CDW AND MICROSOFT: ENABLING SECURE REMOTE WORKING

Gold
Microsoft Partner
Azure Expert MSP
Microsoft

Microsoft
Surface
Authorised Reseller

CDW PEOPLE WHO GET IT

Remote working is a way of life for most of us today. Moving forward, this is unlikely to change as more than seven out of 10 UK employees and managers say they want to continue working from home at least part-time in the future.[1]

Technology is not only enabling but driving this transition. Workers expect to be able to do their jobs remotely as efficiently and productively as they would in the office or on-site. This is intrinsically linked to the user experience – employees having the familiarity of their office desktop, and the ability to access all the applications and data they need at the click of a button.

However, with remote working becoming the norm, security has never been more important. The urgency associated with rolling out remote workforces has in some cases led to an increased risk of cyber attacks. Further, security officials have warned that a growing number of cyber criminals are exploiting people's fears over the global health crisis, targeting them with a range of ransomware and malware as they work from home.[2]

These gaps in traditional cyber defences, combined with changing work patterns and employee behaviour, make it more difficult to spot potentially devastating attacks.

Why security is a priority for remote working[3]

23% of UK firms says cybersecurity incidents have increased since transitioning to remote work – with some tracking as many as double the number of incidents

81% currently view security as an essential function

47% of security pros have been taken off some or all their duties to assist with other IT-related tasks, such as equipping a mobile workforce

15% indicate their information security teams do not have the resources they need to support a remote workforce

41% say their organisations are utilising best practices to secure their remote workforce, while another 50 percent agreed, but admitted they could be doing more

Microsoft and CDW: Enabling secure collaboration

Microsoft is fuelling collaboration, efficiency and productivity for workers with its cloud-based platforms. Microsoft 365 ensures that all employees, whether working from home or in the office, can continue to collaborate seamlessly, securely – and safely.

However, at CDW we understand it can be difficult to keep track of devices and applications that employees may use at home. We can help you manage your devices and apps, while ensuring your collaboration tools don't put your organisation at risk.

For example, Microsoft Cloud App Security can help you detect the apps that employees use, and you can even be alerted when new cloud apps are introduced. In addition, the security features of Intune and the Microsoft 365 suite will also allow you to manage user applications and devices, so you can reduce the impact of shadow IT.

Elsewhere, the use of Windows Virtual Desktop (WVD) tripled in the first quarter of 2020 as organisations deployed virtual desktops and apps on Microsoft Azure to enable secure remote work.

A fully cloud-native platform, WVD is a comprehensive desktop and app virtualisation service running in Azure. It can run over a thin client, desktop or laptop, from wherever there is internet access. This means team members are not constrained by device type or location and can communicate and collaborate as easily as in person.

WVD is the only virtual desktop that delivers simplified management, multi-session Windows 10, optimisations for Office 365, and support for Remote Desktop Services (RDS) environments. This means that users can still have the full Windows 10 desktop experience that they would in the office, while working remotely.

Security made simple

A significant aspect of securing the modern workplace is ensuring that remote working is easy it is to set up and manage. The experience should be as simple as if the user were in the office or on-site.

This has been difficult to accomplish in the past, with remote workers usually having to use a combination of VPN and firewalls to access their applications and data, which could be an awkward and time-consuming experience.

However, with WVD, the infrastructure is delivered by Microsoft via the Platform as a Service (PaaS) model, contributing to a significant reduction in costly admin overhead, maintenance and integration requirements. Existing Microsoft 365 customers may even be eligible to utilise WVD at no extra cost, based on their licence, therefore only paying for their consumption in the cloud.

Also, removing a large chunk of the complexity usually associated with the application of desktop delivery – the front-end components – frees up valuable time and resources for the IT team. And with Microsoft managing the service in Azure, all updates and maintenance are handled automatically.

