

Il backup dei dati all'Università di Napoli



L'UNIVERSITÀ FEDERICO II IMPLEMENTA LA SOLUZIONE DI OVERLAND STORAGE PER PROTEGGERE 5 TB DI DATI GENERATI DA 8.000 MEMBRI DELLO STAFF E 130.000 STUDENTI. NONOSTANTE LA MANCANZA DI PERSONALE DALLE ORE 20:00 ALLE 7:00, L'UNIVERSITÀ DEVE RENDERE I DATI DISPONIBILI PER GLI STUDENTI 24 ORE SU 24 E 7 GIORNI SU 7.

Prima dell'installazione di **Reo 4000** e **Neo 2000**, i due amministratori del sistema eseguivano il backup dei dati della sede centrale direttamente su nastro e l'intera procedura richiedeva cinque giorni. Inoltre, per i dati della sede remota di Montesantangelo, veniva eseguito soltanto un processo di backup nominale, una volta al mese. All'inizio del 2006, le due infrastrutture erano consolidate e il team ha iniziato a cercare una soluzione più

semplice ed efficiente per eseguire il backup dei dati della sede remota sul disco locale, da trasportare sulla libreria di nastri situata nella sede principale. L'Università di Napoli ha così installato l'applicazione di ripristino e backup basati su disco Reo 4000 nella sede remota di Montesantangelo e una libreria di nastri Neo 2000 nella sede centrale per l'archiviazione dei 5 terabyte di dati di server Web, iscrizioni degli studenti ed e-mail. "Non è stato difficile scegliere Overland. Non potevamo impiegare altri due amministratori di backup nel sito remoto; ora, grazie alle soluzioni Neo e Reo, i nostri attuali operatori possono gestire l'intero sistema da un'unica sede", ha dichiarato il **Dottor Giovanni Barone, responsabile dei sistemi informatici dell'Università**. I criteri di selezione erano la convenienza, la gamma di funzioni, quali modularità, scalabilità, supporto di tecnologie Fibre Channel, iSCSI e Ethernet e affidabilità. L'Università aveva bisogno di un sistema aperto: in base alla loro importanza, i dati erano memorizzati su SAN (80%), NAS (18%) o DAS (2%). Inoltre, sono stati implementati diversi sistemi operativi con cui eventuali nuove soluzioni dovranno essere compatibili.

Grazie alla solida strategia di backup offerta dalle soluzioni Overland, oggi l'Università di Napoli può recuperare dati in meno di 30 minuti. Barone sostiene che "Adesso, in caso di perdita di dati, la sede di Montesantangelo è in grado di recuperarne facilmente e rapidamente una copia presso la sede centrale. Il prossimo anno verrà aggiunta una seconda applicazione Reo per implementare una strategia di backup bidirezionale in grado di memorizzare i dati dell'ufficio principale presso la sede dislocata, per una protezione ancora maggiore". "L'Università di Napoli ha rappresentato una grande sfida, considerati l'ambiente eterogeneo esistente, gli esigenti e ampi criteri di selezione e l'alta affidabilità richiesta dal sistema", ha dichiarato **Chris James, Direttore Marketing EMEA di Overland Storage**. "Tuttavia, le nostre soluzioni Reo e Neo soddisfano tutte queste esigenze e, oltre a offrire completa sicurezza, consentono al team IT di concentrarsi sulla fornitura di un accesso ai dati affidabile e continuo ai membri dello staff e agli studenti". Il Dottor Barone ha aggiunto: "La combinazione di funzioni, affidabilità e risparmio fa di Overland la soluzione ideale per l'Università. La versatilità del protocollo della libreria di nastri Neo unita alla scalabilità dell'applicazione disco Reo sono solo due dei motivi che ci hanno spinto a scegliere Overland". "Le soluzioni Reo 4000 e Neo 2000 ci hanno fornito prestazioni fluide. Non saremo riusciti a raggiungere risultati simili senza queste applicazioni".

La configurazione D2D ha ridotto il processo di backup da cinque a due giorni.

