Maximizing Your Licences:
A Zero Trust Journey with Microsoft 365 Business Premium

Written and Curated by PC Corp.

We make I.T. easy

Contents

Why the Zero Trust Journey Matters.....03

What is Zero Trust?.....04

Microsoft 365 Business Premium's Role in Your Security.....05

The Microsoft 365 Business Premium Zero Trust Implementation Journey.....06

A Foundational Element of M365 Security: Conditional Access.....07

- Step 1: Multifactor Authentication.....08
- Step 2: Defender for Office 365.....09
- Step 3: Microsoft Entra ID.....10
- Step 4: Microsoft Intune (and Autopilot).....12
- Step 5: Microsoft Defender for Business (Microsoft 365 for Endpoint Business).....14
- Step 6: Enhanced Conditional Access.....16
- Step 7: Microsoft Purview Information Protection.....17

A Security Journey is Evolving and Continuous.....19

The Growing Importance of Zero Trust.....19

Don't Go I.T. Alone: PC Corp Makes Zero Trust Easy.....20

Why the Zero Trust Journey Matters

Picture this: you're cruising down the highway in a car with basic safety features—just mirrors, brakes, and seatbelts. Sure, it gets you from point A to point B, but it lacks cutting-edge safety tech like automatic braking or collision avoidance. Now, swap that car for your current security setup. Many businesses, big and small, are still relying on "good enough" tools, thinking they're safe just because they haven't been hit yet. But when the risks are increasing in frequency and sophistication, that's not going to cut it.

Cyber threats, they're constantly changing, and you never know when they might strike. It's no longer a question of if but when someone will try to breach your defenses. That's why you need a security strategy that doesn't just look in the rearview mirror but keeps an eye on the road ahead, too. **Enter: Zero Trust.**

Zero Trust is all about shifting gears from the traditional, perimeter-based model to one that protects your data from every angle. You're saying goodbye to the "set it and forget it" approach and instead, treating security as an ongoing journey—one that requires you to think ahead, make proactive moves, and always be ready to adapt.

With a comprehensive tool like Microsoft 365 Business Premium, you can navigate this journey without breaking a sweat. Buckle up and let's explore how its security features can support your Zero Trust strategy and keep your business safe on every front.

What is Zero Trust?

Trust no one. Verify everything.

When you're setting off on a long road trip and want to enjoy a safe experience, you wouldn't just pack for the usual predictable bumps, like night driving or heavy traffic. You would prepare for everything—unexpected detours, sudden weather changes, and even the odd runaway shopping cart in the parking lot. That way, you'll be ready for whatever comes your way, anytime and anywhere.

That's exactly the kind of mindset you need when traversing your organization's digital workspace too: the Zero Trust approach.

With Zero Trust, you don't assume that everything will go smoothly. In fact, you're assuming the opposite—that threats could come from both outside and inside your network. This proactive stance means you're constantly assessing and verifying every user, device, and connection to reduce the risk of unauthorized access.

When employees hop between devices and work from all corners of the globe, a Zero Trust framework puts your organization in the strongest position to protect its most critical assets. It's your best bet amidst increasingly unpredictable and evolving threats, keeping your business prepared for any twists and turns along the way.

The Three Zero Trust Guiding Principles

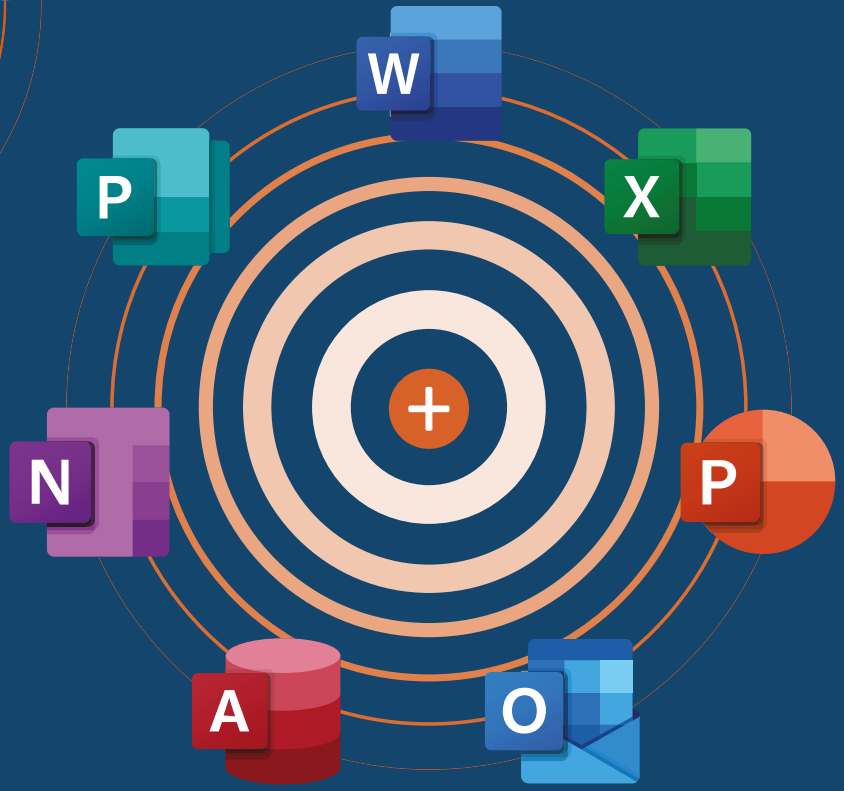
Verify explicitly: Every time you start the car, you prove you're the right driver by putting the correct key into the ignition. Your IT should work the same way—always double-checking who's behind the wheel. Authenticate every access request, action, or transaction, no matter the user's history, device, or location.

Least privileged access: Think of the rules of the road: certain vehicles are restricted to specific lanes, like buses in the bus lane or carpools in the carpool lane. In your IT environment, adopt this same approach by giving users just enough access to the resources they need—and only for the time need it.

Assume breach: Just as a car is equipped with seatbelts, airbags, and emergency brakes, expect the unexpected in your IT environment. Act as if a bad actor infiltrating your system is inevitable and put protections in place to limit a breach's impact.

