kyndryl

Resiliency Orchestration con Cyber Incident Recovery

Resilienza informatica mirata, per un ripristino rapido, affidabile e scalabile in ambienti multicloud ibridi

Contenuti

Potresti essere in ritardo per un cambiamento

Quanto più i tuoi dati e le tue applicazioni attraversano e si sviluppano su un'infrastruttura interconnessa composta da ambienti on-premise, su cloud pubblico e multicloud, tante più sono le possibilità per gli aggressori informatici di interrompere la continuità della tua attività. La natura complessa degli ambienti multicloud ibridi espone i dati critici e le configurazioni di sistema a livelli di rischio sempre più elevati, tanto che la probabilità di riuscita di un attacco informatico è diventata una certezza assoluta. Non importa quanto possa essere vigile il tuo team di sicurezza IT, un attacco informatico alla fine porterà ad un blocco temporaneo dell'attività sotto forma di interruzione del servizio, furto di dati o danneggiamento dei dati, determinando danni alla reputazione e ricadute finanziarie.

Nel recente passato, si poteva fare affidamento sulle tradizionali soluzioni di disaster recovery per mitigare i danni della maggior parte degli attacchi informatici convenzionali. Ma questo era molto prima che gli ambienti multicloud ibridi diventassero una realtà. Con la crescita della complessità delle infrastrutture IT, anche gli aggressori informatici si sono perfezionati. La crittografia dei dati e gli attacchi malware sono ora progettati per mirare ai backup dei dati in modi che una volta erano inimmaginabili. Di conseguenza, questi attacchi puntano ad accedere alle ubicazioni dei backup e di disaster recovery, lasciando inutilizzabili sia i dati primari che quelli di backup e ritardando in modo significativo la capacità di ripristinare le operazioni a livello di produzione.

Kyndryl Resiliency Orchestration con Cyber Incident Recovery, grazie ad un ripristino veloce, affidabile e scalabile in ambienti multicloud ibridi, riduce al minimo l'impatto sul business degli attacchi informatici.

Recupero informatico mirato per un mondo multicloud ibrido
Kyndryl™ Resiliency Orchestration con Cyber Incident Recovery , in caso di interruzione dell'operatività informatica, può recuperare rapidamente i dati e le configurazioni della piattaforma. Fornisce l'automazione intelligente dei flussi di protezione dei dati e di disaster recovery e consente test di ripristino, immutabilità dei dati, rilevamento di anomalie, monitoraggio, gestione e reporting in ambienti multicloud ibridi. La soluzione offre un ripristino automatizzato, affidabile e veloce di carichi di lavoro fisici e virtuali, inclusi processi aziendali, applicazioni, sistemi e database, in seguito ad attacchi informatici.

Cyber Incident Recovery fornisce:
- Facile capacità di test che non influisce sugli ambienti di produzione
- Rilevamento più veloce del danneggiamento dei dati e risposta rapida per ridurre i tempi di inattività
- Efficiente ripristino point-in-time con conseguente ottimizzazione degli RPO (recovery point objectives)
- Scalabilità per gestire il rilevamento e il ripristino di grandi dimensioni a livello di sede, in pochi minuti
- Visibilità e reporting semplificati per aiutare a soddisfare i requisiti normativi

Kyndryl Resiliency Orchestration con Cyber Incident Recovery offre un ripristino automatizzato, affidabile e veloce dei carichi di lavoro fisici e digitali in seguito ad attacchi informatici.

Un'architettura che consente un approccio agile alla resilienza informatica

Gli elementi fondanti della tecnologia, che costituiscono la funzionalità di Cyber Incident Recovery, forniscono una piattaforma che abbraccia i livelli di elaborazione e dati degli ambienti di produzione e di disaster recovery. Ciò consente un approccio agile al ripristino dei carichi di lavoro virtuali e fisici.

Storage inalterabile
L'utilizzo della tecnologia di storage inalterabile per i dati di configurazione o dello storage WORM (write-once-read-many) per i dati delle applicazioni, consente di prevenirne il danneggiamento e garantisce la recuperabilità non consentendo di apportare modifiche ai backup salvati. Per i dati delle applicazioni, questo approccio aiuta anche a ridurre i costi di storage scrivendo solo nuove copie di modifiche incrementali point-in-time.

