

ResOps: El Futuro de los Negocios Resilientes en la Era de la IA



De la Disrupción a la Confianza Continua

La inteligencia artificial está transformando los negocios a una velocidad sin precedentes, pero es solo una de las fuerzas que están incrementando la fragilidad operativa. La complejidad de la nube, el crecimiento del SaaS, la proliferación de identidades, la cada vez mayor dependencia de terceros y el endurecimiento de las regulaciones han creado un entorno en el que las disrupciones superan a los modelos de respuesta tradicionales.

Las organizaciones están invirtiendo fuertemente en GPUs, modelos y automatización, pero las prácticas necesarias para hacer operativa la resiliencia que proporcionan estas capacidades no han avanzado al mismo ritmo. Como resultado, los errores se propagan más rápido, la superficie de ataque se amplía y los riesgos para la integridad de los datos siguen creciendo.

El resultado es una brecha de resiliencia cada vez mayor. La innovación avanza más rápido que las soluciones de protección necesarias para sostenerla. La mayoría de las empresas no están preparadas para este cambio. Según datos de Accenture, el 77% de ellas carece de prácticas esenciales de seguridad de datos e IA, y el 90% no tiene la madurez necesaria para defenderse de amenazas habilitadas por IA¹.

¹ Informe "[State of Cybersecurity Resilience 2025](#)", Accenture



La Brecha en la Resiliencia

Los modelos de resiliencia tradicionales fueron diseñados para una era de perímetros sólidos y procesos de recuperación aislados. Hoy, ese enfoque fracasa cuando las disrupciones se mueven a velocidad de máquina y los sistemas abarcan entornos *híbridos, multcloud, SaaS, edge* y de terceros.

Estos ecosistemas interconectados crean nuevas dependencias, nuevos tipos de fallos y una menor visibilidad. La IA acelera aún más el desafío: las decisiones y los errores se propagan instantáneamente, y los atacantes ahora apuntan tanto a la integridad de los datos como a su disponibilidad.

Funciones aisladas: seguridad, gestión de identidades y recuperación siguen actuando de forma fragmentada, ralentizando la respuesta y creando puntos ciegos.

Datos distribuidos: los ecosistemas híbridos, multcloud y edge han ampliado la superficie de ataque.

Aceleración de la IA: las operaciones a velocidad de máquina hacen que las amenazas se propaguen más rápido de lo que los humanos pueden responder.

Postura reactiva: aún hoy, la recuperación es tratada como último recurso: lenta, parcial y costosa.

Según la Cloud Security Alliance, solo el 2% de las empresas ha implementado ciberresiliencia en todas las áreas críticas, mientras que el 42% de los ejecutivos cita las amenazas relacionadas con la nube como su mayor preocupación. Justo las mismas amenazas para las que los líderes de seguridad se sienten menos preparados².

El resultado es esa **brecha creciente en la resiliencia**, la brecha entre la velocidad a la que evoluciona la tecnología y la lentitud con la que la mayoría de las empresas es capaz de responder cuando algo sale mal.

² Cloud Security Alliance

ResOps: Un Nuevo Modelo Operativo para la Resiliencia

ResOps (*Resilience Operations*) aúna disciplinas que tradicionalmente han operado en silos —seguridad, gestión de identidades, protección de datos, recuperación, gobernanza— en un modelo operativo unificado. Si bien muchos proveedores (incluido Commvault) aportan componentes importantes, el modelo en sí es más amplio que cualquier tecnología o dominio individual.

En esencia, ResOps es un ciclo continuo que fortalece la resiliencia en toda la organización: protege los datos, detecta riesgos, restaura la confianza rápidamente cuando ocurren incidentes y reintegra datos limpios y verificados a los sistemas de negocio.

Descubrir y proteger – protección de los datos en su origen.

Detectar – Detección y respuesta ante anomalías y amenazas en tiempo real.

Recuperar – Restauración de los datos y aplicaciones necesarios para operar más rápidos, limpios y completos.

Validar y mejorar – Demostración de la recuperabilidad y fortalecimiento continuo de la resiliencia probando, aprendiendo y mejorando tras cada señal, cambio o incidente.

Continuidad de negocio – Reintegración de datos seguros y gobernados en los sistemas críticos del negocio.