Microsoft 365 Business Premium's Role in Your Security

Microsoft 365 Business Premium is a comprehensive solution that allows you to run your business securely from anywhere. It brings together various Microsoft 365 applications, such as Word, Excel, PowerPoint, and Outlook, with cloud services and comprehensive securities that can help protect your business against advanced cyber threats.



Desktop, web, and mobile apps and secure cloud services:

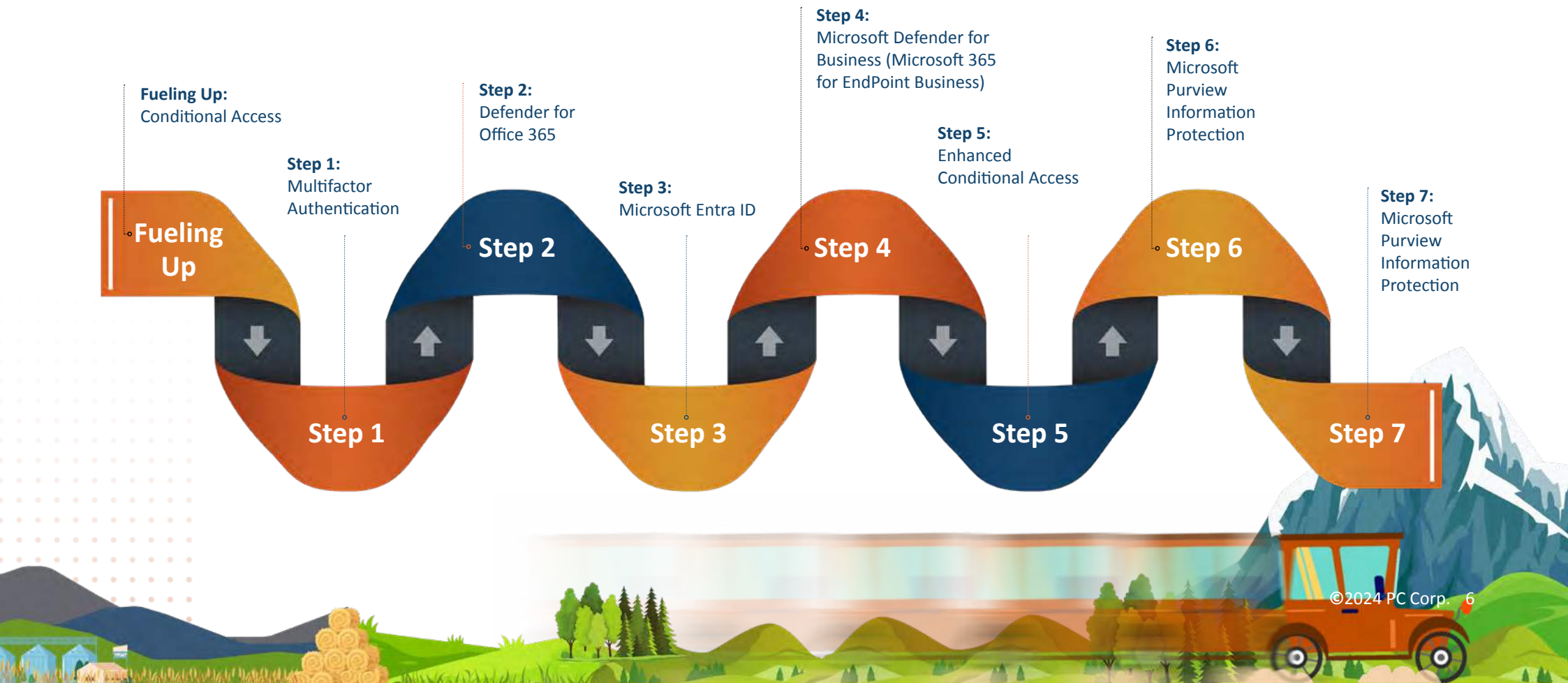
- Word
- Excel
- PowerPoint
- Outlook
- Teams
- OneDrive
- SharePoint
- Exchange
- Clipchamp
- Microsoft Loop
- Microsoft Entra ID
- Intune
- Microsoft Defender
- Microsoft Purview

While many businesses already own a Microsoft 365 Business Premium licence, many don't realize they can leverage its features to create a more secure and resilient network. This guide is here to change that! You'll learn how to get the most value from the tools you may already have in place.

The Microsoft 365 Business Premium Zero Trust Implementation Journey

Now that you understand Microsoft 365 Business Premium's role in building a robust digital environment, it's time to put the plan into action. In the next few pages, we'll take you through the recommended implementation roadmap. We explain how each feature generally works to secure your environment, and how it all comes together to protect your network, data, and systems.

Ready to go on this journey? Let's get into our cars and hit the road toward a more secure digital future!!



A Foundational Element of M365 Security: Conditional Access

One of the most significant security elements of Microsoft 365 that spans across the entire implementation journey is Conditional Access. As the name suggests, Conditional Access operates on a simple yet powerful premise: no one gets access to your network or data unless they meet specific conditions.

Think of this process as a security checkpoint that won't let anyone pass through—trusting no one and nothing—until it gets the necessary proof. It demands to know three things:

