CLOUDFLARE

JOINT SOLUTION BRIEF

Secure Hybrid Work with Microsoft + Cloudflare

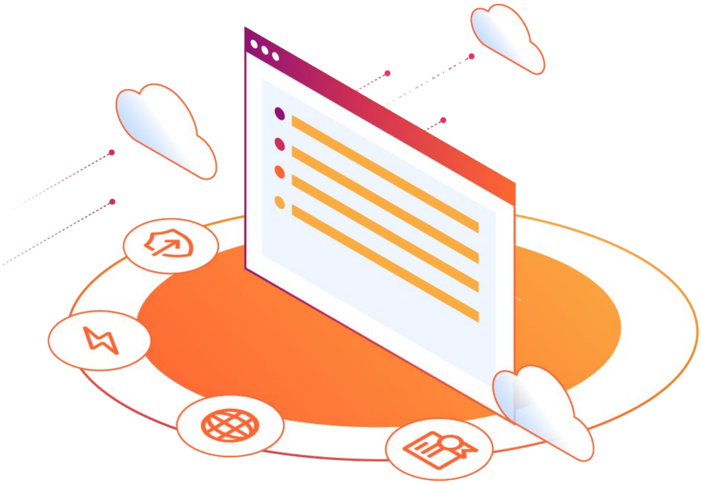
Accelerate cloud modernization and productivity

Cloud migration risks

Addressing hybrid-cloud challenges

With the accelerated shift to hybrid work, organizations are modernizing their environment by turning to Microsoft for many of their cloud migration needs. Unfortunately, due to the popularity of Microsoft's cloud applications and services, this shift to the cloud can often further expose users and applications to a wider range of threats.

Migrating resources to the cloud can also involve managing a combination of SaaS, self-hosted, and non-web applications, which further complicates the ability to secure and control access to those resources. Using outdated technology, such as VPNs, to securely connect users to applications can create security gaps and frustrate employees.



Partnering for greater security outcomes

With multiple integration points across Microsoft's cloud ecosystem, Cloudflare enables customers to eliminate gaps in security, performance, and reliability.

Greater efficiency

Simplify access to hybrid and multi-cloud environments by extending Azure Active Directory (AD) control to non-Microsoft apps while consolidating management with a single, unified interface.

Complete protection

Provide secure access to any resource, regardless of location, with limited access for unmanaged devices – all while protecting users from business email compromise (BEC) and targeted phishing threats.

Continuous productivity

Enable employees to safely access the vital resources they depend on while enforcing policy requirements and ensuring secure and reliable connectivity with zero workflow disruption.

Integrated solutions for hybrid work

Cloudflare Zero Trust

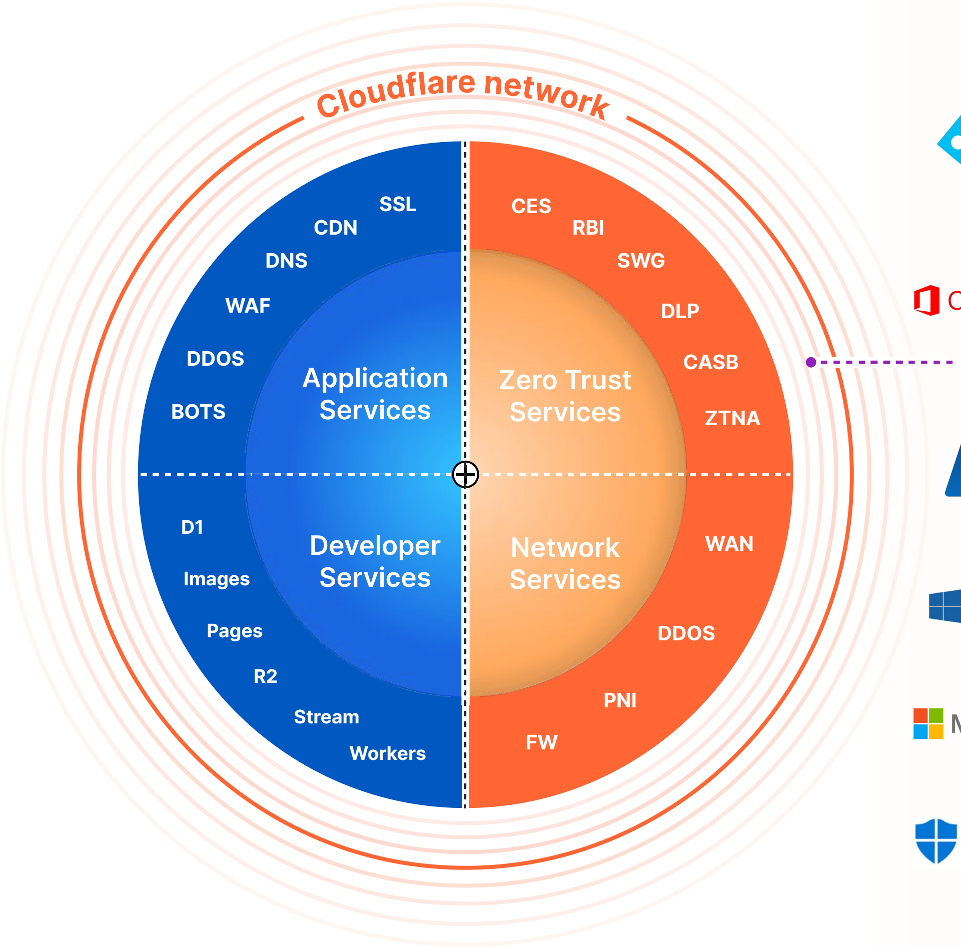
Cloudflare offers Zero Trust services that deliver fast and secure access to applications, while ensuring comprehensive protection against SaaS application exposure, malware, and targeted phishing threats. These services provide:

