



Cybersecurity, Simplified. 

Secure Your Digital Journey with
**Pathway's Microsoft
Enterprise Security Services**

Your Ultimate Guidebook

Table of Content

Prelude	4
The Burning Questions	7
Service Introduction	10
Defender Suite	12
Information Protection Suite	18
IAM Suite	23
Security Management Suite	30
Unify and Conquer	34
Connect with Us	35

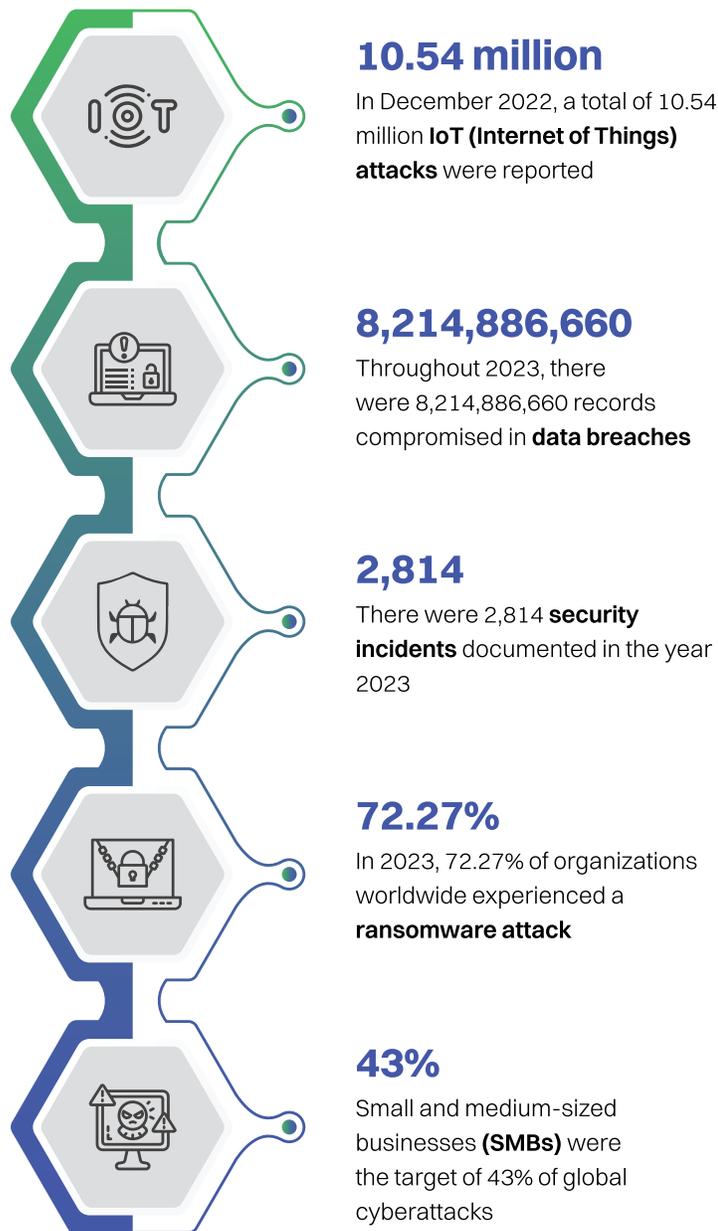




Today's Digital Landscape is Filled with Landmines

The digital landscape offers a wealth of opportunities for businesses, but it also comes with hidden dangers—**cyber threats**. Just like navigating a minefield, one wrong step can have devastating consequences for organizations, such as severe **financial losses**, **irreversible damage to brand reputation**, **theft of intellectual property**, **legal liabilities**, and **a loss of customer trust**.

Here's a glimpse into the ever-evolving threat landscape:



Source: IT Governance, Statista & Verizon

These statistics paint a sobering picture of the challenges faced by businesses in the digital age. With threats lurking around every corner, relying on outdated security measures is like trying to navigate a minefield blindfolded.



It's High Time for Businesses to Go from Being Vulnerable to Fully Vigilant

The digital landscape is not just filled with landmines; it's constantly shifting, with new threats emerging every day. **Being vulnerable in this environment is simply not an option.**

Here's why it's crucial for businesses to transition from a reactive to a proactive approach when it comes to cybersecurity:

Financial Impact

The average cost of a data breach reached an all-time high of USD 4.45 million in 2023. This represents a 2.3% increase from the 2022 cost of USD 4.35 million.

Reputational Damage

Data breaches and other cyber incidents can severely damage a company's reputation, leading to the loss of business and customer trust.

Compliance Risks

Failing to meet industry regulations and data privacy laws can result in hefty fines and penalties.

Sophistication of Attacks

Cybercriminals are constantly refining their tactics, employing advanced techniques like social engineering and zero-day exploits.

New Attack Surfaces

The rise of cloud computing, mobile devices, and the Internet of Things (IoT) has expanded the attack surface for businesses.

Remote Work Challenges

The shift to remote work has introduced new security vulnerabilities that need to be addressed immediately.



By taking proactive steps to secure your business, you can reduce your risk of falling victim to cyberattacks, protect your valuable data and resources, and safeguard your future in the ever-changing digital world.

Did You Know?

In 2023, a Canadian international aviation company **lost a staggering \$50 million** after a massive cyberattack disrupted its online sales for nearly an entire month.

Introducing Pathway's Microsoft Enterprise Security Services

Designed to navigate your digital landscape confidently with Zero Trust strategy



Infrastructure
Azure



Cybersecurity, Simplified. 



Why Partner with Pathway for Your Microsoft Security Solutions?

While advanced Microsoft security solutions offer exceptional capabilities, **unlocking their true value requires more than just technology.** Effective implementation and ongoing support are crucial to achieve **optimal security posture, streamlined operations, and maximized ROI.**

Pathway bridges the gap by providing unparalleled expertise and comprehensive services to help you leverage the power of Microsoft Security Solutions:



People

Dedicated Security Specialists:

Our team comprises **Microsoft-certified professionals** with extensive experience in deploying, managing, and optimizing Microsoft security solutions.