1

01. Is your device authorized?
Your network needs to recognize it before it can proceed.

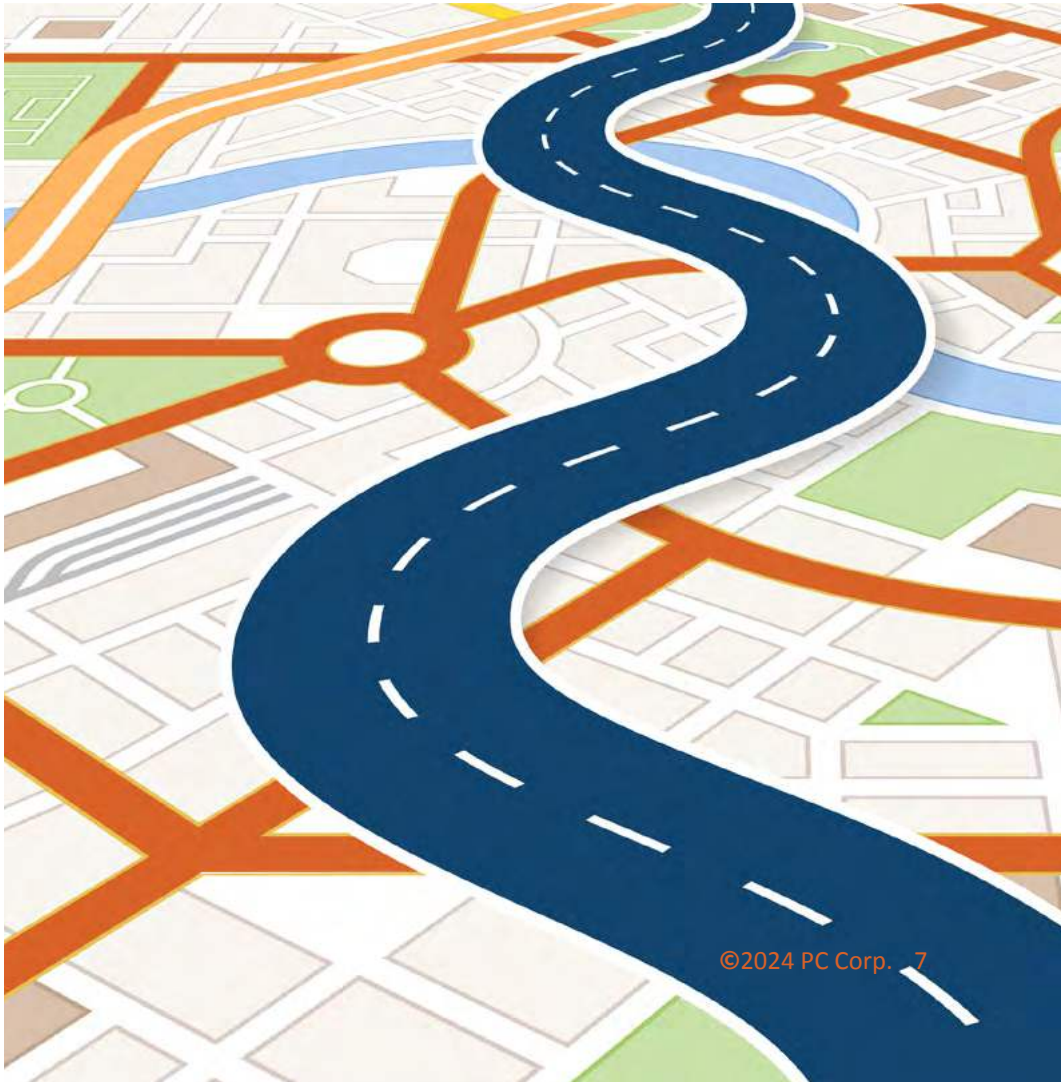
2

02. Is it in the right location?
The system checks whether you're in your usual office or home base, not somewhere unexpected like a foreign IP address.

3

03. Are you an authorized user?
Your identity has to be verified before the platform grants you access.

Now that we understand Conditional Access, let's shift gears and move to the first stop on the Microsoft 365 implementation roadmap.



Step 1: Multifactor Authentication

Multi-factor authentication (MFA) provides an extra layer of protection beyond a password by requiring users to prove their identity before accessing an account or system. They need to provide two or more forms of verification, including:

- Something they know (like a username and password)
- Something they have (like a smartphone, authenticator code, or security token)
- Something they are (biometrics, like a fingerprint or facial recognition)

MFA is like a physical car key embedded with a microchip. It takes the two components working together – the key and the chip inside – to unlock the doors. The car needs to confirm both identifying elements to grant a driver access.

Multifactor Authentication in Microsoft

Microsoft positions MFA as a foundational element of its security offering, making it one of the most effective tools to reduce your risk of data breaches. Even if a hacker manages to get hold of your password, it's rendered useless without the additional verification factor.

The best part? MFA works smoothly both inside and outside your network, maintaining security wherever users are located.

Enabling MFA in your Microsoft 365 Business Premium suite is as essential as having antivirus, antispam, or a firewall—it's the modern standard for keeping your digital environment secure. So, if you're just starting on your Zero Trust journey, MFA should be your first pit stop.

Step 2: Defender for Office 365

Defender for Office 365 is the next stop on your journey to build a stronger Zero Trust framework with Business Premium features. When more than 90% of security incidents are linked to email, this advanced email filtering service is critical for safeguarding your data without slowing down your productivity.

How Defender Tackles Your Security

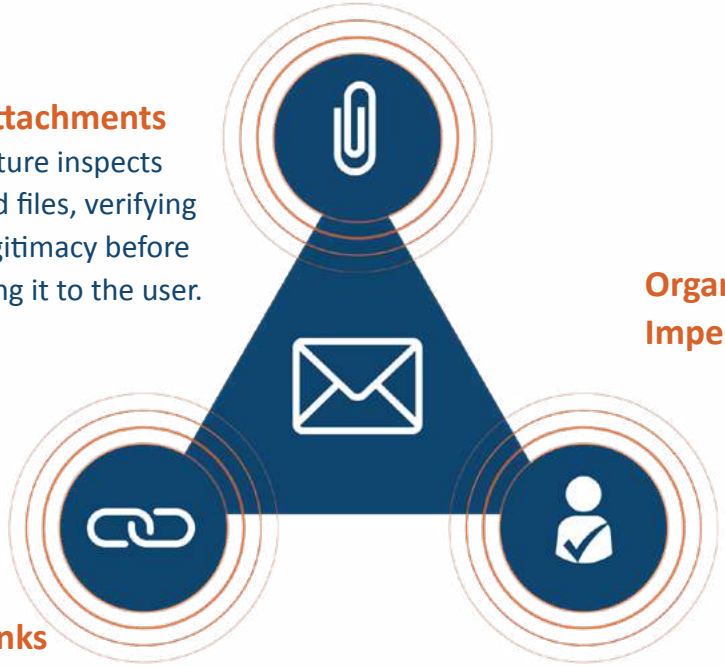
Defender goes beyond basic Exchange Online Protection, employing a multi-layered defense strategy. The software helps address the weakest link in cybersecurity - users. It shoulders the burden of detecting suspicious activity, helping users navigate through their emails to avoid potential social engineering threats with confidence.

