CASE STUDY

How Safer Business Network Protects Sensitive Data at Scale

ABOUT SAFER BUSINESS NETWORK

Safer Business Network is a community-focused organisation working in partnership with businesses, local authorities, and police forces to reduce crime and improve safety across towns and city centres. Supporting a wide range of stakeholders, they handle sensitive data and intelligence that must be shared securely and reliably.

And as their reach and impact continue to grow, having secure, resilient IT systems is essential to protect client data, maintain trust, and ensure their services remain effective.

THE CHALLENGE

As SBN continued to grow, the complexity of managing security across devices and systems also increased. The organisation recognised the opportunity to strengthen oversight and standardise security across all systems.

Security tools were in place, but over time it became less clear what was fully protected, areas where controls could be strengthened, and whether small risks were quietly building up in the background (such as how people accessed systems and data). With information shared across partners, local authorities, and police forces, that lack of clarity needed addressing.

At the same time, the organisation was operating across a mix of device generations, creating an opportunity to standardise device management and ensure consistent updates and lifecycle support across all systems.

> **We knew we wanted to continue to strengthen our security, but we wanted a partner who could guide us clearly without overcomplicating things. Sereno made everything simple, understandable and achievable.**
>
> **Adam Ratcliffe**
> Operations Director
> Safer Business Network CIC

As the organisation grew, SBN wanted to ensure its existing protections continued to scale effectively and that sensitive data remained accessible only to authorised users on approved devices.

What SBN needed wasn't complexity or more tools. They needed clarity. A clear understanding of what was working, what needed improving, and how to strengthen security in a way that felt proportionate, cost-effective, and respectful of day-to-day operations. Just as importantly, they were looking for calm, practical guidance to help them move forward with confidence.

THE SOLUTION

SBN introduced a tailored security strategy, developed with guidance from Sereno IT. By getting clear, practical advice, the team was able to strengthen their security posture and protect client data without adding complexity.

Device Management and Updates
Outdated hardware was replaced, and all devices were upgraded to the latest professional operating systems. This gave the team better control, ensuring that their devices were secure and easy to manage, while ensuring updates and security fixes are applied automatically so everything stays protected over time.

Simplified Cybersecurity Packages
To keep security easy to manage and cost-effective, SBN adopted Sereno's clearly defined Cyber Security Packages. Instead of juggling multiple tools and suppliers, this brought everything together under one consistent approach making it easier to understand, maintain, and trust.

The package focused on key areas:

Device Security
SBN's work involves sensitive information, that is why their devices were set up to protect data quietly in the background. This includes:

- Managed antivirus protection to detect and block viruses and malicious software
- Advanced malware protection and DNS filtering protecting users from malicious websites wherever they are working
- Mobile device security and screen lock policies ensuring company email on phones is protected and devices lock automatically when unattended
- Automatic deployment and enforcement of security controls with proactive fixes if a device falls out of compliance
- Full device encryption protecting data if a laptop or device is lost or stolen
- Remote wipe capability allowing company data to be removed instantly from lost or compromised devices
- Advanced endpoint protection using intelligent monitoring to identify and respond to suspicious activity
- Network quarantine automatically disconnecting infected devices to prevent threats spreading
- Clear compliance reporting providing visibility on device security status and any required actions

Email Security

To protect sensitive communication, email security was strengthened to quietly reduce the risk of scams, unsafe links, and accidental data exposure. This covers:

- Spam and scam filtering to keep dangerous emails out of inboxes
- Safe link and attachment scanning to block hidden threats
- Protection against impersonation to prevent criminals posing as the business
- A year of Microsoft 365 backup, covering email, SharePoint files, and other M365 data for full recovery
- Secure email archiving, storing older emails safely while keeping them easy to access

Employee Security

Rather than relying on technology alone, SBN supported its team with clear security guidance and awareness, helping everyone contribute to keeping sensitive information safe.

- Secure sign-in checks to ensure only authorised users can access systems
- Two-step login protection for an extra layer of security and strong password standards with safe and simple reset options
- Security awareness training to help employees recognise risks and protect sensitive data
- Phishing simulations reinforcing good habits through realistic practice
- Compliance and policy training to support understanding of responsibilities and expectations
- Easy reporting of suspicious emails allowing potential threats to be investigated quickly

Centralised Security Management

With device management centralised through Entra ID and Microsoft Intune, SBN could easily enforce security policies across all devices. This meant that only authorised devices that meet defined security standards could access company systems and sensitive data, reducing the risk of unauthorised access to critical business systems. They also gained full visibility and control, including the ability to remotely wipe a device.

Streamlined Access with Unified Sign-On

A unified sign-on system was set up across Microsoft 365 and other key business applications, making it easier for the team to access the tools they needed securely, without the hassle of remembering multiple logins.

Importantly, these improvements were introduced without disrupting day-to-day work allowing the team to continue supporting partners while security was strengthened in the background.

THE RESULT

SBN now has a stronger, more reliable security setup that protects client information and supports the way the organisation works day to day.

As a result, they now benefit from:

- All staff using secure, up-to-date devices that are easy to manage
- Clear controls over who can access systems and information
- Getting full value from the Microsoft 365 tools they were already paying for
- A simple, easy-to-understand security setup with no unnecessary complexity
- Clear visibility over security and compliance, all managed in one place
- Greater confidence for staff, leadership, and partner organisations
- Security improvements delivered with minimal disruption to daily work

“The improvements have given us real peace of mind. Our team feels more confident, our processes are clearer and our clients can continue to trust SBN with their data. Sereno delivered exactly what we needed.”

Adam Ratcliffe
Operations Director
Safer Business Network CIC

Ready for a quick chat?

Got a specific use case you'd like to discuss? We can help. Arrange your personalised consultation call today.

Michael Johnson
E: michael.j@serenoit.co.uk
T: +44 (0) 203 089 01 40