wanstor

Case Study

Saxton Bampfylde: From audit-driven security to always-on threat protection

Saxton Bampfylde

The Ambition

Saxton Bampfylde is an international executive search and leadership advisory firm operating from London, Guildford and Edinburgh. Their work depends on trust, confidentiality and the protection of sensitive data across clients, candidates and internal operations.

While the organisation had already adopted Microsoft 365, security assurance relied heavily on point-in-time effort. Cyber Essentials and Cyber Essentials Plus certification were achievable, but required concentrated preparation, manual evidence gathering and increased pressure around audit windows. At the same time, the threat landscape had shifted towards identity and SaaS, increasing exposure beyond traditional infrastructure controls.

The ambition reached well beyond certification. Leadership wanted security to become the default state of the business, with risks actively managed, incidents handled consistently, and controls that could be evidenced throughout the year without disruption to day to day work.

Key challenges included:

- Achieve and sustain Cyber Essentials and Cyber Essentials Plus certification
- Introduce SOC Tier 3 protection across the business
- Improve detection and response across identity and SaaS threats
- Establish consistent, auditable incident handling
- Move from audit-driven assurance to continuous visibility and control

The Reality

When the story began, Saxton Bampfylde already had security controls in place, but they were spread across separate tools and processes. Assurance tended to be reactive, with energy concentrated around certification windows rather than woven into everyday operations.

At the same time, visibility across identity risk, SaaS usage and endpoint activity was limited. Signals existed, but not always in a way that could be consistently monitored, triaged and acted upon. This created a gap between capability and confidence.

Saxton Bampfylde faced several key challenges:

- Security assurance reliant on point-in-time audits
- Detection and response processes not fully standardised
- Limited visibility across identity and SaaS activity
- Manual effort required to demonstrate CE and CE+ compliance
- Leadership exposure to unmanaged or delayed security responses
- A need for consistent, repeatable operational security processes

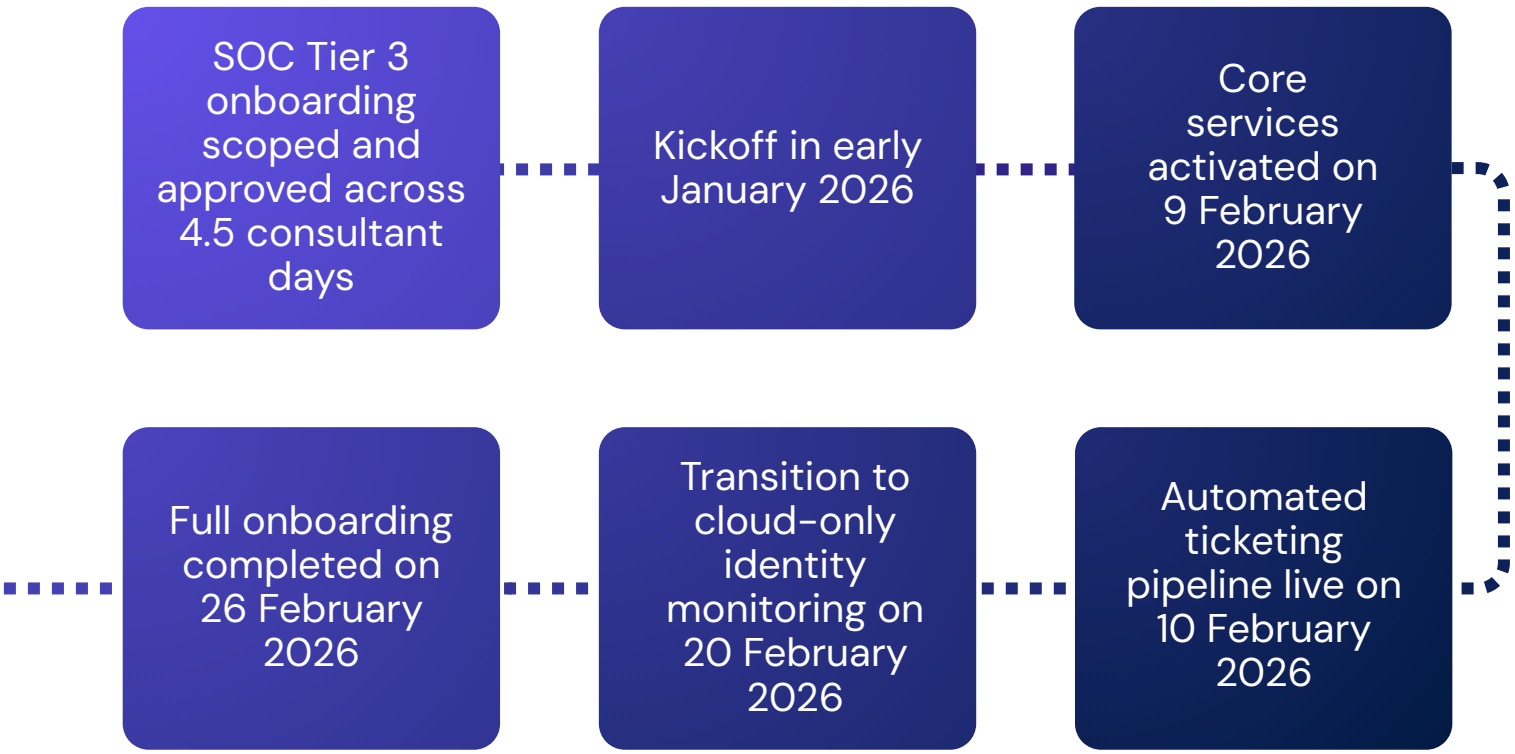
The Moment of Truth

The turning point came when it became clear that certification alone would never be enough. The organisation needed a security model that worked every day of the year, including the long stretches between audits.