Consider it like the mirrors on your car – they help you see what's coming. Defender uses machine learning algorithms for detecting risks in real time, neutralizing threats like zero-day malware, phishing, business email compromise, and ransomware before they can wreak havoc.

When it detects a threat, Defender's response mechanisms act like your car's door locks, unlocking out and blocking malicious entities from entering. It doesn't just do this in your Outlook, but also in Teams, SharePoint, and OneDrive. Key features include:

Safe Attachments

This feature inspects attached files, verifying their legitimacy before delivering it to the user.



Organization Impersonation Protection

This feature alerts users to potential email sender impersonation attempts that use legitimate-looking addresses or domains to deceive recipients.

Safe Links

Defender checks website links before they open, blocking any that are malicious. If a link fails the check, Microsoft won't let users connect to it.

Defender's Self-Serve Quarantine Portal

There's no need to worry about stalled productivity due to quarantined or flagged emails. Defender's self-serve Quarantine Portal lets users review flagged emails and request the release of legitimate ones. Depending on an email's risk level, users can either initiate the release or IT may need to manually review and approve it. This process helps keep security intact while ensuring your employees can access important messages and maintain a steady workflow.

Step 3: Microsoft Entra ID

To truly establish a Zero Trust framework, you need to guarantee that only the right people can access your resources. A strong password alone is no longer enough—credential theft remains a leading cause of data breaches, with Microsoft reporting over 111 million password attacks per day in 2022.

This is where **Microsoft Entra ID** comes into play. The cloud-based solution efficiently secures and manages all identities connected to your organization, including devices, infrastructure, data, Microsoft applications, third-party integrations, and on-premises directories.

Remember that key you used to unlock the car doors earlier? It's now required to start the vehicle and give you access to its functions. Without Entra ID's approval, users are locked out of critical systems or unable to perform tasks. Identity verification uses various methods, including multi-factor authentication and forms of passwordless authentication such as biometrics, an authenticator app, and/or external security keys.

Entra ID Features for Simple Yet Effective Security

Entra ID streamlines your team's ability to make use of organizational resources securely, with features like:

Single sign-on

Access Microsoft and other outside connected apps with the same credential.

Device Auto-Enrollment

Automatically sign up any new corporate-owned devices to InTune, Microsoft's cloud-based mobile device management solution that is considered best practice for administering devices.

Identity Protection

Efficiently identify risk using advanced machine learning tools that automatically detect unusual user behaviour and then either block, challenge, limit, or allow access.

Granular Control with Entra ID

Microsoft Entra ID gives organizations precise control over user access. You can move beyond making simple “yes” or “no” decisions to considering the **what, when, where, how, and why**. Here’s how it works:

Role-based Access Control (RBAC)

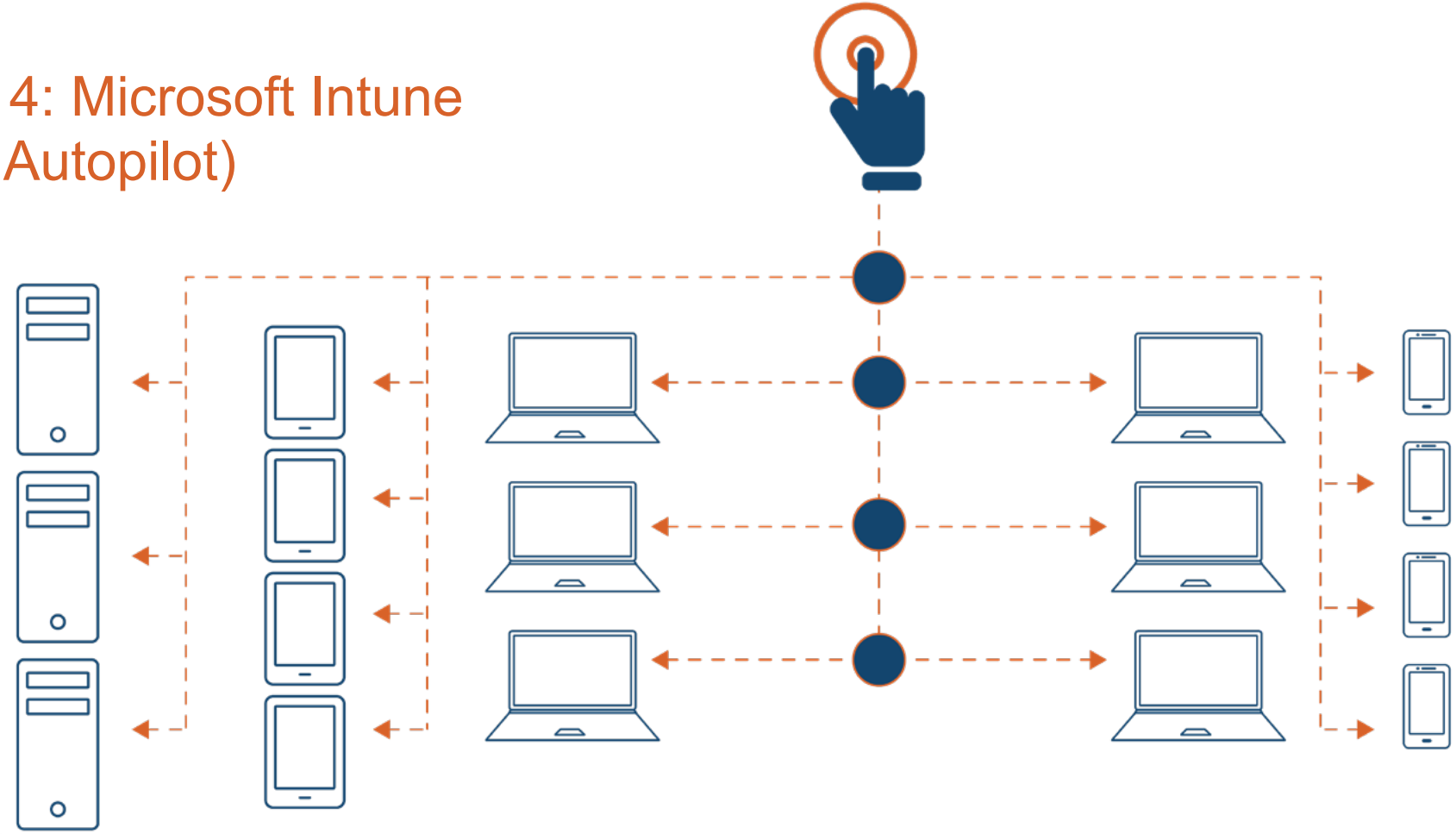
Administrators can assign roles to users and groups and define permissions that align with their responsibilities.