Protezione "air-gapped"
L'isolamento della rete separa gli ambienti di produzione dallo storage WORM che contiene i dati protetti e sottoposti a backup in un sito remoto o di disaster recovery (DR). L'accesso allo storage WORM è inoltre limitato solo ai momenti in cui i dati sono disponibili per il backup. Questo approccio, combinato con lo storage inalterabile, aiuta a prevenire la corruzione dei dati protetti causata da malware che possono attraversare le reti o che sono progettati specificamente per prendere di mira i dati di backup.

Rilevamento di anomalie
Kyndryl Resiliency Orchestration include una capacità di rilevamento delle anomalie che utilizza l'identificazione euristica basata su regole, potenziata dall'AI. Viene addestrato su diversi modelli di modifica dei malware noti, acquisisce e confronta i modelli di modifica nei dati di backup per prevedere le anomalie dei dati con elevata precisione. Questa capacità di rilevamento delle anomalie nel sito di DR aiuterà a identificare le istantanee di backup anomale e ad eseguire il ripristino partendo da copie pulite.

Verifica dei dati della configurazione
Questo componente utilizza la capacità integrata - basata sull'AI - di rilevamento delle anomalie per garantire che la configurazione o i dati da proteggere siano puliti e recuperabili. Il processo, integrato in Resiliency Orchestration, rileverà automaticamente quando le configurazioni del sistema sono state modificate. Resiliency Orchestration si integrerà anche con gli script di convalida dell'applicazione forniti dal cliente per fornire test a livello di applicazione e dati.

Automazione e orchestrazione
Automatizzando il processo di ripristino end-to-end per dati e applicazioni, Resiliency Orchestration consente un rapido ripristino dell'ambiente IT. Resiliency Orchestration sostituisce i tradizionali processi manuali con flussi di lavoro predeterminati, testati e convalidati, che consentono di recuperare un intero processo aziendale, un'applicazione, un database o un sistema separato con un semplice clic. Tali flussi di lavoro orchestrano i molteplici passaggi necessari per recuperare sistemi e dati interconnessi, limitando l'errore umano. Resiliency Orchestration aiuta ad accelerare l'implementazione della soluzione sfruttando un'ampia libreria di oltre 800 modelli predefiniti che possono essere combinati per creare flussi di lavoro.

