Agility CMS:
A Foundation for Better Online Security

Joel Varty – Updated March 2021

Why Online Security

From a corporate point of view, security is the number one consideration regarding the procurement of software and services. We share that point of view when it comes to the security and stability of Agility CMS.

Gone are the days when software could be expected to exist solely behind firewalls or locked inside a limited intranet. The world has become powered by systems that interoperate with each other using strict and secure protocols. Agility CMS lives in that world.

In Search of the Monolithic Dinosaur

40% of the internet runs on WordPress, a system with many known (and emerging) vulnerabilities and attack vectors. The central problem with WordPress, and other systems like it, isn't just its popularity but with how it interoperates with user systems. Namely, using plugins.

> These plugins add to the monolithic codebase that powers a traditional website, making it much more vulnerable.

Modern Techniques for a Secure Digital World

Agility CMS is built using a fundamentally different paradigm.

- Agility follows a modern approach to interoperability with external systems. Where traditional CMS platforms seek to bring integration inside a website's codebase, **Agility maintains a distinct separation content and your code**. This provides developers with the ability not only to reuse content in more places, but more flexibility on how that content is presented.
- Agility stores and delivers a website's content independently from that website's codebase. **A website based on Agility CMS cannot be used as an attack vector**. One example of this is Static Site Generation with tools like Next.js and Gatsby: the website is generated on a build server and static HTML files are served with pre-rendered content.

Authentication with Auth0

Agility CMS utilizes Auth0 for all authentication operations. Auth0 provides the highest level of security for all login operations, including Multi-Factor Authentication, Enterprise Single Sign-On, and Social Logins.

> You control how your organization's user identities are authenticated, even so far as utilizing your existing central login page.

Backed by Microsoft Azure

Agility's infrastructure utilizes Microsoft Azure, bringing with it enterprise grade security benefits.

- All data is encrypted in transmission and at rest
- Each customer instance is segregated into its own container, allowing incremental backup, point-in-time restore, and separation from other instances.
- API access keys are customer-maintained, allowing fine-tuned control over where and how your content can be accessed, and for how long.

Case Study: Secure Solution for a Leading International Bank

The Customer

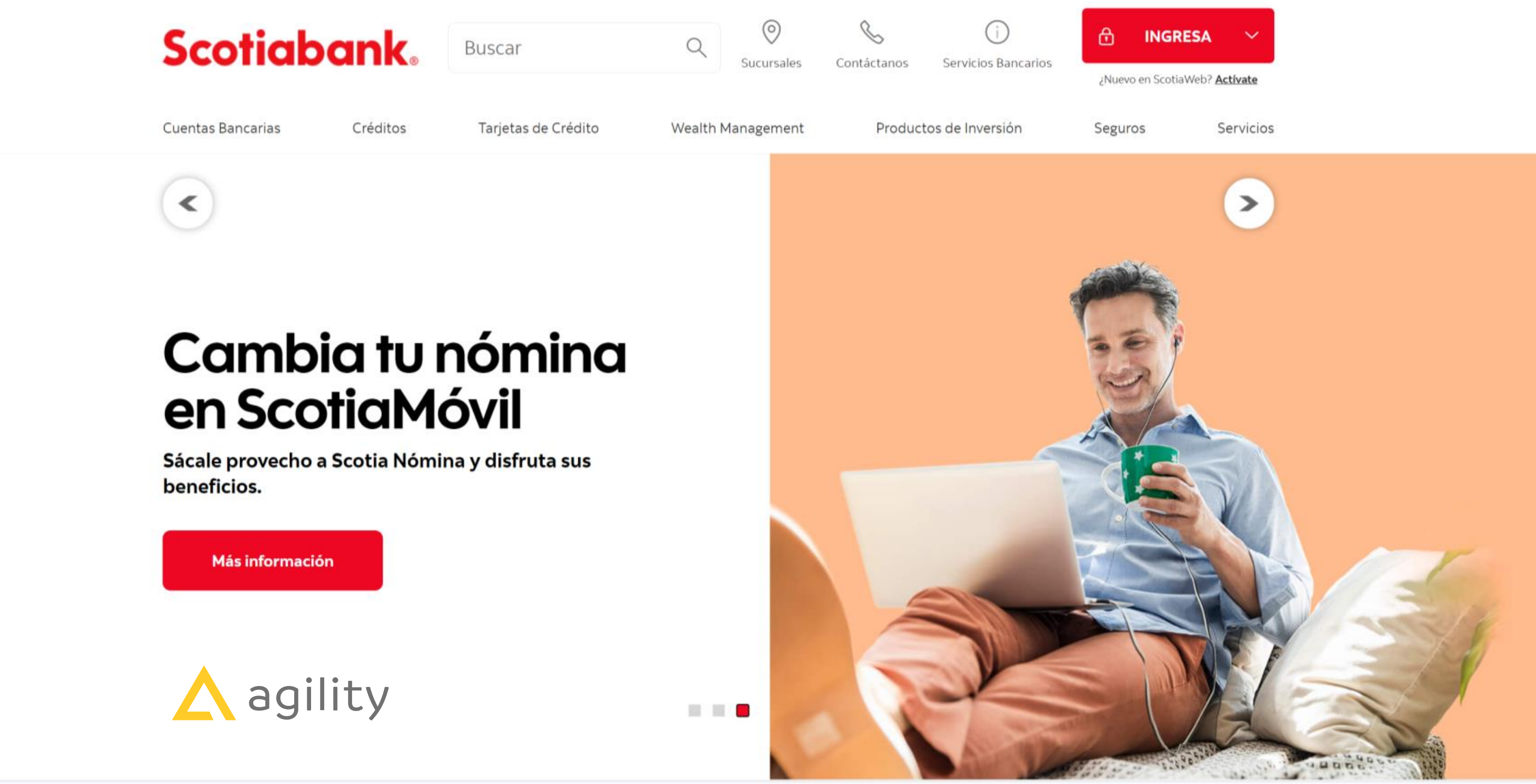
The Bank of Nova Scotia, operating as Scotiabank, is a Canadian multinational banking and financial services company headquartered in Toronto, Ontario. One of Canada's Big Five banks, it is **the third largest Canadian bank** by deposits and market capitalization.

