MASTERING MICROSOFT SECURITY FOR THE MODERN WORKPLACE

How to integrate Microsoft Security into your cyber strategy

Computacenter

SECURING THE EVOLVING WORKPLACE

Today's workplace is a constantly evolving environment, with new devices, new software, new connections, and new modes of working. Whilst this evolution has brought significant benefits in employee experience, flexible and hybrid working, collaboration and ultimately more productive people, it has also created a much broader threat landscape for cyber attackers to target.

The proliferation of devices used outside of the traditional corporate perimeter is exposing additional cyber-attack points. The explosion of devices, along with the increased usage of web applications and the adoption of collaboration technology continues to generate data at unprecedented rates, and more data offers greater potential reward for attackers if they can gain access to it.

As organisations continue to exploit unlimited data resources in the cloud, leveraging hosted applications and environments across multiple devices, the increased attack surface increases the likelihood that organisations will be a victim of cyber-attacks.

With more potential for greater reward and an increasingly broad attack surface to protect, it is no surprise that securing the workplace has never been higher on the corporate agenda. Nor is it surprising that implementing effective levels of control continues to be challenging for most organisations.

THE ADVENT OF ZERO-TRUST

To address these evolving security challenges, security controls, processes and tools also need to evolve. Controls used to be applied at the corporate edge, but they are now also needed on the device, in the cloud, around data, across identities and throughout the internal network.

New architectural concepts such as zero-trust and SASE (Secure Access Service Edge) emphasise the importance of an integrated approach, with multiple security controls coming together to provide workplaces with enhanced levels of security regardless of the location of the worker, what type of device they are using, or where the data they are accessing is being held.

As organisations implement integrated solutions, they gain better visibility and control over their workplace. Data generated by security agents running on devices, allied with access controls, defined identities and data governance protocols, running alongside regular scanning and analysis makes it much easier to detect the anomalous behaviour of attackers. This also has the benefit of allowing response and remediation actions to be enacted more quickly. Integration also offers better options for AI and Automation, helping scale protection, detection and response across multiple environments and devices.

Many security vendors now offer broader portfolios that encompass a large proportion of the recommended components of a zero-trust architecture. These integrated security vendors are increasingly being seen as a solution to the security challenges facing workplace leaders.

FINDING THE RIGHT APPROACH

Finding a core of tightly integrated security solutions that covers all these areas is difficult despite the increasing depth of security vendor portfolios. Existing technology deployments, and their associated technical debt, can impact an organisation's ability to implement a more over-arching solution, resulting in partial deployments and the overhead of additional integrations.

Moving to a smaller core of overarching workplace security platforms offers undoubted benefits but does require an understanding of what technology to retain, what to remove, what and when to integrate new solutions with old, and a deep knowledge of both the new and existing vendor portfolios to ensure there is a minimum of product overlap and an effective exploitation of available licensing.

However, enabling such vendor solutions also delivers tangible value. Moving away from the legacy siloed vendor approach to a platform centric, highly consolidated landscape removes complexity, helps with cost control, enhances data exchange and ensures that gaps are minimised. All of which creates greater opportunity for automation, better visibility and ultimately improves detection of, and response to, cyber threats.

MICROSOFT SECURITY AN INTEGRATED SOLUTION

Microsoft offers integrated security solutions, helping organisations to safeguard their people, data and infrastructure using a single security platform and a single licensing model.

With Microsoft Security products it is possible for enterprise organisations to protect identities and manage access, stop threats with integrated, automated protection, secure apps and resources across the cloud, protect and govern sensitive data and identify and remediate risks.

The Microsoft security products are the result of significant, ongoing investment and are now recognised as market leading by organisations such as Gartner. Microsoft security solutions are now embedded within the broader Microsoft platform, making enablement more a matter of configuration and policy management than wholesale deployment. With solutions linking endpoint protection, identity and access management, anti-virus, data loss protection, CASB and security monitoring, the portfolio is extensive and fully integrated.

