



CASE STUDY

Supporting zero trust networking for boutique developer house Geoactive Limited.

Barracuda CloudGen Access and XDR do the heavy lifting for cloud-first company.

Customer

- Geoactive Limited is a Scottish software developer specializing in products that support collaborative exploration and monitoring of subsurface terrain.
- Although ownership changed in 2022, as a carve out of a larger business with no IT infrastructure, the company's products date back to the 1990s. Since that time, they've built up a loyal userbase among stratigraphers, geologists, petrophysicists, engineers and data managers.

Challenges

- The potential for remote working to introduce threats
- A security team of just one
- Need to secure an entirely cloud-based IT infrastructure

Solutions



Barracuda
Email Protection™



Barracuda
CloudGen Access™



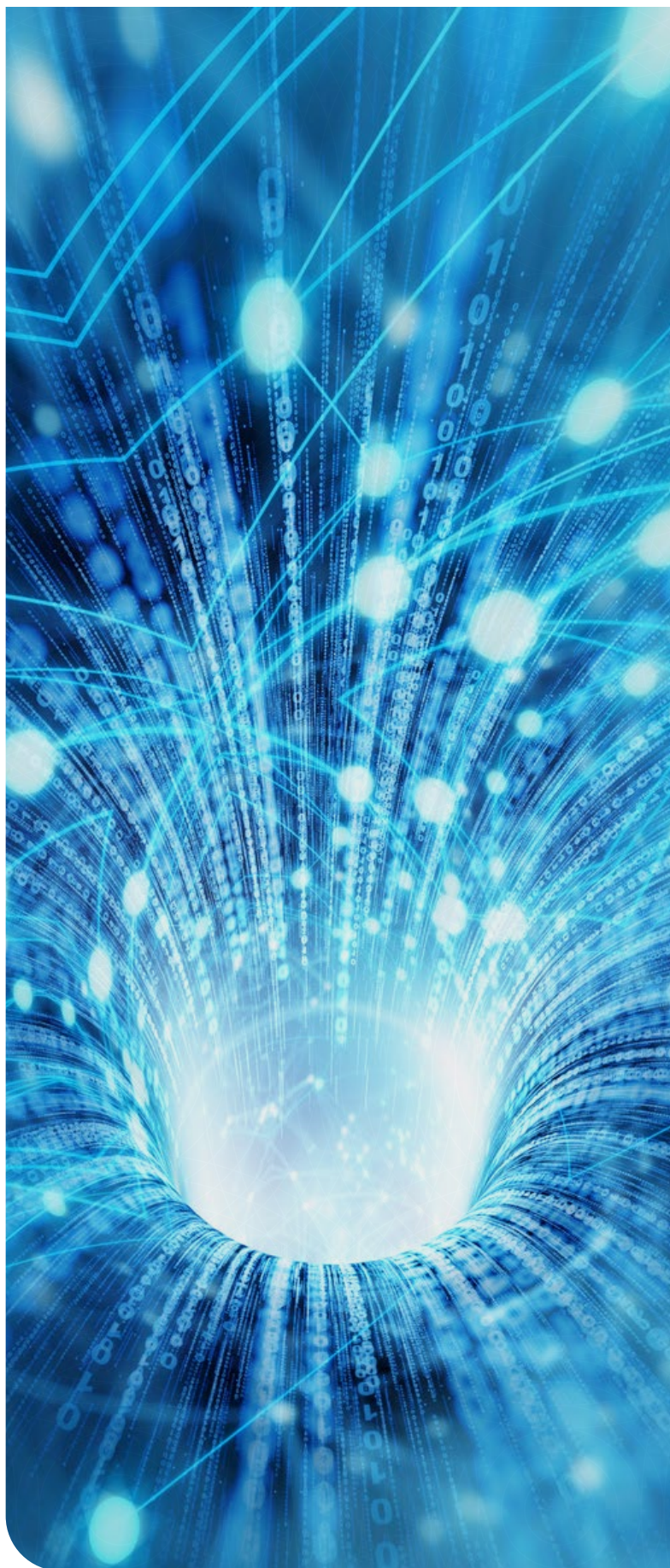
Barracuda
XDR™



Barracuda
CloudGen Firewall™

Results

- Unified visibility into security posture across multiple products
- Ease of use and managed XDR service enables the firm to run a lighter IT team
- Confidence in a long-term vendor partnership
- Support for zero trust networking



How do you secure a business with no IT infrastructure, no IT function and a hybrid working team? That was the challenge facing Malcolm Brown, Global Security Officer & IT Manager at [Geoactive Limited](#), back in 2022. With the fledgling business recently spun out from Lloyd's Register and acquired by new owners Constellation Software Inc., he made a bold decision to proceed without any on-premises infrastructure, and to use zero trust as a guiding principle.

"I've never been a lover of client VPNs. So I said, 'we're going with zero trust networking,'" says Malcolm. "It was a steep learning curve. But the way it has been done with Barracuda — it's very robust and easy to use."

The journey to Barracuda

With the decision made to build the firm's IT infrastructure around Azure and Microsoft 365, Malcolm had a specific set of requirements guided by the parent company's security framework — which he describes as a "stripped back ISO 27001." IT partner Altinet suggested Barracuda's CloudGen Firewalls would be a good fit for the firm, offering multi-layered protection for cloud-centric organizations.