ResOps EN TODA LA EMPRESA



Estas funciones ya existen en la industria, pero ResOps las convierte en una disciplina operativa que alinea equipos, incrementa la responsabilidad y permite demostrar la resiliencia de forma continua en lugar de darla por hecha.

En ese sentido, ResOps introduce una nueva “personalidad” operativa centrada en **abordar los riesgos de resiliencia de manera integral y eficiente en toda la empresa.**

Descubrir y Proteger: Protección de los Datos en Origen

Este es el pilar fundamental de ResOps: saber qué datos existen, dónde residen, cómo están clasificados y si cuentan con la protección y gobernanza adecuadas.

Qué es

El descubrimiento y la protección forman la base de ResOps. Las organizaciones deben saber continuamente qué datos tienen, dónde están y cómo se utilizan. La protección implica aplicar gobernanza y control a medida que se crean, se accede a ellos, se mueven y evolucionan, de forma que sigan siendo fiables durante todo su ciclo de vida

Por qué es importante

Ya sea para proteger datos de clientes, cumplir la normativa o impulsar la innovación con IA, las organizaciones se enfrentan a un reto común: necesitan datos fiables, gobernados y seguros en tiempo real.

Esto es especialmente crítico para organizaciones que usan RAG (*Retrieval-Augmented Generation*) para ampliar modelos de lenguaje con datos propios. Sin descubrimiento y protección adecuados -saber qué datos existen, dónde residen y cómo se han clasificado-, las canalizaciones RAG pueden exponer o contaminar involuntariamente información sensible. Los datos no clasificados o no protegidos pueden fluir directamente a bases de datos vectoriales, convirtiéndose en superficie de ataque para la corrupción de datos o fugas de privacidad.

El descubrimiento, la clasificación y la protección continuos crean los datos confiables y gobernados que impulsan los sistemas de IA. Esto es fundamental para una IA responsable y unas operaciones resilientes.

Cómo lograrlo

Descubrimiento y clasificación unificados:

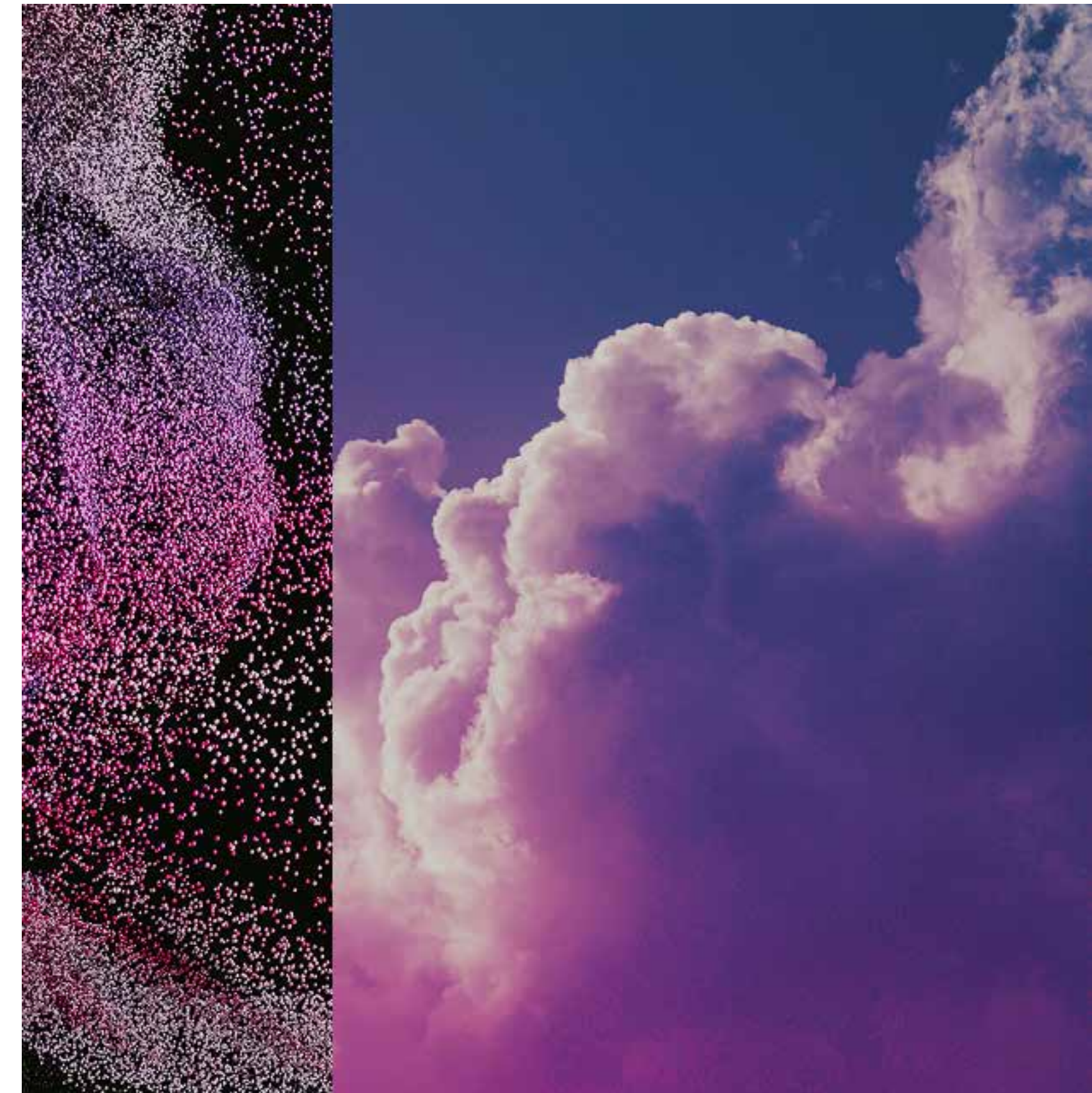
Escaneado continuo en entornos híbridos, *multicloud* y *edge*, clasificando y etiquetando datos en el momento de su creación.