With many organisations already invested in using Microsoft 365 and Windows Operating Systems there is logic in extending the Microsoft product set to take advantage of the security solutions available with it, and in doing so deploy a truly integrated workplace security solution.

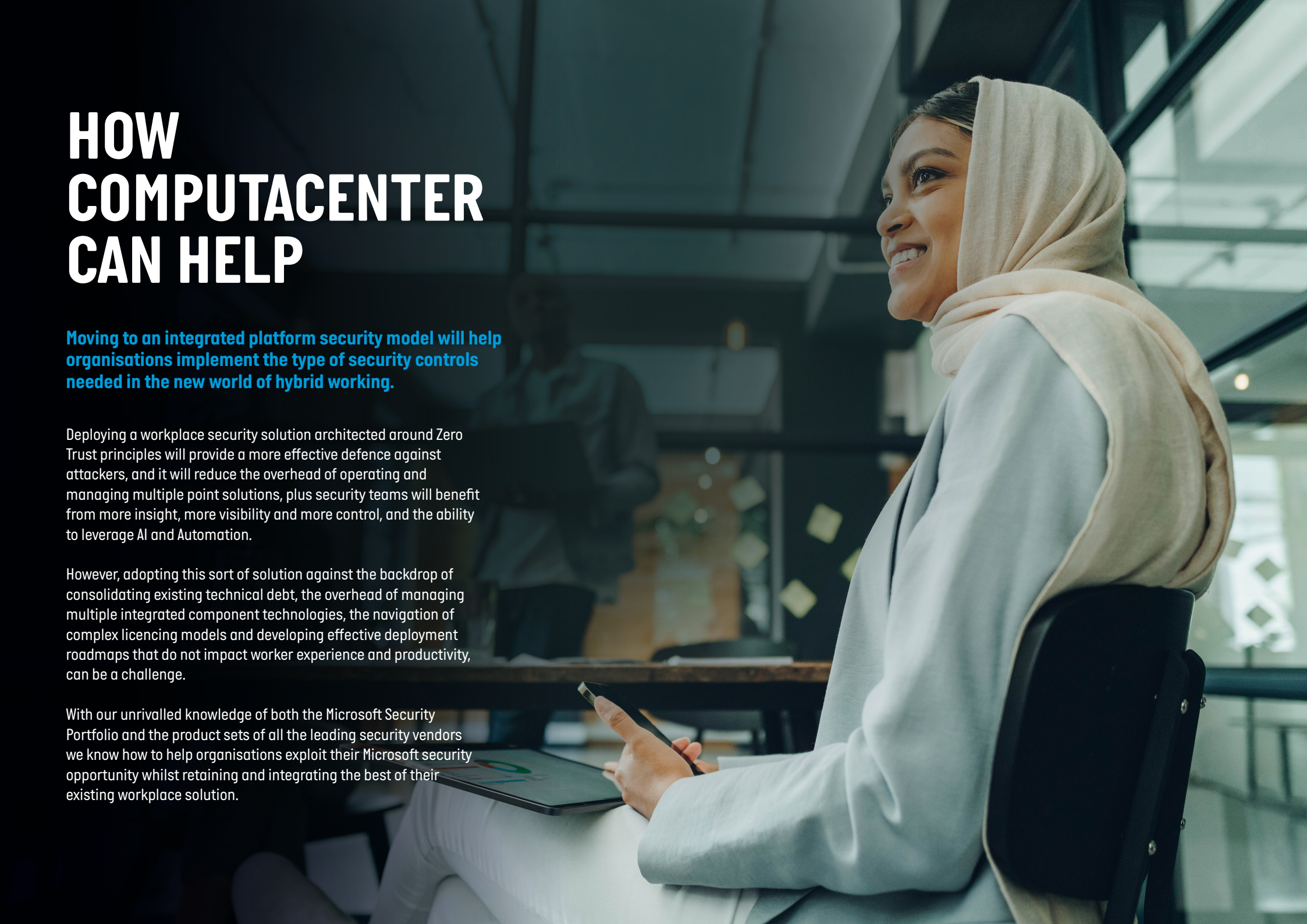
HOW COMPUTACENTER CAN HELP

Moving to an integrated platform security model will help organisations implement the type of security controls needed in the new world of hybrid working.