Next came email protection to enhance native security in Microsoft 365, and then full-powered eXtended Detection and Response (XDR) functionality to build on Geoactive's Microsoft XDR security at the endpoint.

"For us, endpoints are our first line of defense, so we needed to load them with the right tools to do detection and response. AV is almost irrelevant: it's really about seeing who's copying files, or why they're loading an executable into Teams," says Malcolm. "Without visibility coming through in a single pane of glass, this becomes very difficult to manage. And as much as Microsoft has spent a lot of money on its XDR, it's still full of holes, and not very correlated in its approach."

Malcolm was impressed by the Barracuda XDR offering. And he felt that the unified approach of all three product offerings, plus Barracuda CloudGen Access for zero trust network access, would deliver the ease-of-management and centralized visibility he needed.

Putting everything in place

[Barracuda CloudGen Firewall](#) offers Advanced Threat Protection to block sophisticated threats and protect data, users and workloads wherever they reside. [Barracuda Email Protection](#) is a comprehensive suite of email threat detection, protection and response offerings. It features Incident Response for automated remediation and Impersonation Protection, which uses AI to automatically detect and prevent more advanced threats. [Barracuda XDR](#) provides defense-in-depth detection and response managed by a 24/7 Security Operations Center (SOC) to stop attacks in their tracks. And [Barracuda CloudGen Access](#) has been architected to support zero trust across a remote workforce, via web protection and continuous verification of user and device identity.

There was no time to waste, and everything was rolled out with minimum fuss and effort.

"We onboarded everything within a couple of months and learned the toolset. It's been very easy to use and the service from the XDR support desk is great," says Malcolm. "It has been a very easy journey."

"We onboarded everything within a couple of months and learned the toolset. It's been very easy to use and the service from the Barracuda support desk is great. It has been a very easy journey."

Malcolm Brown, Global Security Officer & IT Manager
Geoactive Limited



Zero trust and beyond

Malcolm has been delighted with the security and flexibility that his zero trust project has delivered.

“In a modern world, nearly all software development companies have home working. So your defense is no longer where your firewall is. Zero trust networking has played a huge part in providing the security level we’ve got,” he explains. “It’s much better than VPN technology; it’s more granular and focused. Being able to say ‘only this user group can see that asset’ is fantastic. It’s limiting the opportunity for the threat actor to get anywhere.”

Malcolm also praises Barracuda technology for enabling zero trust in such a seamless manner.

“We don’t even need to open rules on the firewall to allow access,” he says. “It’s all done through CloudGen Access tunnels. Even products that call themselves ‘zero trust’ I don’t trust. Instead, I put them inside the zero trust network and provide access to them that way.”

A related business benefit has been the ability of the firm’s developers to collaborate more seamlessly with external users without increasing the attack surface.

“Zero trust networking has played a huge part in providing the security level we’ve got,” he explains. “It’s much better than VPN technology; it’s more granular and focused.”

**Malcolm Brown, Global Security
Officer & IT Manager**
Geoactive Limited

Learn more:



For organizations that want to protect their businesses, brands, and people against the most advanced email-borne threats, [Barracuda Email Protection](#) is a comprehensive, easy-to-use solution that delivers gateway defense, API-based impersonation and phishing protection, incident response, data protection, and compliance capabilities.



“We’ve had external third parties that needed to co-develop on some stuff, and they needed access to some of our boxes,” explains Malcolm. “I’ve been able to grant them access, but only to the specific devices they need. That’s a powerful business benefit and so easy to do.”

Barracuda Email Protection has “done its job” in the background, with Malcolm tightening rules to block more phishing-related content, rather than quarantine messages. And he’s been even more pleased with the managed XDR service — which enables Geoactive Limited to run a “lighter IT team,” with just Malcolm in charge of security.

“The console is very simple and easy to understand. It gives you the information you need on a daily basis and is backed up by a 24/7 SOC, which is the important piece,” Malcolm says. “They’re doing all the heavy lifting — the triage and everything. It means I’m not getting bombarded with alerts. In the first quarter, the service was triaging 150 million events for a company of just 60 people.”

Malcolm’s also been delighted by the support he’s received from Barracuda over the past year-and-a-half. It bodes well for continued success into the future.

“The group of people we’ve got working with us now is very, very good. The Barracuda CloudGen Access and XDR teams are great at doing deep dives and showing me the product roadmap,” he concludes. “I feel it’s more of a partnership than a vendor-client relationship in that respect.”

Learn more:



[Barracuda CloudGen Access](#) is an innovative ZTNA solution that provides secure access to applications and workloads from any device and location. CloudGen Access continuously verifies that only the right person, with the right device, and the right permissions can access company data or apps, or any infrastructure.



[Barracuda XDR](#) is an eXtended visibility, Detection and Response platform that is backed by a group of tenured security experts in our 24x7 Security Operations Center (SOC), providing proactive cybersecurity-as-a-service for our partners and customers.



[Barracuda CloudGen Firewall](#) provides a comprehensive set of next-generation firewall technologies to ensure real-time network protection against a broad range of network threats, vulnerabilities, and exploits, including SQL injections, cross-site scripting, denial of service attacks, trojans, viruses, worms, spyware, and many more.



About Barracuda

At Barracuda we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.