Regarding security, users can just log into the client, with their admittance to that environment dictated by role-based access. This means organisations can establish different levels of access for different employees. There is also conditional access wrapped around that, auditing compliance that provides information as to who is logged in and has accessed what, as well as multi-factor authentication (MFA) at the front end, confirming user credentials.

CDW: Enabling security and industry compliance

Security and compliance were top of the list of requirements for one occupational health services provider deploying WVD.

The firm wanted to enable a remote workforce and establish a better framework for managing cloud services. The company's software development team – which was dispersed around the globe – needed to access their development environments, while adhering to strict healthcare industry compliance requirements.

As such, CDW rolled out one standard WVD user deployment, and a separate, additional deployment based on the developers' requirements. CDW established hierarchical management groups in the cloud, using a privileged access model to govern three main areas: a sandbox environment for experimentation, a test area with greater controls and a production area that is locked down.

This encouraged innovation within the organisation, improved clarity of management and reduced the risk of non-compliance and unwarranted access that could disrupt vital business services.

Moreover, as part of a Microsoft 365 E5 licence, the deployment was wrapped in additional security layers, such as conditional access and MFA, as highlighted above. The example also shows how CDW can leverage our global presence to support customers both locally and internationally as needed.

Built-in security in Azure

Microsoft makes a huge investment – more than $1 billion annually – on securing its cloud platform, using a range of physical, infrastructure and operational controls. These include:

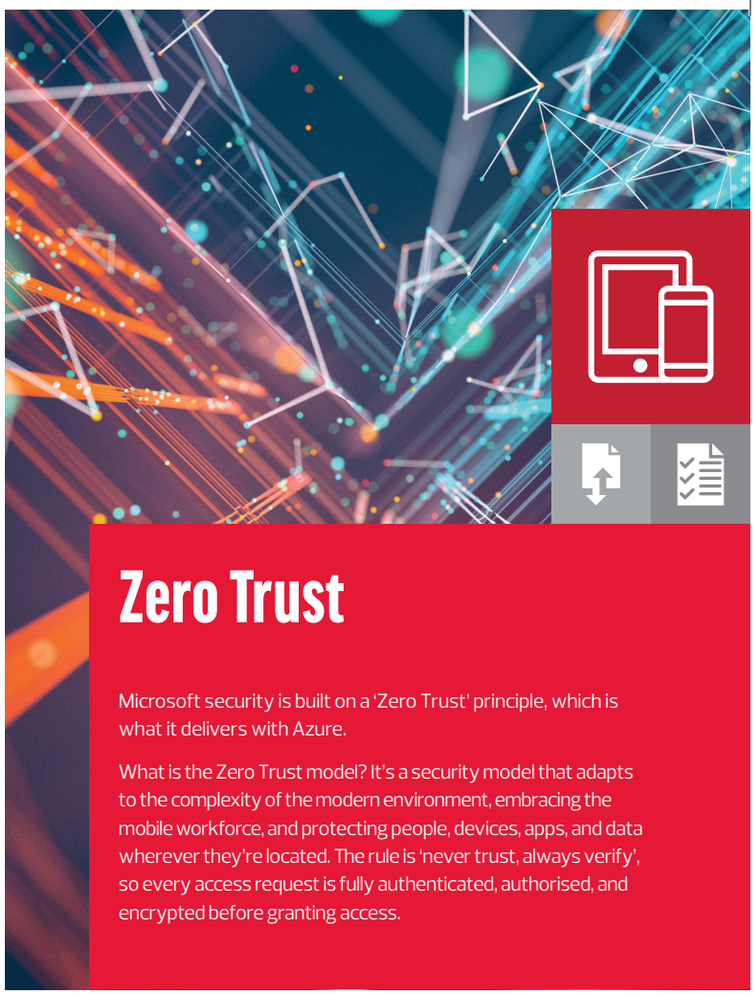
- Application network security groups to configure network security as a natural extension of an application's structure, and group virtual machines and define network security policies based on those groups.
- Azure Secure Score to assess and visualise the security state of the customer's resources in Azure, on-premise and in other clouds.
- Security Center, which is a tool for security posture management and threat protection. As part of this, Azure Defender can help protect hybrid cloud workloads including servers, data, storage, containers and IoT.
- Also part of Security Center, AI and automation can quickly identify threats, streamline threat investigation and help automate remediation.
- Azure Advisor is a personalised AI cloud consultant that advises on best practices to optimise any Azure deployments and enhance security.
- Azure Blueprints offer templates for quick, repeatable creation of fully governed cloud subscriptions.

