Bloor

InPerspective

InPerspective Paper by Bloor
Authors **Fran Howarth**
Publish date **June 2022**

Alert Logic MDR: case studies

“Alert Logic asked Bloor Research to speak to three of its customers, evaluate their experience using its MDR solution, and test whether or not our evaluations are borne out in practice.”

Introduction

Alert Logic is a managed detection and response (MDR) provider. It was founded in 2002 and has its headquarters in Houston, Texas, with further offices in Austin, Cardiff, London and Cali, Colombia. It has more than 4,000 customers worldwide and, whilst catering to organisations of all sizes, it has a keen focus on the midmarket sector. In March 2022, HelpSystems completed its acquisition of Alert Logic, intending that it will become a cornerstone of its cybersecurity portfolio.

Alert Logic differentiates itself with its *"white-glove"* customer experience, personalising its services to the needs of each individual customer and their desired outcomes. Any environment is covered, from on-premises and public cloud, to SaaS and hybrid environments. Its technology is cloud-native and provided on a 24/7 basis, wherever the customer is.

Bloor Research has evaluated Alert Logic's offerings, positioning them favourably as a champion in the MDR market. Alert Logic asked Bloor Research to speak to three of its customers, evaluate their experience using its MDR solution, and test whether or not our evaluations are borne out in practice.

We will first provide the case studies resulting from our discussions with the customers and then provide our own evaluation of their responses.

"Bloor Research has evaluated Alert Logic's offerings, positioning them favourably as a champion in the MDR market."

CASE STUDY 1

Nortek Control

> **The guidance that Alert Logic provided identified and prioritised the worst weaknesses, enabling remediation where it was needed most.**

Nortek Control is a technology company that is active in a wide range of areas, including developing technology for security, home automation, control, power, AV and entertainment, access control, and health and artificial intelligence systems for both commercial and residential markets. Founded in the 1960s, Nortek Control holds more than 200 patents and has 12 brands that are leaders in the market. It is headquartered in Carlsbad in California and has six further offices in the US, as well as one in China.

In October 2021, Nortek was acquired by Nice S.p.A, which has more than 3,000 employees and operations across five continents. Valued at $285 million, this is the largest investment that Nice has made to date.

Bloor Research spoke to Rob Barnes, cybersecurity engineer architect for Nortek Control, regarding its implementation of Alert Logic MDR®.

Two years ago, Barnes was given responsibility for security, including compliance and audit—the first and only dedicated security person within Nortek Control.

Compliance is of critical importance for the company, which requires that it must keep a record of all logs. However, Barnes realised that the system that was in place was not sufficient and an initial search for a new SIEM internet and event manager that fed logs into a dedicated system was also inadequate, especially since managing all the logs and alerts was too great a task for just one person.

Barnes began looking for an alternative that could take the load off his hands in the form of MDR services, providing not only dedicated tools but also expert guidance. Having considered several vendors, he settled on Alert Logic MDR®. Among the reasons for his choice were Alert Logic's expertise with Microsoft tools, which are critical for Nortek Control, and because it offered a dedicated resource who could alert him to the most important events and act as an extension of his team.

According to Barnes, Nortek Control has a 100% cloud-first strategy, covering all its infrastructure and DevOps needs. Alert Logic was pivotal in ensuing DevOps security so Nortek could take full advantage of this environment.

In the first week following implementation of Alert Logic's MDR solution, thousands of critical threats were identified. Alerts were issued regarding issues such as too many ports open, enabling problems to be fixed as soon as they were encountered. Within two weeks it became apparent that security best practices had not always been followed in the DevOps environment. Regular meetings with the Alert Logic dedicated security expert helped pinpoint the problems, without Barnes having to sift through the logs himself. The guidance that Alert Logic provided identified and prioritised the worst weaknesses, enabling remediation where it was needed most.

Nortek Control also implemented vulnerability scanning services from Alert Logic, resulting in detailed security information being conveyed to Barnes every couple of hours. He states that it was great to have them on board and the recommendations that they gave were invaluable. A real advantage was their flexibility. Every time something major happened, they were there to help. Barnes notes that he cannot overstate how important that was for the Nortek Control team, which had been struggling with limited resources in the face of the number of issues impacting the organisation.

Not only was Alert Logic doing what they said they would do, but they were good at it. They built up an extensive knowledge of the environment, instantly providing information as to what they were seeing and what they must pay attention to, and providing a quick response where needed – according to Barnes *"all without blinking an eye."* At this point, the focus is on fine-tuning the service to make sure it provides full intrusion detection across the entire IT environment.

Barnes states that he would absolutely recommend Alert Logic. Alert Logic processes a large number of logs from the Nortek Control network, hybrid cloud environment (Microsoft Azure and Office 365), emails, and on-premise devices without any problem. The cybersecurity company knows what they are doing and acts on it with proficiency. He is also impressed by Alert Logic's wide range of partners, with which they have extremely good relationships.