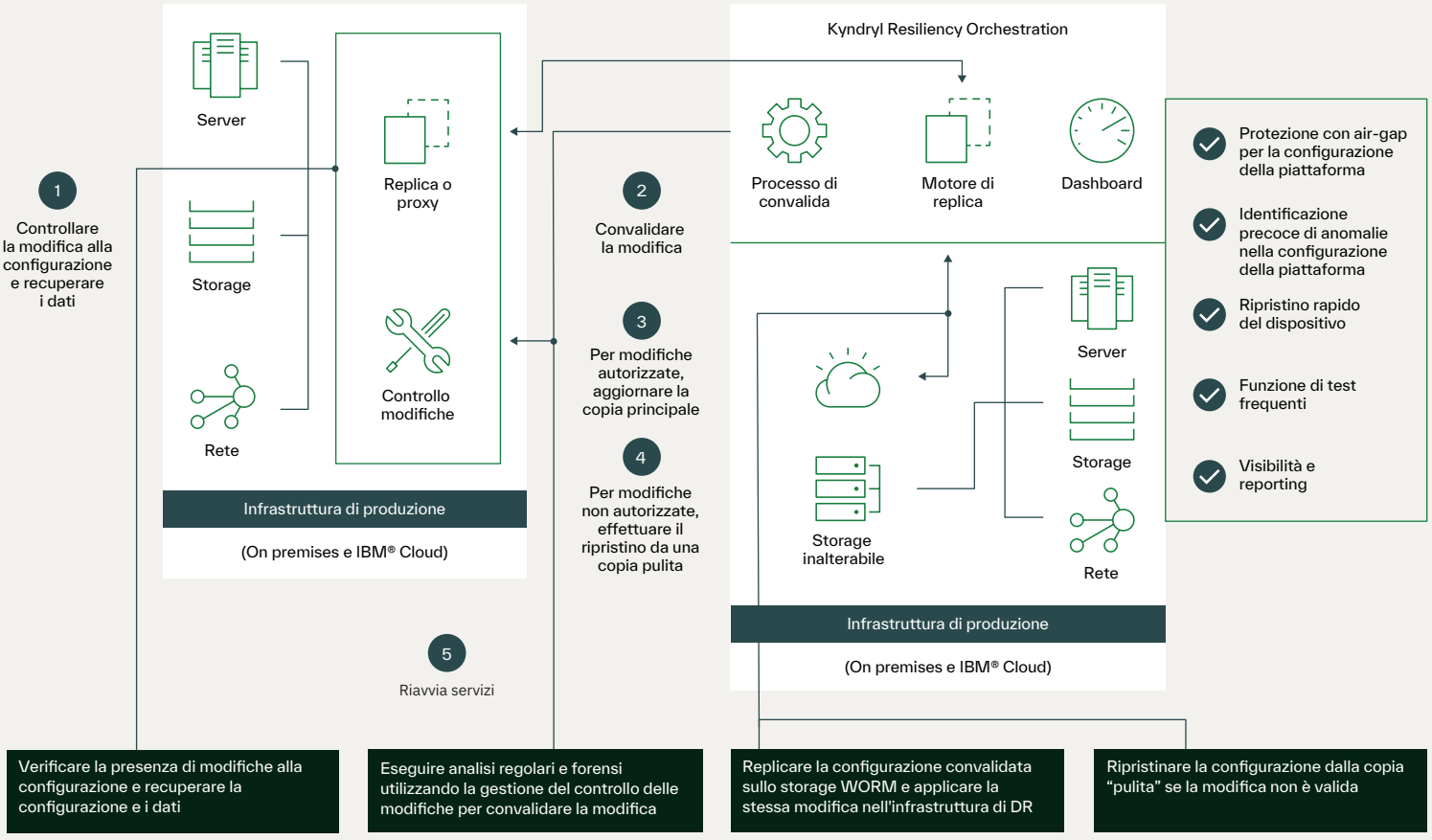
Cyber Incident Recovery per la configurazione della piattaforma

I malware spesso alterano le configurazioni prima di danneggiare gli stessi dati, quindi è fondamentale rilevare eventuali modifiche alla configurazione prima che i dati effettivi vengano infettati. La funzionalità di configurazione della piattaforma di Cyber Incident Recovery protegge i dati di configurazione dei carichi di lavoro virtuali e fisici, delle applicazioni, dei sistemi di storage e dei dispositivi di rete in ambienti on-premise, con cloud pubblico, cloud ibrido e multicloud.

Mantenere l'attività operativa con una "copia principale"
Questo componente utilizza le tecnologie integrate per identificare eventuali modifiche alle configurazioni degli endpoint di produzione e avvisa l'utente di qualsiasi modifica autorizzata e non autorizzata. Gli avvisi possono anche prevedere l'apertura di ticket pertinenti da parte del software di gestione del controllo delle modifiche. Per consentire un rapido ripristino dei servizi, Cyber Incident Recovery replica una "copia principale" dei dati di configurazione di server e dispositivi su uno storage inalterabile protetto da con "air gap".

Risposta a modifiche di configurazione non valide e valide
In caso di modifica valida, i dati di configurazione vengono protetti mediante la replica di una nuova "copia principale" su uno storage inalterabile. Se viene identificata una modifica non valida, sulla base di criteri prestabiliti e con il consenso dei responsabili, Resiliency Orchestration provvede a ripristinare rapidamente nell'infrastruttura di produzione l'ultima copia pulita delle configurazioni del dispositivo. Le configurazioni dedicate e delle macchine virtuali vengono ripristinate su un'infrastruttura di produzione pulita. In caso di modifiche valide, viene creata una nuova "copia principale" in uno storage inalterabile.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery for Platform Configuration