Deploying a workplace security solution architected around Zero Trust principles will provide a more effective defence against attackers, and it will reduce the overhead of operating and managing multiple point solutions, plus security teams will benefit from more insight, more visibility and more control, and the ability to leverage AI and Automation.

However, adopting this sort of solution against the backdrop of consolidating existing technical debt, the overhead of managing multiple integrated component technologies, the navigation of complex licencing models and developing effective deployment roadmaps that do not impact worker experience and productivity, can be a challenge.

With our unrivalled knowledge of both the Microsoft Security Portfolio and the product sets of all the leading security vendors we know how to help organisations exploit their Microsoft security opportunity whilst retaining and integrating the best of their existing workplace solution.



COMPUTACENTER AND MICROSOFT

As a preferred Microsoft partner for more than 30 years, we help organisations adopt and optimise their Microsoft investments, helping them to tackle the challenges and opportunities they face today and to plan and build their modern working future.

We have experience of serving 4.5 million users of Microsoft technologies, 1,500 Microsoft-certified technologists, a track record of managing two million activations of Microsoft Office 365 and we currently manage more than 500,000 systems running Microsoft Windows platforms.

We focus on developing strong and trusted customer relationships that we support through an expert, advisory approach to business. Whether accelerating your digital transformation; building and running cloud-based services; applying AI technologies; unlocking the potential of your people; or building rock-solid security, Computacenter and Microsoft can together help you modernise your operations and secure your long-term success.

We offer services that address the full spectrum of common challenges, these include:

CONSOLIDATION AND LICENCE EXPLOITATION ADVISORY

Our CyberLens service helps organisations understand the scale and scope of the opportunity to consolidate their workplace security around Microsoft. We can provide insight as to what is available within the Microsoft licence model, where there are overlaps with existing technology, where best to consolidate and where to retain existing solutions.

THE BENEFITS

- Clarity on licensing entitlement, current levels of utilisation, and how best to exploit it.
- Insight into where Microsoft security could be deployed to consolidate existing vendor spend.
- Understand how existing or additional vendor solutions could close any gaps in the Microsoft portfolio.

VENDOR ASSESSMENT

We can help organisations undertake a security vendor business value and consolidation assessment to help them understand how Microsoft compares to existing deployed vendors.

THE BENEFITS

- Multi-vendor assessment with Computacenter enhanced analysis of Microsoft capabilities and integration benefits
- Reduce effort and cost of standing up complex PoCs to validate Microsoft value vs other vendors.
- Enable quicker decision making as to the extent and depth of Microsoft security deployments.

SOLUTION DESIGN AND DEPLOYMENT

We offer extensive professional services to enable Microsoft Conditional Access and MFA, Defender for Identity, Defender for Cloud Apps and Purview Information protection and DLP. We help organisations migrate to Defender for Endpoint and Defender for Office 365. We also provide consultancy and professional services to support Sentinel, Entra and Privileged Access Management.

THE BENEFITS

- Access to skilled resources to supplement internal teams.
- Utilisation of proven deployment models
- Can benefit from extensive lessons learnt and experience in design, configuration and deployment.

