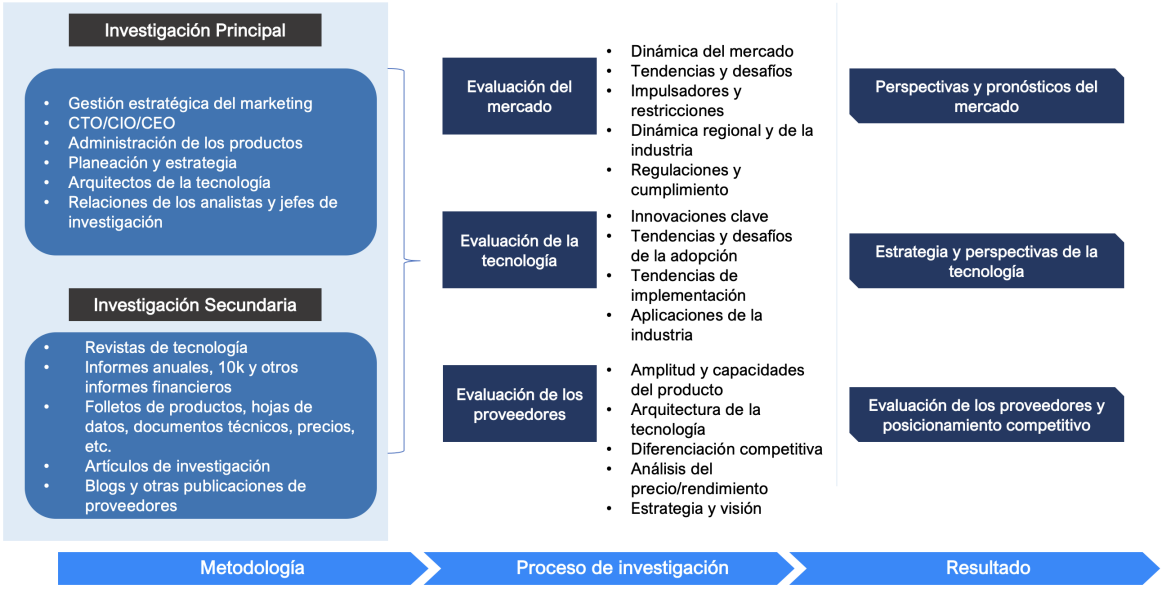
- En cuanto a la presencia geográfica, Appgate tiene una importante presencia en Estados Unidos y América Latina, seguido de la APAC. La empresa admite varios casos de uso, como la detección de phishing en sitios web, información sobre víctimas, monitoreo de redes sociales y marcas, protección de aplicaciones móviles fraudulentas, protección contra publicidad maliciosa y escaneo de deep y dark web. La empresa atiende a las verticales de la industria, como instituciones bancarias y financieras, juegos y atletismo y deportes.

- Los principales desafíos de Appgate incluyen la creciente competencia de proveedores emergentes con ofertas de tecnología innovadoras. La empresa podría enfrentar desafíos para posicionarse como un proveedor de soluciones de extremo a extremo en medio de la tendencia de desarrollar soluciones internas. Sin embargo, con sus capacidades funcionales integrales y su sólida propuesta de valor para el cliente, Appgate está bien posicionada para mantener y aumentar su cuota de mercado con un éxito continuo entre los segmentos de medianas y grandes empresas.

- Como parte de su hoja de ruta tecnológica, Appgate se está centrando en incluir la gestión de superficies de ataque para detectar activos de TI vulnerables que son visibles y accesibles externamente, como servidores y dispositivos de red alojados en las instalaciones o en la nube. La empresa también planea incluir una función de escaneo de seguridad web que puede rastrear el software de una organización y las versiones instaladas para identificar vulnerabilidades divulgadas públicamente de la lista de los diez principales proyectos de seguridad de aplicaciones web abiertas (OWASP). La función permite el monitoreo continuo de la seguridad de las aplicaciones web externas, mejorado con pruebas continuas para el cumplimiento de los requisitos PCI DSS, GDPR o NIST, cifrado TLS, WAF faltante y otras configuraciones erróneas y debilidades.

Metodologías de investigación

Quadrant Knowledge Solutions utiliza un enfoque integral para realizar investigaciones de perspectivas de mercado global para diversas tecnologías. El enfoque de investigación de Quadrant proporciona a nuestros analistas el marco más efectivo para identificar las tendencias del mercado y la tecnología, y ayuda a formular estrategias de crecimiento significativas para nuestros clientes. Todas las secciones de nuestro informe de investigación se preparan con una cantidad considerable de tiempo y proceso de pensamiento antes de pasar al siguiente paso. A continuación, se presenta la breve descripción de las principales secciones de nuestras metodologías de investigación.