The final advantage in adopting Alert Logic MDR® according to Barnes is something that you don't find with most vendors: they are extremely willing to provide a Security Value Report to ensure Nortek Control gets what they pay for. Through monthly meetings with their account representative, Alert Logic is extremely transparent in ensuring that Nortek Control leverages all of the capabilities included in its subscription and in helping them improve their security posture.

With this service in place, the importance of security could be more easily demonstrated as the threats encountered have been reduced to a significant extent, prompting Nortek Control to add more people to its security team and fostering a more pervasive culture of security to better safeguard its operations.

"A real advantage was their flexibility. Every time something major happened, they were there to help. Barnes notes that he cannot overstate how important that was for the Nortek Control team."

CASE STUDY 2

Muir Group

> *...it is just such a holistic product that fulfils our requirements. It is the best fit in terms of the size of our department and provides the assurance of third-party eyes and ears, both on premises and in the cloud.*

Muir Group is a housing association that is based in the northwest of England, although it manages properties throughout the country. Founded in 1968, it has registered charitable status and employs some 130 people. The association manages and maintains some 5,500 properties that meet a diverse range of needs, including rental accommodation for those excluded from the open market, rent-to-buy properties, and housing for those with specific needs or who require sheltered accommodation.

Bloor Research spoke to Ian Whitwell, assistant director of business transformation & technology, regarding Muir Group's implementation of Alert Logic MDR®.

Although it is not a large organisation, Whitwell states that Muir Group's IT infrastructure is larger than many comparable organisations and this enables it to get approval for IT investments. Its IT functions are run out of the head office in Chester, with a second hosted data centre some 50 miles away in Bolton, to which data is replicated every 15 minutes for disaster recovery purposes. The core IT systems are hosted on premises, with cloud services being used for certain functions.

Whitwell states that Muir Group takes a strong view with regard to security, only allowing managed devices to connect to the network via mobile device management capabilities. As a result of Covid, almost all employees have been issued laptops, resulting in there being very few desktop PCs to manage. Flexibility is key as more than half of employees work remotely, especially frontline property management staff who are often on sites doing repairs or managing tenants. A wide footprint of access is required, with various levels of security according to need. Authentication is performed in Azure Active Directory.

A key driver behind the decision to implement an MDR solution was that the team did not necessarily know what vulnerabilities they were facing on a day-to-day basis. Muir Group was performing vulnerability assessments quarterly and pen tests once a year. But it felt that this was too static in terms of allowing it to address issues as needed.

There was also the realisation that the world of cyber defence and attacks moves quickly and requires a highly coordinated approach. Simple controls such as antivirus are no longer good enough and, even with more technology, there was no way the team could handle everything on a 24/7 basis. With too much to do internally, the search began for a separate security service that would act as independent eyes and ears, monitoring servers and endpoints for vulnerabilities or signs of a cyber attack.

Buoyed by an audit that confirmed that an MDR solution was the best option for Muir, Whitwell started looking at the options. Alert Logic MDR® was chosen as it offers the most holistic service, giving a complete picture of the entire network and every endpoint. Other offerings were not as cloud-based as Muir Group wanted since it uses Office 365 and was looking to migrate some of its on-premises resources to Azure servers. According to Whitwell, *"it is just such a holistic product that fulfils our requirements. It is the best fit in terms of the size of our department and provides the assurance of third-party eyes and ears, both on premises and in the cloud."*

A proof of concept began in January 2021, although Whitwell admits that it was a bit of a learning curve as you need to consider what to put into it to get the most out of it. But help was at hand, as Alert Logic agreed to extend the pilot until Muir Group's team was satisfied and ready.

Full implementation began in June 2021. Agents are now on all servers and endpoints proactively reporting to Alert Logic, which analyses them in real time. To test the response, Whitwell and his team created new administration accounts. Within one minute, an account manager from Alert Logic was on the phone with Whitwell's team checking on this new development. According to Whitwell, this gave the required comfort factor and level of assurance that were it an attacker using privileged credentials, it would be flagged in real time. However, the learning curve continues as the implementation progresses, including tuning the system to eliminate false positives and checking reports to ensure that the entire network is included in scanning and reporting.

At this point, threat detection and response are the two key elements of the Alert Logic MDR® solution for Muir Group, with a host of systems, including firewall logs, integrated so all traffic is analysed in Alert Logic's SOC. Whitwell stated plans are underway to expand its use of the solution's capabilities. Muir Group is currently configuring automated reporting to reduce the need to run ad hoc reports and provide tailored key performance indicators for the service to Muir Group's executive team. This will prove with a high level of assurance that IT systems are well managed from a cyber perspective. Whilst they already find the service to be proactive, this will up the ante further and will also help them with their cyber insurance needs, since requests for information are more detailed than they used to be and there are questions specifically related to whether the customer has deployed an MDR service.

