Windows 365

Zero Trust

Four Ways to Better Secure Your Hybrid Workplace

Bringing Zero Trust to your digital environment

Whether your organization is fully in-office, remote, or somewhere in between, creating a secure digital environment is critical. For flexible, agile workplaces, the solution needs to be secure from any access point, including both in-office and remote environments. To simplify this effort, organizations should consider a comprehensive solution that creates a secure and collaborative experience for employees no matter how and where they choose to work.

Overcoming the security and productivity challenges associated with the flexible workplace are made possible by adopting an endpoint solution and management strategy that adheres to a Zero Trust security posture. Microsoft technology is anchored in Zero Trust, making it robust and agile enough to secure your IT infrastructure, regardless of environment.

What is Zero Trust?[2]

A proactive security model.

Zero Trust treats every attempt at access, regardless of identity or endpoint, as though it's coming from an open network. That means every access request must be verified before it can be approved.

Like the name suggests, Zero Trust teaches us to "never trust, always verify."

The result is a secure framework that protects against and prevents bad actors who seek to take advantage of security vulnerabilities that could arise from identities and endpoints existing outside a traditional work environment.

Now, so much about how technology interacts with the world is rapidly changing.

Many organizations are still on a journey toward Zero Trust to help ensure they have a proactive security model that addresses the unique risks that stem from hybrid work. Often, a threat might have been detected first and IT took steps to mitigate and eliminate the risk before shoring up the system's defenses against future threats.

Now, so much about how technology interacts with the world is rapidly changing: how and where employees do their work, how data is shared and stored, how regulations and compliance laws are defined, and the constant refinement of privacy laws. Reactive security techniques are simply no longer fast enough or sufficient for a workplace that includes a wide range of diverse endpoints.

Designed to be our most secure operating system yet and anchored in Zero Trust, Windows 11 integrates directly with your existing Microsoft infrastructure to deliver a productive Windows experience—with protection extending from the cloud all the way down to the physical device it's installed on.

Accessible from any device, anywhere, Windows 365 streams the Windows experience to Windows 365 Cloud PCs. A software as a service (SaaS) solution rooted in Zero Trust, Windows 365 makes it easier than ever to ensure all your employees have safe, reliable access to the tools and data they work with every day.

By deploying and managing endpoints of all kinds with Microsoft Intune and Microsoft Intune Suite, organizations can effectively secure their data regardless of device location or type. The combination of these Microsoft products enables organizations to quickly scale computing resources to meet the changing needs of their employees.

Here are four ways Zero Trust enables a more secure IT infrastructure for your flexible workforce

01

Mitigate **endpoint security** risks

→

02

Close security gaps to improve **regulatory compliance** and IP protection

→

03

Reduce password risks with multifactor authentication

→

04

Maintain business continuity with effective disaster recovery

→

Mitigate Endpoint Security Risks

A growing use of personal devices increases security risks

Flexible work continues to drive an increase in the diversity of enterprise-owned and personal devices used to access corporate resources. With the rise of Bring Your Own PC (BYOPC) policies, it's not uncommon to have a higher number of both company-owned and personal endpoints accessing your business's data and network. On top of that, personal PCs are harder to safeguard than company-provided hardware.

Even if your employees use company devices, their home networks are typically less secure and reliable than what you can provide in-office. This proliferation of endpoints exposes organizations to additional security risks that may be mitigated by adopting a Zero Trust security posture.

What is BYOPC?
Bring Your Own PC, or BYOPC, is a deployment strategy that provides employees the flexibility to access corporate applications, services, and data from the device of their choice.

Endpoints can become a further risk in scenarios with high turnover or a sudden influx of employees, like with temporary and contract workers or through mergers and acquisitions. Employees in both situations need to be able to onboard as quickly as possible without jeopardizing the security of the data they need to access.

Cloud PCs are a solution to the risk posed by the multitude of endpoints attached to hybrid work. Cloud PCs grant users access to your organization's network from any device they use, without requiring any additional security on that device. In other words, employees store their apps and data in the Microsoft Cloud, reducing the risk of data loss and the threat of a ransomware attack.

