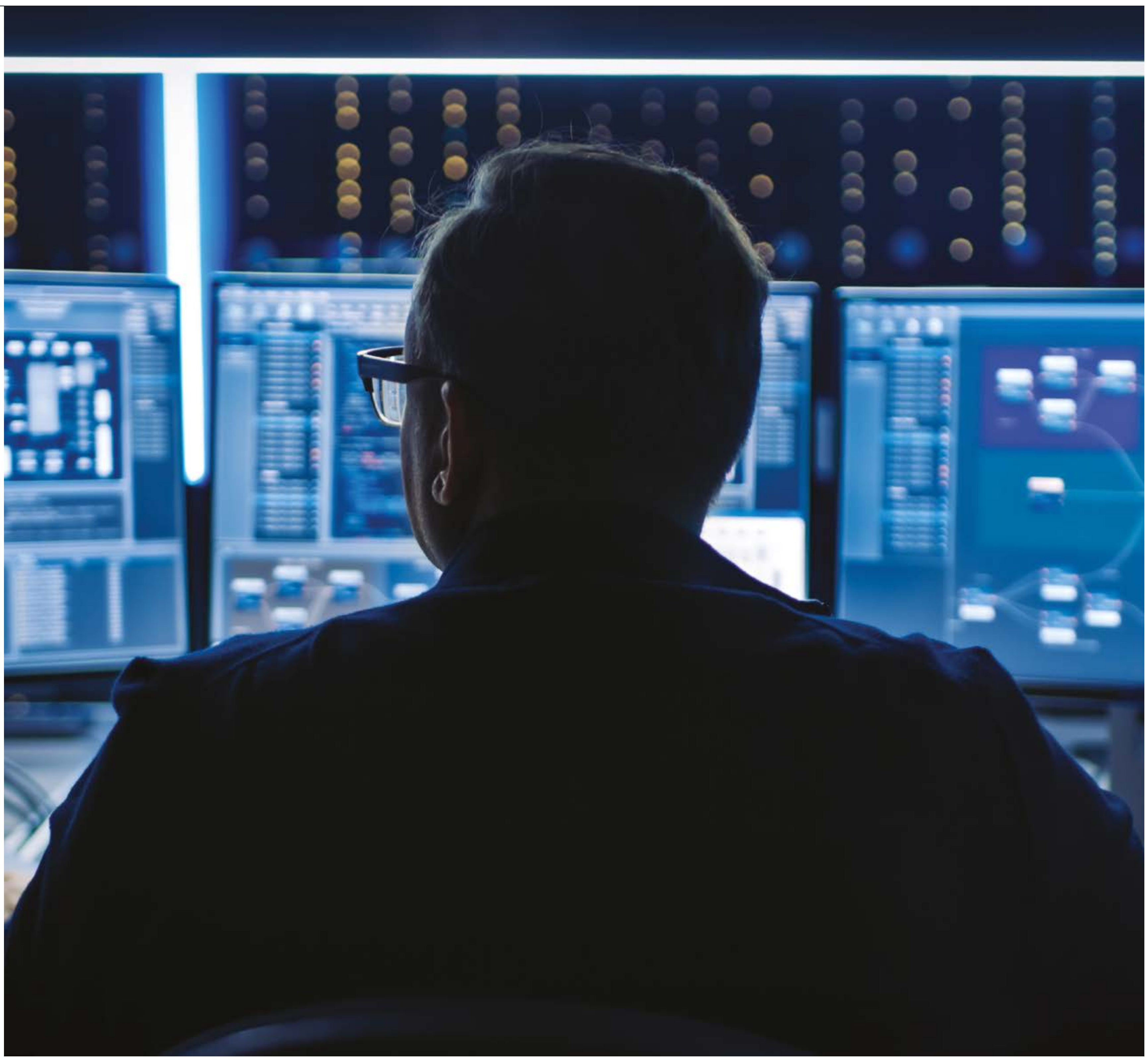
Commercial feature

Why businesses are moving to managed multi-vendor cybersecurity

Mid-market companies face evolving IT security demands as they advance digital experience, accelerate cloud connectivity and enable disparate remote operations. Given their limited time and constrained budgets, the most effective solution is to bring in managed best-of-breed setups, backed by risk transfer services



As mid-market businesses advance their cloud computing, digital transformation, and hybrid work models, significant cybersecurity challenges are emerging.