CDW specialist security architects

There are additional actions CDW takes to help safeguard the customer's workloads to protect them from data loss, cyberattacks or non-compliance. CDW has trained and certified specialists in modern workplace technologies such as WVD, and can help customers understand the shared responsibility that comes with securing their data and applications within Microsoft Azure.

We also have a team of trained and certified practitioners who can provide technical and real-world guidance to support customers' more complex or in-depth security requirements. These include 18 individuals who hold 35 Microsoft security certifications. These dedicated architects aren't just confined to the cloud – their knowledge and expertise stretches across private and public cloud, on-premise, or a combination of all of them, with the capability to support the full user environment.

If a customer needs to secure their data in compliance within industry regulations, or geographical boundaries, CDW has that knowledge and security clearance to help the customer meet their success criteria in those areas. Our expertise also isn't confined to Microsoft; as a technology-agnostic company, CDW can secure the entire environment, across the customer's entire solution stack.



Zero Trust

Microsoft security is built on a 'Zero Trust' principle, which is what it delivers with Azure.

What is the Zero Trust model? It's a security model that adapts to the complexity of the modern environment, embracing the mobile workforce, and protecting people, devices, apps, and data wherever they're located. The rule is 'never trust, always verify', so every access request is fully authenticated, authorised, and encrypted before granting access.

Security by Design

CDW ensures that security is baked-in to every part of the customer's journey.

"CDW ensures that security is woven into the conversation with the customer from the beginning. This means security remains a priority from the architectural and design stage,"
– CDW Azure Solution Architect

Post-deployment, CDW has a Health Check service that ensures our customers are fully optimising their cloud environment. This offers customers the opportunity to spot inefficiencies, reduce complexity and identify any security vulnerabilities, to help them reduce costs and maximise performance.

[1] https://news.microsoft.com/en-gb/2020/09/08/for-remote-working-to-be-a-success-the-first-thing-we-need-to-change-is-how-we-think-about-it/
[2] https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update
[3] https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/04/28/ISC2-Survey-Finds-Cybersecurity-Professionals-Being-Repurposed-During-COVID-19-Pandemic

WVD managed service

We saw earlier how stretched IT teams have been with the shift to remote working, exacerbated by security specialists being repurposed into other roles. CDW offers a WVD managed service that takes the heavy lifting away from your organisation, freeing up IT to concentrate on the accelerated digital transformation projects many are undertaking.

In addition, Microsoft has awarded CDW the **Azure Expert MSP accreditation**. This means we are one of a handful of companies recognised by Microsoft as going above and beyond to demonstrate the highest degree of knowledge, skill, services capabilities and focus on customer service at a global level. Ultimately, providing you with best-in-class cloud migration services. These include planning and discovery, server and application assessment, developing a migration plan, building out the Azure environment to support this plan, Infrastructure as a Service (IaaS) migration, and tenant-to-tenant migration.

Soon, 'home working' is likely to be shortened to just 'working', meaning IT teams need to provide employees with technology that is a perfect fit to enable them log on from anywhere, securely and safely. Email us here, or speak to your Account Manager today about how CDW can ensure your remote workforce remains secure, on the right device, regardless of location.

CONTACT
+44 207 7916000
CloudServices@uk.cdw.com
uk.cdw.com

Gold Microsoft Partner
Azure Expert MSP
Microsoft

Microsoft Surface
Authorised Reseller

CDW PEOPLE WHO GET IT