



CASE STUDY

Alert Logic's 24/7 Monitoring Improves Muir Group's Security Posture

Muir Group is a housing association based in northwest England that 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.

Challenge

Muir Group's core IT systems are hosted on premises, with cloud services being used for certain functions. Ian Whitwell, Assistant Director of Business Transformation and Technology for Muir Group, 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. Flexibility is key as more than half of employees work remotely. 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 Muir Group felt this was too static in terms of allowing them to address issues as needed.

There was also the realization that the world of cyber defense and attacks moves quickly and requires a highly coordinated approach. 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 cyberattack.

AT-A-GLANCE

WE'RE
MUIR

Company	Muir Group
Location	England, U.K.
Industry	Housing Association/ Property Management
Number of Employees	130

Business Impact

- Alert Logic's 24/7 monitoring allows Muir to focus on their core business.
- Threat detection capabilities have improved dramatically, exposing vulnerabilities and improving Muir's overall security posture.
- Automated reporting helps fulfill cyber insurance needs and keeps the Muir executive team updated.

"Alert Logic MDR 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."

Ian Whitwell / Assistant Director of Business Transformation and Technology, Muir Group

Solution

Buoyed by an audit that confirmed that an MDR solution was the best option, Whitwell started looking at the options. Fortra's Alert Logic MDR® was chosen as it offers the most holistic service, giving a complete picture of the entire network and every endpoint. "It is just such a holistic product that fulfills our requirements," said Whitwell. "Alert Logic MDR 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."

Agents are now on all servers and endpoints proactively reporting to Alert Logic MDR, which analyzes them in real time. To test the response, Whitwell and his team created new administration accounts. Within one minute, an expert from Alert Logic's Security Operations Center (SOC) 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.

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 analyzed in Alert Logic's Security Operations Center (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. While 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.

Overall, Whitwell is very impressed with the service from Alert Logic. One thing that makes it so good is the quality of the customer success managers (CSM) and support teams. According to Whitwell, "There are very few suppliers I would say that about; support from others is usually patchy." They are focused on ensuring 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," said Whitwell.

Summary

Since starting the service, Muir Group's 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 good insight into their overall security posture.

As more organizations are suffering cyberattacks and often don't realize until it is too late, Whitwell believes that its implementation of Alert Logic MDR puts Muir Group much further along than many other organizations.

*This case study was originally published in an **InPerspective** paper by Bloor.*

FORTRATM

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.