

## Nominee: Alert Logic

---

### Nomination title: Alert Logic

Alert Logic was founded in 2002 by a visionary group of security professionals who saw a need that was lacking in the IT security industry – a multi-tenant security solution that could detect the latest security threats, serve companies of all sizes and in all industries, delivered as a service. After launching the first Security Operations Centre and began a series of partnerships that would redefine ‘Security as a Service’ across the industry. To meet the needs of global customers, in 2014 Alert Logic created international headquarters in the UK – and a Security Operations centred based in Cardiff.

The international operation in the UK now employs more than 200 employees. The company now has more than 4,000 customers globally using its Security-as-a-Service solutions to protect their cloud, hybrid or on-premises IT infrastructure. Built for cloud scale, Alert Logic’s patented platform stores petabytes of data, analyses over 400 million events and identifies over 250,000 security incidents each month, which are managed by its 24x7 Security Operations Centre.

Alert Logic cloud-based solutions are available for the major public clouds (AWS, Google Cloud, Microsoft Azure etc.) and hosting environments (Rackspace, Sungard, Navisite, Cogeco Peer1, etc.) Through these partnerships, Alert Logic protects organisations worldwide.

The Alert Logic Security-as-a-Service solution combines cloud-based software and innovative analytics with expert services to assess, detect and block threats to applications and other workloads. Protection extends to the full stack of web application components and infrastructure to defend against a broad range of server-side threats – including hard-to-detect web application attacks such as SQL Injection, part traversal and cross-site scripting.

The service provides better cloud and web application protection—at a fraction of the cost and resources required with traditional security tools— reducing risk without adding additional staff or security expertise. Alert Logic defends customer’s full web application and infrastructure stack, this approach is imperative as it leads to:

- Exposing attackers as they move across layers - attackers can use any layer of your stack to gain access, build footholds, and laterally move within your system. Full-stack visibility helps us spot the move so you can disrupt the attack—before it’s too late.

- **Covering more of customer’s growing attack surface – companies inherit vulnerabilities as they use commercial and open source tools like Joomla, Wordpress, Magento, PHP and ASP.NET. So Alert Logic invests in proprietary research and threat intelligence to understand these vulnerabilities, exploits and attack behaviors.**
- **Detecting advanced web attacks – businesses add their own vulnerabilities like those in the OWASP Top 10, when rapid development cycles leave little time to implement and test secure coding and configuration. Advanced detection analytics techniques including machine learning and anomaly detection give Alert Logic experts an industry-leading toolset for detecting stealthy attacks like SQL injection.**

### **Customer Service in the Delivery**

**Alert Logic provides technology together with experts which leads to more valuable outcomes. With Alert Logic, experts are “included” as part of an integrated solution with people, process and technology to deliver outcomes you need such as actionable incident reports, live notifications of threats and accurate blocking of malicious web requests.**

**There’s also no need for customers to BYOT (Bring Your Own Tech) - Unlike Managed Security Service Providers (MSSPs) who operate tools their customers buy from different vendors, Alert Logic experts share a common set of tools and processes they help to develop and continuously improve.**

**Alert Logic’s security professionals ensure proper deployment, configuration, tuning and optimisation of Cloud Defender. Every customer is assigned an Alert Logic onboarding project manager (OPM) to manage the process and onboarding team of 20+ specialist.**

### **Industry Accreditations**

- **Forrester – “As one of the first MSSPs to build on-demand and usage-based models ready for cloud environments, Alert Logic possesses an advantage for clients migrating toward off-premises solutions. More than any other provider, Alert Logic offers API-based integrations with clear and robust documentation, setting the stage for improved automation and orchestration. The company’s UI is clean and easy to use, and its dashboards are cloud native. Alert Logic is an**

excellent fit for clients looking to secure their current or planned cloud migrations, clients requiring a provider than can span seamlessly between hybrid architectures, and those that demand strong API capabilities for integrations”

- Info Security products guide named them a Global Excellence Gold Winner in the category of Cloud Security Product Excellence for Cloud Defender v1.5.
- Silver winner in the category of Product Excellence– Vulnerability assessment, Remediation and Management for the Cloud Insight product (v1)
- 451 Research - #1 Cloud Infrastructure Security vendor in 451 Research report for the second year in a row.

### Customer Endorsements

Funky Pigeon, a leading online retailer of personalized gifts commended Alert Logic’s products, and excellent customer service, included their ability to ‘scale up’ during the highest points of yearly traffic. Brett King, Service Delivery Manager at Funk Pigeon said: “The Alert Logic service is helping the team because its enabling us to tick the box for security. Its enabled us to put all our logs into one place for both the AWS environment and the production environments, so were able to look at the whole thing from end to end rather than little bits in isolation. Because we’re a small team, we can concentrate now on the business growth, new products, the ongoing development, improving the site, and not worry about whether we’re dealing with security. Also, because of the speed and the way it grows and the way it interacts with our Amazon environment, we’re doing slowing down our dev teams in any shape or form.”

Hillary’s Blinds two IT staff members tasked with security management spend a mere 5% of their time reacting to only the high priority security incidents Alert Logic brings to their attention. Julian Bond, Head of ICT at Hillary’s said: “We saved thousands of dollars and many hours every week by choosing this cost-effective technology with experts included. Alert Logic ensures that our cloud security extends being the reactive to a truly proactive stance- allowing us to continue successfully growing the Hillary’s brand.”

### Why nominee should win

Alert Logic was founded in 2002 by a visionary group of security professionals who saw a need that was lacking in the IT security industry – a multi-tenant security solution that could detect the latest security threats, serve companies of all sizes and in all industries, delivered as a service. After



launching the first Security Operations Centre and began a series of partnerships that would redefine 'Security as a Service' across the industry. To meet the needs of global customers, in 2014 Alert Logic created international headquarters in the UK – and a Security Operations centred based in Cardiff.