The requirement was straightforward. Controls needed to be visible, measurable and consistently applied. Detection needed to lead to action. And response needed to be predictable, repeatable and free from reliance on any single person.

This led to the decision to implement SOC Tier 3 services alongside structured CE and CE+ certification support.

Key milestones included:



The Intervention

Discovery

Wanstor assessed Saxton Bampfylde's existing security posture, focusing on visibility gaps, identity exposure and response workflows. This included aligning current controls with CE and CE+ requirements and identifying where improvements would deliver the most impact. Supporting infrastructure work, including removal of legacy dependencies.

Solution

A SOC-led security model was introduced, built around Microsoft Defender and supported by Wanstor's Tier 3 service. At its core sat a SOC Tier 3 managed service, operating fully in the cloud and drawing on seven Defender detection sources across Endpoint, Cloud, Office 365, Cloud Apps, Identity, XDR and Entra ID Protection. User Risk and Sign-in Risk policies were enabled for all users, and automated incident creation was wired in through Azure Logic Apps across five detection sources.

Outcome

Within that short window, SOC Tier 3 was fully deployed and operational, automated ticketing and incident handling were in place, and identity-led detection and response was embedded across the business. Certification work was aligned to the live operational environment, and the reliance on manual intervention was reduced.

Adoption

Security moved into a consistent operating rhythm. Detection, response and reporting became part of normal operations rather than a separate effort. Monthly reporting and review cycles ensured that improvements were tracked and maintained, supporting both operational performance and certification requirements.

The Impact

With SOC Tier 3 in place, Saxton Bampfylde now operates with continuous monitoring and structured response.

As of May 2026:

- **81** endpoints under continuous cyber security monitoring
- **Ongoing** monthly vulnerability scanning
- **Dual-platform** patch validation across Endpoint Central and Qualys
- **Two** zero-day threats proactively managed: Red Sun fully remediated, and MiniPlasma actively monitored with automated patching scheduled on vendor release
- **Four** consecutive months of Threat & Vulnerability and Defender reporting delivered

This provides clear, ongoing visibility across the environment and supports informed decision-making.

By May 2026 the picture looked very different. Saxton Bampfylde now operates with a more controlled, visible and resilient security posture, and for the first time the day to day protection can be shown in numbers. The first full month of managed monitoring, covering 6 to 31 May 2026, shows what that looks like in practice.

> The quiet win was getting certified without the drama. Wanstor helped us over the line on Cyber Essentials Plus and modernised our security operations in the same breath; now we're tightening identity and SaaS so the numbers prove our posture month by month.
>
> **David Adams, Management Accountant**

2,180 confirmed threats blocked

Between 6 and 31 May 2026, 2,180 genuinely malicious items were stopped before they reached users, made up of 1,955 malicious emails blocked automatically and 225 risky network connections halted at the endpoint.

218 risks under active management, zero high-risk users

Microsoft Secure Score reached 69.41%, around 44% higher than the peer average of 48.13%. 218 recommendations are managed through Secure Score and a further 148 through Defender for Cloud, with zero high-risk users across the period and the two security incidents raised in May both triaged and closed with no breach.

Microsoft Secure Score up 1.47 points

Secure Score improved from 67.94% in February to 69.41% in May, climbing across four consecutive months of monitoring.

SOC Tier 3 protection established

Continuous monitoring, triage and response now embedded into operations.

Improved detection and response

Incidents identified and handled through consistent, auditable workflows.

Operational risk reduced

Faster escalation, clearer ownership and fewer unmanaged threats.

Certification achieved and sustained

Cyber Essentials and CE+ aligned to the live environment.

Greater visibility across the estate

Endpoint, identity and SaaS activity monitored and reported regularly.

Why Wanstor

Saxton Bampfylde knew the security posture they wanted, but they did not have the in-house capability to run continuous monitoring and response, or to keep certification evidence current throughout the year. They needed a partner who could:

- Turn point-in-time certification effort into continuous, evidenced assurance
- Run it as a managed service, without adding internal headcount
- Stand up SOC Tier 3 detection and response across identity and SaaS

From the initial discovery and scoping, Saxton Bampfylde had confidence that Wanstor understood their environment and could deliver a working security operating model within a realistic timescale.

What set Wanstor apart was the way of working:

1. Microsoft Defender expertise across seven detection sources
2. Monthly reporting that keeps risk visible and decisions informed
3. A single, consistent pathway from detection through to action
4. Certification work aligned to the live environment

Ready to strengthen your Microsoft Defender protection?

Wanstor's Managed Defender SOC helps you move from alert noise to always-on monitoring, triage and response across your Microsoft security estate.

Book a discovery session to see where you are exposed and how quickly you could respond.

Book a discovery session with Wanstor