*Air-gap non supportato per lo storage inalterabile su cloud

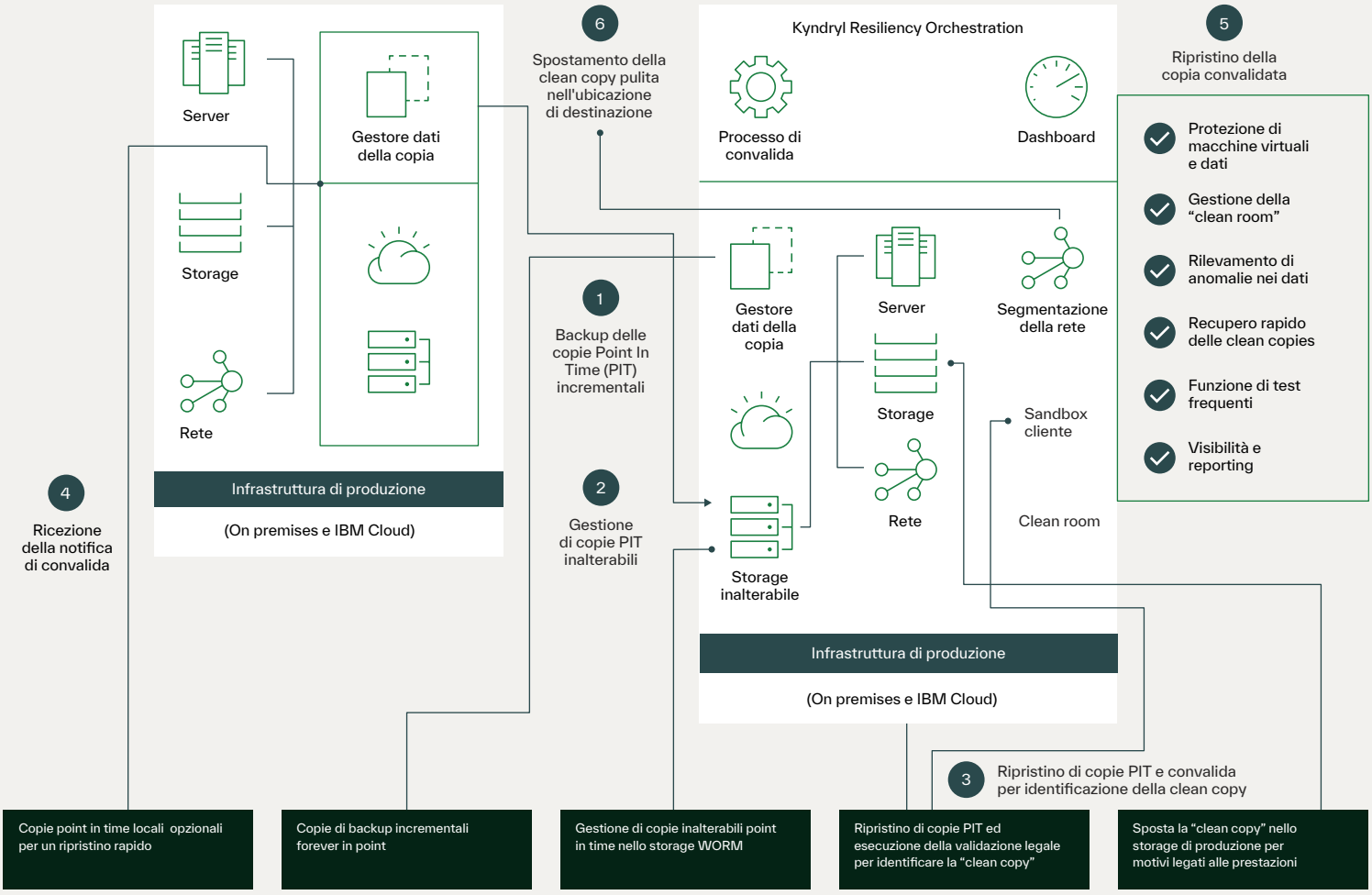
Cyber Incident Recovery per i dati

La funzione dati di Cyber Incident Recovery abilita un ripristino molto affidabile e veloce in caso di attacchi informatici che danneggiano i dati stessi. Protegge i dati tramite l'uso di una protezione air gap e di storage inalterabile, orchestrando il ripristino rapido presso il sito di disaster recovery.