The Group is also implementing cloud-based SAP, which will involve a host of connectors sending data to the Alert Logic solution.

Overall, Whitwell is very impressed with the white-glove service from Alert Logic. One thing that makes it so good is the quality of the account management and support that comes with it. According to Whitwell, *"there are very few suppliers I would say that about; support from others is usually patchy."* There are daily reports as to what has been checked and what, if anything, has been found, and monthly meetings with the account manager from Alert Logic are extremely useful, including reports that show a detailed picture of their security posture. They are focused on ensuring that customers get the maximum benefit from the investment. When additional functionality becomes available, Muir jumps on it. "*Why wouldn't we? New threats and new security sources mean more useful information flowing to the SOC.*"

Since starting the service, threat detection capabilities have improved dramatically. The technology shows them where they are in terms of vulnerabilities and what they are missing. Any gaps regarding what and why they are seeing something can be filled in by the technical team, giving a good insight into their overall security posture.

As more and more organisations are suffering cyber attacks and often don't realise until it is too late, Whitwell believes that its implementation of Alert Logic puts Muir Group much further along than many other organisations. But it still won't be resting on its laurels.

"...plans are underway to expand its use of the solution's capabilities. Muir Group is currently configuring automated reporting to reduce the need to run ad hoc reports and provide tailored key performance indicators for the service to Muir Group's executive team."

CASE STUDY 3

Rewards Network

Rewards Network is a fintech company that provides marketing services, loyalty rewards programmes and financing for the restaurant industry. It was founded in 1984 and has its headquarters in Chicago.

Individuals sign up for the programme and in return receive awards for dining at participating restaurants, ranging from airline miles and hotel points, to retail discounts and cash bonuses.

Bloor Research spoke to Ghiath Masri, director, security and compliance at Rewards Network, regarding its implementation of Alert Logic MDR®. Rewards Network has a relatively small dedicated security team, but leverages people from different teams, primarily network and DevOps, to drive security throughout the organisation. Security is particularly important to it since it is an assessed PCI DSS environment, and must protect against sensitive information breaches.

Rewards Network uses a variety of services from Alert Logic, including web application firewall, log management and PCI scanning services since PCI DSS compliance is a key requirement. Logs are driven from multiple applications, servers and appliances to Alert Logic's SOC and regular scans are run on external website and IP properties, as well as its internal network for vulnerabilities and unwanted file changes. Rewards Network uses Alert Logic for on-premises systems and the cloud – primarily AWS – to gain valuable visualisation of the health of the environment, including suspicious traffic and any changes that have happened.

Since implementing the service, Rewards Network has certainly seen a reduction in threats since most are captured by Alert Logic MDR®. It has recently added Alert Logic's Threat Intelligence Center, which Masri states is an excellent addition. This provides insight into Alert Logic security content coverage and allows configuration requirements to be investigated.

Overall, Masri is satisfied with Alert Logic's services and would definitely recommend the vendor. He is particularly impressed by Alert Logic's personnel and the speed with which they address issues. For example, when anything critical is spotted, Alert Logic immediately calls Masri's team to alert them and will sometimes escalate on their behalf to get deeper into the root of the problem.

Rewards Network holds monthly meetings with account managers from Alert Logic in which changes to consumption and goals are discussed, along with any other aspects with which that the vendor can assist them.

"...when anything critical is spotted, Alert Logic immediately calls Masri's team to alert them and will sometimes escalate on their behalf to get deeper into the root of the problem."

Analysis

All of the customers interviewed for this report state that they are satisfied with the service provided by Alert Logic and would recommend it to others. All have seen a reduction in threats, which is a prime objective for an MDR service. But it is the quality of the service that all call out in terms of account management, flexibility, speed of response and quality of support that they have received.

These testimonials attest to Alert Logic's claims of a white-glove approach, tailoring its offerings to the unique needs of each customer and its desired outcomes. Two of the customers also spoke of the vendor's desire to ensure the service provided is working to their complete satisfaction and that they are achieving value from their investments. What Bloor Research has heard in the discussions with the vendors is that Alert Logic's claims regarding its services are borne out and that our favourable evaluations are well founded.

FURTHER INFORMATION
Further information about this subject is available from
www.bloorresearch.com/company/alertlogic/

“These testimonials attest to Alert Logic's claims of a white-glove approach, tailoring its offerings to the unique needs of each customer and its desired outcomes.”

About the author

FRAN HOWARTH
Practice Leader, Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including ***Silicon***, ***Computer Weekly***, ***Computer Reseller News***, ***IT-Analysis*** and ***Computing Magazine***. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of ***InfoToday***.

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of ***Mutable*** business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

tel: **+44 (0)1494 291 992**
web: **www.Bloorresearch.com**
email: **info@Bloorresearch.com**