Protección basada en políticas:

Aplicación de políticas de seguridad, backup y retención automática en la capa de datos mediante cifrado, masking, controles de acceso y preparación para la recuperación a medida que los datos se crean, transfieren y almacenan.

Gobernanza proactiva:

Supervisión y aplicación continua de políticas de acceso a datos, backup y retención para un cumplimiento uniforme en todos los entornos.



Detectar: Observación de Cambios en Tiempo Real

La detección en ResOps va más allá de las alertas de seguridad. Incluye monitorizar la integridad de los datos, el comportamiento de las identidades, posibles cambios en los sistemas o cualquier otra desviación que pueda comprometer la resiliencia.

Qué es

La detección consiste en una observación permanente para identificar anomalías, ataques y cambios no previstos en las identidades y en los datos accesibles a lo largo de la organización, incluyendo las copias críticas.

Por qué es importante

Las operaciones de negocio -incluyendo las decisiones tanto humanas como impulsadas por IA- se basan en datos que deben ser fiables. Cada segundo que los datos son inexactos o poco fiables, o se ven comprometidos, se pone en riesgo el negocio. La detección acorta ese tiempo, permitiendo que la resiliencia surta efecto con rapidez.

Cómo lograrlo

Detección de anomalías impulsada por IA:

Monitorización de datos y comportamiento de identidades prácticamente en tiempo real, detectando desviaciones rápidamente para minimizar el riesgo.

Auditoría y visibilidad:

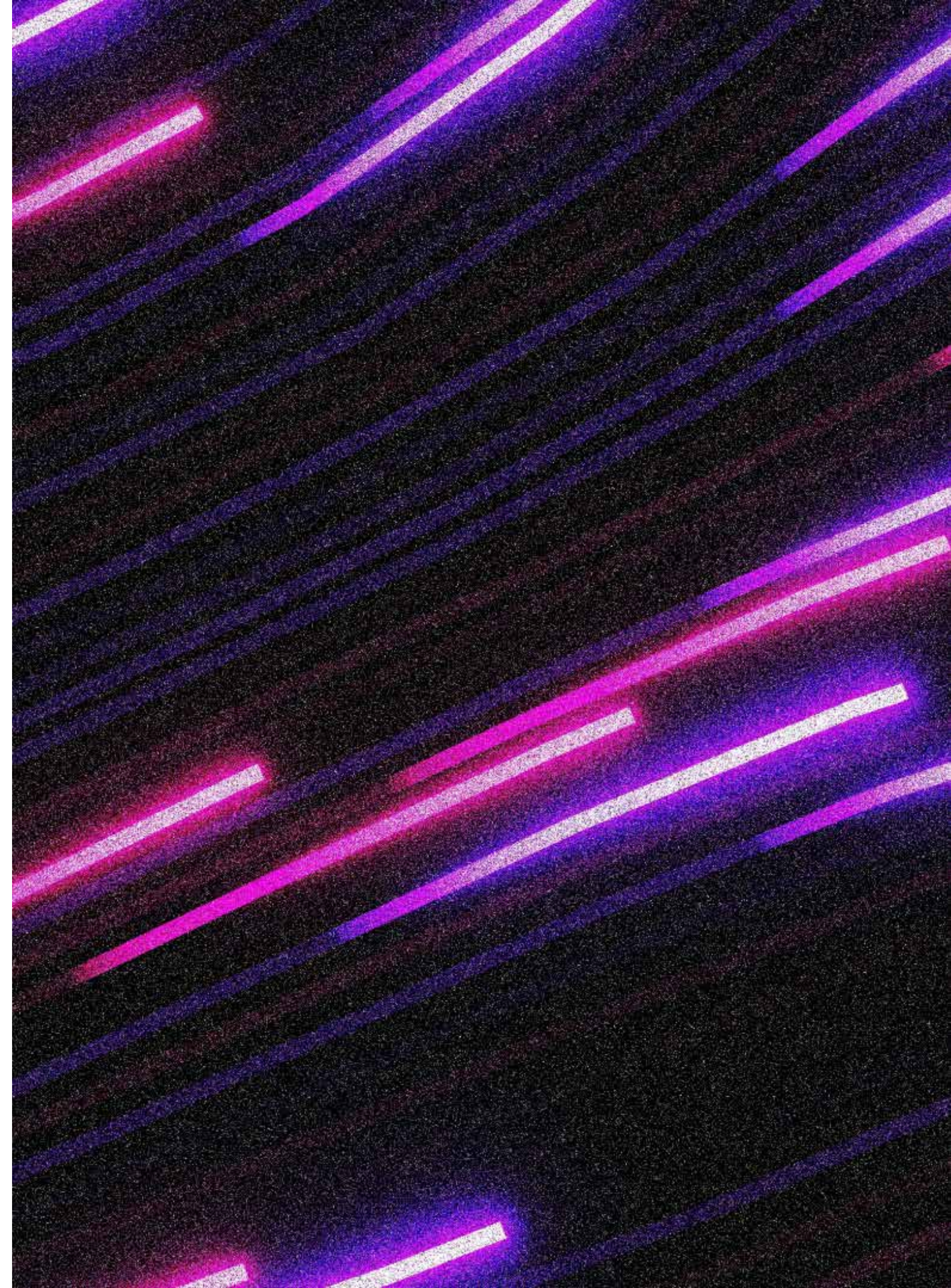
Información no solo sobre qué cambió, sino también sobre quién (sea un humano o un agente digital) realizó el cambio.

Correlación automatizada:

Separación de la actividad normal de negocio respecto a los diferentes indicadores de compromiso para reducir los falsos positivos y la saturación de alertas.

Inteligencia procesable:

La detección se integra directamente en los manuales de respuesta, por lo que la información se traduce instantáneamente en acciones.



Recuperar: La Recuperación Más Rápida, Limpia y Completa

La recuperación ya no es solo restaurar copias de seguridad: ahora implica restaurar servicios de negocio completos con confianza, rapidez e integridad.

Qué es

La recuperación es un pilar fundamental de ResOps, pero en modelos más amplios a nivel de industria ya no se limita a sólo restaurar backups, sino que incluye la restauración de servicios de negocio completos con fiabilidad, rapidez e integridad.

Por qué es importante

Las operaciones modernas, desde los sistemas de IA hasta las aplicaciones de gestión de clientes, dependen de datos completos, precisos y sin riesgos. Cuando la recuperación falla, la confianza del cliente se tambalea y el cumplimiento normativo se pone en riesgo. La verdadera resiliencia significa poder restaurar el negocio en cualquier momento con integridad y seguridad.

Cómo lograrlo

Monitorización continua:

Chequeo de las rutas de recuperación a diario para que la preparación sea siempre fiable y demostrable.