The Goal

Scotiabank came to Agility when they needed to **quickly and security launch several websites** for new regions that they expanded into. These regions included several countries such as Mexico and others in South America.

The Challenge

Scotiabank's new regions each had unique language requirements, product offerings, and local needs. **Each region needed to be onboarded securely and separately from a central content hub** that could be managed separately by each region and administered at a high level from the digital headquarters in Canada. Also, each country needed to follow the design guidelines put forth by Scotiabank HQ.



Cambia tu nómina en ScotiaMóvil

Sácale provecho a Scotia Nómina y disfruta sus beneficios.

The Solution

Part 1: Digital Property Creation

Separate content instances were created in Agility CMS for each representative country. This allows each country to use their own content teams to **manage the content that's specific and important to them**. This was especially important because of the regionality of the languages in Latin America.

Part 2: Authentication

All users of the Scotiabank CMS instances need to be **authenticated securely** to Agility using their existing corporate logins. This authentication process should carry forward any rules and branding that are already in use at Scotiabank.

The Outcome

Each of the six countries in Scotiabank's Latin America portfolio are able to independently manage the content on their websites. Further, they are able to authenticate to Agility CMS using their Scotiabank corporate credentials via their existing Azure Active Directory login page.

Scotiabank's security team has performed independent audits of the Agility CMS platform, which Agility has passed with flying colours each year. Scotiabank has successfully rebranded and rebuilt the website front-ends for each country over the many years that they've been on the Agility CMS platform. The development teams have re-used the existing content from Agility to save time and resources on each rebuild and design refresh.

> *Agility CMS allows Scotiabank to maintain consistent content infrastructure and high security performance across numerous international locations and lines of business.*