Training and Knowledge Transfer:

We invest in **empowering your team** through customized training programs, ensuring they can confidently utilize the chosen solutions.



Process

Strategic Planning and Assessment:

We collaborate closely with you to understand your unique security requirements and vulnerabilities and **design a tailored implementation plan.**

Seamless Deployment and Configuration:

Our experts handle the **configuration and integration** of Microsoft Security solutions, ensuring their smooth integration with your existing infrastructure.

Ongoing Management and Support:

We provide **continuous monitoring, proactive maintenance, and expert guidance** to ensure your security environment remains optimized and robust.

Pathway goes beyond technology to deliver a comprehensive security experience. We are your trusted partner, dedicated to ensuring your organization thrives in a secure and resilient digital landscape.

Benefits of Partnering with Pathway



Maximized ROI



Enhanced Security Posture



Streamlined Operations



Reduced Risk and Improved



Compliance



Empowered Workforce



24/7 Support

What is the Zero Trust Strategy?

Imagine your organization's data as a vault filled with priceless treasures. Traditionally, security is focused on fortifying the castle walls (your network perimeter). However, the modern threat landscape demands a new approach - the Zero Trust Mindset.

In a Zero Trust environment, trust is never assumed, not even for users or devices already inside the network. Every access attempt is continuously verified, regardless of the origin. This layered approach minimizes the impact of breaches and safeguards your sensitive information.

How Pathway's Microsoft Security Solutions Apply Zero Trust Principles

Continuous Verification:

Pathway configures Microsoft security tools to constantly authenticate users and devices, ensuring only authorized access to critical resources.

Micro-segmentation:

Pathway can help segment your network into smaller zones, limiting the lateral movement of attackers within your system, even if they gain initial access.



Least Privilege Access:

We implement the principle of least privilege, granting users only the minimum permissions required to perform their jobs. This minimizes the potential damage if a breach occurs.

Data Loss Prevention:

Our data loss prevention solutions powered by Microsoft Purview DLP prevent sensitive information from being accidentally or intentionally shared or exfiltrated.

By partnering with Pathway, you gain a security partner dedicated to implementing the Zero Trust approach with Microsoft security solutions. We'll configure, manage, and optimize these tools to create a watertight security posture that safeguards your organization's sensitive data.



“Rather than fearing or ignoring cyber attacks, do ensure your cyber resilience to them.”

- Stephane Nappo



About Pathway's Microsoft Enterprise Security Services

The digital age brings immense opportunity but also complex security challenges. Businesses of all sizes face a minefield of threats – malware, ransomware, phishing attacks, unauthorized access – that can impede operations and compromise sensitive data.

Pathway's Microsoft Enterprise Security Services empower you to take proactive control. Our team of security professionals leverages the robust features of Microsoft's cloud-based security platform to create a comprehensive solution tailored to your organization's needs. We go beyond just technology, providing ongoing guidance and expertise to ensure your security posture is constantly evolving to meet tomorrow's threats.

Our comprehensive suite of services provides:

Threat Protection

We protect devices, email, and cloud workloads from various cyber threats, including malware, ransomware, phishing attacks, and unauthorized access attempts.

Our Offerings: 1. Defender for Cloud Apps | 2. Defender for Endpoint
3. Defender for Identity | 4. Defender for Office 365



Information Protection

We discover, classify, and protect sensitive data across your organization. This can include data stored on devices, emails, and cloud storage platforms.

Our Offerings: 1. Purview Information Protection (PIP) | 2. Purview Data Loss Prevention (DLP)



Identity & Access Management

We manage user identities and access permissions across your various applications and resources. This ensures that only authorized users have access to the data and resources they need.

Our Offerings: 1. Entra ID | 2. Entra ID Protection | 3. Entra ID Governance
4. Entra ID Connect | 5. Identity Manager



Security Management

We provide tools and services to help you monitor your security posture, identify and respond to threats, and ensure compliance with relevant regulations. This can involve collecting security data from various sources, analyzing it for suspicious activity, and automating responses to security incidents.

Our Offerings: 1. Defender for Cloud | 2. Sentinel



With Pathway's Microsoft Enterprise Security Services, you gain a **trusted security partner** with the expertise to navigate the ever-changing threat landscape. We help you embrace the digital world confidently, secure today, and prepare for what lies ahead.

Why Pathway's Microsoft Enterprise Security Services?

In today's complex digital landscape, safeguarding your business requires a **comprehensive and unified approach**. Pathway's Microsoft Enterprise Security Services offer a powerful solution, delivered by our team of security professionals, to empower you to have the following business advantages:

Consolidated Security. Simplified Management.

Pathway streamlines your security with a unified Microsoft platform customized to your needs. Gain centralized visibility with our expert insights for better threat detection. We ensure seamless integration of Microsoft's pre-built solutions for optimal response.



Proactive Defence. Maximum Uptime.

Pathway leverages advanced threat intelligence from Microsoft to stay ahead of cyberattacks. We automate routine tasks like vulnerability scanning and free up your IT resources. Our strategic oversight enhances Microsoft's real-time response, minimizing disruption to your business.

Focus on Growth. We Handle Security.

Pathway manages your Microsoft security solutions, letting you focus on core business activities. Our services minimize risks and ensure smooth operations, keeping you compliant. Build trust with stakeholders by demonstrating a robust security posture powered by Pathway and Microsoft.



Expert Guidance. Tailored Solutions.

Our Microsoft-certified professionals deliver ongoing support and guidance. We adapt your security measures to evolving threats, leveraging the latest Microsoft advancements. Get tailored recommendations to optimize your security and achieve your business goals.