Conditional Access

Administrators set specific conditions that an identity must meet to access resources, such as a user location, device, or the action being taken (like resetting a password.)

By integrating Microsoft Entra ID into your Zero Trust strategy, you can rely on a smarter, more flexible way to manage identities and keep your digital environment secure at its entry points.

Step 4: Microsoft Intune (and Autopilot)



Since your employees' devices are the vehicles that connect them to your organizational resources, they need robust security to keep bad actors out. That's where Microsoft Intune can help! As a cloud-based endpoint management solution, Intune ensures that devices operate securely and efficiently—like a car manufacturer providing regular maintenance to keep a car running smoothly.

And much like manufacturers mass-produce vehicles to offer a consistent driver experience, Intune maintains uniformity across workplace endpoints, giving you a central hub for managing, configuring, and securing devices. From there, you can enforce compliance policies on corporate-owned and personal devices, as well as across operating systems like iOS, Android, and Windows.

Intune supports the three Zero Trust principles— “verify explicitly,” “least privileged access,” and “assume breach”— by offering a range of robust features:

Integrate with Entra ID

Intune authorizes a user’s access to apps and data based on specific permissions, ensuring a finely controlled experience.

Authenticate Users

You can ensure that only authorized users gain access to your resources with authentication methods like multi-factor authentication (MFA) and single sign-on (SSO.)

Establish Conditional Access

Intune enforces data loss prevention policies by granting access to users based on device compliance. For example, you can use the solution to prevent non-compliant devices from using your services, restrict devices that host specific apps, or block personal devices entirely.

Remove Data

In the case of lost or stolen devices, you can use Intune to minimize any negative impact by remotely wiping data, blocking critical information from falling into the wrong hands.

Resolve Threats

Intune uses tools like Microsoft Defender Advanced Threat Protection to automatically respond to threats and enhance overall security.

Secure Windows Machines

Your organization can leverage Intune to build endpoint security policies that establish your desired device settings for protecting user accounts, reduce your attack surface, and address specific defense components such as your organization’s antivirus/EDR solutions, firewall or disk encryption.

Seamlessly deploy new devices with Intune and Autopilot

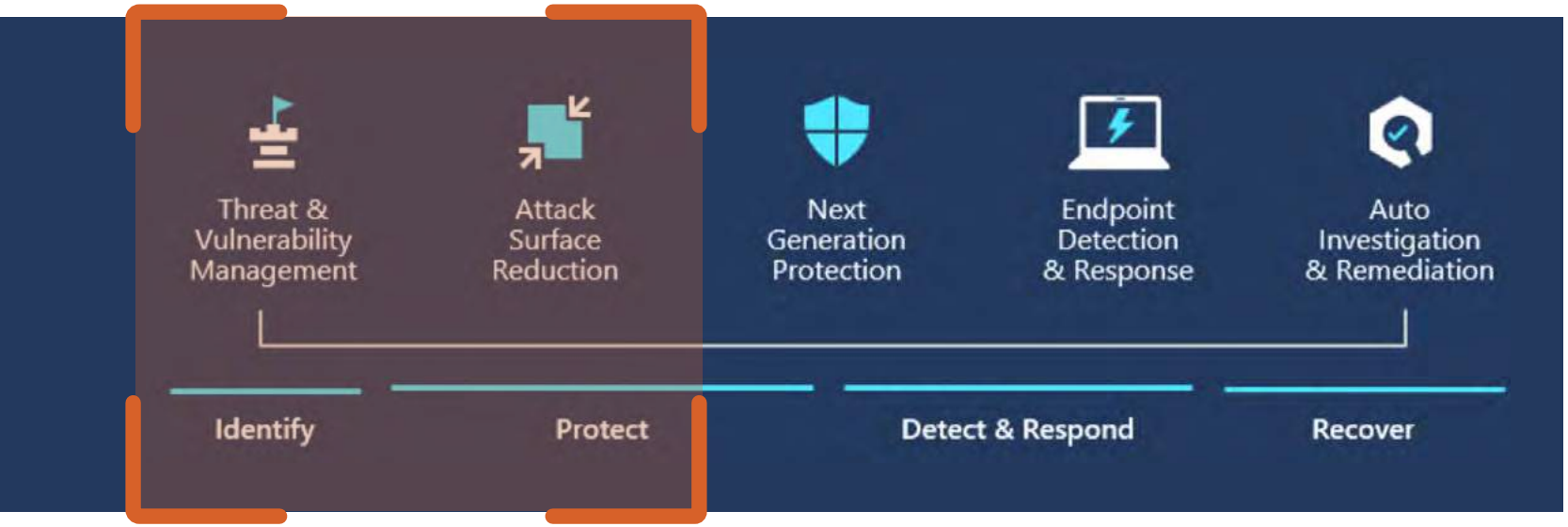
For new Windows devices, Intune works hand-in-hand with Autopilot, Microsoft’s modern deployment technology, to streamline setup from the moment you unbox your devices. It automates the process of connecting devices to Entra ID, installing apps, and configuring settings to create a consistent experience right from the start.

