Microsoft Surface
Authorised Reseller

Computacenter

# THE MANY FACES OF SECURITY

LET'S GO

# PEOPLE FIRST SECURITY

In the office. At home. On the wards. In the community. No matter where or how your people work, one thing remains constant: Your workforce sits at the heart of security.

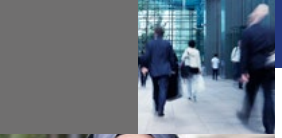
People are working in new ways. They're using digital technologies to communicate. To collaborate. To do more. And to do it faster. As organisations empower their employees with modern digital workplaces, cloud and flexible anywhere, any device business models, they must ensure that networks, data and devices are secure.

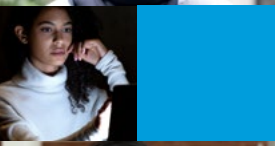
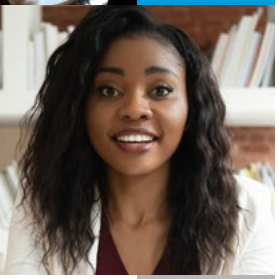
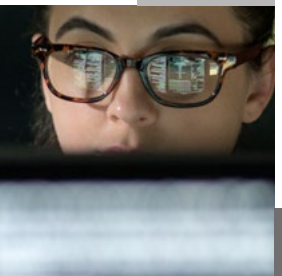
Of course, the constantly changing world in which we live and work demands ever greater levels of security. The sudden and massive shift to remote working, and the need to just keep things going, has seen many organisations implementing quick-fix solutions. These have left some vulnerable to opportunistic hackers.

Can you afford a data security breach that could cost your organisation huge reputational, operational and financial damage? Are data protection regulations proving a big headache as you respond to the massive shift to distributed working? Or perhaps more and more employees are asking to use their own devices for work, raising the prospect of employee-introduced vulnerabilities.

Your people sit at the heart of all security decisions. They're most likely to be the cause – inadvertently or not – of a data breach. They want to know that how, where and when they work doesn't pose a risk to your organisation, its data and its assets.

**In this Executive Briefing, we'll look at the steps being taken to bolster security and consider the impact on productivity of different approaches, such as a Zero Trust model. We'll describe how Computacenter and Microsoft come together to safeguard organisational assets from the core to the edge, and ask what policies, digital tools and cultural changes are needed to secure today's digital workplace.**



# BUILDING NEW DEFENCES

It's time to rebuild the castle walls. The traditional approach to security was all about the perimeter. You built your castle and dug a deep moat around it. That's all changed.

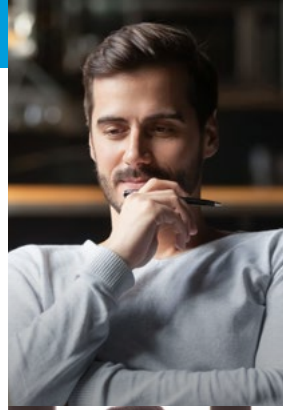
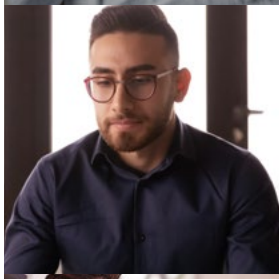
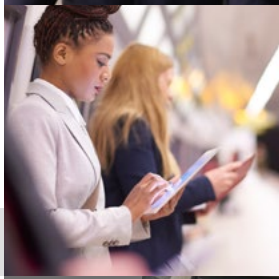
Switching off your workplace computer and leaving it all behind at the end of the day seems outmoded in today's distributed workplace. People have been taking their work home with them, working remotely on network-connected mobile devices, and accessing corporate assets on the move for several years.

It is true that the global COVID-19 pandemic accelerated the uptake of remote working, but it was always going to happen. So, it's time to rethink and reshape the security strategy you've had in the past.

## Zero Trust

Many of the conversations Computacenter is having with customers nowadays are about a Zero Trust approach. This is a big change in the way organisations are addressing security concerns. Security follows the data, from within the enterprise and out to whatever device it is consumed on.

The concept of Zero Trust is predicated on a person's identity, device and location. Their level of access to data is derived from these three components. As companies became better at building more defensive perimeter walls, so we began to see a lot of social engineering, with cybercriminals tricking people to give away their information. This meant the criminals could use an employee's credentials to access the organisation internally. Zero Trust is a response to this. Trust nothing. Assume a breach. Prove everything.


## Distributed working

While the move to working-from-home was already under way, there's no doubt that when COVID-19 hit, people didn't have the security they should have. Business continuity plans did not consider that employees wouldn't have an office to go to. Or that they would need to access corporate networks and assets – fast – from outside the traditional perimeter. And while you can enforce security measures in an office environment, you can't always dictate what people do in their at-home office spaces.