Protezione di grandi volumi di dati in tutti gli ambienti
Cyber Incident Recovery è progettato per gestire grandi volumi di dati applicativi, indipendentemente da dove questi risiedano. Impiega la tecnologia di gestione dei dati delle copie per creare e gestire copie incrementali point-in-time (PIT) dei dati Poiché tali copie vengono conservate in uno storage inalterabile come ad esempio il Cloud Object Storage o uno storage con funzionalità WORM, sono copie "eterne" che non possono essere modificate. Il software di gestione dei dati delle copie replica i dati su sito di disaster recovery o sito alternativo, creando le copie PIT. È inoltre possibile eseguire copie PIT e conservarle presso il sito di produzione per assicurare una funzionalità di ripristino rapido.

Rispondere rapidamente agli attacchi informatici per mantenere la continuità aziendale
Quando un responsabile del disaster recovery riceve una notifica che è stata rilevata una violazione dei dati o un'infezione da malware crittografato, presso il sito di disaster recovery, vengono eseguiti test automatici delle copie PIT per verificare la recuperabilità dei dati. L'ultima copia "pulita", identificata dal processo di test e verifica, viene quindi ripristinata sull'infrastruttura di disaster recovery dal software Resiliency Orchestration. Presso il sito di disaster recovery è anche possibile condurre frequenti test, contribuendo così a garantire la recuperabilità dei dati senza influire sulle operazioni aziendali. Resiliency Orchestration consente di garantire che le piattaforme possano essere ripristinate rapidamente, e in parallelo.

Kyndryl Cyber Recovery as a Service
Cyber Incident Recovery for Data



Dashboard e reporting che semplificano la gestione

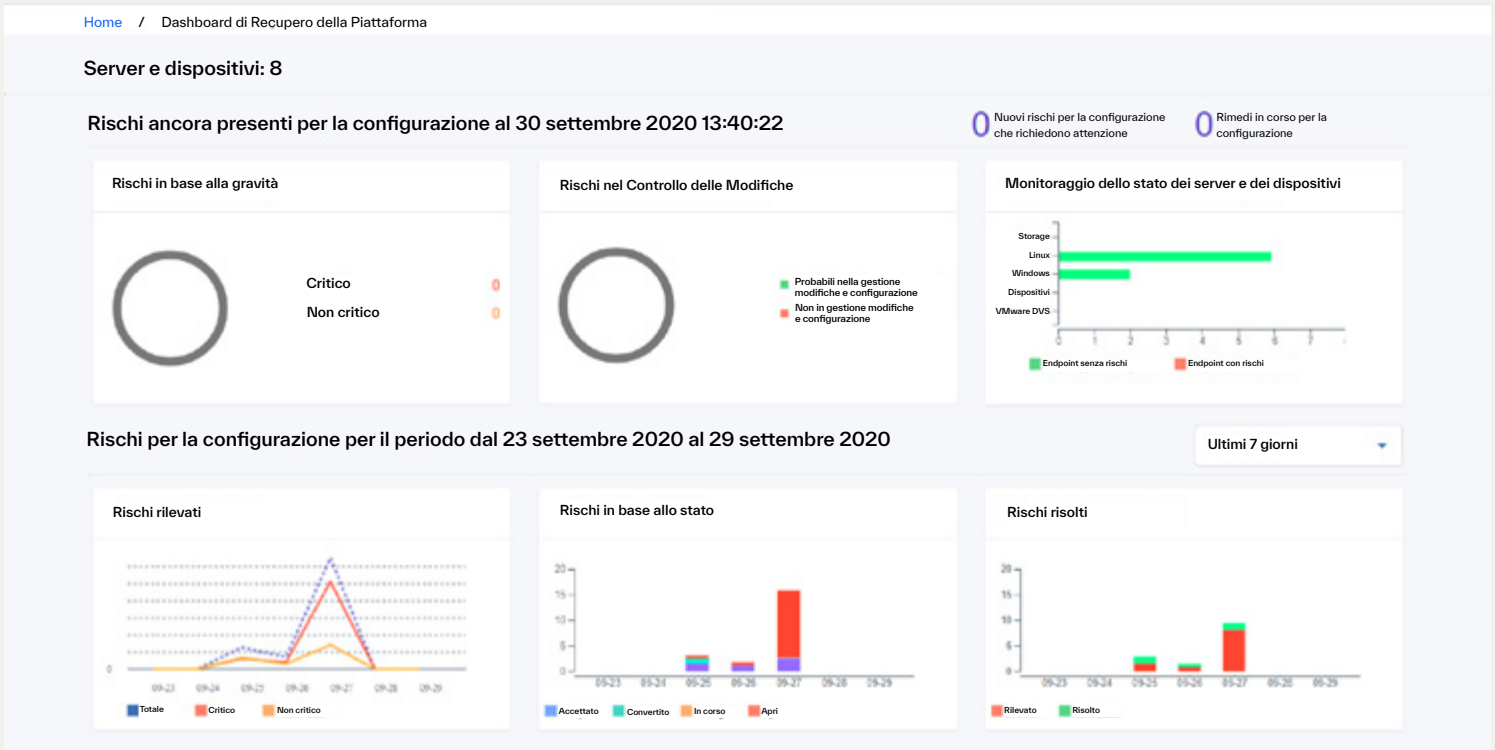
Cyber Incident Recovery include un dashboard che semplifica la gestione del recupero informatico e il monitoraggio delle modifiche alla configurazione della piattaforma e dei dati. Fornisce visibilità in tempo reale sulle discrepanze rispetto all'RPO e all'RTO (recovery time objective), sullo stato di convalida delle istantanee e sugli aggiornamenti critici del recupero informatico.

