CASE STUDY

Artificial intelligence company replaces legacy VPN with ZTNA in 10 Minutes

BlastWave
www.blastwave.io

THE PROBLEM
A VPN Alternative Needed in Retail Fuel Pricing

PriceCast Fuel (PCF) is the world's first industry-specific retail fuel pricing, management and optimization solution developed by A2i. By combining state-of-the art artificial intelligence and machine learning with big data, PCF brings dynamic, predictive consumer-behavior-based pricing to the retail fuel industry.

During the pandemic, A2i was growing and adding staff, making their existing VPN untenable in terms of performance and dropped connections. In one case, an employee was unable to work at all due to the limitations of a "centralized" architecture. The performance was just too slow to get their basic job done. Furthermore, A2i realized that the security vulnerabilities and exploit opportunities mandated finding a VPN alternative.

A2i already had a hardware VPN solution, but it was generic and built for small business, so it scaled poorly. With a large number of people working from home and using a lot of bandwidth, it became unacceptably unstable, a huge security risk, and therefore unusable.

A2i

"The security of our data and our customers' data is our highest priority and we needed a secure platform to provide access to our hybrid data services, hosted both in the cloud and on-premise. BlastShield filled both these needs for us with their patented solution."

- Emil Erlandsson,
Vice President of Professional Services at A2i

THE CHALLENGE
In search of a viable ZTNA VPN alternative

In exploring options, A2i looked at several different VPN alternatives. One was to add more hardware to add VPN concentrator capacity, but this was just kicking the can down the road. Another option was to use some of the more modern VPN alternatives that funnel all traffic requests through a proxy server and then fan out to connect to those services (proxy-fan architecture). Although these approaches have grown in popularity, they still suffer from a bottleneck (the proxy server) and don't allow east-west traffic between nodes downstream of the bottleneck. They were also concerned about phishing, social engineering, and other credential attacks, and really wanted to find something easy to use that eliminated usernames and passwords.

The security of A2i's data and their customers' data is their highest priority and A2i wanted a more modern ZTNA solution that:

- **Creates a secure platform to provide access to their hybrid data services, hosted both in the cloud and on-premise;**
- **Allows for higher flexibility in terms of people working from the office and remotely, while preserving optimal security;**
- **Is very secure, with multi-factor authentication, including biometric logins and other state of the art features; and**
- **Is easy to use, fast, reliable, and easy to roll out within the organization.**

A2i needed a reliable ZTNA solution that could stop:

1. Account takeover
2. Lateral movement
3. Remote access compromise

THE SOLUTION
Zero Trust Network Access in 10 minutes

BlastWave's BlastShield™ rapidly filled these needs for A2i with its patented ZTNA solution, which made it the obvious VPN alternative. **A2i was pleased with BlastShield's secure, flexible, and blazing-fast performance.**

Most surprisingly to A2i, they fell in love with BlastShield's ease of use. A2i signed up for the initial trial and built a rudimentary network crossing two continents with two users in just 10 minutes. It was very easy to roll out to the rest of the organization. A2i experienced little resistance from staff due to the elimination of usernames and passwords, allowing them to enjoy both convenience and heightened security. Employees no longer had to come up with new passwords every 90 days or keep track of their credentials. They also didn't need tedious training on how to avoid phishing campaigns, since there was nothing to be phished. This ease of use saved time and money that would have been spent on installing and configuring other expensive VPN solutions or remote access alternatives (such as RDP or remote access/remote control apps) that provide little protection and in some cases introduce new vulnerabilities.

With BlastShield's microsegmentation, A2i also recognizes the advantage of bringing their end users - their customers - under the same security solution. As a provider, they know their industry continuously encounters things like site-to-site VPNs or IP white listing, etc. And, the increased prominence of supply chain attacks made them realize they could protect their customers and suppliers by creating a fine-grained ecosystem of control that would not allow malware to move through the supply chain unchecked. A2i saw that BlastShield™ could add a robust level of security coupled with secure remote access without being a burden for their customers to use.

Aside from the ease of use and security benefits offered by BlastShield™ A2i had also made themselves less likely to be the victim of a breach resulting in among other things, ransomware. **A2i could reduce the likelihood of a ransomware attack, saving them thousands, as the average ransom payment has increased from $115k to $570k in the last 3 years.** BlastShield™ continuously saves users money by protecting them from ransomware attacks and the other costs associated to a breach. **Prevention is MUCH cheaper than detection and remediation.**

BlastShield™ helps prevent and isolate attacks, mitigating the spread of malware by reducing the “blast radius” of a breach. BlastShield™ also enables cloud-native app development by securing microservices, containers and Kubernetes clusters.

BlastShield™ is the first all-in-one SDP patented solution that combines infrastructure cloaking and passwordless multi-factor authentication (MFA) for identity-based secure remote network access for organizations that have adopted a zero-trust security model. BlastShield™ enables organizations to hide on-premise and cloud workloads from outsiders and insider threats, concealing an organization's infrastructure from cyberattacks through software-defined microsegmentation without modifications to existing network fabric and hardware.