Investigación Secundaria

Las siguientes son las principales fuentes de información para la realización de investigaciones secundarias:

Base de datos interna de Quadrant

Quadrant Knowledge Solutions mantiene una base de datos patentada en varios mercados de tecnología. Esta base de datos proporciona a nuestro analista una base adecuada para poner en marcha el proyecto de investigación. Esta base de datos incluye información de las siguientes fuentes:

- Informes anuales y otros informes financieros
- Listas de participantes de la industria
- Datos secundarios publicados sobre empresas y sus productos

- Base de datos de tamaños de mercado y datos de pronóstico para diferentes segmentos del mercado
- Principales tendencias del mercado y la tecnología

Investigación bibliográfica

Quadrant Knowledge Solutions aprovecha varias suscripciones a revistas y otras publicaciones que cubren una amplia gama de temas relacionados con la investigación tecnológica. También utilizamos la extensa biblioteca de directorios y revistas en varios dominios tecnológicos. Nuestros analistas utilizan publicaciones de blog, documentos técnicos, estudios de casos y otra literatura publicada por los principales proveedores de tecnología, expertos en línea y publicaciones de noticias de la industria.

Aportes de los participantes de la industria

Los analistas del cuadrante recopilan documentos relevantes como documentos técnicos, folletos, estudios de casos, listas de precios, hojas de datos y otros informes de todos los principales participantes de la industria.

Investigación Primaria

Los analistas de Quadrant utilizan un proceso de dos pasos para realizar investigaciones primarias que nos ayudan a capturar información de mercado significativa y más precisa. A continuación, se muestra el proceso de dos pasos de nuestra investigación primaria:

Estimación del mercado: basado en el enfoque de arriba hacia abajo y de abajo hacia arriba, nuestro analista analiza a todos los participantes de la industria para estimar su negocio en el mercado de tecnología para varios segmentos del mercado. También buscamos información y verificación del desempeño comercial del cliente como parte de nuestras entrevistas de investigación primaria o a través de un cuestionario de mercado detallado. El equipo de investigación de Quadrant realiza un análisis detallado de los comentarios e insumos proporcionados por los participantes de la industria.

Entrevista al cliente: el equipo de analistas de Quadrant realiza una entrevista telefónica detallada de todos los principales participantes de la industria para obtener sus perspectivas de la dinámica actual y futura del mercado. Nuestro analista también obtiene su experiencia de primera mano con la demostración del producto del proveedor para comprender sus capacidades tecnológicas, experiencia del usuario, características del producto y otros aspectos. Con base en los requisitos, los analistas de Quadrant se entrevistan con más de una persona de cada uno de los participantes del mercado para verificar la exactitud de la información proporcionada.

Por lo general, nos relacionamos con el personal del cliente en una de las siguientes funciones:

- Dirección Estratégica de Marketing
- Gestión de productos
- Planeación de productos
- Planeación y estrategia

Comentarios de los asociados del canal y los usuarios finales

El equipo de investigación de Quadrant investiga con varios socios del canal de ventas, incluidos distribuidores, integradores de sistemas y consultores para comprender la perspectiva detallada del mercado. Nuestros analistas también obtienen comentarios de usuarios finales de múltiples industrias y regiones geográficas para comprender los problemas clave, las tendencias tecnológicas y las capacidades de los proveedores en el mercado de la tecnología.

Análisis de datos:
Pronóstico del mercado y análisis de la competencia

El equipo de analistas de Quadrant reúne toda la información necesaria de la investigación secundaria y la investigación primaria a una base de datos informática. Estas bases de datos se analizan, verifican y tabulan de numerosas maneras para obtener la imagen correcta del mercado general y sus segmentos. Después de analizar todos los datos del mercado, las tendencias de la industria, las tendencias del mercado, las tendencias tecnológicas y los problemas clave, preparamos pronósticos preliminares del mercado. Este pronóstico preliminar del mercado se prueba contra varios escenarios de mercado, escenario económico, tendencias de la industria y dinámica económica. Finalmente, el equipo de analistas llega al escenario de pronóstico más preciso para el mercado general y sus segmentos.

Además de los pronósticos del mercado, nuestro equipo realiza una revisión detallada de los participantes de la industria para preparar el panorama competitivo y el análisis de posicionamiento del mercado para el mercado general, así como para varios segmentos del mercado.

SPARK Matrix:
Evaluación estratégica del desempeño y posicionamiento

SPARK Matrix de Quadrant Knowledge Solutions proporciona una muestra del posicionamiento en el mercado de los participantes clave del mercado. La representación de SPARK Matrix proporciona una representación visual de los participantes del mercado y proporciona información estratégica sobre cómo se clasifica cada proveedor en comparación con sus competidores, con respecto a varios parámetros de rendimiento basados en la categoría de excelencia tecnológica y el impacto en el cliente.

Preparación del Informe Final

Después de finalizar el análisis y los pronósticos del mercado, nuestro analista prepara los gráficos, tablas y cuadros necesarios para obtener más información y preparar el informe de investigación final. Nuestro informe de investigación final incluye información que incluye pronósticos del mercado; análisis competitivo; las principales tendencias del mercado y la tecnología; impulsores del mercado; perfiles de proveedores, entre otros.

Atención al cliente

Para obtener información sobre reimpresiones impresas o electrónicas, comuníquese con el servicio de Atención al Cliente en:
rmehar@quadrant-solutions.com | www.quadrant-solutions.com