infoblox

活用事例

Sicredi は、ブラジルの金融部門のリーダーとして成長を続けるために、NIOS DDI と BloxOne Threat Defense を導入

概要

Sicredi は 120 年以上前に設立された協同組織金融機関です。過去 20 年にわたり、当金融機関は内部再編を経験し、拡大を加速してきました。この成長をサポートし、金融部門でのイノベーションをリードするために、Sicredi はデジタル変革に投資してきました。

信用協同組合は、従来の金融機関と同じ金融商品とサービスのポートフォリオ (当座預金、カード、投資) を取り揃えていますが、主にその管理モデルによって区別されます。従来の金融機関とは異なり、信用協同組合では組合員が実質的なビジネスオーナーです。

このビジネスモデルをうまく実行するために、Sicredi は、ビジネスオーナーの役割を果たす 700 万人を超える組合員の参加を活用する経営戦略を採用しています。2,500 を超える支店を持つこの協同組合金融機関は、ブラジルのすべての州と連邦管区に店舗を有し、あらゆる種類の金融および非金融サービスを提供しています。

状況

地理的拡大とデジタル化で信用協同組合事業を推進

Sicredi は支店と組合員の基盤の点で大幅に成長し、近年ブラジルの金融部門での主要企業の 1 つとなっています。現在、300 以上の金融商品やサービスを提供し、当座預金やカードから投資、保険、コンソーシアム、カード機、個人、法人、地方の生産者向けの 100% デジタル口座までに広がっています。

> *Infoblox* により当機関の商品が組合員とエンドユーザにより迅速に提供されるようになりました。
>
> より迅速に提供されるようになりました。以前はマシンのプロビジョニングに平均して *5* 日かかっていました。現在では、*15* 分で同じことを行うことができます。しかも以前より柔軟かつ迅速に行えます。」

Sicredi、
インフラストラクチャ・アナリスト、
Juliano Luz 氏

Sicredi

この進歩に伴い、Sicredi は 2017 年にデジタル変革のプロセスを開始し、「コアバンキング」として知られる商品やサービスを処理するための古いシステムをより最新のプラットフォームに徐々に置き換えることを目指しました。この最先端テクノロジーの導入は、組合員により良い体験を提供し、ブラジルの活発な金融市場で競争力を維持する上で極めて重要でした。

長年にわたり、Sicredi は、「オープンソース」DHCP と Linux ツール上の技術インフラストラクチャと仮想マシンを使用して動作していました。2008 年に Sicredi に入社したインフラストラクチャアナリストの Juliano Luz 氏は、時代遅れの環境を次のように回想しています。「拡張性と迅速性が不足していることに関連した問題があり、ビジネスには新しいアプリケーション、新しい環境が必要でした。」

古い環境はオープンソースソリューションで動作していたため、外部からのサポートがなく、すべての問題を内部で解決する必要があり、IT 部門からの集中的な関与を必要としていました。Sicredi 氏のもう 1 つの懸念は、サイバー攻撃に対するセキュリティを強化することでした。

Sicredi はすでに 2013 年に Infoblox ソリューションを導入していました。そして、2021 年に技術環境を刷新することを決定しました。「DDI の最初の実装は社内チームによって行われました。Infoblox NIOS DDI を拡張・更新したときに、NTT がパートナーとして加わりました」と Luz 氏は述べています。

課題

陳腐化した技術インフラのため、時間のかかる手作業によるメインテナンス

Sicredi の金融プロジェクト、サービス、商品の数は増加の一途で、より高いリスク管理と拡張性を備えた環境が必要でした。時代遅れの技術により成長計画が制限を受けていました。「私たちの古いシステムは最終的にボトルネックになってしまいました。IP を割り当てて IP アドレスマネージャーに DNS 名でレコードを作成するのに時間がかかりました」と Luz 氏は言います。「IP の予約と名前の登録が複雑で、アドレス指定の制御不足やインフラストラクチャの問題を作り出していました。」

インフラストラクチャでは、たとえば、別のマシンにファイルを手動ではなく、自動的に複製できるように、DNS サーバーでより高い可用性が必要でした。また IT チームは、プロジェクトを有効化するプロセスを簡素化して加速化させ、インフラストラクチャチームとネットワークチームをこの種のタスクから解放したいと考えていました。「私はネットワークチームに行き IP と名前を取得し、それから最後の部分に進み、いくつかのルールを提供します。仮想マシンが作成され、オペレーティングシステムにインストールされました。とても時間がかかりました」と Luz 氏は語っていました。

新しいソリューションは、サイバー攻撃やデジタル詐欺の脅威がますます深刻かつ頻繁になっているため、従業員と組合員の保護を保証する必要もありました。規制環境もさらに厳しくなり、ブラジル中央銀行は金融機関に対し、より堅牢な自動制御方式のセキュリティ管理とシステムを要求し始めました。