Business leaders cited home internet security and leakage of sensitive company data among their top security challenges.[3]

Cloud PCs deliver secure access to company resources

Windows 365 delivers a Windows experience from the Microsoft Cloud to a Cloud PC, and because it's built as a SaaS solution, it includes security and management features designed for endpoint admins. Unlike virtual desktop infrastructure (VDI) or desktop as a service (DaaS), Windows 365 doesn't require specialized skillsets to quickly get it up and running for your employees.

Windows 365 enables your organization to access Windows 11 Enterprise—the most advanced and secure operating system from Microsoft to date—no matter what devices your employees use.

This is because endpoint management for Windows 365 Enterprise is done seamlessly through Microsoft Intune, a simple, holistic management solution that allows your IT administrators to manage both physical and Cloud PCs side by side without requiring additional expertise to implement.

Microsoft Cloud endpoint solutions

Which solution is right for you?

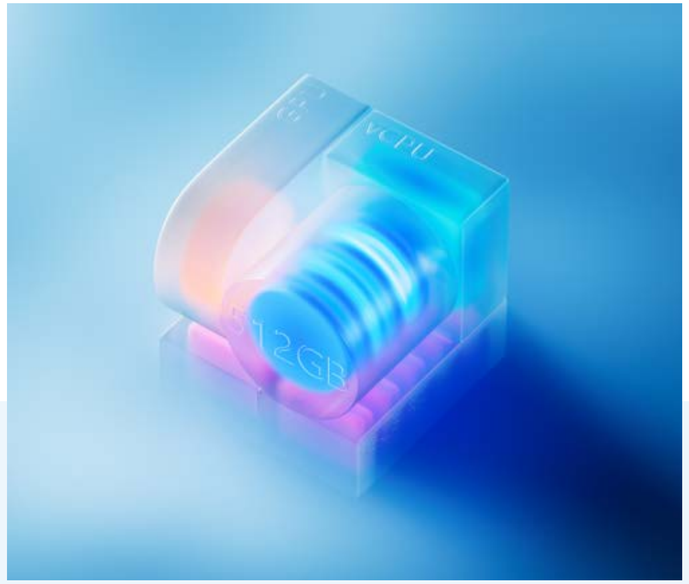
Windows 365 and Azure Virtual Desktop are built on top of Azure and can deliver a secure Windows experience from anywhere. Deploy them side-by-side or individually depending on your organization's needs.

Windows 365

A SaaS solution known for simplicity of use and fast deployment that delivers the Windows experience on a Cloud PC streamed to any device. Scale as needed to meet the requirements of your evolving workforce.

Azure Virtual Desktop

A cloud VDI platform that allows users to access their desktop and applications from almost anywhere. Good for organizations with IT resources equipped to configure, deploy, and manage the solution.



Learn more about Azure Virtual Desktop →

Gain better visibility across your organization and achieve unified endpoint management

Microsoft Intune and Microsoft Intune Suite simplify endpoint management, helping make Windows 365 and Windows 11 productive, secure solutions for both users and IT teams.

Microsoft Intune

Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management, rooted in the Zero Trust security model with built-in device compliance and reporting features.

Cross-platform
Manage on-premises, cloud, mobile, desktop, and virtual endpoints across all platforms and operating systems

Built-in Security
Automatically detect and remediate threats

Mobile Application Management (MAM)
Provide workers a flexible, non-intrusive experience that protects data without requiring mobile device enrollment

Specialty Shared Devices
Support the diverse needs of frontline workers with shared device mode, maintenance windows, and specialty device management

Microsoft Intune Suite

Intune Suite adds additional advanced capabilities beyond Intune's core offering:

Remote Help
Enable secure, cloud-based connections between helpdesk and users

Endpoint Privilege Management
Allow standard users to perform tasks that normally require an administrator, such as password reset

Advanced Endpoint Analytics
Help IT administrators understand, anticipate, and improve end-user experiences

Enterprise Application Management
Deploy, configure, update, and manage applications across all managed endpoints within your organization