In short, partnering with Pathway helps you unlock the full potential of Microsoft security solutions, perfectly designed to protect and propel your business forward in the digital age.

Threat Protection Services

Let's explore in detail:

- Defender for Cloud Apps
- Defender for Endpoint
- Defender for Identity
- Defender for Office 365

Achieve Extended Detection and Response (XDR) with Pathway's 365 Defender

The digital landscape mirrors a vast network of highways. Valuable data streams freely, but like any major transportation system, it attracts threats. Pathway's expertise with Microsoft 365 Defender acts as your comprehensive traffic control center, offering Extended Detection and Response (XDR) to secure your digital highways and ensure smooth data flow.

96%

Organizations spend 96% less time monitoring suspicious activity when utilizing Microsoft Security.

Source: The Total Economic Impact™ of Microsoft 365 E5 Compliance, 2021



What is XDR?

Extended Detection and Response (XDR) by Pathway, powered by Microsoft 365 Defender, transcends traditional security measures, offering a more unified and comprehensive approach. Our strategy integrates critical data points from:



Cloud Applications



Email Systems



Identity Platforms



Endpoints: Desktops, laptops, and mobile devices

Pathway leverages Microsoft 365 Defender to correlate this data, providing a holistic view of potential threats across your entire digital ecosystem. This empowers you to:



Detect threats faster and more effectively



Investigate incidents with greater clarity



Respond with coordinated, automated actions

In the following sections, we'll explore how Pathway utilizes each Microsoft 365 Defender component to build you a robust XDR ecosystem.



Defender for Cloud Apps

The explosion of SaaS applications brings both productivity and security challenges. Managing and protecting sensitive data across these cloud environments is complex and time-consuming. Traditional security often falls short, leaving you vulnerable.

Leveraging Microsoft Defender for Cloud Apps, Pathway delivers a specialized security service tailored to **secure your SaaS environment effectively**. Our approach transcends the capabilities of conventional Cloud Access Security Brokers (CASB), offering a robust, cloud-focused security solution.

What our service can do for your business



Gain Comprehensive Visibility and Control:

Pathway leverages Defender for Cloud Apps to give you complete oversight of all your SaaS apps, identify shadow IT, and enforce usage policies.



Stop Advanced Threats:

We harness the power of Microsoft Defender XDR to detect and respond to sophisticated cyberattacks targeting your SaaS data.



Protect Your Sensitive Information:

Pathway helps identify and safeguard sensitive information stored in cloud applications, preventing unauthorized access and data loss.



Simplify Security Management:

Our experts utilize Defender for Cloud Apps' SSPM features to identify misconfigurations and recommend best practices for each connected app.



Benefits



Protect Sensitive Data



Streamlined Operations



Gain Insights into Shadow IT



Maintain Regulatory Compliance



Defender for Endpoint

In today's ever-evolving threat landscape, keeping your devices secure is crucial. Pathway provides a security service enhanced by Microsoft Defender for Endpoint, designed to **protect and address advanced threats** on devices like laptops, phones, tablets, PCs, access points, routers, and firewalls.

What our service can do for your business



Proactive Defence

- Our experts configure Defender for Endpoint's **built-in behavioural sensors** to monitor device activity and identify suspicious behaviour.
- We utilize **cloud-based security analytics** and **advanced threat intelligence** to translate data into actionable insights, enabling proactive threat detection and response.



Multi-layered Protection

- Pathway helps identify, prioritize, and **address vulnerabilities** and misconfigurations, **minimizing attack surfaces**.
- We configure attack surface reduction features to **block malicious elements** and next-generation protection to **detect and block emerging threats**.



Advanced Detection and Response

- Pathway utilizes Defender for Endpoint's EDR (**Endpoint detection and response**) capabilities to investigate and respond to advanced threats.
- We enable **proactive threat hunting** and leverage **automated investigation and remediation** features to streamline incident response and reduce security team burden.



Benefits



Comprehensive Protection



Centralized Management



Advanced Threat Detection



Improved Visibility



Defender for Identity

In today's digital world, compromised identities are a gateway to devastating cyberattacks. Leveraging the advanced capabilities of Microsoft Defender for Identity, Pathway delivers a cloud-based security service that **protects your organization's identities** against evolving cyber threats and integrates seamlessly with our Defender XDR for comprehensive threat detection and response across your hybrid environment.



What our service can do for your business



Proactive Threat Detection

- We utilize Defender for Identity to grant you a **clear view of your identity security posture**.
- Pathway identifies and addresses vulnerabilities before they're exploited, leveraging **real-time analytics and data intelligence** to detect suspicious activities and potential breaches.
- Our experts **uncover advanced threats** across the entire cyberattack lifecycle, safeguarding your organization



Enhanced Security Posture

- Pathway helps **reduce your attack surface** by identifying and mitigating security misconfigurations.
- We translate security assessments into **actionable recommendations** to improve your overall security posture.
- Pathway simplifies security operations by prioritizing relevant **security alerts** and providing user activity timelines for efficient threat investigation.



Suspicious Activity Detection across Attack Stages

- **Reconnaissance:** We uncover attempts to gather information about your users, groups, and resources.
- **Compromised Credentials:** Pathway detects brute force attacks, suspicious sign-ins, and compromised user accounts.
- **Lateral Movement:** We identify attempts to move laterally within the network to access valuable assets.
- **Domain Dominance:** Pathway detects attempts to gain control of domain controllers, preventing widespread compromise.

Benefits



Proactive Defence



Improved Visibility



Reduced Attack Surface



Simplified Management



Defender for Office 365

While Office 365 offers basic security, today's threats require advanced protection. By enhancing the robust capabilities of Microsoft Defender for Office 365, Pathway delivers tailored security services that safeguard your organization against sophisticated attacks across email, links, attachments, and collaboration tools like SharePoint, OneDrive, and Teams.



70 billion

Microsoft blocked 70 billion emails and identity attacks in 2023.