Configure Update Settings

Intune also keeps devices stable by managing how and when Windows updates are installed, ensuring that users always have the latest security updates without disrupting their productivity.

By combining all these features, Intune helps your employees easily and securely access corporate resources, helping them stay productive wherever they work.

Step 5: Microsoft Defender for Business (Microsoft 365 for Endpoint Business)



Given that Microsoft blocked 4000 identity authentication attacks per second in 2023, encountering cyber threats is as inevitable as encountering poor drivers on a road trip.

Just as modern vehicles have built-in collision avoidance systems to prevent accidents, your business also needs a solution that can automatically apply the brakes and lock down devices and infrastructure when security incidents happen.

How Defender for Business Stops Threats in Their Tracks

Microsoft Defender for Business acts as your digital workplace's collision avoidance system, providing easy-to-use enterprise-grade endpoint protection for your business. It is designed to simplify configuration, making it easy to onboard new systems while setting up effective protection for your devices and infrastructure.

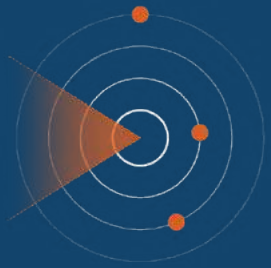
The solution holistically addresses your security risks by integrating with other Microsoft 365 Defender technologies like Defender for Office 365 and Defender for Identity and supports a wide range of devices across iOS, Android, Windows, and MacOS.

Key Features of Defender for Business

Here's how Defender for Business helps protect your organization from threats:

Continuously Monitor End-User Devices

It leverages its endpoint detection & response (EDR) capabilities and next-generation antivirus (NGAV) protection, which use advanced artificial intelligence and machine learning algorithms to automatically detect, investigate, and prevent hacking attempts in real-time.



Reduce Your Attack Surface

Defender for Business minimizes potential entry points for bad actors by leveraging features like network and web protection, which block user access to dangerous web and email content.

Manage Risks

The solution assesses and prioritizes risks across your entire IT environment with its threat and vulnerability management, helping you promptly address any weaknesses or misconfigurations in your setup.

Analyze Your Cybersecurity

It offers detailed analytics and reports on your organization's security posture, including the **Microsoft Secure Score.** This tool provides a numerical grade, highlighting areas for improvement based on completed and recommended security tasks that enhance your endpoint protection.

By combining all these security products into one simple package, your organization can build a strong, streamlined defense that protects your precious resources from the rising threat of sophisticated cyberattacks.

Step 6: Enhanced Conditional Access

On any long road trip, there's always a moment when you pull over at a scenic overlook to take in the view and reflect on the journey so far. Enhanced Conditional Access serves as that point in your Microsoft 365 Business Premium security roadmap, offering a clearer perspective of your organization's digital operating environment.

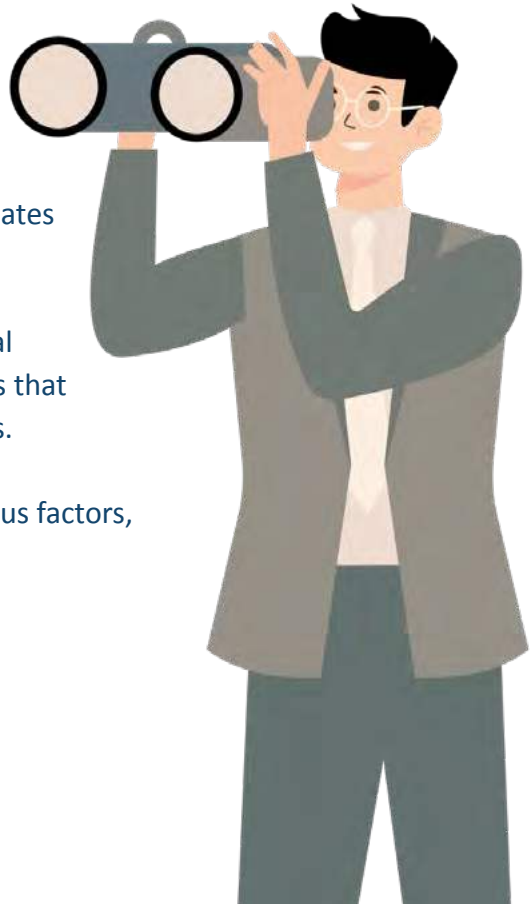
With the security and conditional access policies you've already put in place during steps 1-5, this pause allows you to reassess your broader security posture. It's the perfect time to spot any remaining gaps and apply any additional policies that you need to enhance your defenses even further.

Assessing and Strengthening Access Control

This is the point when your organization evaluates its setup to identify where you can tighten access controls. If you find any exposed areas, administrators can set up rules and conditional access policies that enforce specific conditions that an identity or device must meet to gain access.

These granular controls can be based on various factors, such as:

- User identity
- Device type or health
- Location
- Application sensitivity level



The Tools for Establishing Enhanced Conditional Access

Your organization doesn't have to make these decisions on its own: enhanced conditional access means leveraging tools that automatically analyze signals from various sources to make access decisions for you.

This technology continuously assesses your risk based on threat intelligence and the information stored within your existing Microsoft 365 setup, including:

- **Identities,** through Entra ID and Defender for Identity
- **Data,** using Information Protection
- **Applications,** via Defender for Cloud
- **Network,** monitored by Cloud App Security
- **Endpoints,** managed by Defender and Endpoint Manager

By combining these signals, your organization can proactively remediate threats and ensure that only authorized people and devices access your resources.

With Enhanced Conditional Accesses fine-tuned, your organization will have a reliable and secure technology framework that protects resources and helps you maintain smooth operations. Like a well-planned route on a road trip, you get the framework to navigate safely and confidently toward your security goals.

Step 7: Microsoft Purview Information Protection

Congratulations on reaching this milestone on your security implementation journey! Having completed the previous seven steps, you're now ready to implement Microsoft Purview Information Protection.

Purview Information Protection is a unified, intelligent platform designed to simplify how you configure and manage data policies while keeping your data secure and accessible. Like your car's electronic dashboard, where you'd monitor and control key settings like radio stations, speaker volume, or cruise control, with Microsoft Purview you can monitor and control data protection all from one place.

