

CASO DI STUDIO

Sicredi adotta NIOS DDI e BloxOne Threat Defense per continuare la sua crescita come leader nel settore finanziario brasiliano



PANORAMICA

Sicredi è un istituto finanziario cooperativo fondato più di 120 anni fa. Negli ultimi due decenni, l'azienda ha visto una riorganizzazione interna e ha accelerato la sua espansione. Per sostenere questa crescita e guidare l'innovazione nel settore finanziario, Sicredi ha investito nella trasformazione digitale.

Le cooperative di credito presentano lo stesso portafoglio di prodotti e servizi finanziari degli istituti finanziari tradizionali (conti correnti, carte, investimenti), ma si distinguono principalmente per il modello di gestione. A differenza degli istituti convenzionali, nelle cooperative di credito gli associati sono i veri proprietari dell'attività.

Per attuare con successo questo modello di business, Sicredi adotta una strategia di gestione che si avvale della partecipazione dei suoi oltre sette milioni di associati, che svolgono il ruolo di proprietari dell'attività. Con oltre 2.500 filiali, questo istituto finanziario cooperativo è fisicamente presente in tutti gli stati brasiliani e nel distretto federale, fornendo una gamma completa di soluzioni finanziarie e non finanziarie.

LA SITUAZIONE

L'espansione geografica e la digitalizzazione stimolano l'attività delle cooperative di credito

Sicredi è cresciuta in modo significativo in termini di filiali e di base di associati, diventando uno dei principali attori del settore finanziario brasiliano negli ultimi anni. Attualmente offre più di 300 prodotti e servizi finanziari, dai conti correnti e carte agli investimenti, alle assicurazioni, ai consorzi, ai bancomat e ai conti 100% digitali, per persone fisiche, persone giuridiche e produttori rurali.

“ Infoblox ha accelerato la consegna dei nostri prodotti agli associati e agli utenti finali. In precedenza, la fornitura di una macchina richiedeva in media cinque giorni. Oggi possiamo farlo in 15 minuti. È più flessibile e agile.”

Juliano Luz,
Infrastructure Analyst, Sicredi

Per accompagnare questo progresso, nel 2017 Sicredi ha avviato un processo di trasformazione digitale, con l'intenzione di sostituire gradualmente i vecchi sistemi per l'elaborazione di prodotti e servizi, noti come "core banking", con una piattaforma più moderna. L'adozione di una tecnologia all'avanguardia è stata fondamentale per offrire una migliore esperienza agli associati e mantenere la competitività nel dinamico mercato finanziario brasiliano.

Per molti anni, Sicredi ha funzionato con un'infrastruttura tecnologica e macchine virtuali su strumenti DHCP e Linux "open source". L'Infrastructure Analyst Juliano Luz, entrato in Sicredi nel 2008, ricorda un ambiente obsoleto: "C'era una sfida legata alla mancanza di scalabilità e agilità. L'attività aveva bisogno di una nuova applicazione, di un nuovo ambiente", afferma.

Poiché funzionava con soluzioni open source, il vecchio ambiente non aveva alcun supporto esterno e tutti i problemi dovevano essere risolti internamente, richiedendo un intenso coinvolgimento da parte del reparto IT. Un'altra preoccupazione di Sicredi era il rafforzamento della sicurezza contro gli attacchi informatici.

Sicredi aveva già implementato una soluzione Infoblox nel 2013, ma nel 2021 ha deciso di aggiornare l'ambiente tecnologico. "L'iniziale implementazione di DDI è stata effettuata dal team interno. NTT si è unita come partner quando abbiamo ampliato e aggiornato NIOS DDI di Infoblox", ha detto Luz.

LA SFIDA

L'infrastruttura tecnologica obsoleta mantiene processi manuali lenti

Il numero crescente di progetti, servizi e prodotti finanziari Sicredi necessitava di un ambiente con maggiore contingenza e scalabilità. La tecnologia obsoleta limitava i piani di crescita. "Il nostro vecchio sistema si è rivelato un collo di bottiglia. Era lento assegnare l'IP e creare record in un gestore di indirizzi IP nel nome DNS", ha detto Luz. "Era complicato prenotare l'IP e registrare il nome, generando una mancanza di controllo dell'indirizzamento e problemi con l'infrastruttura."

L'infrastruttura necessitava di una maggiore disponibilità sui server DNS, ad esempio, in modo da poter replicare i file su un altro computer in modo automatico, non manuale. Il team IT desiderava anche semplificare e accelerare il processo di attivazione dei progetti per liberare l'infrastruttura e i team di rete da questi tipi di compiti. "Andavo dal team delle reti per ottenere un IP e un nome e poi passavo alla parte finale per fornire alcune regole. Sul sistema operativo è stata creata e installata una macchina virtuale. Era tutto molto lento", ha detto Luz.

La nuova soluzione doveva anche garantire protezione a dipendenti e associati a causa della minaccia sempre più grave e frequente di attacchi informatici e frodi digitali. Anche l'ambiente normativo stava diventando più severo, con la Banca Centrale del Brasile che iniziava a richiedere controlli e sistemi di sicurezza cibernetica più solidi nelle istituzioni finanziarie.