Managed Public Key Infrastructure (PKI)
Establish and manage a secure infrastructure for digital certificates within your organization

Tunnel for Mobile Application Management (MAM)
Remove the need for device enrollment through a lightweight VPN solution for iOS and Android

Close Security Gaps to Improve Regulatory Compliance and IP Protection

Maintain compliance with policies and regulations

Each industry has specific requirements it must meet to protect data and privacy. In the same vein, each business has to ensure its intellectual property is safeguarded. Data protection regulations and privacy laws can change quickly, and IT teams need to be ready to adapt as soon as new policies go into effect.

Compliance can also lend itself to innovation. When policies dictate a change in the way data is protected, shared, and stored, it encourages companies to come up with new ways to serve their customers while adhering to those rules.

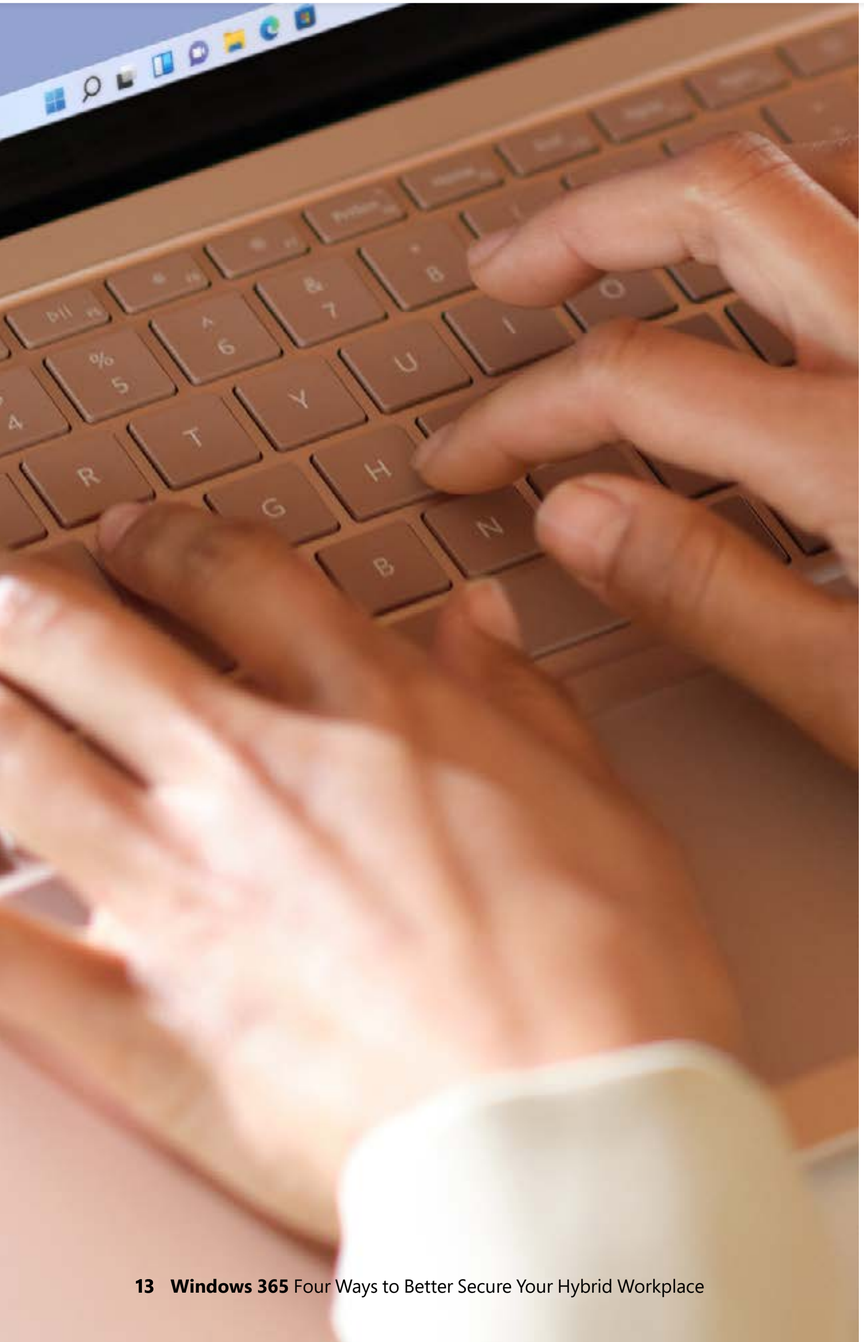
Even with new regulations, data breaches pose a growing risk—occurring as much as 68 percent more often than the year before, with an average cost of over $4M each.[5] Organizations need solutions that minimize the vulnerabilities which allow breaches without negatively impacting productivity or cost.