This increases the risk level and has led to a rise in the use of multi-factor authentication (MFA) as part of the Zero Trust story. Machine learning and artificial intelligence (AI) within MFA solutions enable us to understand how people work. Do they typically travel to a certain region or use specific apps? Have they sought access to documentation they wouldn't ordinarily use? What data do they have clearance to download – and onto what device? MFA puts protection around an organisation's data assets, coupled with conditional access.

## Compliance

When we talk about security and protecting the enterprise, it is often from the perspective of external threat actors and viruses. However, any security conversation should also include compliance as a core element of the risks posed. The cost of non-compliance with data security regulations can run into millions, which has the potential to shut down a business.

Data Loss Prevention (DLP) capabilities must now be part and parcel of a compliant data security strategy, with education spelling out why policies are there and how to comply. This brings us back to our earlier statement that your people must sit at the heart of your security decisions.

**Microsoft Teams supports more than 90 regulatory standards and laws, including HIPAA, GDPR, FedRAMP, SOC, and Family Educational Rights and Privacy Act (FERPA).**

# PEOPLE. POLICY. PROTECTION.

In adopting Zero Trust models, enabling distributed working, and ensuring compliance, your data security policy is business critical.

Yes, you can encrypt everything possible, but if your workforce doesn't understand why, how and the part they need to play, then your security could fail. And your compliance with it.

A Data Protection Officer (DPO), or equivalent within the organisation, will be responsible for ensuring that the policy is in play. But it's not a standalone responsibility. The DPO should work with your compliance team, HR and IT to define and enforce the policy.

**User first**

A poor employee experience is often the reason security falls down. If adhering to the policy is too hard – or seen to be too hard – people will ignore it. And if they don't understand why a restriction is in place, they will often find a way round it.

The key is to adopt an approach of proportional security, whereby you make it easy, but do not compromise. Do as much as is necessary, without stopping people working.

A simple example of this is a security policy that forbids the use of USB sticks. What impact might this have on the experience of employees needing to move data from A to B? In many cases we see them using shadow IT, such as unsecured file storage in the cloud. This can be open publicly to the internet. Security in this instance is ad hoc and the protection poor. It also raises the risk of regulatory non-compliance if the data held in unsanctioned cloud storage isn't discoverable by the organisation.

## Weakest link

What's needed is a security policy that offers proportional and frictionless security. One that puts users at the heart of security, while finding a balance between the employee need for productivity and the organisation's need to keep everything secure.

That same approach to security must take account of the fact that people can be the weakest link. Whether it's a disgruntled employee intent on causing damage, or someone who's left their work tablet on the train, it's important to pre-empt these possibilities. And the best place to start is with a sound understanding of what your people do, day in, day out.

At Computacenter, we use our Workstyle Analysis service to match the right security controls to the right users, ensuring they remain both protected and productive. Essentially, this takes away the option for non-compliance. How? By understanding what data and systems people need access to in order to do their jobs. Then, if something shouldn't happen for a specific persona, it can be prevented from doing so.

## Technology-led security

Microsoft's approach to mitigating risks is to simplify things. For example, automation tools within Microsoft 365 offer simple prompts to help people comply with policy at certain moments, such as when they're sending an email containing credit card numbers. In this instance, they might receive an automated 'are you sure?' or 'seek approval' message and, depending on the policy's parameters, they could be blocked from sending the email altogether.

It's interesting to note that Microsoft has enabled tens of thousands of its own employees to work securely from home during the COVID-19 outbreak with a Zero Trust model and multi-factor authentication (amongst other security tools and approaches). So, even if someone's credentials have been hacked, the security layers will stop the hacker accessing files, applications and more that are not within the employee's role.

# LIFE ON THE EDGE

As workforce mobility dismantles traditional perimeter defences, the number of entry points vulnerable to attack will increase.

This demands end-to-end security that extends from the core data center to the ever-expanding edge of devices, users and locations from where data can be accessed. But this security can't simply be quickly bolted on. Rather it should be built in as part of a holistic three-step approach:

1. **Protect**
2. **Detect**
3. **Respond**

### Step 1: Protect

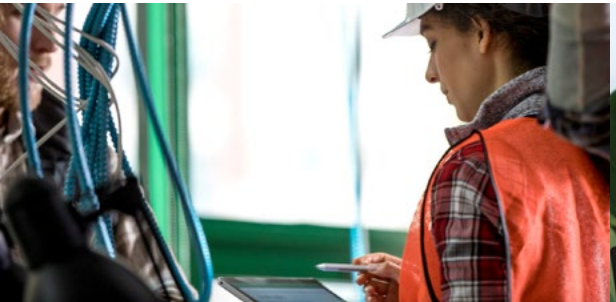
CIOs and other C-suite enterprise executives are under pressure to deliver a new, more resilient workplace strategy. This has been accelerated to the top of the corporate agenda by the COVID-19 pandemic. In a distributed working environment, resilience goes hand-in-hand with the need to protect corporate assets, data and networks.

