UK Real Estate Organization Balances Security With Mobile Workforce Requirements.

‘Sophos XG Firewall is light years ahead.’

Andrew Chaplin
IT Infrastructure Manager, Spicerhaart Group Services Ltd
Through growth and multiple acquisitions, UK-based Spicerhaart Group Services Ltd has evolved into a full-service real estate organization with over 200 branches in England and Wales. Spicerhaart offers a wide array of services: home sales and purchases, rentals and leasing, property management, mortgages, and surveying. It is also the only real estate group in the UK with its own dedicated contact center, which leverages voice and data communications technology to stay in touch with customers and guide them through selling, buying, renting, leasing, legal, and financing processes.

How do you fully secure corporate data while respecting the needs of business users?

Andrew Chaplin, IT infrastructure manager at Spicerhaart, leads a team of three at the headquarters location that oversees the company’s entire infrastructure: servers, firewalls, user services, mobile provisioning, and endpoint and network security. While both Chaplin and IT network and systems administrator David Skingley strive to keep Spicerhaart as secure as possible, they are always balancing the need for protection with allowing users to do their jobs unobstructed. Additionally, now that the European Union General Data Protection Regulation (EU GDPR) is in effect, they are extremely vigilant about protecting personal and business data to maintain compliance with the strict mandate and avoid hefty fines.

‘With Sophos Mobile, I can deploy our apps to both Google Android phones and Apple iPhones through a single interface.’

David Skingley
IT Network and Systems Administrator, Spicerhaart Group Services Ltd
Chaplin, who has been with Spicerhaart for over three years, had become dissatisfied with the company’s previous endpoint security and firewall vendors. Their antivirus and encryption solutions proved difficult to configure and manage, and the level of support was inadequate. The firewalls were outdated and were also overly complex to administer.

He decided to research other options and discovered Sophos. “We liked what Sophos had to offer and were particularly impressed with the advanced detection and protection capabilities of Sophos Intercept X,” remarks Chaplin. “We realized that we could acquire Sophos endpoint and firewall solutions as a cost-neutral option versus renewing or upgrading our legacy solutions, which weren’t working well. Financially, it was a no-brainer, and, equally important, we definitely believe in the Sophos suite of products and what it could do for us.”

With onsite technical assistance from Chess Cybersecurity, Spicerhaart deployed three Sophos XG Firewalls and Sophos Central Endpoint Protection Advanced, along with Sophos Intercept X, to 2,000 devices. According to Chaplin, the process was seamless: “It was a joy to see how easy it was to install our Sophos solutions. Configuration and policy setting was effortless. I definitely appreciate the Sophos ‘kit.’ It’s simple, and anyone can pick it up very quickly.”

With ransomware on the upswing, how do you ease concerns about potential attacks?

Prior to the Sophos deployment, Spicerhaart experienced several CryptoLocker-style ransomware attacks. Because of robust backups, Chaplin and his team managed to restore the data, and the company did not have to pay any ransom to the perpetrators. In spite of these precautions, it has always been in the back of Chaplin’s mind that Spicerhaart could become a target again.

“There can be more targeted attacks on large firms, and we are as likely to get attacked as any other organization of our size. Another big concern for us is GDPR compliance. If someone’s data is encrypted and you can’t get to it, you could get fined. Our clients are important and we never want to put them at risk, despite the threat of fines or reputation loss,” he points out.

Now, with Sophos Intercept X in place, Chaplin feels greater peace of mind in a world where ransomware is on the rise. Sophos Intercept X provides an integrated approach to combating advanced and zero-day threats and incorporates deep learning, an advanced form of machine learning, to more quickly and accurately detect known and unknown malware.

“Sophos Intercept X is our insurance policy against future attacks. The root cause analysis feature is an added advantage because it provides us with a clear graphical representation of where attacks start and where they spread. We feel so much more comfortable now that we have it in our security toolbox,” observes Chaplin.

What’s the best way for a large organization to simplify security management while ensuring comprehensive protection?

When it comes to network security, Chaplin has noticed a significant difference between Sophos XG Firewall and his previous Juniper firewall appliances. “Sophos XG Firewall was light years ahead of our Juniper solution,” Chaplin remarks.

As a leader in the Gartner Magic Quadrant, Sophos XG Firewall provides on-box reporting to identify potential issues before they become problems. It also safeguards the Spicerhaart network with advanced technologies, such as intrusion prevention system (IPS), advanced threat protection, sandboxing, web and application control, and anti-phishing capabilities.