Windows 365 is regularly updated to stay current with data protection laws and can be configured to comply with your industry's specific regulations. With centralized, cloud-based endpoint management using Microsoft Intune and Intune Suite, these updates can be automated—meaning potential threats and security gaps are constantly and continuously being identified, assessed, and restricted.

68%

more data breaches occurred against organizations compared to the previous year.[5]

Reduce Password Risks with Multifactor Authentication



Password attacks are on the rise

Passwords can be among the easiest ways for bad actors to find vulnerabilities in an otherwise secure system. A study by Microsoft found that password attacks had risen by 74 percent in just one year.[6] A number of guidelines exist to mitigate that risk, ranging from suggestions for password length and variation to the potential for removing passwords as an access gate altogether.

Passwords can be an inevitable weak point in a system's security framework. A password alone doesn't adhere to a Zero Trust policy because passwords can be susceptible to hacking. This is especially true for many people who use the same or similar password across multiple accounts.

How to reduce password risks

One of the simplest, most effective ways to mitigate the risk of password hacks is multifactor authentication (MFA). With multifactor authentication, users attempting to log in to a device must confirm their identity on a separate known device or application. MFA policies are rooted in Zero Trust because they require users to verify their identity before gaining any kind of access to sensitive data.

Because Windows 365 delivers a Windows experience on a Cloud PC, login credentials can be made immediately available to new, temporary, or third-party employees. This allows for a secure solution that is also convenient and conducive to productivity, especially with Microsoft's MFA requirements in place. MFA can also be used without a password at all, eliminating the security gap created by poorly implemented password protocols.

of business leaders agree that passwordless authentication—using a secondary device or biometric to verify identity rather than a password—is a priority for their company.[1]

Maintain Business Continuity with Effective Disaster Recovery

93%

more ransomware attacks occurred compared to the same period in the year before.[7]

99.99%

reliability as defined by the Windows 365 Service Level Agreement[8]

Deliver uninterrupted productivity

Uninterrupted productivity can be the key to a business's ability to succeed, but even the most well-prepared organizations can be susceptible to disaster scenarios. Most common are security-specific attacks, like ransomware, which can devastate companies of any size. For hybrid and remote environments, another major interruption to business continuity can be lost, damaged, or stolen equipment. Natural disasters can also create time and cost disruptions, especially for smaller or medium-sized businesses, with as many as 40 percent never reopening.[9]

Resiliency and business continuity can mean the difference for an organization's ultimate success. Cloud PCs are a reliable solution because user data and user context are portable. Even in the case of a machine-specific failure, Cloud PCs can be more easily recovered or reprovisioned, and the user may experience almost no interruption.

Windows 365 delivers Microsoft solutions, features, and tools, like OneDrive and Windows Sync Your Settings, in the cloud to ensure portability and resiliency. Backed by Azure, a Windows 365 Cloud PC can identify failures in the system and move a user's workload to another resource. Even if a non-Azure failure occurs—like a problem with a physical machine—Windows 365 ensures limited interruption because the Cloud PC is easily accessed from another device.

Why Choose Windows 365?

BYOPC

The Need

A secure, resilient way to access apps, settings, and content from a personal device.

How Windows 365 helps

Windows 365 allows users to do their work from their preferred device, no matter where they are, with comprehensive data protection in transit and at rest.

