

SECURITY UNDER SPOTLIGHT AS CLOUD ALTERS THE LANDSCAPE

Sophos and Trilogy are at the forefront of the drive to deliver innovative, effective IT security solutions

As cloud computing becomes a game-changer for SMEs by offering flexible, cost-effective access to IT infrastructure, security is coming more firmly under the spotlight.

Organisations today are now more dependent than ever on IT to run their businesses. As external demands driven by security and compliance needs grow dramatically, many are finding flaws in their systems the hard way.

Security and availability of IT systems are not just about having a carbon copy somewhere, but about being resilient. Even with the most robust data recovery solution in place, the cost to a business of being without their systems while that data is being restored, can be highly significant.

The cloud is having a fundamental impact on how IT services are delivered across the business landscape, and nowhere more so than in the area of IT security. Next generation security software company Sophos is harnessing the power of the cloud to deliver innovative new IT security solutions, with simplified deployment and management and previously unseen levels of protection.

Sophos Cloud has given us the ability to connect the endpoint and network security domains that, until now, have required distinct standalone security products that never communicated with each other. This is called synchronised security, as both these critical areas now work together in tandem sharing information via the cloud where previously they couldn't.

Cybercriminals are using increasingly sophisticated attack methods that span these two areas and take advantage of the fact that most companies' defences are still

stove-piped along endpoint and network lines, so it's critical that companies recognise this and organise their synchronised defences in a way that data can easily be shared between the endpoint and network.

The Sophos Central cloud-based platform now enables us to deliver endpoint and server security, mobile device management, email and web gateway, wifi and all associated reporting via a single management console. Critically, though, it also enables the different elements to share pertinent security state information via Sophos's unique security heartbeat, which greatly strengthens security and improves visibility in a way that just would not be possible without the cloud. It's even enabled synchronisation of encryption, so that if a computer is compromised, the keys are automatically revoked in real-time, thereby preventing any data being taken off the compromised device.

While the industry has been using cloud services for many years in facilitating delivery of some of its services such as definition updates, it has been the development from scratch of cloud-based platforms such as Sophos Central that have facilitated the huge step change in simplicity of management, improved integration and sharing of information and reporting. What the use of this platform means to Trilogy, as a provider of managed IT as a service, is that the provision of managed security becomes both a proactive and preventative process.

We see organisations now looking for a single partner to manage and advise on all aspects of their IT infrastructure, including cloud services



Edel Creely, Group Managing Director, Trilogy Technologies

and security. A typical Trilogy Managed IT as a Service solution today embraces proactively managing and securing private, hybrid or cloud environments. The added value that one company brings as a single managed service provider ensures a swift response to any security or technology emergency. This will minimise downtime, and ensure the integrity and resilience of all systems.

Despite the investments companies may have made in technology, without a continuous detailed audit of its effectiveness and a proactive element to its management, there is a low level of likelihood that it is 100 per cent effective.

The true value of a secure infrastructure is only visible at the detailed level – it's not appropriate to expect a one-size-fits-all approach will work for every company. That's why an approach which starts with a deep audit and analysis of the full IT infrastructure, followed by a customised plan to implement solutions to tackle exposed areas in the short-term and more comprehensive protection in the medium and longer term, and then by a proactive security management regime, is recom-

mended.

More organisations are today tasked with the need to deliver governance and compliance, which includes the operation of its IT systems and data security. These are, for many, critical elements of the organisations' operational being. Securing your business goes beyond just implementing some firewall rules, anti-virus software and data backup solutions. Today, it requires a comprehensive programmatic approach.

Being compliant with



We see organisations now looking for a single partner to manage and advise on all aspects of their IT infrastructure, including cloud services and security



Dermot Hayden, Sophos Country Manager

standards might protect you from litigation, but will it ensure you are fully protected and your business safe?

Part of auditing your IT infrastructure should include observing and interviewing staff, reviewing processes and examining the equipment and surroundings.

When examining sites, employee network access is one of the most frequent issues Trilogy uncovers. This includes something as simple as forgetting to remove employee access after they have left the company. Other common and easily fixed issues we observe relate to implementation of password policy, removal of unauthorised software, enforcement of data loss protection systems including USB lockdown, and updating or upgrading firewall and server firmware.

Such an audit should initially deliver a RAG (Red/Amber/Green) report which

will identify significant issues requiring corrective action, problems with a negative effect but not deemed critical, and those areas performing to plan. Addressing the red and amber action items assist in mitigating the entry points for a targeted attack.

By taking this approach, an organisation can quickly identify a clear infrastructure security roadmap and start on a continuous journey of proactive protection for its business.

Trilogy implements, manages and secures agile IT infrastructure across virtual and cloud platforms, helping clients to enhance their operations, mitigate risk and enable business strategy. The company incorporates expertise in both infrastructure transformation and managed IT as a service to deliver business-wide IT services. Trilogy is a Sophos Gold partner and implements the full range of Sophos solutions

TECHNOLOGIES
trilogy

SOPHOS

Security made simple.