“We don’t have to worry about unknown threats or underlying, hidden risks. XG Firewall has intuitive policy options and responds instantly to any incident,” continues Chaplin.

Chaplin is especially enthusiastic about the intelligence behind Sophos Synchronized Security. Powered by Security Heartbeat™ technology, it allows endpoints and firewalls to communicate bidirectionally and to share threat, health, and security information across multiple Sophos products, delivering unparalleled protection, automated incident response, and real-time insight and control. Working in concert with Sophos Synchronized Security, Spicerhaart’s Sophos XG Firewalls can instantly identify and automatically isolate compromised systems, saving the team time and enabling faster remediation.
“Staying ahead of today’s cyber threats is paramount. With Synchronized Security, we have coordinated our defenses and maximized all of our resources. Regardless of the attack complexity or surface, we are now more prepared than ever before,” adds Chaplin.

Overall, Chaplin and his team find it much easier to manage and coordinate all aspects of security for the entire enterprise thanks to the Sophos Central Advanced platform. With its intuitive, single-pane-of-glass management console, it saves time and provides visibility across the entire organization, including the 200 branch offices and mission-critical servers at headquarters that house valuable and sensitive personal and business data and essential applications. Spicerhaart’s physical and virtual servers are secured with Sophos Server Protection, which uses a combination of traditional and next-generation methods to defend against ransomware and other threats—without impacting performance.

How do you safeguard corporate assets while giving mobile users freedom?

Securing mobile devices was also on the team’s list of priorities. When Skingley joined the company less than a year ago, he was tasked with evaluating mobile device management solutions. In a side-by-side comparison with MobileIron, Sophos Central Mobile Advanced came out on top, primarily because of its built-in security, its simplicity, and overall resource efficiency.

Sophos Mobile is currently deployed on 400 devices, and Skingley plans to extend the implementation to all 1,200 devices in the near term. Sophos Mobile manages and secures device across multiple operating systems – Microsoft Windows 10, Apple macOS, Apple iOS, and Google Android – via Spicerhaart’s existing unified Sophos Central Advanced administrative interface.

Sophos Mobile makes it easy for the IT team to consolidate endpoint management and enforce consistent policies, provide comprehensive and consistent security, and allow users to be productive on the devices they prefer. Recently, Skingley provisioned an in-house productivity app that helps users plan their day, their diary, and their Google Map route to their next location.

“At Spicerhaart, employees can choose to use their personal devices to access corporate email or opt for a corporate-issued device. If users prefer the bring-your-own-device (BYOD) option, they must have Sophos installed on their devices to access company email and other proprietary apps built by the in-house development group. The only thing Chaplin’s team controls on personal smartphones is the container—the Sophos Secure Email app. When users need to have corporate email enabled, all they have to do is register and follow an instruction guide that instructs them on the installation of Sophos Mobile and Sophos Secure Email.

As Chaplin sees it, the mobility aspect of computing at Spicerhaart is on an expansion path. Aside from gradually getting all users and their devices up and running on Sophos Mobile, the team also has plans to install Sophos Access Points for Wi-Fi, which he describes as “plug-and-play,” at every branch within six months. Furthermore, all home-based employees will soon be using Sophos RED 15, a small network appliance that provides a secure tunnel from its deployment location to a Sophos Firewall. Also in the works are plans to migrate the organization’s computer environment to VMware, where Sophos antivirus clients will be implemented. Finally, Chaplin and his team look forward to rolling out industry-standard BitLocker encryption, which is fully integrated and managed by Sophos Central Device Encryption. They believe this will be a more reliable and robust alternative to their legacy encryption solution.

“We’ll be turning ‘Sophos blue’ very soon,” jokes Chaplin. “But all kidding aside, I believe Sophos solutions go hand in hand with what we’re trying to achieve as a company. We are at the cutting edge of our industry, with a security solution that won’t hold us back and which will allow us to focus on IT initiatives that support the business.”
'Sophos Intercept X is our insurance policy against future attacks. The root cause analysis feature provides us with a clear graphical representation of where attacks start and where they spread. We feel so much more comfortable now that we have it in our security toolbox.'

Andrew Chaplin
IT Infrastructure Manager, Spicerhaart Group Services Ltd
Start your free trial of Sophos XG Firewall today to get started with Synchronized Security.