Temporary Workforce

The Need

Immediate access to a Windows environment from anywhere for contractors, interns, and third-party users.

How Windows 365 helps

As a SaaS solution, Windows 365 makes it easy for admins to provide immediate user access anywhere in the world with the designated controls and restrictions suitable to that user's needs.

Mergers and Acquisitions

The Need

A simplified, secure management solution for multiple endpoints and data coming together in a new environment.

How Windows 365 helps

Windows 365 Enterprise uses Intune to seamlessly provision as many endpoints and users as a company needs in one action from centralized cloud operations.

Windows 365 is rooted in Zero Trust

Secure by design

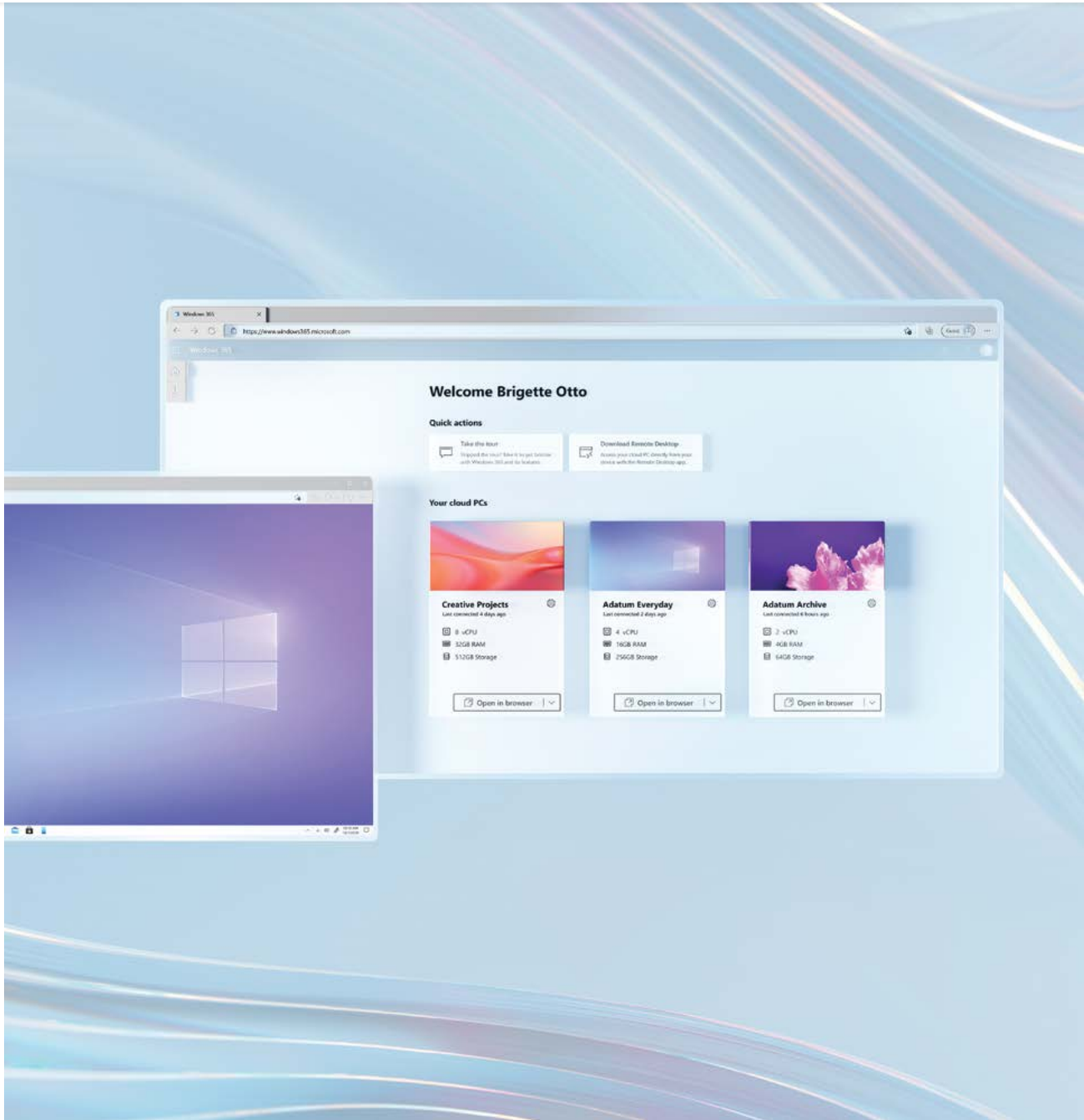
Combine the power and security of Windows with the scalability of the cloud for better protection against security risks.

