CUSTOMER CASE STUDY

How Fairstone protects a growing business without growing complexity

By standardizing security for every new firm, Fairstone delivers consistent protection, coordinated threat response, and greater visibility across more than 50-plus locations.

SOPHOS

Fairstone

Industry
Financial Services

Overview
500+ regulated advisers

50+ locations

£20bn+ assets under management

120,000+ clients

Sophos solutions
Sophos Endpoint

Sophos Firewall

Sophos Switch

Sophos Wireless

Sophos Managed Detection and Response (MDR)

Sophos Network Detection and Response (NDR)

Sophos Mobile

Challenges:

- **Protecting sensitive client data** as a high-value target in financial services.
- **Securing 15 to 20 newly acquired firms each year** with consistent cybersecurity controls from day one.
- Maintaining security across more than 50 offices in the U.K. and Ireland with a lean IT team.
- Defending against increasing volume and sophistication of **AI-driven cyberattacks**.

Outcomes:

- Consistent, day-one cybersecurity for every acquired firm through a standardized Sophos deployment.
- 24/7 threat monitoring and response without the cost of building an in-house SOC.
- Estimated £30,000–£40,000 in annual savings on data ingestion and storage costs compared to alternative solutions.
- Greater visibility across the environment through connected security controls.
- Enabled a lean IT team to support a growing business more efficiently.

Fairstone Group is one of the fastest-growing financial wealth organizations in the U.K. and Ireland, managing more than £20 billion in assets on behalf of more than 120,000 clients. With more than 500 regulated advisers operating across 50-plus locations, the company has built its reputation on trusted, independent advice.

Each year, Fairstone brings 15 to 20 advisory firms into the business, creating a constantly evolving IT environment that must be securely integrated and managed without slowing growth.

For Aaron Carrier, Director of Infrastructure and Cybersecurity at Fairstone Group, ensuring security can scale as quickly as the business itself is a constant challenge. His lean team supports infrastructure, cybersecurity, and service desk operations across the U.K. and Ireland while securely integrating new firms into the organization.

"Financial wealth management is one of the biggest targets for cyber malicious actors," Carrier said. "So, it's important that we protect our systems and protect our data. And we continuously review the threat landscape to understand what those challenges are going forward, as things do change on a daily and weekly basis."

"That means we do have a need for a cybersecurity partner to help us defend against cybercriminals 24/7, 365 days of the year."

Aaron Carrier
Director of Infrastructure and Cybersecurity at Fairstone Group

SOPHOS

Fairstone needed a cybersecurity approach that could secure new firms quickly, maintain consistent protection across the organization, and provide around-the-clock coverage without increasing the burden on its internal team.

"It's important that my team is used across the business where it's going to be the most impactful," Carrier said. "That means we do have a need for a cybersecurity partner to help us defend against cybercriminals 24/7, 365 days of the year."

Sophos in a Box: Securing acquisitions from day one

At the heart of Fairstone's acquisition playbook is a deployment model Carrier calls "Sophos in a Box" - a standardized kit that includes a Sophos Firewall, Switch, Access Points, and Endpoint protection, all deployed on day one when a new firm joins the Fairstone Group.

"When we acquire a firm, we always carry out due diligence, as you would expect," Carrier said. "We understand their environment, we understand their security and their controls, and we deliver and deploy a standardized set of kit, which ensures that when they onboard into the Fairstone family, they're as secure as the wider group."

The approach solves one of the most pressing challenges in Fairstone's growth model: ensuring that each of the 15 to 20 firms acquired every year is brought into a consistent, centrally managed security environment, without slowing the business down.

"It's speed, consistency, and efficiency," Carrier said. "Having that single policy for firewalls in terms of configuration, switching, and access points is really important. Having to audit 50 to 60 devices on their own is impossible to do, regardless of the size of team. So for us, it's having that centralized control, consistency, and policy-driven configuration."

Fairstone's standardized security approach has delivered benefits beyond operational consistency. Carrier estimates Sophos MDR saves the company £30,000 to £40,000 per year in data ingestion costs compared to alternative solutions, helping keep security both scalable and cost-effective as the business grows.

> "Having all of our security data, login, and audit information centralized in one portal that is monitored and managed by my team, but more importantly by Sophos' MDR team as well, as an extension to what we deliver — that's what allows me to sleep at night."

Aaron Carrier
Director of Infrastructure and Cybersecurity at Fairstone Group

Better Visibility without added complexity

Fairstone uses Sophos products across its endpoint, network, and mobile environments, helping security controls work together more effectively across the organization. With centralized visibility into those environments, Carrier's team can manage security more efficiently as the business grows.

