Entrust aiuta Zerto a garantire l'integrità delle sue applicazioni per le aziende

Fondata nel 2010, Zerto si è posta una vision unica, che mira a far percepire le tecnologie di disaster recovery come un vantaggio competitivo, non una semplice polizza assicurativa.

L'azienda elimina i rischi e le complessità legati alla modernizzazione dell'IT e all'adozione del cloud, aiutando i propri clienti ad accelerare la trasformazione tecnologica attraverso la resilienza. L'esclusiva piattaforma software IT Resilience Platform™ di Zerto raggruppa funzionalità di disaster recovery, back-up e mobilità nel cloud in un'unica soluzione, sostituendosi a vari sistemi legacy. Caratterizzata da una scalabilità di livello aziendale, offre inoltre una disponibilità continua per un'esperienza cliente senza interruzioni e agevola, al tempo stesso, la mobilità dei carichi di lavoro per proteggere, recuperare e spostare liberamente le applicazioni attraverso ambienti ibridi e multi-cloud.

Zerto ha rivoluzionato i mercati dell'IT ridefinendo il concetto di disaster recovery. In un mondo in cui le imprese esigono un'esperienza tecnologica ininterrotta, l'azienda ha sviluppato un prodotto innovativo che, garantendo la protezione continua dei dati, offre ai clienti maggiori vantaggi rispetto a un semplice strumento di ripristino di emergenza.

> **«Se confrontate con quelle di altri fornitori, le implementazioni e l'assistenza di Entrust sono migliori, gli HSM nShield Solo sono più semplici da usare e anche il processo di back-up non è per nulla complesso. Abbiamo apprezzato anche la loro interfaccia utente grafica (GUI).»**
>
> – Nadav Svirsky, Responsabile dell'infrastruttura IT aziendale, Zerto

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Zerto

LA SFIDA COMMERCIALE

Fornitore leader nel settore della resilienza IT, per Zerto era importante assicurare che i propri sistemi aziendali non presentassero rischi di compromissione. La strategia più efficace per raggiungere questo obiettivo era garantire l'affidabilità dell'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure).

Un'infrastruttura PKI è costituita da un insieme di hardware, software, criteri, processi e procedure necessari per creare, gestire, distribuire, usare, archiviare e revocare certificati digitali e chiavi pubbliche. Le PKI contribuiscono a determinare l'identità di utenti, dispositivi e servizi, consentendo l'accesso controllato a sistemi e risorse, la protezione dei dati e l'attribuzione della responsabilità delle transazioni. Le applicazioni aziendali di nuova generazione si affidano sempre di più alla tecnologia PKI al fine di garantire un elevato livello di sicurezza. L'evoluzione dei modelli di business, infatti, sta portando a una dipendenza maggiore dalle interazioni elettroniche, che richiedono l'autenticazione online e il rispetto di normative più severe in materia di sicurezza dei dati.

Le PKI utilizzano i certificati digitali per collegare le chiavi pubbliche al relativo utente, ovvero il proprietario della chiave privata, semplificando la verifica delle identità di chiunque sia coinvolto in una transazione. Proprio come il passaporto identifica una persona come cittadino di un determinato Paese, il certificato digitale stabilisce l'identità degli utenti all'interno dell'ecosistema. Tali certificati sono impiegati per verificare l'identità tanto degli utenti a cui sono inviati i dati cifrati quanto del firmatario delle informazioni, per cui è indispensabile proteggerne l'autenticità e l'integrità al fine di garantire che l'intero sistema sia affidabile. Tutto ciò si è rivelato essenziale per il modello di business di Zerto, che si propone come fornitore di fiducia.

LA SFIDA TECNICA

Le autorità di certificazione (CA) emettono le credenziali digitali utilizzate per certificare l'identità degli utenti e, in quanto pilastri su cui si fonda la sicurezza di una PKI e dei servizi che supporta, finiscono spesso nel mirino di attacchi sofisticati. Per attenuare i rischi di attacchi alle CA, l'integrità di una PKI è garantita da controlli logici e fisici e da meccanismi per la creazione di un ambiente temprato, come il ricorso agli hardware security module (HSM).

Zerto utilizza una piattaforma Microsoft e, grazie alla collaborazione con il gigante del settore tecnologico, il reparto IT dell'azienda sapeva che la best practice di protezione delle CA consiste nell'impiego di un HSM. Parte integrante della sicurezza delle chiavi sensibili e dei processi aziendali, gli HSM offrono un ambiente a prova di manomissione certificato da enti indipendenti.

Zerto

> **Gli HSM nShield Solo di Entrust garantiscono la protezione di cui abbiamo bisogno per le nostre CA. I nostri dirigenti ritengono che la riduzione dei rischi valga decisamente l'investimento.**
>
> – Nadav Svirsky, Responsabile dell'infrastruttura IT aziendale, Zerto

LA SOLUZIONE

Forte della grande esperienza con vari fornitori, il team IT di Zerto ha scelto di implementare gli HSM nShield® Solo di Entrust. Secondo Nadav Svirsky, Responsabile dell'infrastruttura IT aziendale, Zerto ha preferito Entrust perché "se confrontate con quelle di altri fornitori, le implementazioni e l'assistenza di Entrust sono migliori, gli HSM nShield Solo sono più semplici da usare e anche processo di back-up non è per nulla complesso. Abbiamo apprezzato anche la loro interfaccia utente grafica (GUI)."

I RISULTATI

Zerto ha scelto di non condividere i risultati quantificabili dell'installazione degli HSM nShield di Entrust per proteggere le sue CA. Riferendosi al raggiungimento di un livello di sicurezza in linea con le best practice del settore, come previsto sin dall'inizio per il progetto, Svirsky ha commentato: "I nostri clienti devono avere la certezza che i nostri sistemi siano sicuri e affidabili. Sfortunatamente, spesso non si comprende il valore della sicurezza dei dati fino a quando non si incontra un problema. È in quel momento che, di solito, si assiste al tracollo della reputazione di un'azienda, delle vendite e del prezzo delle azioni. Gli HSM nShield Solo di Entrust garantiscono la protezione di cui abbiamo bisogno per le nostre CA. I nostri dirigenti ritengono che la riduzione dei rischi valga decisamente l'investimento."

Zerto

PRESTAZIONI, AFFIDABILITÀ E SICUREZZA

Obiettivi commerciali

- Riduzione del rischio di problemi interni di sicurezza dei dati

Obiettivi tecnici

- Introduzione di una root of trust sicura per i server delle CA a un costo contenuto

La soluzione

- HSM nShield Solo di Entrust

Il risultato

- Riduzione dei rischi
- Fonte di tranquillità per i dirigenti di Zerto

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Scopri di più su
entrust.com/HSM

ENTRUST

Per contattarci:
HSMinfo@entrust.com