Island

The Bank of Marion Success Story

Improving Visibility

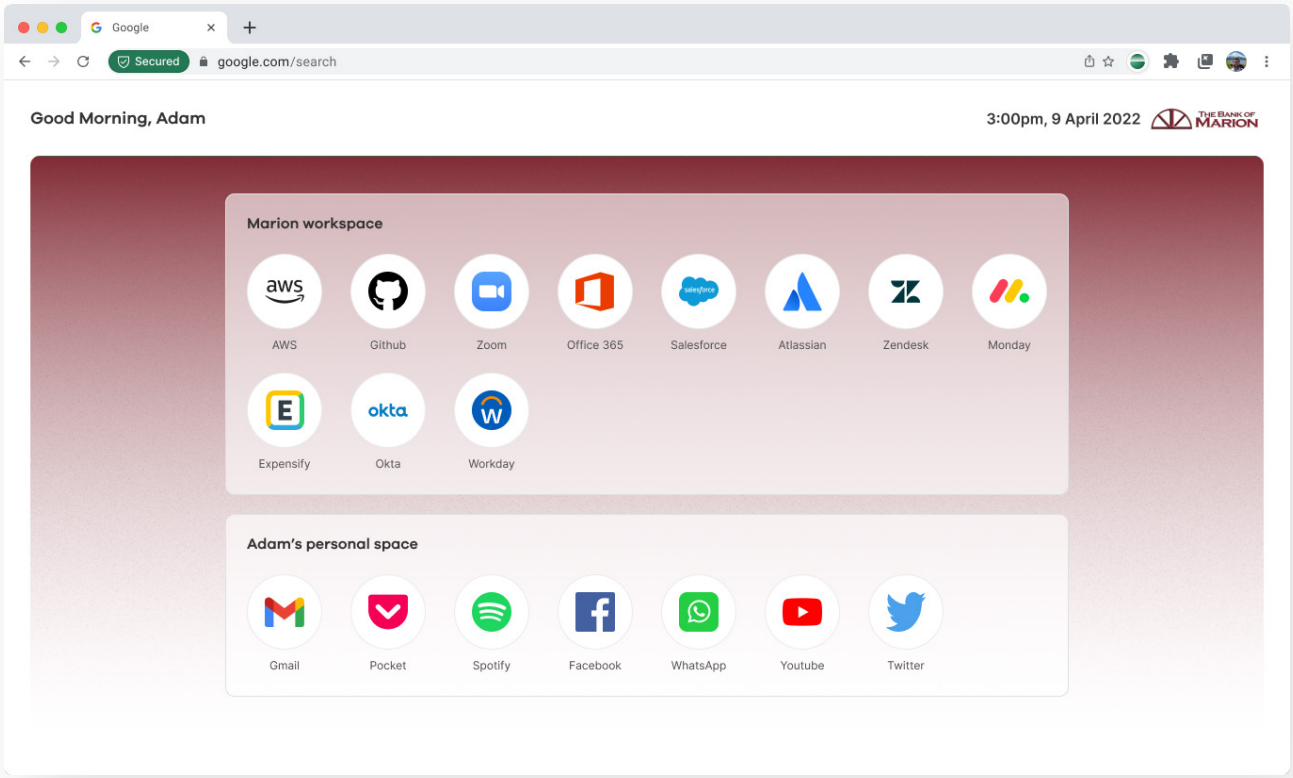
Founded in 1874, The Bank of Marion is a regional bank based in southwest Virginia with over a dozen branches across Virginia and Tennessee. Their philosophy is to provide the personal service that is all too often lost in modern banking, while delivering a secure, convenient, and efficient experience powered by technology. Unlike many other banks that rely on third-party service providers, The Bank of Marion's technology teams are employees of the bank. They invest in the people, processes, and technologies necessary to maintain their stellar reputation. After nearly 150 years in business, it's safe to say that their approach is working.

All banks are frequent targets of cyber attacks, and The Bank of Marion is no exception. In today's banking environment, far more money is exchanged digitally than through cash, so threat actors are constantly searching for vulnerabilities to exploit. Malware, phishing, and social engineering are routine, requiring defense-in-depth and a perspective of assumed attack. The days of a single secure network perimeter are long gone.

The InfoSec team implemented a number of security tools to protect their information and assets, including:

- **Remote Browser Isolation (RBI)** to protect against malware
- **Web Proxy** to filter harmful or untrusted domains
- **Email Attachment Sandboxing** to defuse potentially dangerous payloads
- **Data Loss Prevention (DLP)** to safeguard sensitive customer data

Individually, each of these tools fill an important role in helping protect the bank. But in practice, when responding to real-world attacks, a gap emerged. Because each tool captured its own slice of event logging, it could take hours of hands-on expertise to put these pieces together into a contextual understanding of a security incident. During any security incident response, every minute counts. Yet, reassembling the full event from these disparate systems could take days.



Flipping the model

Tim Ringley is the Vice President & Information Security Officer and has been at the bank since 2010. He's seen every security vendor pitch how their new solution is better, faster, smarter, and cheaper than the rest. When he learned about The Island Enterprise Browser at a financial services security conference, he finally saw something new: instead of adding yet another security tool to a growing network stack, Island flipped the model and put the control plane within the browser. This approach offers the same security protections as the collection of tools mentioned above, but with a new paradigm of high fidelity visibility into all the activity within the browser. From the Island management console, Tim and his staff get a detailed view of all users, devices, and activities – in context.

The Moment of Truth: Defeating a Spear Phishing Attack

Within weeks of rolling out The Enterprise Browser to bank employees, Tim and the security team faced a real-world attack when a bank employee was targeted with a spear phishing attempt.

A local business (and The Bank of Marion customer) was attacked by a threat actor who successfully compromised their email server. The threat actor went on to craft a targeted phishing attack against a bank employee who regularly emailed with this customer. This was a near perfect phishing setup: the threat actor could use examples of previous email correspondence to craft a believable message and send it from the actual server of a trusted customer. In fact, the first phase of the phishing attack succeeded: On the receiving end, the bank employee opened the email and clicked the malicious link.

At that moment, The Enterprise Browser warned the user that they were visiting a suspicious website and blocked them from inputting their credentials. The employee immediately stopped, closed the page, and reported the incident. The incident response team pulled up the timeline logs from the Island management console and verified that no credentials were compromised and the phishing attack was thwarted. An investigation that might previously take days was completed in minutes. The Enterprise Browser successfully stopped the spear phishing attack and gave critical visibility to both the end-user and the incident response team.

Looking Ahead

For Tim and the InfoSec team, the decision to implement The Enterprise Browser was easy to make. They simplified their tech stack, improved their security posture, and dramatically improved visibility for all web activity. But the story doesn't stop here.

The relationship between The Bank of Marion and Island is still early days, and there's more value to discover in the future. Already, the team was pleasantly surprised at how quickly their requests for new features turned into working software. Instead of submitting requests through an impersonal web form, Tim and his team can open Slack and instantly connect with their Island support team. Personal connections and customer focus are values that both organizations share.

With their intentional investments in people, process, and technology, The Bank of Marion is well positioned to build on their success and deliver the quality hometown banking service that their customers expect.