お客様： *Sicredi* 銀行
業種： 銀行業
場所： ブラジル

取り組み：

- 増え続ける Sicredi のプロジェクト、金融サービスと商品に対して、より高いリスク管理と拡張性を備えた環境を確立する
- 成長計画を制限していた旧式の技術製品を置き換える
- DNS サーバー内で、ファイルを手動ではなく自動的に別のマシンに複製できるようにするなど、インフラストラクチャの可用性を向上する

結果：

- リソースをビジネスに提供するための品質と俊敏性の向上
- 組合員とエンドユーザーへの商品提供の迅速化
- プロビジョニング時間の改善：以前は 1 台のマシンのプロビジョニングに平均 5 日かかっていたが、現在では 15 分で達成

解決策：

- NIOS DDI
- BloxOne® Threat Defense

解決策

DNS 管理の簡素化とサイバー攻撃に対するセキュリティ強化

Sicredi は、Infoblox の基本ネットワークサービスを強化する Infoblox NIOS DDI の実装を開始し、インフラストラクチャの継続的な運用を可能にしました。実装はパートナーの NTT と共同で行いました。まず、Sicredi は DNS ベースを新しい Infoblox インフラストラクチャに移行しました。時間の経過とともに、内部的にも外部的にも機能が拡張されました。Infoblox NIOS により、Sicredi の DNS、DHCP、IPAM (DDI) サービスの単一プラットフォームへの統合と一元化が促進されました。

「VMware に加えて、Infoblox との統合があり、これらすべてが自動化されました。現在では、ポータルにアクセスしてマシンを注文し、IP 名を登録して IP を予約できます。オペレーティングシステムがインストールされ、VM が提供され、すぐに使用できるようになります」と Sicredi のインフラストラクチャアナリストの Andrius Lima 氏は説明します。Infoblox で、他のチームのアプリケーションによるアクセスを支援する API を介した自動化も可能になりました。この機能には、ブラジルの「オープンバンキング」および「オープンファイナンス」プログラムにおける Sicredi の先駆的な行動を示すために不可欠でした。

Infoblox NIOS により、セキュリティ、制御、可視性が強化されました。2021 年、Sicredi は Infoblox のハイブリッドセキュリティソリューションである BloxOne Threat Defense を採用しました。この実装により、DNS、記録、制御の点でより組織化され、全体的なセキュリティ体制の向上による恩恵を受けることができました。このツールは、ファイアウォールや DDR など、以前の環境に備わっていた機能を補足しています。

「Infoblox のおかげで、DNS、DHCP インフラストラクチャを拡張し、ビジネスの成長に対応できる環境を体系化できました」と Luz 氏は言います。

結果

Infoblox で運用コストを削減し、Sicredi のビジネスをさらに推進

Infoblox ソリューションへの移行は、ビジネスにリソースを提供する際の品質と迅速性の点で、Sicredi にとって大きな利益をもたらしました。新しいインフラストラクチャにより、ネットワーク管理タスクが単一のインターフェースで管理され、以前はデータセンターで手動で実行する必要があった重要なプロセスが自動化され分散されたため、運用コストが削減しました。協同組合自体がキュー管理を使用して独自のリソースを管理できるようになりました。

「Infoblox により、商品を組合員やエンドユーザーに迅速に提供できるようになりました。以前はマシンのプロビジョニングに平均して 5 日かかっていました。現在では、15 分で同じことを行うことができます。より柔軟で迅速性に優れています」と Luz 氏は言います。

インフラストラクチャの可用性が高いため、2 つのデータセンター間でサービスを分散でき、サービスを中断することなく強制介入できます。

「コンプライアンスと事業継続のため、定期的にテストを実施しています。Infoblox のおかげで、Sicredi の業務に影響がないことがわかっているので、安心してこれらのテストを実行できます」と Luz 氏は言います。

サイバネティックセキュリティの観点から、Sicredi はマルウェアやランサムウェア攻撃を防止する対策を採用し、BloxOne Threat Defense サービス拒否 (DoS) 保護ツールを実装しました。マネージャーは、今日では Infoblox ソリューションなしの Sicredi を想像するのは難しいと述べています。

「Sicredi 内では、Infoblox は基本サービスの一部と見なされています。NIOS DDI が失われると、財務面とイメージ面で影響が出ます。これはビジネスを機能させるために不可欠なツールです」と Luz 氏は言います。

Sicredi は近い将来、Infoblox クラウド DNS を統合し、Threat Analytics ライセンスを取得し、セキュリティ機能を拡張する予定です。

Infoblox 株式会社
〒 107-0062 東京都港区南青山 2-26-37
VORT 外苑前 I 3F

03-5772-7211
www.infoblox.com

バージョン : 20230824v1