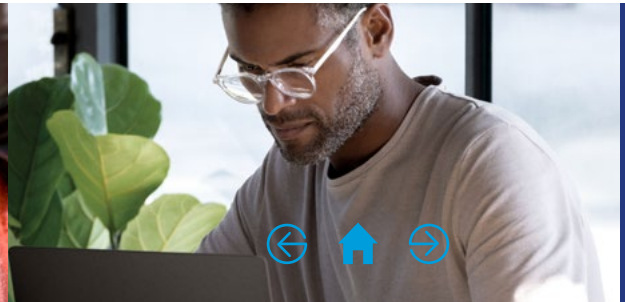
Tools such as those in the Microsoft 365 Defender suite are part of the modern 'protect' toolkit. It is built into the Microsoft 365 services and helps with attack surface reduction – the first line of defence – across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

### Step 2: Detect

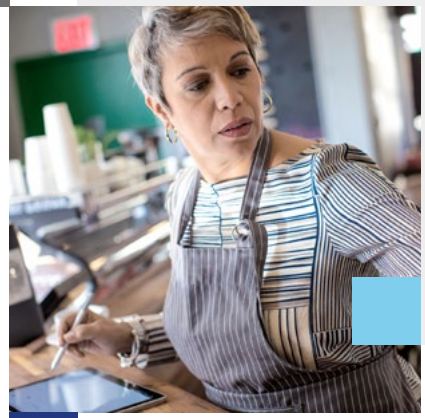
Every organisation will be breached, no matter how strong its security. For example, one source suggests that in the first quarter of 2020, exposed records increased at a pace of 273 per cent over last year.

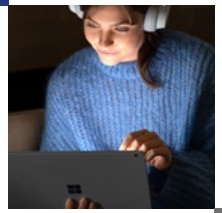
Attackers don't stay still. They move around once they've breached your defences to find weak points of entry deeper into the system. Monitoring via a coordinated security operations center (SOC) enables security teams to track what is happening. A SOC can monitor network traffic and manage detected events. Behavioural analytics are also part of the 'detect' toolkit, collecting logs and alerts from data sources and identifying anomalous activity against a behavioural baseline.





**Microsoft processes more than 8 trillion security signals every day and uses them to proactively protect against security threats. Data is encrypted in transit and at rest, stored in a secure network of datacenters.**





### Step 3: Respond

As the threat landscape continues to evolve and become more sophisticated, technology and policies must keep up to ensure an effective response. Microsoft invests $1 billion a year on security capabilities and always has exciting developments in the pipeline. Its automated playbooks are a case in point. These will activate when a breach is detected to isolate the threat, remediate the exposure where possible, and flag to the security team for further investigation and action as needed

In today's global business landscape, an integrated approach to threats supports a simultaneous response across regions. This is increasingly being enabled by cloud connectivity and informed by data.

### Data-rich insights

A modern approach to security management embeds data and analytics across all three 'protect, detect, respond' steps. Microsoft leads the way in using data in the cloud, aggregating it in a single place to provide insights that support a holistic, enterprise-wide approach to threats.

At Computacenter, we draw on our workplace expertise and Microsoft technology capabilities to guide our customers' security choices. For example, we might recommend Microsoft Secure Score, which provides a view on your security posture and identifies areas in need of improvement.

# MODERN MOBILITY

A modern, user-centric workplace is enabled by mobility. Employees are no longer tied to the office – and never more so than in 2020.

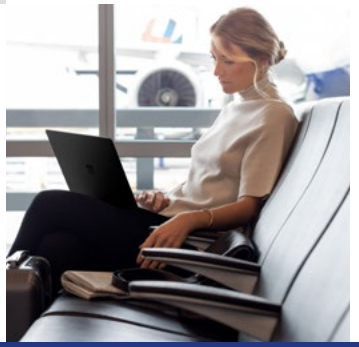
Mobile device management (MDM) strategies for the workplace need to reflect how we communicate in our personal lives. Indeed, there are early signs of this shift being underway. Consumer and enterprise mobility are beginning to converge as we see a blending of work and home life, with employees increasingly using the same device for both.

Securing and improving control of this evolving mobile estate is a constant challenge. You need to support different provisioning models, from bring your own device (BYOD) and corporate owned, personally enabled (COPE), to choose your own device (CYOD).

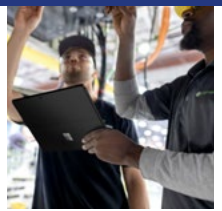
At the same time, 'how' you secure these devices must become more user friendly to ensure compliance with security policies. Single Sign On (SSO) is a good example of this and can play a significant role in avoiding employee-introduced vulnerabilities.

