CASE STUDY

Protecting Enterprise-Level Data With Alert Logic

BCS, The Chartered Institute for IT, promotes wider social and economic progress through the advancement of information technology science and practice. Founded in 1957, BCS is on a mission to ensure everyone has a positive experience with technology by raising standards of competence and conduct across the IT industry. In addition to its 68,000 members across 150 countries, and a wider community of business leaders, educators, practitioners and policy-makers, BCS delivers a vast number of digital apprenticeships in the UK.

BCS's growing portfolio of digital products and services is managed in a hybrid environment combining on-premises and multi-cloud. Most of its systems are in a hybrid-cloud infrastructure, which includes Amazon Web Services (AWS) and Microsoft Azure.

The increasing use of hybrid environments that includes both multi-cloud and on-premises workloads presented BCS with a great challenge to the effective application of IT security policies, especially with the company having limited security and IT staff. The company was in need of a partner who specializes in Azure and AWS security. And they found the security they needed from Fortra's Alert Logic.

> "One of the reasons why Fortra's Alert Logic is so useful for us is because it gives us the ability to have security visibility across all our estates."
>
> *Dale Titcombe | Head of IT at BCS*

Challenge

Managing the security of workloads in a hybrid environment can be a complex endeavor. As such, BCS needed a full picture of its cybersecurity posture, as the lack of visibility of cyber threats and vulnerabilities could lead the organization to miss obvious signs of a cyberattack.

One of BCS's security priorities is its AWS-hosted public cloud as it hosts all of its internet-facing servers. This includes hundreds of websites with backend databases and APIs. Another area of concern was BCS's centralized logging system, which is web facing due to the nature of its log sources. They needed a unified log management and monitoring across their environments in order to trace activity to gain a deeper understanding of events that occur.

AT-A-GLANCE

Company	**BCS, The Chartered Institute for IT**
Industry	**IT**
Location	**United Kingdom**
Number of Employees	**500+**

BUSINESS IMPACT

- Alert Logic's 24/7 Security Operations Center helps maintain the integrity of BCS's member data
- Deploying Alert Logic enabled BCS to stay compliant with prospective client requirements, GDPR, and helped with ISO 27001 certification
- By providing external security intelligence, Alert Logic helps augment the skills and knowledge of BCS's IT team

> “Having a strong security posture is paramount and Fortra's Alert Logic helps us maintain our multi-layered security strategy.”
>
> *Katrina Zoldak, IT Operations Manager*

Although BCS has a large membership body and a wide volunteer network, its operation is classified as a small-to-medium enterprise. With 24/7 services and many members, BCS is always on, which means any downtime from a cyber threat would have a negative impact.

“The security of our data and our members data is critical,” said Dale Titcombe, Head of IT at BCS. “As the Chartered Institute for IT, it’s imperative that we protect and maintain the integrity of our volunteers, members, the exams, and the apprenticeships that we deliver. Reputation is everything to us."

Keeping ahead of emerging malware that gets through email filtering or antivirus solutions — especially malware that communicates to a command-and-control server on a network port — was an ongoing challenge. Unpatched, unknown OS vulnerabilities were also a concern, along with an accidental or purposeful insider threat.

Solution

When BCS began its relationship with Fortra's Alert Logic, it was the first time its executives decided to work with an outsourced Security-as-a-Service provider to support active threat detection and response. With Alert Logic’s 24/7 security operations center (SOC), BCS gets threat detection and management capabilities staffed round the clock by threat experts. This team identifies threats faster with event-time detection of suspicious activity which enables BCS to uncover threats as they happen and take action to stop potential attacks faster. "One of the reasons why Alert Logic is so useful for us is because it gives us the ability to have security visibility across all our estates,” said Titcombe.

“Deploying Alert Logic assisted the improvement of BCS statements of compliance to ourselves and prospective customers, including any GDPR questionnaires we receive,” Titcombe continued. “Using Alert Logic’s services means we can explain to our customers that we deploy real-time threat detection. This helps our security posture in terms of prospective client compliance statements, as well as playing a key role in our ISO 27001 certification. When we’re audited, we can positively mention the assurance Alert Logic gives us.”

Advanced analytics from Alert Logic also provide a holistic view of the BCS hybrid environment and in-depth insights into activity, events, and potential incidents. “Most of the medium-level alerts we receive are from things we know about and expect, but we know that if there was anything that looked like a data leak or successful SQL injection attack, we’d get an immediate call from Alert Logic to notify us,” said Titcombe. “Alert Logic provides us a useful reminder of the volume of scans and attacks going on all the time. It helps us focus our efforts.”

Cybersecurity is increasingly on the agenda of c-suites, and BCS is no exception. With their executive team, there’s a feeling of reassurance when the IT team can say that the eyes of Alert Logic are always watching. Knowing that there’s an enterprise-level vendor viewing the BCS estate 24/7 always gets a good reception.

Alan Hilton, BCS Cloud Operations Manager, added, “Alert Logic is an insurance policy. On AWS, we get a lot of medium-level threats, and Alert Logic adds an extra layer of protection. It’s comforting to know it’s there.”

Summary

When talking about the business benefits of using Alert Logic, Titcombe said, “Alert Logic helps augment and extend the skills and knowledge our current team of IT professionals has by giving us external security intelligence, which goes hand in glove with assurance. Alert Logic comes within our top five strategic investments.”

“You can’t put a price on the worst-case potential problems we’d have if we weren’t using Alert Logic alongside other security measures,” said Katrina Zoldak, IT Operations Manager. “A reputational hit for the Chartered Institute for IT would be very damaging. Having a strong security posture is paramount and Alert Logic helps us maintain our multi-layered security strategy.”

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We’re the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.