For IT departments, the most pressing demand will be to manage and operate an unprecedented array of disparate connected devices, enabling users to access applications and data from branches, stores and field locations and home-working environments. They must also ensure there is a consistent quality of experience, without compromising security.

The problem for these technology teams is they often lack the resources of IT departments in larger corporations. They also face a confusing, extensive array of options when trying to make purchase and deployment decisions. Some respond to this issue by investing in services from a single vendor. This strategy may seem appealing from a management standpoint, but it typically involves using one-size-fits-all systems with limited effectiveness. Others attempt to combine multiple advanced technologies, and become submerged in the expense and intricacy of operating them.

Moving towards insurable setups

"Traditionally, many businesses have been advised by experts to put in a single vendor solution, with the aim being to reduce the integration burden and simplify control," explains Gareth Davies, executive vice-president, managed services at Fulcrum IT Partners. "But this can be very misguided, as the vendor providing them with a firewall is not necessarily proficient at endpoint protection, for example. Moving to a single vendor also involves a significant operational transition that is costly and resource heavy."

Some businesses are instead adopting the best-of-breed approach, choosing the most effective security and business continuity services in each area to achieve the strongest possible protection. However, these systems must be both fully integrated and independently managed on an ongoing basis to keep up with new security threats.

"For many companies, this is far too complicated and costly a challenge, and they will always lag behind the threats that are out there," Davies says. With cybercrime and data breaches becoming increasingly commonplace, companies also need to consider their options for risk transfer. It is essential they put in place cyber insurance to cover financial losses associated with a cyber attack, such as legal expenses, data restoration costs and reputational damage.

However, buying cyber insurance can be a challenge in itself. As a relatively new type of cover, there are many uncertainties and complexities associated with it. Cyber risks are constantly evolving, which makes it difficult for insurers to accurately assess the potential risks and develop adequate policies. As a result, it can be difficult to find an insurer willing to take on the risks associated with a particular business, and many insurers have either backed out of the market entirely or substantially reduced their cover.

> “For companies, demonstrating robust cybersecurity practices can be so difficult that many insurers will simply refuse to provide policies

"Insurers often rely on simple questionnaires that fail to establish satisfactory insights, leading them to decide they cannot quantify the risks with enough clarity," Davies explains. "For companies, demonstrating robust cybersecurity practices is so difficult that many insurers will simply refuse to provide policies. When insurers do consider approving a client for cyber coverage, it's often not at the price point or offering the level of cover that the customer requires."

The rise of managed services

These dynamics have prompted the rise of more effective forms of managed security, which are capable of addressing the concerns of both mid-market businesses and the insurers seeking to financially protect them. These managed security providers have several core focus areas: implementing best-of-breed security from across different vendors, integrating those services, administering them, providing insights and protecting customers both operationally and financially.

Businesses are increasingly working with managed service providers like Fulcrum IT Partners to ensure they have this level of defence and financial protection.

Fulcrum IT Partners takes a comprehensive approach to protecting all aspects of its customers' cybersecurity, using the most sophisticated technologies and processes in each area, implementing them and managing them. The company also has a strong connection to the cyber-risk transfer market, which means it can demonstrate to insurers the quality and strength of its customers' security posture, enabling businesses to buy the cybersecurity coverage they need at an affordable price.

"It's incredibly challenging for businesses in the mid-market to ensure they have the right levels of protection in place, and to be sure they can recover systems quickly in the event of a breach. We work with our customers to assess their setup, advise on security choices, implement the relevant systems, and then manage the technology on an ongoing basis," Davies says. "We invest heavily to ensure our staff are fully up-to-date with the latest innovations in cybersecurity and emerging threats, so we can better protect businesses."

Secure SD-WAN in practice

One of the first steps Fulcrum IT Partners takes is to implement a managed, secure SD-WAN layer for clients. By adding this virtualised layer to their wide area networks, the businesses become more agile and can unlock cost savings in their connectivity, all while increasing security and observability.

"We offer businesses a secure SD-WAN solution called Titanium, which converges high-performance SD-WAN and virtual, next-generation firewall-security capabilities into a single managed service. This removes the complexity of managing multiple network and security point products, while delivering a secure, optimised network experience across users, devices and applications. And for many companies, this can also unlock the opportunity for some cyber risk transfer and warranty, providing additional protection and peace of mind," Davies explains.