La migrazione dei dati su nastro, che ancora richiede cinque giorni, viene fatta sullo sfondo, senza che l'unica copia di dati subisca problemi. ■



F-Secure protegge il divertimento a Mirabilandia

Mirabilandia è la meta ideale per chi desidera divertimento e relax, offrendo attrazioni e spettacoli tra i più coinvolgenti d'Europa, pensati per tutti i gusti e le età, che in estate si arricchiscono di Mirabilandia Beach, la splendida spiaggia tropicale. Il Parco però era alla ricerca di una soluzione di sicurezza che consentisse di proteggere in maniera efficiente tutti i 150 client utilizzati dalle varie strutture: dagli uffici amministrativi fino alle casse. Si cercava una soluzione in grado di offrire protezione reattiva e preventiva, garantendo così operatività ininterrotta ai sistemi, una soluzione che si affiancasse alla tradizionale protezione da virus e che potesse monitorare comportamenti sospetti all'interno dei sistemi e indicatori di infiltrazioni di malware di varia natura. In passato infatti il parco macchine era rimasto addirittura bloccato per giorni a causa di un noto virus che aveva bucatto i sistemi di protezione.

"Eravamo alla ricerca di una protezione più completa e affidabile, che ci permettesse di ottimizzare tempo e risorse", spiega **Pierluigi Carboni, responsabile dei sistemi informativi di Mirabilandia**. "I prodotti utilizzati fino a quel momento non erano riusciti a garantirci una protezione a 360° e rallentava troppo il nostro sistema". Dopo un'attenta valutazione, nel 2006 Mirabilandia ha scelto **F-Secure Client Security 6** per la totalità del suo parco macchine, passando poi alla versione 7 appena questa si è resa disponibile. F-Secure Client Security è la soluzione per la sicurezza dedicata agli ambienti aziendali, che fornisce una protezione avanzata non solo da virus noti, ma anche da minacce sconosciute, rootkit e spyware. Fin dall'inizio, l'impiego di Client Security ha apportato diversi vantaggi a Mirabilandia. La soluzione di F-Secure ha garantito da subito una protezione totale e non si sono più verificati episodi di vulnerabilità ad attacchi virali o da minacce di altro genere. Tra gli elementi della soluzione F-Secure particolarmente apprezzati da Mirabilandia, con una dotazione di macchine sparsa per tutta l'estensione del parco, la possibilità di gestire in modo efficiente da remoto il software (installazioni, aggiornamenti e monitoraggio) e di poter contare su un'assistenza tecnica prontamente attivabile e competente - come spiega sempre il responsabile dei sistemi informativi del parco - che

IL PARCO DIVERTIMENTI PIÙ GRANDE D'ITALIA HA SCELTO F-SECURE® CLIENT SECURITY™ PER LA SICUREZZA E L'OPERATIVITÀ ININTERROTTA DELLA TOTALITÀ DEI PROPRI DESKTOP. MIRABILANDIA È IL PARCO DIVERTIMENTI PIÙ GRANDE D'ITALIA. E' SITUATO NEI PRESSI DI RAVENNA E SI ESTENDE SU UN'AREA DI 850.000 METRI QUADRATI.

diverse volte ha fornito supporto telefonico immediato e chiarimenti in fase sia di installazione che di operatività.

A testimonianza dell'esperienza positiva con Client Security, Mirabilandia ha da poco avviato l'upgrade alla nuova versione 7, andando così a potenziare ulteriormente le funzionalità anti-virus e aggiungendo potenti funzionalità anti-spyware.

Pierluigi Carboni si dice pienamente soddisfatto del livello di protezione offerto dalla soluzione F-Secure, sulla quale il Parco ha deciso di standardizzare la sicurezza sia attuale che futura dei propri clienti. ■



Punti chiave di F-Secure Client Security:

- DeepGuard™, la tecnologia di intrusion prevention sviluppata da F-Secure per impedire l'esecuzione del codice maligno sconosciuto al sistema.
- Blacklight™, lo scanner di rootkit, che li individua prima che possano attivarsi.
- Individuazione e rimozione dello spyware.
- Messa in quarantena completa di virus, spyware e riskware.
- Sistema di aggiornamento automatico, affidabile e ad alte prestazioni.
- Gestione remota centralizzata per l'amministrazione globale del sistema.
- Scansione di posta elettronica e navigazione Web.
- Firewall con sistema anti-intrusione.