Biometric authentication is another great tool. It reflects a trend in the consumer world that began with fingerprint recognition. For enterprise mobility, swapping difficult to remember passwords for biometric forms of identification means there are no codes to remember (or forget!) and the authenticating mode is harder to replicate, making everything more secure.

Computacenter's heritage in mobile IT and MDM combined with Microsoft's commitment to enterprise security give Chief Information Security Officers and other IT leaders the assurance they need to invest in modern mobility. It's a global partnership focused on enabling people to work securely – wherever that work is.



**Microsoft detects 5 billion threats on devices every month and analyses 470 billion emails per year.**



# CLOSE THE GAP

There is no permanently right answer to securing the many faces of work. That's because the threats are moving at such a rapid rate.

The key is to keep on top of this evolving landscape. Do the basics because the longer you leave it, the harder it will be to close the security gap. It's not just about leveraging the best security tools, but ensuring your people know why and how to use them.

With the Microsoft operating system more closely related to the hardware than ever before, it is easier to extend security from the core to the edge of your enterprise. Computacenter works with Microsoft to bring together this technology in user-centric solutions for a secure digital workplace.

## BUILD YOUR DEFENCES

**Security and IT leaders must work with the business to ask – and answer – a set of important questions that will guide how they limit security risks and build solid defences:**

**Do you truly know your employees?**

What data, systems and applications do your employees need access to – when and from where? A Workstyle Analysis from Computacenter helps to build this knowledge, enabling you to define role-based levels of access that are also proportionate to your enterprise data and assets.

**Do your employees understand the importance of security?**

If they're not aware of the risks posed by a security breach – data loss, reputational damage, financial loss and penalties for non-compliance – your employees are unlikely to take security seriously. Education and policy are crucial.

**Is employee experience a fundamental part of your security?**

Employees have different expectations of their workplace, from flexible working to mobility and device choice. It is important to understand what these are and to build this into your secure workplace.

**Is the employee experience frictionless?**

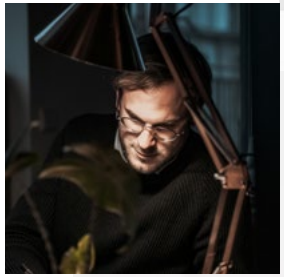
The easier it is to comply with the security policy, the stronger your defences will be. It's all about the user experience. Make it easy and your employees won't feel that policy compliance is a chore.

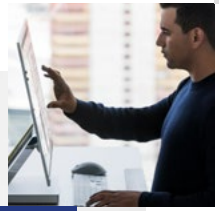
**Is your security policy appropriate and proportionate?**

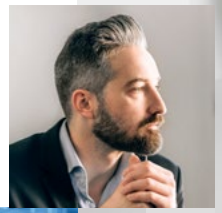
Define security parameters that are proportionate to the task in hand. Some people won't need certain tools that others must have. For example, employees that update public-facing services will have a different security posture to the CEO and colleagues with access to customer data.

**Do your technology choices enhance security?**

It makes sense to select technology from vendors that are committed to confidential computing. Devices like Microsoft Surface that are managed through the cloud, can be easily secured from a central control point. A solution such as Microsoft Endpoint Defender protects all endpoints, whether they are Windows or others, such as iOS, Android, and Linux.







## Integrated security strategies

At Computacenter, we know that users, data and devices are dispersed across multiple locations and geographies, making IT environments ever more complex and expensive to secure. This means that today's digital workplace is also more vulnerable to attack.

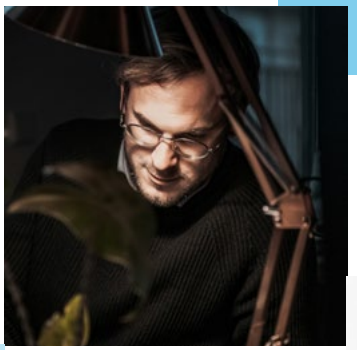
Working with Microsoft, we help our customers adopt complete and integrated security strategies that mitigate significant risk to their businesses and reputation. With a truly end-to-end approach, from the core to the edge, we help to secure the modern workplace and its many faces of work.

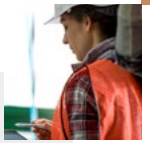
# GET IN TOUCH

For more information about Computacenter's partnership with Microsoft and how it helps to accelerate business in a hybrid IT landscape, please contact your Computacenter Account Manager, call 01707 631000 or email enquiries@computacenter.com.

Visit our website to find out more about how Digital Me solutions from Computacenter are already helping to empower, equip and assist our customers' teams.

Learn more **here**

**About Computacenter**

Computacenter is a leading independent technology partner, 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 16,000 people worldwide.

**www.computacenter.com**

Microsoft Surface
Authorised Reseller

Computacenter