Cliente: Sicredi Bank
Settore: Banca
Sede: Brasile

INIZIATIVE:

- Stabilire un ambiente con una maggiore contingenza e scalabilità per il numero crescente di progetti di Sicredi, i suoi servizi finanziari e prodotti
- Sostituire i prodotti tecnologici obsoleti, che limitavano i piani di crescita
- Aumentare la disponibilità dell'infrastruttura, ad esempio, nei server DNS per poter replicare i file su un'altra macchina in modo automatico e non manuale

RISULTATI:

- Miglioramento della qualità e dell'agilità nella consegna delle risorse all'azienda
- Accelerazione della consegna dei prodotti ai membri e agli utenti finali
- Miglioramento dei tempi di fornitura: in precedenza la fornitura di una macchina richiedeva in media cinque giorni; oggi può essere effettuata in 15 minuti

SOLUZIONI:

- NIOS DDI
- BloxOne® Threat Defense

LA SOLUZIONE

Amministrazione DNS semplificata e maggiore sicurezza contro gli attacchi informatici

Sicredi ha iniziato a implementare Infoblox NIOS DDI, che alimenta i servizi di rete di base di Infoblox, consentendo il funzionamento continuo dell'infrastruttura. L'implementazione è stata effettuata con il partner, NTT. Per prima cosa, Sicredi ha migrato la base DNS alla nuova infrastruttura Infoblox. Nel tempo ha ampliato le funzionalità, internamente ed esternamente. Infoblox NIOS ha facilitato l'integrazione e la centralizzazione dei servizi DNS, DHCP e IPAM (DDI) di Sicredi su un'unica piattaforma.

“Insieme a VMware, c'era un'integrazione con Infoblox, e tutto questo era automatizzato. Oggi possiamo andare su un portale, ordinare un computer, registrare il nome IP e prenotare l'IP; viene installato un sistema operativo e viene fornita una macchina virtuale pronta all'uso”, ha descritto Andrius Lima, Infrastructure Analyst di Sicredi. Infoblox ha anche abilitato le automazioni tramite API per facilitare l'accesso alle applicazioni di altri team. Questa funzionalità è stata essenziale nelle azioni pionieristiche di Sicredi nei programmi “Open Banking” e “Open Finance” in Brasile.

Infoblox NIOS ha rafforzato la sicurezza, il controllo e la visibilità. Nel 2021, Sicredi ha investito in BloxOne Threat Defense, la soluzione ibrida per la sicurezza di Infoblox. Questa implementazione ha permesso all'organizzazione di diventare più organizzata in termini di DNS, record e controlli e di beneficiare di una migliore postura di sicurezza in generale. Questo strumento integra le funzionalità dell'ambiente precedente, come firewall e DDR.

“Infoblox ci ha permesso di scalare la nostra infrastruttura DNS, DHCP e organizzare il nostro ambiente per gestire la crescita dell'attività”, afferma Luz.

IL RISULTATO

Infoblox ha ridotto i costi operativi e facilitato l'attività di Sicredi

La transizione alle soluzioni Infoblox ha rappresentato un enorme guadagno per Sicredi in termini di qualità e agilità nell'offrire risorse all'azienda. La nuova infrastruttura ha ridotto i costi operativi perché le attività di amministrazione della rete sono ora gestite in un'unica interfaccia, automatizzando e decentrando i processi essenziali che in precedenza dovevano essere eseguiti manualmente nel data center. Le cooperative stesse ora possono amministrare le proprie risorse con il queue management.

“Infoblox ha accelerato la consegna dei nostri prodotti agli associati e agli utenti finali. In precedenza, la fornitura di una macchina richiedeva in media cinque giorni. Oggi possiamo farlo in 15 minuti. È più flessibile e agile”, afferma Luz.

La maggiore disponibilità dell'infrastruttura consente di distribuire i servizi tra i due data center e di effettuare interventi obbligatori senza interrompere il servizio.

“Effettuiamo test periodici per garantire la conformità e la continuità dell'attività. Con Infoblox possiamo stare tranquilli quando eseguiamo questi test, sapendo che non ci sarà alcun impatto sulle operazioni di Sicredi”, afferma Luz.

In termini di sicurezza cibernetica, Sicredi ha adottato misure per prevenire gli attacchi malware e ransomware e ha implementato lo strumento di protezione denial-of-service (DoS) BloxOne Threat Defense. Il manager afferma che oggi è difficile immaginare Sicredi senza le soluzioni Infoblox: “All'interno di Sicredi, Infoblox è considerato parte di un servizio base. La perdita di DDI NIOS avrebbe un impatto in termini finanziari e di immagine. È uno strumento essenziale per il funzionamento dell'attività”, afferma Luz.

Nel prossimo futuro, Sicredi intende integrare il DNS cloud di Infoblox, acquisire una licenza di Threat Analytics ed espandere le funzionalità di sicurezza.



Infoblox unisce networking e sicurezza per offrire prestazioni e protezione senza pari. Scelti dalle aziende Fortune 100 e dagli innovatori emergenti, forniamo visibilità e controllo in tempo reale su chi e cosa si connette alla tua rete, in modo che la tua organizzazione funzioni più velocemente e blocchi le minacce prima che avvengano.

Sede centrale
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com