Recuperación sintética:

Eliminación quirúrgica de datos comprometidos y automatización para una recuperación precisa, rápida, limpia y completa.

Orquestación automatizada:

Automatización de *runbooks* y flujos de trabajo para pruebas, análisis forense y validación de producción, permitiendo recuperaciones aisladas y rápidas que minimizan la necesidad de procesos e intervenciones manuales.

Restauración a escala empresarial:

Restauración de la versión más rápida, limpia y completa del negocio en todas las cargas de trabajo, nubes y conjuntos de datos.

Es importante destacar que las métricas tradicionales que se han venido utilizando para medir la restauración son insuficientes en el contexto de la recuperación moderna, impulsada por el modelo ResOps. Los objetivos de tiempo de recuperación y los objetivos de punto de recuperación, por ejemplo, no consideran que los datos deben estar limpios de daños antes de restaurarlos a los entornos de producción.

Ahora están surgiendo nuevas métricas, cada vez más adoptadas por las empresas modernas, que se ajustan mejor a las necesidades específicas de la tarea en cuestión. Una de ellas es el tiempo medio hasta una recuperación limpia (*Mean Time to Clean Recovery*), que puede ser utilizada por la dirección para 'hacer la pregunta correcta' a su equipo de ResOps en relación con la capacidad de la empresa para recuperarse de un ciberataque.

Un Enfoque Unificado Para Unas Operaciones Resilientes

Ya sea para protegerse contra el ransomware, respaldar el cumplimiento normativo o impulsar la innovación en IA, los fragmentados ecosistemas actuales no pueden ofrecer resiliencia a gran escala. Las herramientas de seguridad, los sistemas de gestión de identidades y los procesos de recuperación nunca se diseñaron para funcionar en conjunto. El resultado: duplicación, inconsistencia y brechas que los atacantes aprovechan.

Datos unificados:

La verdadera resiliencia requiere consistencia entre datos estructurados y no estructurados, aplicaciones SaaS, *endpoints* y servicios *cloud-native*. Sin resiliencia, se multiplican los riesgos y los costes para las organizaciones debido al uso de herramientas fragmentadas y procesos redundantes: diferentes equipos acaban resolviendo el mismo problema, de diferentes maneras, cada uno añadiendo complejidad en lugar de control.

Gobernanza unificada:

Al extender políticas consistentes a las cargas de trabajo de producción actuales y a las pilas de IA futuras, la gobernanza ayuda a reducir el riesgo drásticamente, ya que minimiza la superficie de exposición a medida que los datos se dispersan a través de nubes, regiones y ubicaciones perimetrales.

Seguridad, identidades y recuperación, unificadas:

La integración de las disciplinas de seguridad de datos, resiliencia de identidades y ciberrecuperación incrementa la integridad y la fiabilidad de los datos críticos. Centralizar ecosistemas de herramientas fragmentadas será clave para la recuperación y la resiliencia en toda la empresa.

Inteligencia unificada:

La inteligencia continua aumenta la disponibilidad de datos críticos. Al aplicar información basada en IA, las organizaciones pueden confiar en que sus datos siempre estarán disponibles, con una recuperación más limpia, rápida y completa cuando más importa.

ResOps Como Ventaja Competitiva

ResOps no es simplemente una evolución de las prácticas existentes, sino una nueva categoría de operaciones de negocio diseñada específicamente para la era de la IA. Del mismo modo que DevOps redefinió la forma en que se crea y entrega el software, ResOps establece la disciplina operativa necesaria para salvaguardar, gobernar y restaurar la confianza para las organizaciones *data-driven*.

Este concepto unifica lo que históricamente ha estado fragmentado (seguridad, identidad, protección de datos, gobernanza y recuperación) en una única estructura diseñada para una resiliencia continua. Esta integración crea una nueva clase de capacidad operativa que valida continuamente la integridad de los datos, preserva la fiabilidad de los sistemas de IA y permite a las empresas resistir y recuperarse ante interrupciones en el mínimo tiempo posible.

En un mundo donde las decisiones de IA se propagan instantáneamente y los ecosistemas digitales están profundamente interconectados, la resiliencia ya no puede ser episódica ni aislada ni dada por supuesto. Debe diseñarse, automatizarse y probarse continuamente.

Ése es el propósito que define ResOps.