What our service can do for your business



Powerful Threat Detection

- **Anti-Phishing:** We leverage Defender for Office 365's AI-powered anti-phishing to protect against credential theft, spoofing, impersonation attacks, and unusual sender activity.
- **Safe Attachments & Links:** We identify malicious files and unsafe web destinations before they compromise your systems.



Automated Response

- **Zero-Hour Auto Purge (ZAP):** We remove malicious emails even after they've reached inboxes, protecting users from delayed threats.
- **Automated Investigation and Response (AIR):** We save your security team time and effort by automating threat analysis and remediation processes.



Simplified Security Management

- **Preset Security Policies:** Pathway sets you up for success with pre-configured security policies, customizing them to your organization's unique needs.
- **Real-Time Reporting:** Pathway offers detailed insights into threat activity and the effectiveness of your protection measures.

Benefits



Proactive Protection



Reduced User Burden



Improved Productivity



Centralized Management

Information Protection Services

Let's explore in detail:

- Purview Information Protection
- Purview Data Loss Prevention (DLP)

Information Protection Services

In the digital age, safeguarding your sensitive information is paramount. Whether it be financial records, intellectual property, or customer data, protecting this information is critical for maintaining trust, preventing breaches, and ensuring compliance with regulations.

Pathway offers a comprehensive suite of services leveraging Microsoft Information Protection solutions to secure your data throughout its lifecycle. We:

Pathway's Information Protection services empower you to:



Minimize the risk of data breaches and regulatory non-compliance



Foster secure collaboration by minimizing security risks



Enhance trust with stakeholders, customers, partners, and employees



In the following sections, we'll explore how Pathway utilizes specific Microsoft Information Protection solutions to design a customized information protection strategy that perfectly aligns with your organization's unique needs.



Purview Information Protection (PIP)

In today's digital landscape, protecting sensitive information is more critical than ever. Pathway offers a comprehensive service leveraging Microsoft Purview Information Protection (formerly Microsoft Information Protection) to discover, classify, and safeguard your data wherever it resides. Our information protection capabilities give you the tools to **know your data, protect your data, and prevent data loss**. Think of it as your digital bodyguard for sensitive documents, emails, and other crucial information.

What our service can do for your business



Expert Data Classification

Our experts identify and categorize your sensitive data based on pre-defined or custom criteria. This comprehensive understanding empowers informed decision-making around data protection strategies.



Customized Labeling and Protection

Pathway configures data labeling to enforce security policies and automate protection measures. This ensures sensitive information receives the appropriate level of safeguards based on its classification



Proactive Protection Controls

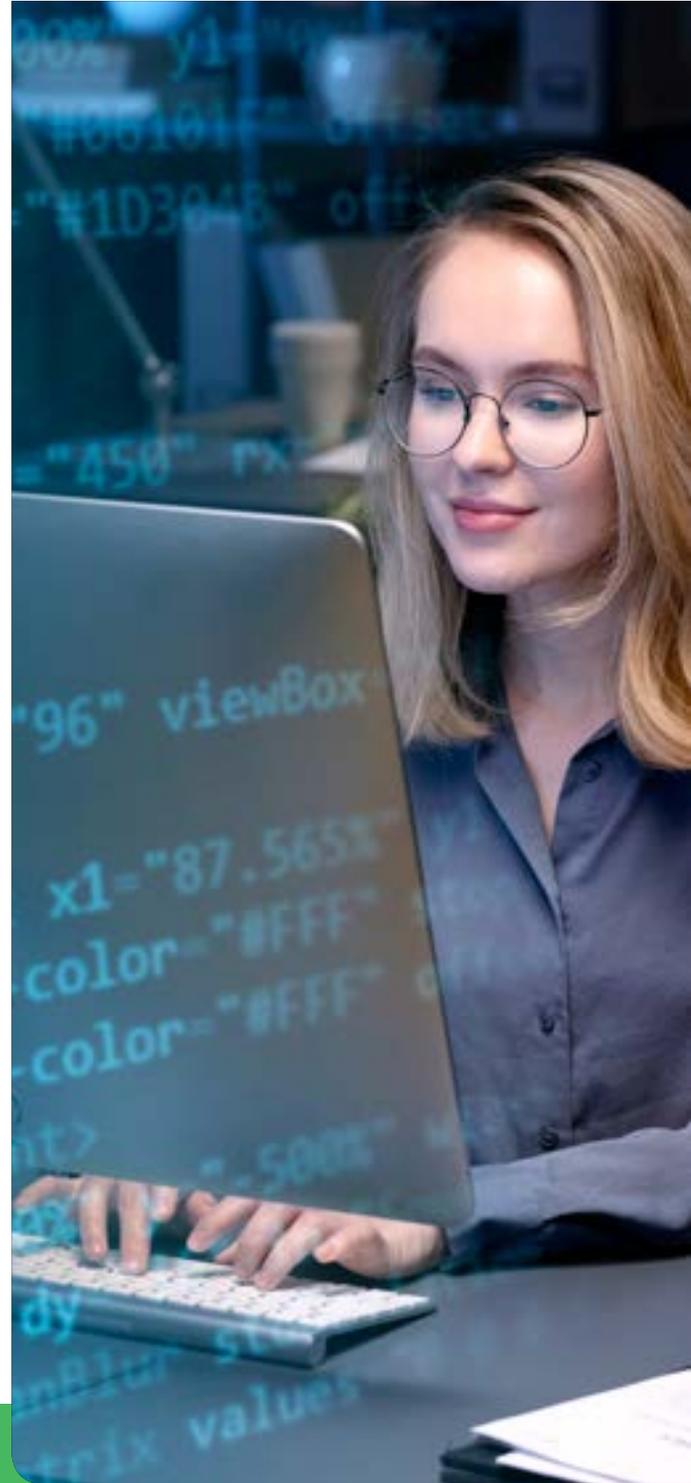
We leverage Purview to implement a robust security posture. This includes:

-  **Encryption:** Protecting data at rest and in transit.
-  **Access Control:** Restricting access to authorized users or groups.
-  **Data Loss Prevention (DLP):** Preventing unauthorized data exfiltration



Insightful Activity Monitoring

Pathway utilizes Purview's Activity Explorer to gain insights into user activity related to sensitive data. This enables proactive monitoring and mitigation of potential security risks.