Companies using Titanium by Fulcrum IT Partners often operate highly distributed environments, spanning multiple industries and geographies. They include IVC Evidensia, a major veterinary-care provider, whose rapid expansion had led to a complex setup. Migration to a managed, secure SD-WAN solution enabled the introduction of effective multi-layered security, reduced costs and improved application effectiveness and control. Similarly, with the help of Fulcrum IT Partners's managed secure SD-WAN service, Sense, a charity supporting people living with disabilities, was able to upgrade its network and reduce operational bottlenecks, all while strengthening and integrating advanced security.

For mid-market businesses, although there is no silver bullet to protect against the ever-growing array of cybersecurity threats, there are some highly innovative response services available. With new approaches to layering security with SD-WAN technology, backed by strong access to relevant cyber insurance, companies can protect their business operations and data from an evolving threat landscape. And they can do it in a way that is both simple and affordable.

To find out more about managed multi-vendor cybersecurity, with embedded risk transfer services, visit fulcrumtitanium.com

TITANIUM
BY FULCRUM IT PARTNERS

Q&A

The evolution of SD-WAN

The advancement of SD-WAN services has enabled effective edge security, says **Gareth Davies**, executive vice-president, managed services at Fulcrum IT Partners

Q What is driving the adoption of SD-WAN?

A Managed, secure SD-WAN is becoming increasingly popular among businesses because it can provide improved network security, scalability and flexibility. Companies gain an extra layer of protection against cyber threats, while also being able to easily scale networks as their needs change.

Until very recently, many mid-sized businesses might not have considered themselves as a target for cyber criminals, yet they often are. At the same time, the complexity of risk mitigation and product management is greater than ever. A managed secure SD-WAN service reduces this complexity by providing a unified, centrally managed platform that allows safe and reliable access to distributed applications and data across the enterprise.

Q What have been the key stages in the technology's evolution to this point?

A SD-WAN emerged as a way to deliver reliable and cost effective connectivity, but has now evolved to be an essential part of securing the edge, including for remote workers. Companies use secure SD-WAN for all forms of connectivity at all their sites, connecting users to applications, and ensuring optimal performance, uptime and resilience across the network.

SD-WAN also provides the critical foundation of secure-access service edge (SASE). This network architecture supports cloud-enabled organisations by combining SD-WAN with additional network-security features – such as zero-trust network access and automated enforcements like cloud-access security brokers and secure-web gateways – into a single cloud-based offering. It provides consistent security and access to all cloud applications, so organisations simplify management, improve visibility and maximise network protection across users, devices and applications.

Q How do you work with companies to overcome their security challenges?

A We understand that every business has its unique set of challenges and objectives. We take a consultative approach to engagement to ensure we fully understand what the challenges and desired business outcomes are, before designing and implementing a solution that supports those needs now, but is also flexible enough to support future growth opportunities.

When it comes to cybersecurity, business leaders need to ensure they have all the right levels in place. The services we provide allow companies to reduce the complexity of network and security management, so they can free up critical resources, time and energy for mission-critical pursuits.

Q How can you help IT leaders answer the important questions they get from the C-suite on cybersecurity?

A We don't believe businesses are getting the best outcomes and value from their security investments. At Fulcrum IT Partners, we aim to change that by providing a service that brings together the required expertise and best-of-breed technologies that help IT managers to implement effective protection.

This means they can also accurately report to the chief executive and the chief financial officer on cost and effectiveness. By implementing robust observability measures, organisations gain timely insights to evaluate their spending and make informed decisions on system changes, thereby optimising their operations and maximising returns. Our services are also unique in that they are backed by risk-transfer services that offer operational and financial cyber resilience.

> “We don't believe businesses are getting the best outcomes and value from their cyber security investments. We aim to change that

Q What lies ahead for companies' cybersecurity strategies?

A While threats are constantly evolving, so too is the ability to protect against them. Companies are taking smart steps to advance their security. They recognise they no longer need to be the experts in each domain or have the capacities to constantly update and advance systems. Modern IT teams have a far greater responsibility in contributing to wider business goals.

By bringing in security specialists who integrate best-of-breed solutions across their operations, backed by risk-transfer services, companies are protected against threats, mitigating the damage from breaches and positioning themselves for effective business continuity. This allows them to focus their resources on other business priorities and gives them the peace of mind that their network and data are secure.