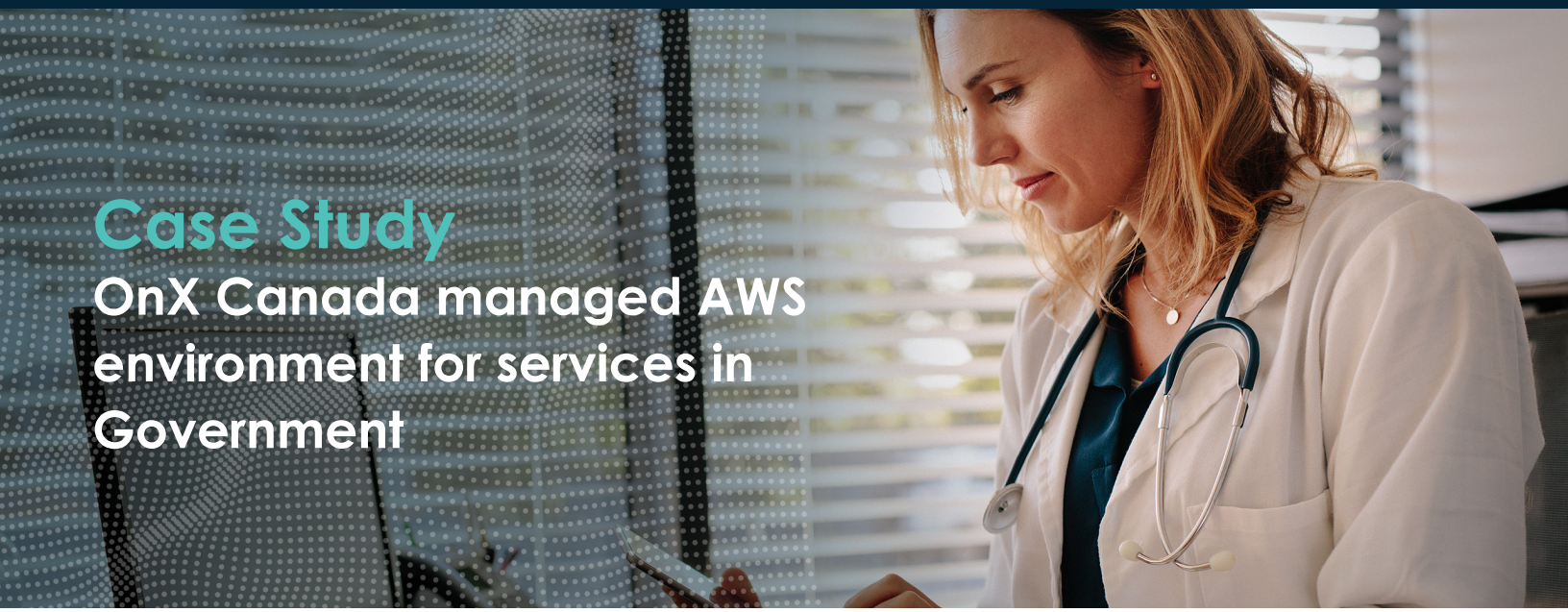

Case Study

OnX Canada managed AWS environment for services in Government

Client

A healthcare information systems company

The client develops and supports mission-critical healthcare information systems in the Mental Health, Long Term Care, Community and Social Service, and Hospital sectors for over 200 clients in North America. The client solutions include Blockchain, Mobile, and Web-Based Assessment and Electronic Health Record solutions. The client is headquartered in Toronto, Canada where they provide services to the region.

Challenge	OnX Canada solution	Results
• New contract with Government of Nova Scotia focused on Healthcare • Looking to consume IT in a cloud model for elasticity, cost-effectiveness, and high availability • They need 24/7 support and wanted a managed outcome • Locked down for Canada users only • Wanted AWS to address security concerns • GNS approved AWS	• Required their AWS environment to be configured exactly as they have it on-premises • Use web application firewall to block any non-Canadian traffic • Intrusion Prevention from Fortigate • Client VPN • EC2 instances – all data resides in Canada • Well architected review on entire workflow	• We provided best practice recommendations for cloud, powered by AWS • Phase 1 is live of a multi-phase approach • Looking at containerization and automation • Full Disaster Recovery, secondary site • Entire environment is in terraform and we can relaunch in minutes (Infrastructure as Code)

Challenge

The client was contracted by the Canadian province of Nova Scotia to host and manage a healthcare solution for those in NS. The client wanted a solution that could be quickly relaunched and deployed in the case of a disaster. Because of Nova Scotia's government regulations, this solution had to have 100% of its data stored within Canada to support personnel being Canadian Citizens. In addition, there were more stringent security concerns, and the solution would be required to deploy a Web Application Firewall, Intrusion Prevention System, strict firewall rules, and only accessible via a client VPN.

The client had an AWS priority for this environment as it is an approved platform for the government. AWS supports the Canadian region with two availability zones that, in the event of a disaster, the application can be recovered in the secondary location with minimal impact. AWS would eliminate the need to maintain and host a local data center, instead, the client would be able to take advantage of the OnX managed cloud computing model of resource use.

OnX Canada solution

The client required that the AWS environment be configured similarly to their on-premises environment. Reserved EC2 instances were used to provide the same architecture and a cheaper cost compared to on-demand resources. All web requests going into the environment first pass through a Fortigate appliance and AWS Web Application Firewall / Application Load Balancer before reaching the production or test web server.

OnX provided a number of security features to the client solution's environment:

- **AWS WAF.** A Web Application Firewall was set up for both production and test environments. This WAF is configured to use Fortinet's managed ruleset to protect against the complete OWASP top 10 web application threats. In addition, the WAF was configured to only allow access for those users not in the Canada geographic region.
- **IPS.** A Fortigate cloud appliance was deployed in the client's AWS environment for all incoming traffic to pass through and provide an Intrusion Protection System.
- **AWS Canada Region.** All data and services are hosted in AWS's ca-central-1 region, ensuring data remains in Canada at all times.
- **Client VPN.** All-access to the environment by the client is done through Forticlient VPN, which connects to Fortigate and allows only certain AD users to connect.
- Trend Micro AV. OnX managed Trend Micro Antivirus provides protection for the client servers.

The client AWS environment is regularly backed up via snapshots of the EC2 instances' EBS volumes. These snapshots will be used in order to re-stand up the environment in the case of disaster. This process was automated through Terraform, only requiring a small number of changes to re-launch the environment. In the same manner, it was provisioned in the failing availability zone.

Results

The client's AWS efficient public cloud environment is currently live and functional in AWS while following best practices. Phase 1 of the infrastructure has been wholly deployed, while more phases, which provide such things as load-balanced web servers, will be built out in time. A Well-Architected Review was conducted on the client AWS environment providing important key items to evaluate and improve on by OnX and the client.

A disaster recovery test is prepared and ready for deployment - additional public IP addresses and a Terraform codebase is ready for a parallel deployment in AWS to ensure, in the event of a disaster, a smooth and quick recovery will be made.

By working with OnX, the client can meet the needs of an important government agency, mirror their current application and infrastructure environment, and rest assured that the environment is built on the highest of industry standards.