Benefits



Persistent Protection



Centralized Management



User Empowerment



Flexible Deployment



Purview Data Loss Prevention (DLP)

Sensitive data breaches can disrupt your business. Pathway offers a comprehensive service leveraging Microsoft Purview Data Loss Prevention to safeguard your data across various platforms – Office 365, OneDrive, SharePoint, Teams, and Endpoints. Our tailored service can identify, monitor, and automatically **protect sensitive data from being accidentally or intentionally shared**, used, or transferred in unauthorized ways.



What our service can do for your business



Policy Creation

Our experts create DLP policies that define:

-  **What sensitive data to look for:** Pre-defined types (credit card numbers, social security numbers, etc.) or custom patterns (like project code names).
-  **Where to look for this data:** Exchange email, SharePoint sites, OneDrive for Business, Teams chats, on-premises repositories, and more.
-  **Actions to take:** Block sharing, encrypt the content, display policy tips to users, generate alerts, or audit the actions.



Detection

Utilizing Microsoft Purview DLP, Pathway scans content continuously in specified locations, looking for matches against your defined policies.



Enforcement

With Pathway, data protection is not reactive but proactive. If sensitive data is detected in a way that violates the pre-defined policy, the actions specified are automatically enforced to protect the data.

Benefits



Proactive Prevention



Centralized Management

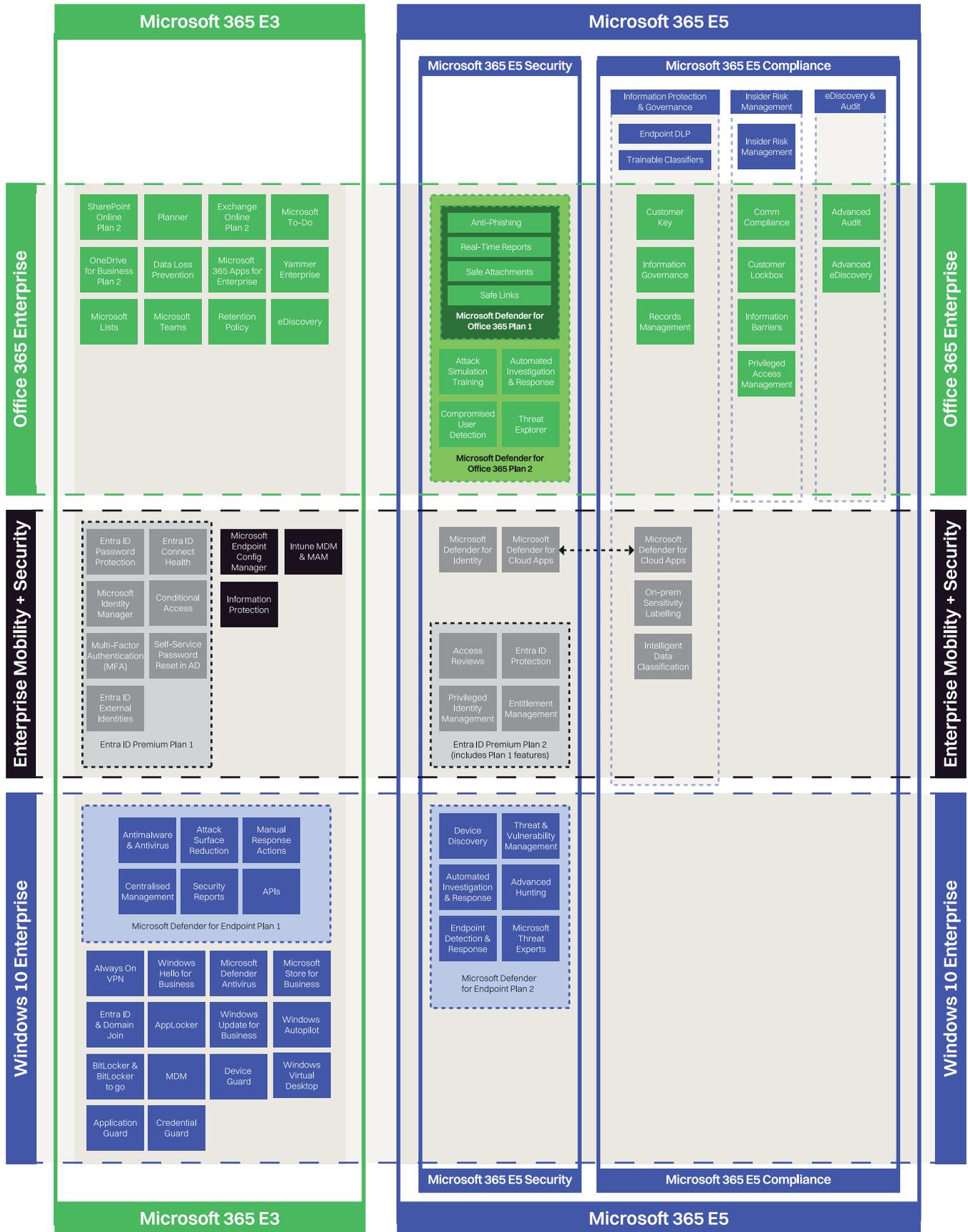


Flexibility



Insights and Reporting

Microsoft 365 Licensing



Infographic for guidance only. Details accurate at time of publishing but subject to change. Please check before investing.