Productivity on any device

Onboard employees quickly with access to Windows 365 from any device. Employees enjoy the same user experience and settings wherever they sign in.

Manage more with less

Manage and configure as many endpoints as necessary from a single console without the need for additional IT resources or specialized skills.



How Windows 365 supports Zero Trust for a more secure hybrid work environment

Windows 365 is a quickly scalable and customizable SaaS solution that delivers the Windows experience in a Cloud PC environment, allowing flexibility for all of your employees, whether they're permanent, contractors, or newly onboarding through mergers or acquisitions.

Because Windows 365 Enterprise works with Intune and other Microsoft security features and controls, your data is protected no matter where you access it.

Centralized in the cloud, Windows 365 enables a simplified management experience for IT, requiring no special expertise.

As a SaaS solution, Windows 365 is easy to set up, with predictable, per-user per-month pricing. Windows 365 delivers savings in cost, productivity, and time for your organization's workforce, no matter how and where your team works.

The findings of the Total Economic Impact™ of Windows 365, a study conducted by Forrester Consulting.[4]

40%
ROI

$1.1M
IT cost savings

$2.2M
productivity savings for power users

$1.1M
cost savings through BYOPC enablement

$719.1K
accelerated productivity savings for M&A employees

$253.2K
savings in improved contractor productivity

Windows 365

Learn more about Windows 365 Enterprise →

Sources:

[1]Knuth, G., & Gruber, D. (2023, February). "Managing the Endpoint Vulnerability Gap. Enterprise Strategy Group" by Tech Target.
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWXwKT

[2]"Embrace proactive security with Zero Trust." Zero Trust Model - Modern Security Architecture | Microsoft Security. Accessed April 20, 2023.
https://www.microsoft.com/en-us/security/business/zero-trust.

[3]"Hybrid Work Is Here to Stay, but Security Concerns Are High." Help Net Security, September 1, 2021.
https://www.helpnetsecurity.com/2021/09/01/hybrid-work-security-concerns/.

[4]Ponemon Institute LLC. (2020). The Third Annual Study on the State of Endpoint Security Risk.
https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

[5]Armstrong, Brian. "Discover 5 Lessons Microsoft Has Learned about Compliance Management." Microsoft Security Blog. Microsoft, July 25, 2022.
https://www.microsoft.com/en-us/security/blog/2022/07/25/discover-5-lessons-microsoft-has-learned-about-compliance-management/.

[6]Microsoft Digital Defense Report 2022. Microsoft, 2022.
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.

[7]Skelton, Sebastian Klovig. "Ransomware Attacks Increase Dramatically during 2021: Computer Weekly." ComputerWeekly.com. ComputerWeekly.com, August 3, 2021.
https://www.computerweekly.com/news/252504676/Ransomware-attacks-increase-dramatically-during-2021.

[8]"Business Continuity and Disaster Recovery." Business continuity and disaster recovery with Windows 365 | Microsoft Learn. Microsoft, February 24, 2023.
https://learn.microsoft.com/en-us/windows-365/enterprise/business-continuity-disaster-recovery.

[9]Finlinson, Joe. "Council Post: Why Disaster Recovery Is No Longer Optional for Today's Businesses." Forbes. Forbes Magazine, October 12, 2021.
https://www.forbes.com/sites/forbestechcouncil/2021/10/12/why-disaster-recovery-is-no-longer-optional-for-todays-businesses/?sh=5fb19ef56fd1.

Windows 365