"For us, it's the simplicity and efficiency that it brings," Carrier said. "Having all of our security data, login, and audit information centralized in one portal that is monitored and managed by my team, but more importantly by Sophos' MDR team as well, as an extension to what we deliver — that's what allows me to sleep at night."

Rather than operating as separate security tools, Fairstone's Sophos products work together to provide shared visibility and coordinated response across the environment. This helps the team investigate potential threats more efficiently while reducing operational complexity.

"The importance of Synchronized Security is how they share telemetry data across the suite of products, which then allows the Sophos team to look at activity that's happened in one area and how that might be triggering it across other areas as well," Carrier said. "That gives greater insight into what might be happening or what somebody is potentially doing to gain access to the environment."

For Carrier's team, the operational impact is significant. Rather than monitoring multiple consoles and correlating alerts manually, the team works from a unified view - reducing the risk of human error and freeing time for higher-value work.

"Having that synchronized single pane of glass gives them one area to look. It reduces the chance of missing something that's important," Carrier said. "And then having Sophos there backing the team up as well is that vital second pair of eyes."

Sophos MDR: An extension of the team

Sophos MDR serves as Fairstone's around-the-clock security operations capability. For a team that can't staff 24/7 monitoring in-house, the MDR service provides continuous coverage backed by expert analysts - particularly during the periods when risk is highest.

"The Sophos MDR suite providing that 24/7, 365-day cover means that we don't have to have personnel operating 24/7," Carrier said. "We've got experts that are doing this for us through those critical times — out of hours, bank holidays, Christmas periods."

The holiday period is a concern Carrier takes personally. When the business shuts down and staff take time off, it creates an ideal window for attackers. Sophos MDR ensures that window is never left unguarded.

> "Whilst no breach occurred, just understanding that something could be occurring and the team reacting is really important to us because we're proactively defending our environment,"
>
> **Aaron Carrier**
> Director of Infrastructure and Cybersecurity at Fairstone Group

SOPHOS

"Knowing that Sophos is listening, monitoring, watching and reacting and alerting my team in the event of something is peace of mind," Carrier said. "It's not just an insurance policy — it's having them stood by you as that bodyguard, that security team."

That coverage has already proven its value. Fairstone has seen an increase in malicious actors attempting to impersonate user accounts outside normal business hours. In one instance, Sophos MDR detected login activity from a user that was inconsistent with their normal behavior and originating from outside Fairstone's operating countries. The MDR team shut the account down and prevented further access until Carrier's team was active the following morning.

"Whilst no breach occurred, just understanding that something could be occurring and the team reacting is really important to us because we're proactively defending our environment," Carrier said.

Beyond incident response, the MDR service has also helped Carrier's team grow their skills. Working alongside Sophos analysts gives Fairstone's in-house staff access to specialist cybersecurity expertise they wouldn't otherwise encounter in a lean financial services IT operation.

"The team get to grow. They're learning knowledge from industry specialists in cybersecurity, as well as doing their day-to-day job," Carrier said.

Building an equivalent SOC in-house would be both costly and risky. Carrier values the investment savings and the assurance that comes from trusting monitoring to a dedicated, expert team.

"For us, employing a SOC team would be very difficult. Not only is it the investment that's required, but it's ensuring that they are the best in the industry," he said. "Having Sophos MDR allows me to know that not only are our user base secure, but my team is acting in the best interests of the business as well."

"It's a partnership. It's about us working together strategically to defend our business, our systems, and our client data, rather than being a transactional service."

Aaron Carrier
Director of Infrastructure and Cybersecurity at Fairstone Group

A partnership, not a transaction

Carrier's relationship with Sophos spans more than a decade and multiple organizations. Over that time, what began as a technology investment has evolved into a trusted partnership built around helping Fairstone strengthen its security strategy and adapt to new challenges.

"I chose to partner with Sophos because of the relationship that I have both with the business and our account director," he said. "It's a partnership. It's about us working together strategically to defend our business, our systems, and our client data, rather than being a transactional service."

Over time, the relationship has expanded beyond day-to-day support to include customer advisory discussions, roadmap reviews, and ongoing collaboration on Fairstone's security strategy.

"They're very keen to understand what works for their customers and what gaps the customer has in their tooling that they could potentially fulfill," Carrier said. "It does feel like a partnership. It's not just about selling a solution that matches their competitors."

If you're ready to start your journey with Sophos, speak to an expert today.

To learn more visit Sophos.com