infoblox

CASE STUDY

# Sicredi Adopts NIOS DDI and BloxOne Threat Defense to continue its growth as a leader in Brazil’s Financial Sector

## OVERVIEW

**Sicredi is a cooperative financial institution established more than 120 years ago. Over the last two decades, the business has seen an internal reorganization and accelerated its expansion. To support this growth and lead innovation in the financial sector, Sicredi has invested in digital transformation.**

Credit cooperatives have the same portfolio of financial products and services as traditional financial institutions (current accounts, cards, investments), but are mainly distinguished by their management model. Unlike conventional institutions, in credit cooperatives the associates are the real owners of the business.

To successfully execute on this business model, Sicredi employs a management strategy that utilizes the participation of its more than seven million associates, who play the role of its business owners. With more than 2,500 branches, this cooperative financial institution is physically present in all Brazilian states and in the Federal District, providing a complete range of financial and non-financial solutions.

> “*Infoblox accelerated delivery of our products to associates and end users. Provisioning a machine previously took five days, on average. Today, we can do it in 15 minutes. It is more flexible and agile.”*
>
> **Juliano Luz,**
> **Infrastructure Analyst, Sicredi**

## THE SITUATION

### Geographic expansion and digitalization propel credit cooperative business

Sicredi has grown significantly in terms of its branches and base of associates, becoming one of the main actors in the Brazilian financial sector in recent years. It currently offers more than 300 financial products and services, from current accounts and cards to investments, insurance, consortia, card machines and 100% digital accounts, for individuals, legal entities and rural producers.

Sicredi

To accompany this progress, in 2017 Sicredi began a process of digital transformation, intending to gradually replace old systems for processing products and services—known as 'core banking'—with a more modern platform. This adoption of cutting-edge technology was crucial in offering a better experience to the associates and maintaining competitiveness in Brazil's dynamic financial market.

For many years, Sicredi functioned with a technological infrastructure and virtual machines on 'open source' DHCP and Linux tools. Infrastructure Analyst Juliano Luz, who joined Sicredi in 2008, remembers an obsolete environment: "There was a challenge in relation to lack of scalability and agility. The business needed a new application, a new environment," he says.

Because it worked with open source solutions, the old environment did not have any external support and all problems had to be resolved internally, demanding intense involvement from the IT department. Another concern of Sicredi was strengthening security against cyberattacks.

Sicredi had already implemented an Infoblox solution in 2013, but in 2021, it decided to refresh the technological environment. "The initial implementation of DDI was carried out by the internal team. NTT joined as a partner when we expanded and updated the Infoblox NIOS DDI," said Luz.

## THE CHALLENGE

### Obsolete technological infrastructure maintains slow manual processes

The growing number of Sicredi financial projects, services and products needed an environment with greater contingency and scalability. Out-of-date technology limited growth plans. "Our old system ended up being a bottleneck. It was slow to allocate IP and create records in an IP Address Manager in the DNS name," said Luz. "It was complicated to reserve the IP and register the name, generating lack of control of addressing and problems with infrastructure."

The infrastructure needed higher availability on DNS servers, for example, so they could replicate files on another machine in an automatic, non-manual way. The IT team also wanted to simplify and accelerate the process of activating projects to release the infrastructure and network teams from these types of tasks. "I would come to the networks team to get an IP and a name and then go to the final part to provide some rules. A virtual machine was created and installed on the operating system. It was very slow," said Luz.

The new solution also needed to guarantee protection for employees and associates due to the increasingly serious and frequent threat of cyberattacks and digital fraud. The regulatory environment was also becoming more stringent, with Brazil's Central Bank starting to demand more robust cybernetic security controls and systems in financial institutions.

*Customer:* *Sicredi Bank*
*Industry:* *Banking*
*Location:* *Brazil*

**INITIATIVES:**

- Establish an environment with greater contingency and scalability for the growing number of Sicredi's projects, financial services and products
- Replace outdated technology products, which were limiting growth plans
- Increase infrastructure availability, for example, in the DNS servers to be able to replicate the files to another machine automatically and not manually

**OUTCOMES:**

- Improved quality and agility to deliver resources to the business
- Accelerated the delivery of products to members and end users
- Improved provisioning times: one machine previously took an average of five days to provision; today it can be achieved in 15 minutes

**SOLUTIONS:**

- NIOS DDI
- BloxOne® Threat Defense

## THE SOLUTION

### Simplified DNS administration and greater security against cyberattacks

Sicredi started implementing Infoblox NIOS DDI, which powers the Infoblox basic network services, enabling continuous operation of the infrastructure. Implementation was done with the partner, NTT. First, Sicredi migrated the DNS base to the new Infoblox infrastructure. Over time it has expanded functionalities, internally and externally. Infoblox NIOS facilitated the integration and centralization of Sicredi's DNS, DHCP and IPAM (DDI) services on a single platform.

"Along with VMware, there was an integration with Infoblox, and all this was automated. Today we can go to a portal, order a machine, register the IP name and reserve the IP; an Operating System is installed and a VM is supplied, ready to use," described Andrius Lima, Infrastructure Analyst at Sicredi. Infoblox also enabled automations via APIs to help with access by applications from other teams. This functionality has been essential in Sicredi's pioneering actions in the 'Open Banking' and 'Open Finance' programs in Brazil.

Infoblox NIOS reinforced security, control and visibility. In 2021, Sicredi invested in BloxOne Threat Defense, Infoblox's hybrid security solution. This implementation enabled the organization to become more organized in terms of DNS, records and controls and benefit from improved security posture overall. This tool complements functionalities that the previous environment had, such as firewall and DDR.

"Infoblox enabled us to scale our DNS, DHCP infrastructure and organize our environment to handle the growth of the business," says Luz.

## THE RESULT

### Infoblox reduced operational costs and facilitated business for Sicredi

The transition to Infoblox solutions represented a huge gain for Sicredi in terms of its quality and agility in delivering resources to the business. The new infrastructure reduced operational costs because network administration tasks are now managed in a single interface, automating and decentralizing essential processes that previously had to be manually carried out in the data center. The cooperatives themselves can now administer their own resources with queue management.

"Infoblox accelerated delivery of our products to associates and end users. Provisioning a machine previously took five days, on average. Today, we can do it in 15 minutes. It is more flexible and agile," says Luz.

The higher availability of infrastructure allows services to be distributed between the two data centers and makes compulsory interventions without interrupting the service.

"We run periodic tests because of compliance and business continuity. With Infoblox we have the peace of mind when running these tests, knowing there won't be any impact on Sicredi's operations," says Luz.

In terms of cybernetic security, Sicredi adopted measures to prevent malware and ransomware attacks and implemented the BloxOne Threat Defense denial-of-service (DoS) protection tool. The manager says that today it is difficult to imagine Sicredi without the Infoblox solutions: "Within Sicredi, Infoblox is considered to be part of a base service. Losing the NIOS DDI would have an impact in financial and image terms. It's an essential tool for the functioning of the business," says Luz.

In the near future, Sicredi intends to integrate Infoblox cloud DNS, acquire a Threat Analytics license and expand security functionalities.

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

**Corporate Headquarters**
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230824v1