- Secure network access
- Risky user isolation
- Phishing and BEC protection
- Application and data visibility

Microsoft Cloud

Microsoft offers cloud applications and services that support and accelerate hybrid work, while delivering essential protection across identities, devices, data, applications, and infrastructure. These services include:

- Cloud productivity suite
- Cloud-hosted applications
- Identity protection
- Endpoint security



Azure Active Directory
Enable secure authentication and conditional access across hybrid work

Microsoft 365
Improve protection with a preemptive defense from socially engineered phish and misconfiguration risks

Azure Apps and VPCs
Enable secure access to on-prem or Azure-hosted apps without needing a VPN

Endpoint Security Mgr
Identify and remediate threats faster, and securely manage devices from a single platform

Networking Partner
Deliver a fast, secure Office 365 experience to customers' employees

Defender & Sentinel APIs
Integrate XDR & SIEM context into access policies

Simplify and secure access

A faster and safer way to connect users to apps

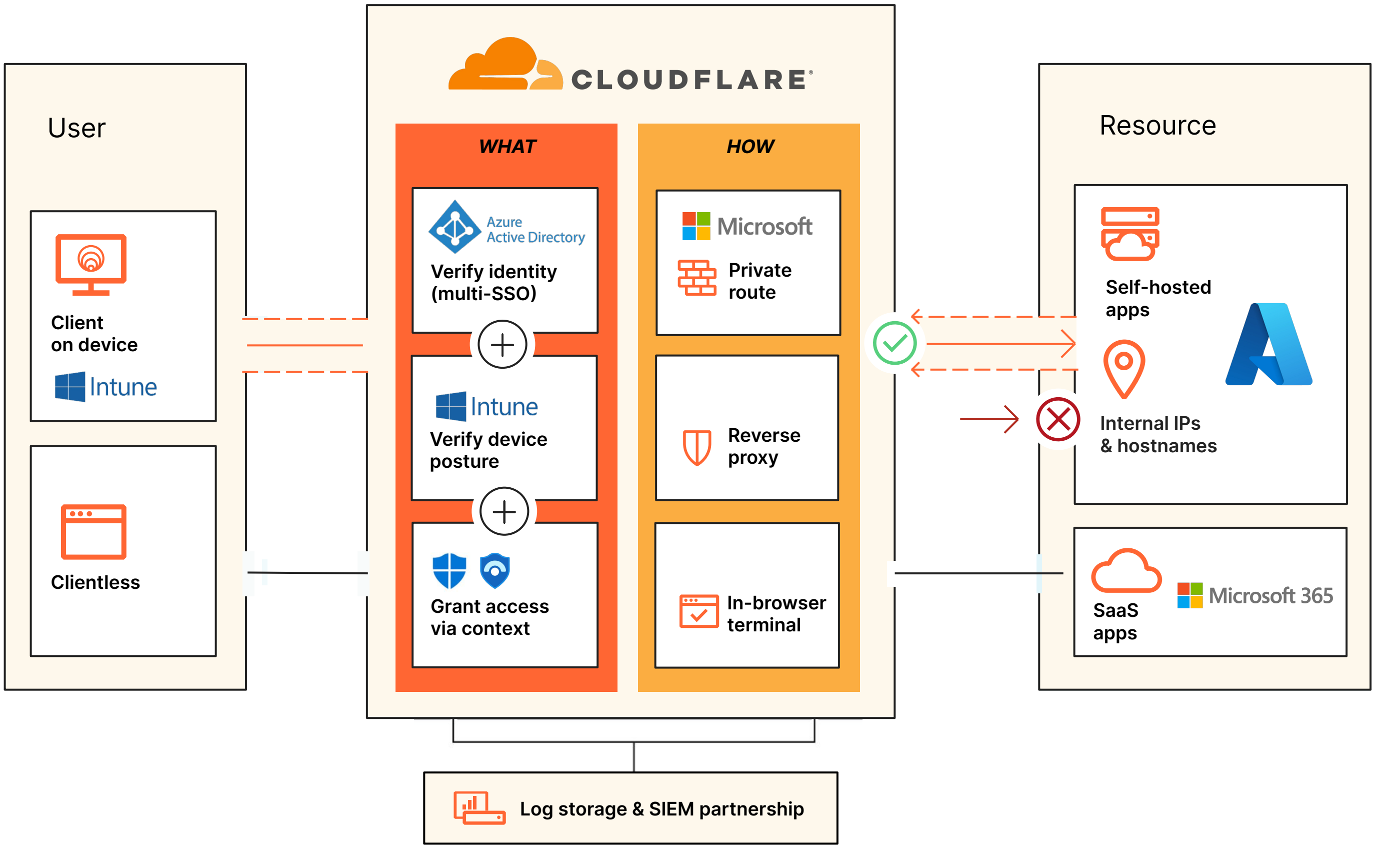
Traditional perimeter-based access controls (like VPNs) are increasingly a liability. Sluggish performance hurts end-user productivity, administrators struggle with unwieldy configuration, and lateral movement is hard to contain. Accelerated cloud adoption and hybrid work have further exposed these flaws and made VPNs more vulnerable.