Case Study: Content Solution for Cybersecurity Leader

ActZero

The Customer

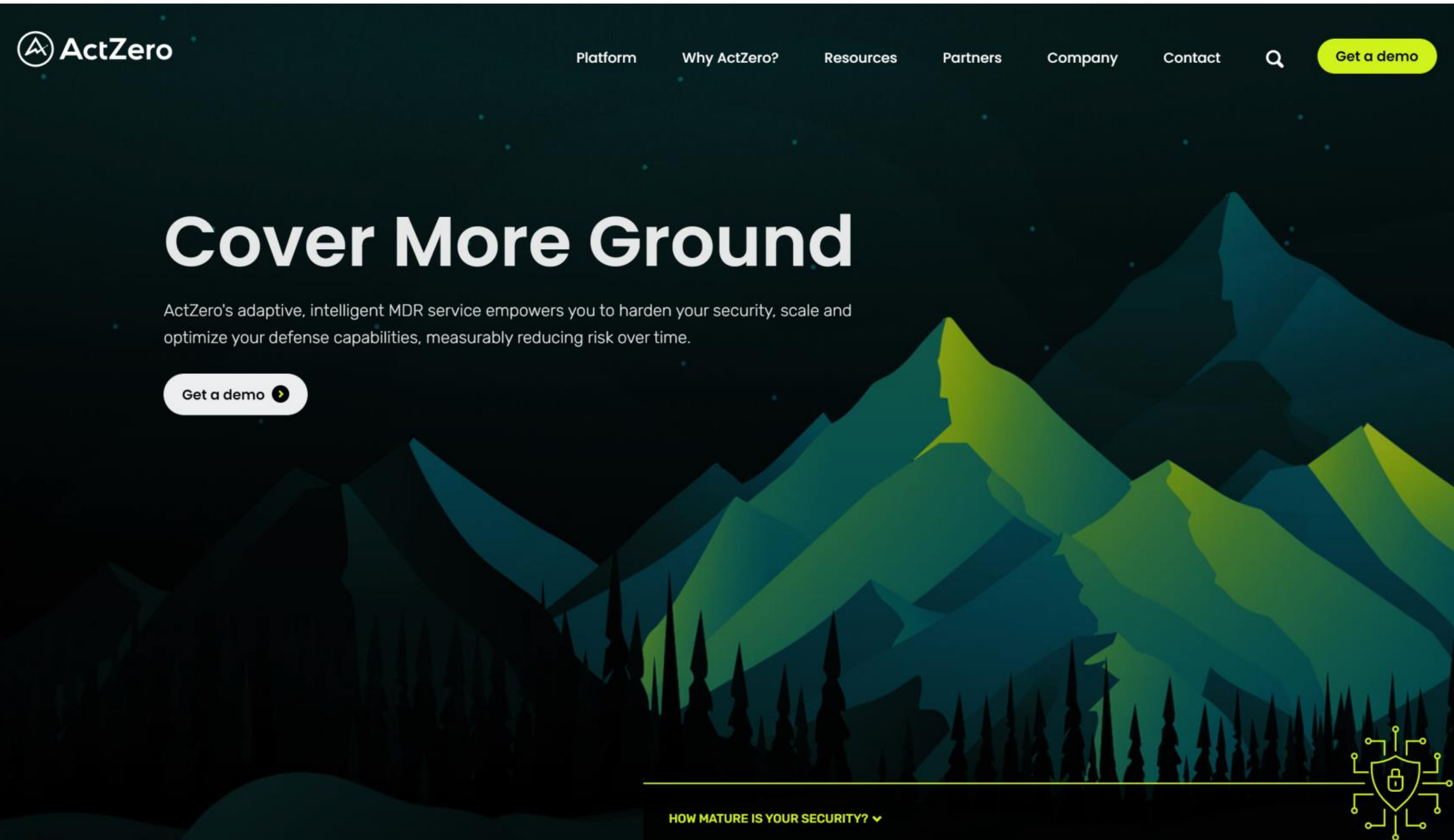
ActZero's platform monitors, detects, and thwarts attacks in real-time, getting smarter every second. Their cybersecurity experts validate detected threats, advise customers of threats, remediate the threat where possible, recommend corrective action while feeding threat intelligence back to their machine learning models for continuous improvement.

The Goal

ActZero needed **the most secure website possible**, while still allowing their editorial staff the freedom to create inspiring and compelling content in real-time. Previously their website had been hosted on a traditional CMS with known vulnerabilities.

The Challenge

ActZero's reputation and compliance posture requires them to have top-notch security at every level of their business, including their website. Most CMS controlled websites have attack vectors that are exposed by allowing real-time publishing and editing.



Cover More Ground

ActZero's adaptive, intelligent MDR service empowers you to harden your security, scale and optimize your defense capabilities, measurably reducing risk over time.

The Solution

Part 1: Authentication

Agility's Enterprise package provides authentication via Single-Sign-On (SSO). ActZero's authentication system is through OneLogin, which supports the SSO configuration provided by Agility CMS.

Part 2: Real-time Edits

Agility CMS supports an approach known as *static site rendering*. This provides a separation between the website and the content editing layer, allowing the site to have very few attack vectors. The ActZero website implementation using Agility's content APIs follows this development pattern.

The Outcome

The ActZero content editors and marketing team are able to utilize their OneLogin sign-on screen to authenticate within Agility CMS. The corporate login rules configured by their IT team carry through to the CMS automatically.

The website itself was implemented using Gatsby, a static site generator. The site is hosted with no web server vulnerabilities such as those that are found in traditional CMS platforms. The ActZero content team has complete, real-time control of the content on the website, and can still manage pages and content throughout the site.

The site is hosted with no web server vulnerabilities while content team has complete, real-time control of the content on the website using Agility CMS's Page Management.