ALERT LOGIC™

CASE STUDY

The Sky is the Limit

Maintaining Consistent and Scalable AWS Cloud Security

BC in the Cloud provides private and public-sector organizations with a complete, turnkey cloud computing solution for business continuity and disaster recovery. Developed by an experienced team of certified cloud computing industry experts, the BC in the Cloud platform is designed to be used immediately out of the box, while delivering the scalability customers need to make changes as business grows. Easy to customize, the platform supports a powerful suite of full-featured cloud computing applications to simplify all business continuity and disaster recovery activities — from risk and incident planning to testing to governance and compliance to vendor management.

A rapidly growing business with clients ranging in size from 300 to over 1 million employees, BC in the Cloud is focused on delivering a strong yet flexible platform that can adapt to the needs of its dynamic, world-wide client base.

The Challenge

BC in the Cloud has always been a cloud first, cloud only business — an approach designed to give the company the horizontal and vertical scalability needed to serve a geographically diverse client base. Frank Shultz, BC in the Cloud Managing Director explains, "We chose a cloud-based environment so we could

BC in the Cloud

ABOUT

Customer: BC in the Cloud
Industry: IT Services
Location: PENNSYLVANIA, US

SOLUTIONS

ALERT LOGIC® PROFESSIONAL

An integrated suite of intrusion detection, vulnerability scanning and log management for the cloud, on-premises, hosted, and hybrid infrastructures.

serve our customers no matter where they were located around the globe."

To support this level of agility, BC in the Cloud hosts its critical infrastructure on Amazon Web Services (AWS). In addition to providing significant cost savings when compared to an in-house data center, using AWS enables BC in the Cloud to focus on its core business. Notes Patrick Escudero, BC in the Cloud Director of Technology, "Working with Alert Logic allows me to focus on making sure that everything is working great for our customers, rather than spending time worrying about the underlying hardware infrastructure."

Using the cloud to deliver business-critical disaster planning and recovery services did present BC in the Cloud with some challenges; however, mostly related to clients' concerns about cloud security. "When we started marketing our product three-and-a-half years ago, the cloud was still a scary word to enterprise companies. They didn't understand it," notes Shultz. About two years ago, Shultz began to sense a shift in customers' attitudes as they began moving some of their own workloads into AWS. He found that approaching new customers became easier as they grew more familiar with the cloud.

But even as customers grew more confident in the security of cloud-based solutions, BC in the Cloud's rapid growth and rate of worldwide expansion presented a new set of IT security challenges. Explains Escudero, "You start out as a young company with just a few customers, but as you keep growing and growing the cybersecurity threats become greater. I would be up at night wondering, 'are we really doing enough?'"

"The philosophy in our industry used to be that businesses would want to keep their data internal," Shultz adds. He goes on to point out the flaws in that approach, explaining that an organization's own data center is the least secure place for recovery plans and other critical recovery data when the network goes down. In that respect, BC in the Cloud's ability to host data remotely provides a major advantage. When their customer's systems are down, BC in the Cloud can still facilitate a successful response and recovery.

The high value of these advantages motivated Shultz and his team to place an even greater focus on cybersecurity. He explains, "We need to make sure we are available when our customers need us. With the rise of global malware and rapidly spreading ransomware, we need to ensure our systems aren't impacted by these events. Our customers rely on us to help them recover. We must make sure our systems are secure and operational." BC in the Cloud realized that to meet this commitment, it needed a security infrastructure capable of countering evolving cyber threats and providing 24/7/365 monitoring; while scaling effectively to support continuous, rapid expansion.

Why Alert Logic?

When searching for a cloud security solution, BC in the Cloud focused on how well various products integrated with AWS. At the time, the company was using Qualys for manual scans, but Qualys wasn't authorized for scanning ahead of time from AWS. This forced Escudero and his team to notify Amazon if schedules changed or risk having the company's servers shut down by AWS intrusion detection. Shultz, "The fact that Alert Logic is recognized by AWS as valid traffic eliminates that problem."

Alert Logic's tight integration with AWS is what ultimately drove the decision. Shultz states, "Alert Logic knew the

challenges and benefits built into AWS. I had never seen a company that had actually tied its solution directly into AWS. It seemed like Alert Logic would make for a great partner."

Alert Logic's advanced security features were also important. Shultz explains, "AWS was coming out with additional security features including a web application firewall, but we didn't want to put all of our eggs in the Amazon basket. We felt it improved our security posture to have a third party outside of AWS providing our security and vulnerability scanning."

Shortly after deployment, Alert Logic's tight integration with AWS began to pay dividends. The information provided by Alert Logic allowed Escudero to take effective actions before cyber threats were detected. He notes, "The ability to be proactive in this way helped to improve our security stance."

Escudero has also been impressed with Alert Logic's Security Operations Center team. He points out in particular an experience receiving a critical alert warning from Cloud Defender while on vacation. He reflects, "The fix was to whitelist the IP addresses for the application servers. But because I was dealing with this while I on vacation, the Alert Logic Security Operations Center team wrote down all the IP addresses and did the whitelisting for me."

As a fast-growing company, BC in the Cloud faces resource challenges every day. Escudero notes, "Alert Logic has functioned like an extra IT person that is always there, looking at the log and monitoring traffic. Not having to dedicate resourcs to those functions has really helped our business. Our 24/7 resource is Alert Logic's

> *"We need to make sure we are available when our customers need us. With the rise of global malware and rapidly spreading ransomware, we need to ensure our systems aren't impacted by these events. Our customers rely on us to help them recover. We must make sure our systems are secure and operational."*
>
> **FRANK SHULTZ,**
> **BC IN THE CLOUD**