Cloudflare Access replaces VPN clients to protect any application, in any on-prem network, public cloud, or SaaS environment. By integrating with Microsoft Intune and Azure Active Directory (AD), Cloudflare can enforce default-deny, Zero Trust rules and provide conditional access to internal resources based on identity and device posture.

Per-application conditional access

Cloudflare's integrations with Azure AD and Intune enable both identity and device posture-aware policy enforcement. Azure AD allows administrators to create and enforce policies on both applications and users using Conditional Access. It provides a wide range of parameters that can be used to control user access to applications (e.g. user risk level, sign-in risk level, device platform, location, client apps, etc.).

For client-based deployment, policies can leverage the enhanced telemetry and context that Intune provides surrounding a user's device posture and compliance state. This allows security teams to define their security conditions in Azure AD and enforce them through Cloudflare Access.



Prevent user deception & exploitation

Safeguard users and data with layered security

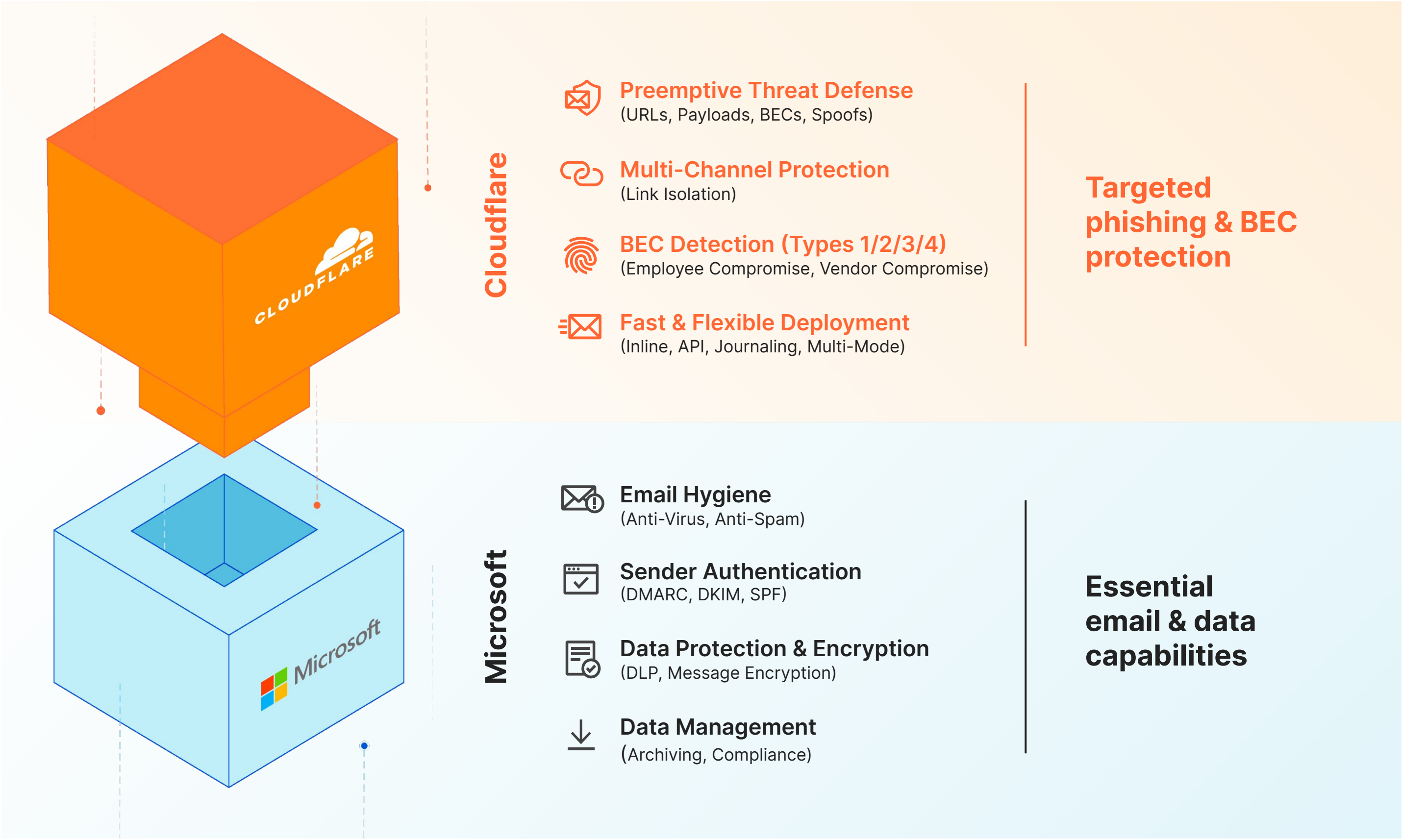
As modern phishing threats increase in sophistication and social engineering tactics become more convincing, the exploitation of individual users continues to represent the largest risk to organizations. To reduce this risk, Microsoft continues to develop and deliver essential controls for email hygiene and outbound data protection.

However, targeted and evasive attacks can often bypass built-in security controls. By preemptively detecting phishing campaigns early in the attack lifecycle and automatically blocking or isolating malicious content, Cloudflare can augment native Microsoft controls to provide comprehensive protection against threats that target users across email and other collaboration applications.

Stop targeted phishing and BEC attacks