Key Features of Microsoft Purview Information Protection

Microsoft Purview Information Protection strengthens your Zero Trust framework by enhancing the measures that safeguard your data. Key features include:

Data Classification

Categorize and label data based on sensitivity across various environments, including Microsoft cloud solutions, third-party applications, and your on-premises infrastructure. You can also use AI and machine learning algorithms to apply "intelligence classifiers" to automatically identify and catalogue data.

Automatic Protection

Once you classify your data, you can apply automated protection actions such as encryption or restrictions based on the established rules. This ensures that you secure sensitive data without requiring manual intervention.

Conditional Access

You can authorize or block user access to data based on compliance criteria like Entra ID membership, device type, or user permissions. The system can also enforce extra steps like multi-factor authentication for guest users, so only the right people have access.

Data Management

Manage data throughout its lifecycle, from audits to compliance checks to insider risk assessments, ensuring that all data policies align with regulations and business needs.

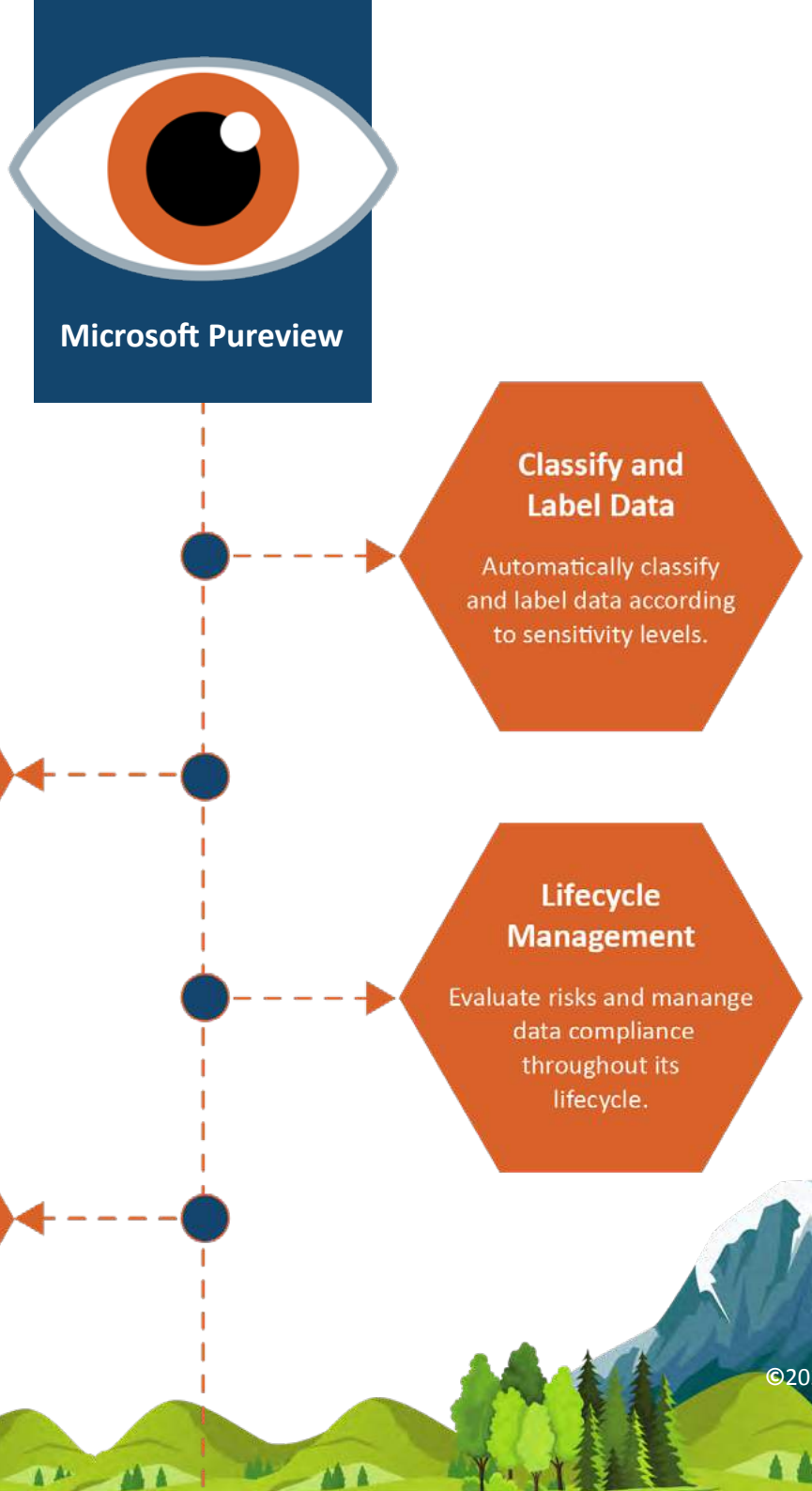
Tracking User Activity

Use the "Activity Explorer" to monitor how users interact with labeled content and track their actions like reading, deleting, modifying, printing, copying, or renaming. This transparency helps you identify potential risks and keep your data secure.

Why Purview Information Protection Matters

In 2023, the global average cost of a data breach was $4.45 million -- a significant financial impact that underscores the importance of robust data protection. Microsoft Purview Information Protection strengthens your overall security strategy, giving you a tool to more easily manage data policies and compliance to protect your confidential information.

With Purview Information Protection in place, you've completed your current Zero Trust journey with Microsoft 365 Business Premium. Now, you've secured your environment and built a resilient digital infrastructure.



A Security Journey is Evolving and Continuous

A security journey is never complete. Unlike a road trip, where you eventually reach a destination, protecting your business is ongoing. Every step forward strengthens your environment, helping you adapt and improve to stay ahead of evolving threats.

Since risks are never static, Microsoft and other IT manufacturers will continuously enhance their products with new features to address the latest challenges. Keeping up to date with these innovations will be crucial as you work to solidify your “trust no one, verify everything” Zero Trust framework.