Identity and Access Management Services

Let's explore in detail:

- [Entra ID](#)
- [Entra ID Connect](#)
- [Entra ID Protection](#)
- [Entra ID Governance](#)
- [Identity Manager](#)

Identity and Access Management (IAM)

In today's digital landscape, secure access to critical resources is vital for any organization. Leveraging Microsoft Identity and Access Management (IAM), Pathway offers comprehensive services that manage user identities and access permissions. Our services ensure that the **right people have access to the right resources, at the right time, using the right device.**

80%

More than 80 percent of breaches can be attributed to identity-based attacks, and that number is only growing.

Source: Microsoft

Our IAM services help you accomplish this through:



Identity Management: Pathway ensures every user's identity is accurately verified and continuously updated by leveraging Microsoft's cutting-edge technologies to maintain an up-to-date user database within your organization.



Access Management: We customize access management solutions to grant the right levels of access to the right resources, aligning with individual roles and business requirements and ensuring secure and efficient operation.



Pathway's IAM as the Foundation for Your Security Strategy

Our IAM serves as the foundation for a robust security posture. It provides the essential groundwork for other security solutions, such as:



Multi-factor authentication (MFA)



Conditional access



Data encryption

Pathway's Microsoft Entra and other Microsoft security services build upon this foundation, offering a comprehensive suite of tools to address your specific security needs.

By implementing a robust IAM strategy, we empower your organization to **collaborate securely, increase productivity, and stay compliant** in the ever-evolving digital landscape.

In subsequent sections, we'll unlock the full power of secure and efficient access with a suite of powerful IAM services from Pathway.



Entra ID

Managing user access across hybrid and multi-cloud environments can be complex. Pathway revolutionizes your access control mechanisms by integrating Microsoft Entra ID, a leading cloud-based identity and access management (IAM) platform. Our service transforms how users interact with your resources across hybrid and multi-cloud environments, ensuring secure and seamless access.

What our service can do for your business



Adaptive Access

Our experts configure Entra ID to enforce dynamic access policies based on real-time risk factors. This ensures that only authorized users gain access to critical resources, minimizing security vulnerabilities.



Multi-factor Authentication (MFA)

Pathway implements Multi-Factor Authentication (MFA) as an extra layer of security beyond passwords. This significantly reduces the risk of unauthorized access to user identities.



Identity Protection

We leverage Entra ID's automated tools to proactively identify and mitigate identity-based threats. This minimizes the potential damage caused by compromised credentials.



Unified Identity Management

Pathway streamlines identity management by enabling you to manage all user identities and access permissions centrally through Entra ID. This simplifies administration and reduces the risk of human error.



Single Sign-On (SSO)

Say goodbye to multiple logins! Pathway configures Entra ID to offer Single Sign-On (SSO), allowing users to access all authorized applications seamlessly with a single login.



End-User Self-Service

Pathway helps you set up Entra ID's self-service portals. This empowers users to manage their passwords, access requests, and other settings independently, reducing IT burden.



Benefits



Enhanced Security



Improved User Experience



Scalability and Flexibility



Seamless Integration



Entra ID Connect

Managing identities and access across cloud and on-premises environments can be a challenge. Pathway offers a streamlined service with Microsoft Entra ID Connect, an on-premises application that synchronizes identities and permissions between your existing directory and Microsoft Entra ID. This allows users to **seamlessly access both cloud and on-premises resources** with a single identity.



What our service can do for your business



Password Hash Synchronization

We securely synchronize password hashes for on-premises user accounts, eliminating the need to store passwords in the cloud.



Pass-through Authentication

We enable users to maintain familiar login credentials for both cloud and on-premises resources, simplifying access management and reducing user frustration.



Comprehensive Synchronization

Pathway ensures that user accounts, groups, and directory objects are accurately mirrored across environments, facilitating smooth operations.



Robust Health Monitoring

Pathway provides centralized monitoring and insights into synchronization and sign-in activity for complete visibility.

Benefits



Simplified User Experience



Increased Productivity



Enhanced Security



Streamlined Management



Entra ID Protection

Compromised identities are a major security concern in today's digital landscape. Pathway offers a comprehensive service leveraging Microsoft Entra ID Protection, a powerful cloud-based solution that helps you **prevent, detect, and remediate identity compromise in real time**. By analysing user and sign-in patterns based on integrated risk scores from various sources, we protect your organization against identity-based attacks, such as password spray, brute force, phishing, infected devices, and leaked credentials.



What our service can do for your business



Prevent Account Takeovers

We leverage integrated risk scores to identify and block unauthorized access attempts in real time, protecting sensitive data and resources from account takeovers



Safeguard against Credential Theft

Pathway implements high-assurance authentication methods to add extra security layers that safeguard against credential theft and unauthorized access attempts.



Gain Deeper Security Insights

Gain valuable intelligence on potential threats and attack patterns for proactive defence.



Automate Threat Detection and Response

We leverage machine learning to automatically identify high-risk users, sign-ins, and potential attacks, enabling a faster and more efficient response to security threats.



Have Dynamic Access Controls

Pathway configures Entra ID Protection to automatically adjust access privileges based on changing risk factors, such as location or device type. This ensures that only authorized users have access to critical resources based on the real-time risk assessment.

Benefits



Proactive Threat Detection



Automated Response



Improved Visibility and Reporting



Easy Integration



Entra ID Governance

Managing access rights across complex on-premises, cloud, and hybrid environments can be a daunting task. Pathway offers a comprehensive service leveraging Microsoft Entra ID Governance, a powerful tool that helps you **establish clear rules and automate access control for your organization**. Think of it as your organization's rulebook for who can access what, when, and under what circumstances.

What our service can do for your business



Entitlement Management

Our experts configure Entra ID Governance to automate access request workflows, assignments, reviews, and expirations. This simplifies access lifecycle management, saving you time and minimizing the risk of human error.