MANAGED MICROSOFT SECURITY

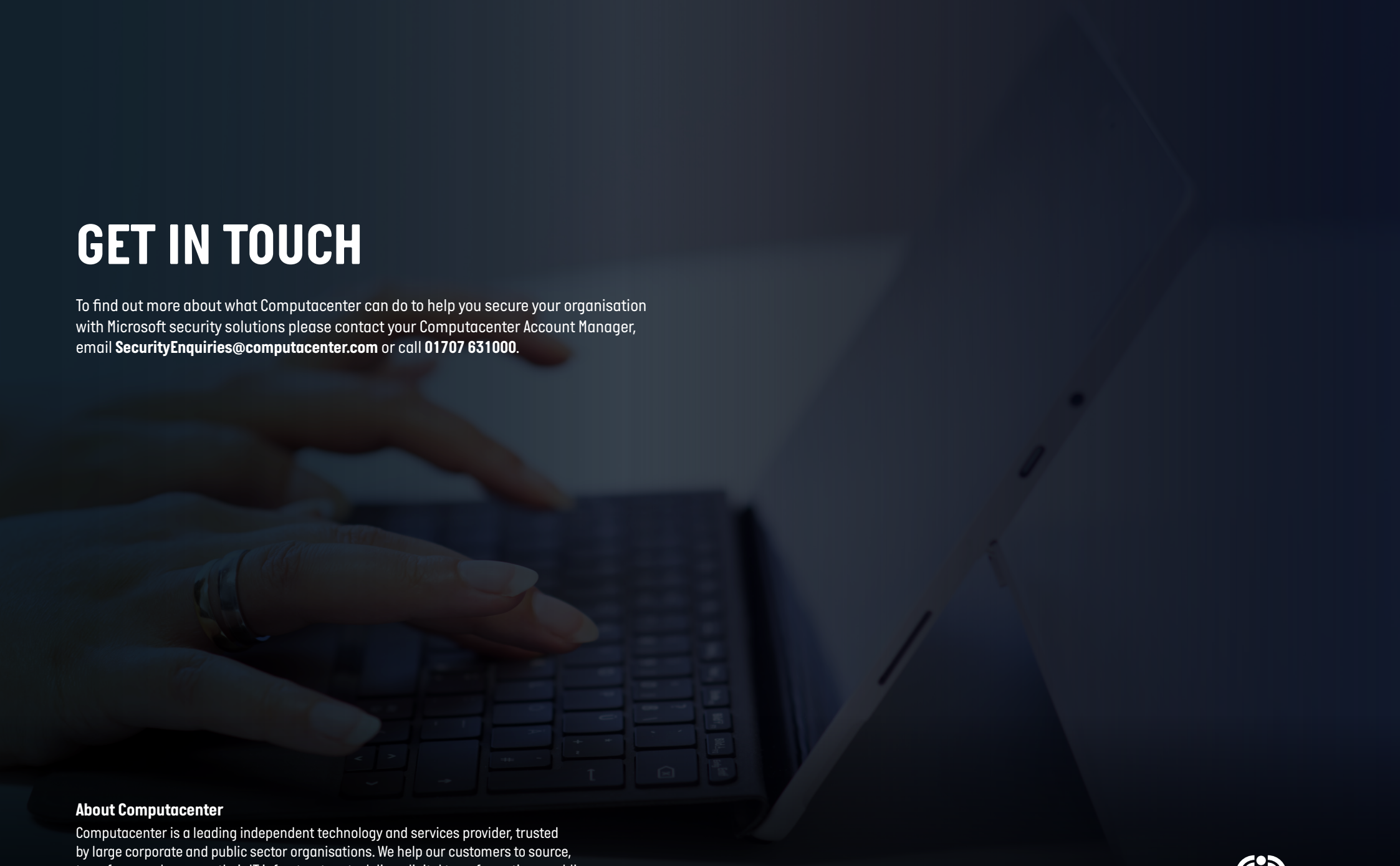
Managing and supporting the Microsoft security platform, during migration and beyond can tie up key security resources. Computacenter offers a full managed Microsoft Security platform service, which in turn enable us to offer solutions such as Anti-virus services, Managed Endpoint and Vulnerability lifecycle services, all delivered using Microsoft Security tooling.

THE BENEFITS

- Outsourcing of platform management to free up in-house resources for more strategic activities
- Access to standardized support playbooks and processes.
- Operation of key workplace security services – providing enhanced support scale and hours of operation.

GET IN TOUCH

To find out more about what Computacenter can do to help you secure your organisation with Microsoft security solutions please contact your Computacenter Account Manager, email **SecurityEnquiries@computacenter.com** or call **01707 631000**.



About Computacenter

Computacenter is a leading independent technology and services provider, trusted by large corporate and public sector organisations. We help our customers to source, transform, and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 20,000 people worldwide.

www.computacenter.com

Computacenter