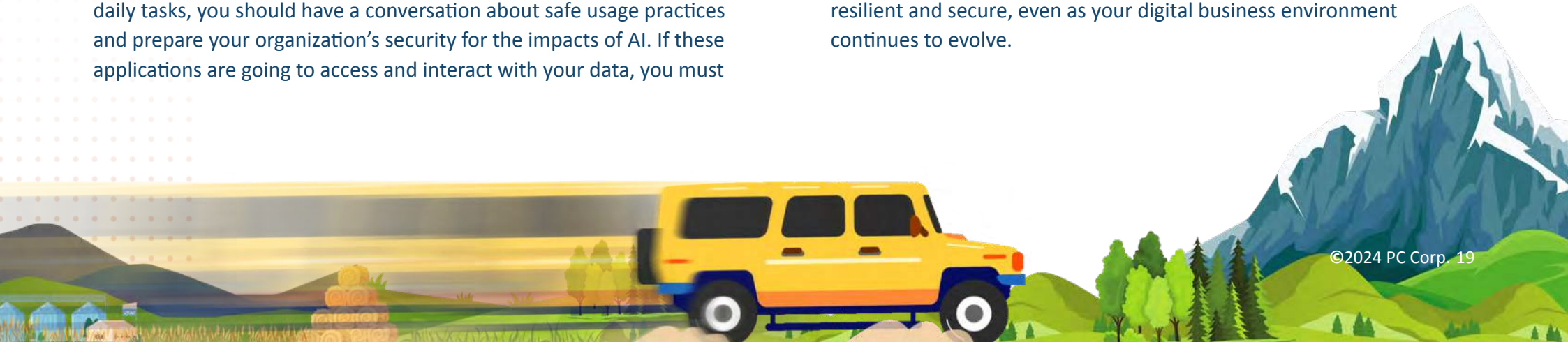
If Microsoft 365 solutions are like the sophisticated safety systems in your vehicle—airbags, collision alerts, and anti-lock brakes—then Zero Trust is the roll cage. As your encompassing and protective framework, it provides the parameters that guide how you protect your business, your sensitive data, your devices and people.

The Growing Importance of Zero Trust

That framework is becoming even more critical now. Aside from cyber threats, new AI applications are tantalizing businesses with their potential for enhanced productivity -- Microsoft’s Copilot, ChatGPT, Google Assistant, Alexa, and Siri, to name a few.

Before your business starts leveraging these tools to complete their daily tasks, you should have a conversation about safe usage practices and prepare your organization’s security for the impacts of AI. If these applications are going to access and interact with your data, you must first ensure that data is well protected from potential breaches or third-party bad actors.

By proactively addressing these challenges and continuously refining your security measures, you can empower your team to embrace new technology confidently and safely. Your organization will remain resilient and secure, even as your digital business environment continues to evolve.



Don’t Go I.T. Alone: PC Corp Makes Zero Trust Easy

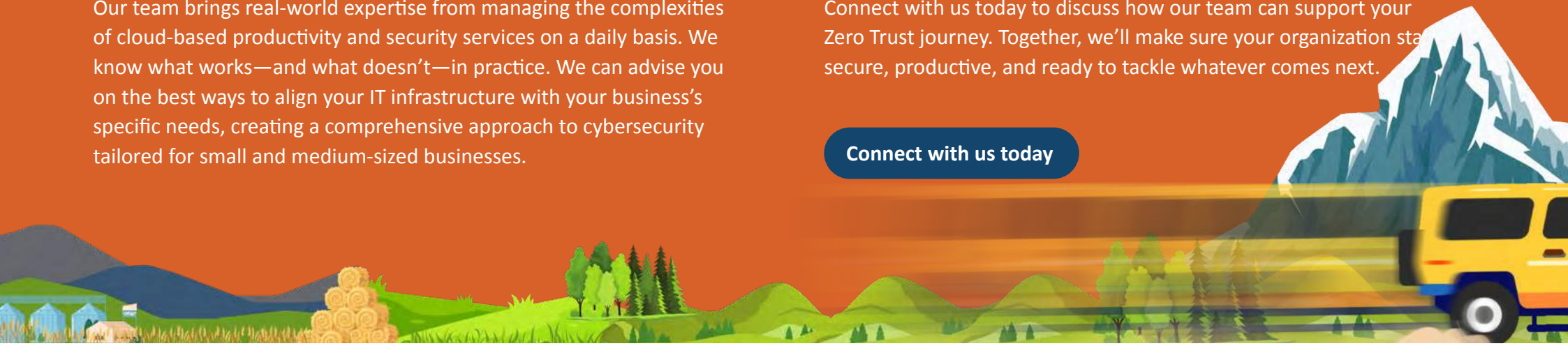
You don’t need to undergo this security journey alone. PC Corp is here to be your reliable partner in this adventure, supporting you through the steps of implementing Microsoft 365 Business Premium’s powerful security features. We’ll provide expert oversight to make sure your organization effectively builds a strong, layered Zero Trust defense.

Our team brings real-world expertise from managing the complexities of cloud-based productivity and security services on a daily basis. We know what works—and what doesn’t—in practice. We can advise you on the best ways to align your IT infrastructure with your business’s specific needs, creating a comprehensive approach to cybersecurity tailored for small and medium-sized businesses.

Partnering with PC Corp means collaborating with an IT service provider backed by over 40 years of experience, strong vendor partnerships, and a proven methodology. But we’re more than just experts—we are people who genuinely care about you and your success. We’re always ready to answer the phone, meet with you, and provide thoughtful, helpful responses to your questions.

Connect with us today to discuss how our team can support your Zero Trust journey. Together, we’ll make sure your organization sta secure, productive, and ready to tackle whatever comes next.

Connect with us today



pc corp
We make I.T. easy

Edmonton Office
9947 109 Street
Edmonton, AB T5K 1H6

Phone: (780) 428-3000

Calgary Office
100, 820 10 Street SW
Calgary, AB T2P 2X1

Phone: (403) 266-3000

Toll-free number 1-888-257-8525
info@pccorp.com