Nel frattempo, la direzione generale o il consiglio di amministrazione possono ricevere aggiornamenti critici in tempo reale sul ripristino informatico per consentire un processo decisionale più rapido e informato.

Migliore tracciabilità delle vulnerabilità e maggiore visibilità
La dashboard di Cyber Incident Recovery indica il numero di vulnerabilità negli ambienti, insieme al relativo livello di gravità. È possibile tenere traccia delle vulnerabilità aperte e prendere decisioni informate grazie al rilevamento delle discrepanze rispetto all'RPO, all'RTO, allo stato di convalida dell'istantanea e alla disponibilità informatica attuale.

Solida funzionalità di reportistica
Il modulo di reporting integrato offre un ricco set di report, tra cui la posizione di disaster recovery o la resilienza informatica, che possono essere esportati e condivisi con le autorità di regolamentazione per scopi di conformità, insieme ai grafici acquisiti durante le normali attività aziendali.

Cyber Incident Recovery fornisce visibilità in tempo reale su discrepanze rispetto agli RPO e RTO, stato di convalida delle istantanee e aggiornamenti critici



Kyndryl Resiliency Services ha decenni di esperienza nel consentire ai clienti di tutto il mondo di soddisfare le loro esigenze in termini di backup e ripristino.

Vantaggio Kyndryl
- Competenza sull'intero il ciclo di vita della resilienza
- Recupero automatico dei carichi di lavoro fisici, virtuali e cloud
- Oltre 800 modelli predefiniti per un'implementazione e una scalabilità più rapide ed efficienti
- Selezione di cloud, tra cui AWS, Azure e IBM Cloud, per una scalabilità aziendale

Affidabile
- Oltre 9.000 clienti sono protetti con la disaster recovery e i DMS (data management services) di Kyndryl
- Kyndryl ha più di 3,5 exabyte sottoposti a backup ogni anno e in gestione

Una portata globale
- Esistono più di 300 IBM Resiliency Center in più di 50 paesi in tutto il mondo
- IBM dedica oltre 6.000 professionisti in tutto il mondo alla resilienza

Perché Kyndryl?

Kyndryl vanta una profonda esperienza nella progettazione, esecuzione e gestione dell'infrastruttura tecnologica più moderna, efficiente e affidabile da cui il mondo dipende, ogni giorno. Kyndryl è profondamente impegnata nel far progredire l'infrastruttura critica che supporta il progresso umano. Stiamo creando sistemi sulla nostra base di eccellenza, in modi nuovi: aggiungendo i partner più validi, investendo nel nostro business e lavorando fianco a fianco con i nostri clienti per realizzare il massimo potenziale.

Vuoi scoprire qualcosa di più?

Per saperne di più su ciò che Kyndryl Resiliency Orchestration with Cyber Incident Recovery può fare per te, contatta il tuo rappresentante Kyndryl o visita www.kyndryl.com

kyndryl

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

Prodotto negli USA
Luglio 2021