Lifecycle Workflows

Pathway helps you design automated workflows for user onboarding, access changes, and offboarding. This ensures a smooth user experience and eliminates manual tasks associated with access management.



AI-driven Access Reviews

We assist you in utilizing automated workflows for regular access reviews, ensuring only authorized users have access to critical resources.



Privileged Identity Management (PIM)

Pathway implements PIM within Entra ID Governance to establish granular controls for privileged users. This minimizes the risk of unauthorized access to sensitive data and resources.



Benefits



Improved Security



Enhanced Compliance



Increased Efficiency



User Self-Service



Identity Manager

Pathway leverages Microsoft Identity Manager (MIM), an established on-premises identity and access management solution, as a foundational element for **managing user identities in hybrid IT environments**. Our expertise bridges the critical gap between your on-premises systems and cloud services, ensuring seamless synchronization and management.

What our service can do for your business



User and Group Synchronization

We expertly synchronize identity data (users, groups, and attributes) between various systems, which primarily include Active Directory, other directories like LDAP (Lightweight Directory Access Protocol), HR systems, and databases. This ensures consistency and accuracy in identity information.



Workflow and Policy Management

Our team designs custom workflows tailored to your organization's needs for activities, such as account provisioning and de-provisioning, enforcing access control policies and rules, and approval workflows



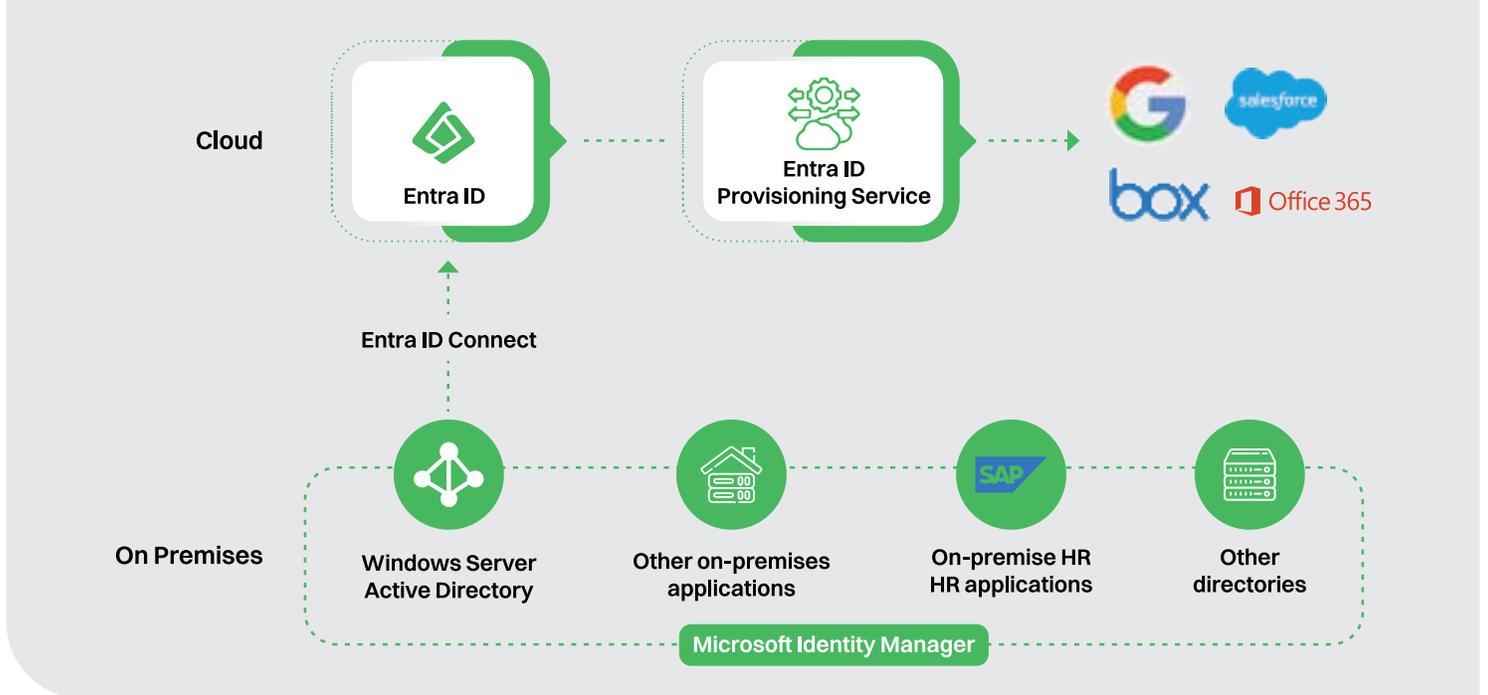
Self-Service Identity Management

Pathway enhances user autonomy by providing self-service options for password resets, profile updates, and group management, streamlining the user experience.



Privileged Access Management (PAM)

We implement PAM features within MIM to manage privileged accounts, such as time-limited access and approval process for access elevation



Benefits



Enhanced Security



Increased Productivity



Improved Efficiency and Cost Savings



Easy Integration

Security Management Services

Let's explore in detail:

- Defender for Cloud
- Sentinel

Security Management

In today's ever-evolving threat landscape, protecting your organization requires a comprehensive and centralized approach. Pathway offers powerful services leveraging Microsoft Security Management, which is designed to empower you:



Gain Comprehensive Visibility: We leverage Microsoft Security Management to provide a unified view of your security posture across cloud, on-premises, and hybrid environments. This holistic view empowers you to identify and address potential security gaps effectively.



Detect and Respond to Threats Faster: Pathway configures advanced analytics and machine learning within Microsoft Security Management for real-time identification and prioritization of security incidents. This enables a swifter and more effective response.



Automate Security Tasks: Our experts help you automate security tasks like threat detection, investigation, and remediation within Microsoft Security Management. This frees up valuable IT resources and lets your team focus on strategic initiatives.

In the following sections, we'll explore the powerhouses within Microsoft Security Management—Microsoft Defender for Cloud and Microsoft Sentinel dangers—to understand how Pathway can help you leverage them for enhanced security.





Defender for Cloud

Managing security across multi-cloud environments can be complex. Pathway offers a comprehensive service leveraging Microsoft Defender for Cloud, a powerful Cloud-Native Application Protection Platform (CNAPP) designed to safeguard your cloud-based applications from various cyber threats and vulnerabilities. Our service combines the power of:



DevSecOps: Unifies security management across your codebase, from development to deployment, in multi-cloud and multi-pipeline environments.



Cloud Security Posture Management (CSPM): Identifies and prioritize actions to prevent security breaches proactively.



Cloud Workload Protection Platform (CWPP): Provides specific protection for your servers, containers, databases, and other workloads.

What our service can do for your business



Visualize and Improve Your Security Posture

Gain continuous assessments, built-in benchmarks, and recommendations to proactively improve your cloud security across various platforms, including Azure, AWS, Google Cloud, and DevOps pipelines.



Protect Workloads from Various Threats

Benefit from **broad workload security coverage** supported by leading security intelligence, safeguarding your virtual machines, containers, databases, and storage from malware and other attacks.



Prioritize Critical Risks

Leverage **cyberthreat path analysis and contextual threat data** to identify vulnerabilities with the highest potential impact, enabling efficient resource allocation for remediation.



Unify Visibility for DevOps Security

We provide comprehensive insights into your DevOps environment, including application code, configurations, and security posture across multi-cloud and pipeline deployments.



Secure Configurations throughout the Development Lifecycle

Pathway helps you implement security measures for infrastructure-as-code templates and container images to minimize misconfigurations reaching production environments.



Accelerate Remediation of Critical Issues

We prioritize critical issues and deliver **actionable guidance** directly within your developer tools. This contextual insight empowers swift remediation of security vulnerabilities.

Benefits



Enhanced Security Posture



Prioritized Threat Response



Streamlined Security Operations



Comprehensive Protection





Sentinel

Managing security incidents across a complex IT landscape can be overwhelming. Pathway offers a comprehensive service leveraging Microsoft Sentinel, a powerful cloud-native SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platform. Think of it as your security command center, designed to help you **collect, analyze, and respond to security threats across your entire environment.**

What our service can do for your business



Centralized Data Collection

We help you leverage Sentinel's built-in connectors to gather data from diverse sources across your IT environment. This provides a comprehensive view of your security landscape, empowering you to identify and address potential threats effectively.



Advanced Analytics and Hunting

Pathway configures Sentinel to utilize AI and machine learning to detect hidden threats, analyze entity behaviour, and uncover potential attacks before they cause damage.



Incident Management and Visualization

You'll be able to investigate related alerts, visualize attack timelines, and make informed decisions during threat responses.



Automated Response

Pathway helps you design automated workflows and playbooks within Sentinel. This allows for the automation of repetitive tasks, significantly reducing manual effort and accelerating your overall security response.



Benefits



Enhanced Threat Detection



Improved Efficiency



Faster Response Times



Reduced Operational Costs

Unify and Conquer

Today's cyber landscape demands a multifaceted approach to security. While our individual Microsoft Enterprise Security Services provide excellent protection in their respective areas, **unifying them creates an interconnected ecosystem that offers unparalleled defence against modern threats.**

In doing so, you'll benefit from:



Enhanced Visibility

Gain a **centralized view** of your entire security posture across cloud, on-premises, and hybrid environments. Identify and prioritize threats effectively with a unified overview of security data.



Streamlined Operations

Eliminate the complexity of managing separate solutions. Leverage a **unified platform for deployment, configuration, and management**, simplifying routine tasks and maximizing security team efficiency.



Improved Threat Detection and Response

Benefit from **unified threat intelligence and analytics** across all security solutions. This holistic view enables faster identification and remediation of potential threats, minimizing potential damages and downtime.



Enhanced Insights and Decision-Making

Gain a **deeper understanding of your security posture** by correlating data from various sources. This enables informed decision-making and proactive strategies to address evolving security threats.



Simplified Compliance Management

Streamline compliance efforts by leveraging the unified capabilities of Microsoft Security Solutions. Meet industry standards and regulations with greater ease and efficiency.



Investing in our unified Microsoft Enterprise Security ecosystem empowers your organization to confront cyber threats with confidence, allowing you to **focus on your core business objectives**. By unifying our Services, you gain a truly comprehensive security posture, equipping your organization to face ever-evolving threats head-on.

Ready to Elevate Your Security Posture?

Take the next step towards a more secure future. Partnering with Pathway unlocks the full potential of Microsoft Security Solutions, empowering you to:



Unify and simplify your security environment for enhanced visibility and streamlined operations.



Strengthen your defences with comprehensive protection against evolving cyber threats.



Empower your security team with the expertise and tools to achieve peak performance



Make informed decisions based on actionable insights and data-driven strategies

Schedule a free consultation with our security specialists to discuss your unique needs and explore how we can help you achieve your security goals.

Together, let's build a robust and resilient digital landscape for your organization.

Call Us Today!



About Pathway Communications

Pathway Communications specializes in providing innovative and cost-effective IT, Cybersecurity, and Communication solutions for businesses of all sizes. Rooted in Canada, we offer a wide range of services, including Managed IT Services, Security Solutions, Data Center, Cloud, Colocation, Voice, Data, and Internet, to help our clients stay connected and operate securely in today's fast-paced world.



The certifications mentioned above represent a selection of our achievements and do not encompass the complete range. Please get in touch with us for a comprehensive list of our certifications.



Follow us for regular updates



Contact us

- +416-214-6363
- cybersecurity@pathcom.com
- 95 Apple Creek Blvd., Markham
- www.cybersecurity.pathcom.com

Scan the QR code to visit our website