Deploy advanced protection in minutes with flexible configuration options and a cloud architecture that scales to any requirements. By enhancing native M365 controls with Cloudflare, organizations can:

- **Prevent malware-less financial fraud** with machine learning (ML) that analyzes message context to detect compromised accounts.
- **Block emerging threats in real-time**, without needing to constantly tune a secure email gateway or wait for signature/policy updates.
- **Discover impersonated accounts and domains**, including lookalike and proximity domains that attackers use to bypass DMARC, DKIM, and SPF.
- **Isolate deferred and multi-channel attacks** that often evade traditional email security controls using deceptive links.



Cloudflare

Preemptive Threat Defense
(URLs, Payloads, BECs, Spoofs)

Multi-Channel Protection
(Link Isolation)

BEC Detection (Types 1/2/3/4)
(Employee Compromise, Vendor Compromise)

Fast & Flexible Deployment
(Inline, API, Journaling, Multi-Mode)

Targeted phishing & BEC protection

Microsoft

Email Hygiene
(Anti-Virus, Anti-Spam)

Sender Authentication
(DMARC, DKIM, SPF)

Data Protection & Encryption
(DLP, Message Encryption)

Data Management
(Archiving, Compliance)

Essential email & data capabilities

Eliminate SaaS and data exposure

Greater visibility across SaaS applications

Modern workforces rely on SaaS applications and cloud productivity suites, like Microsoft 365, now more than ever. Microsoft's mission-critical SaaS applications drive business productivity, but also introduce security risks, visibility challenges, and access control roadblocks.

As organizations adopt dozens of SaaS applications, it becomes increasingly difficult to maintain consistent security, visibility, and performance. With every application having a different configuration and requiring unique security considerations, IT teams are challenged with staying compliant and protecting sensitive data across a wide landscape.

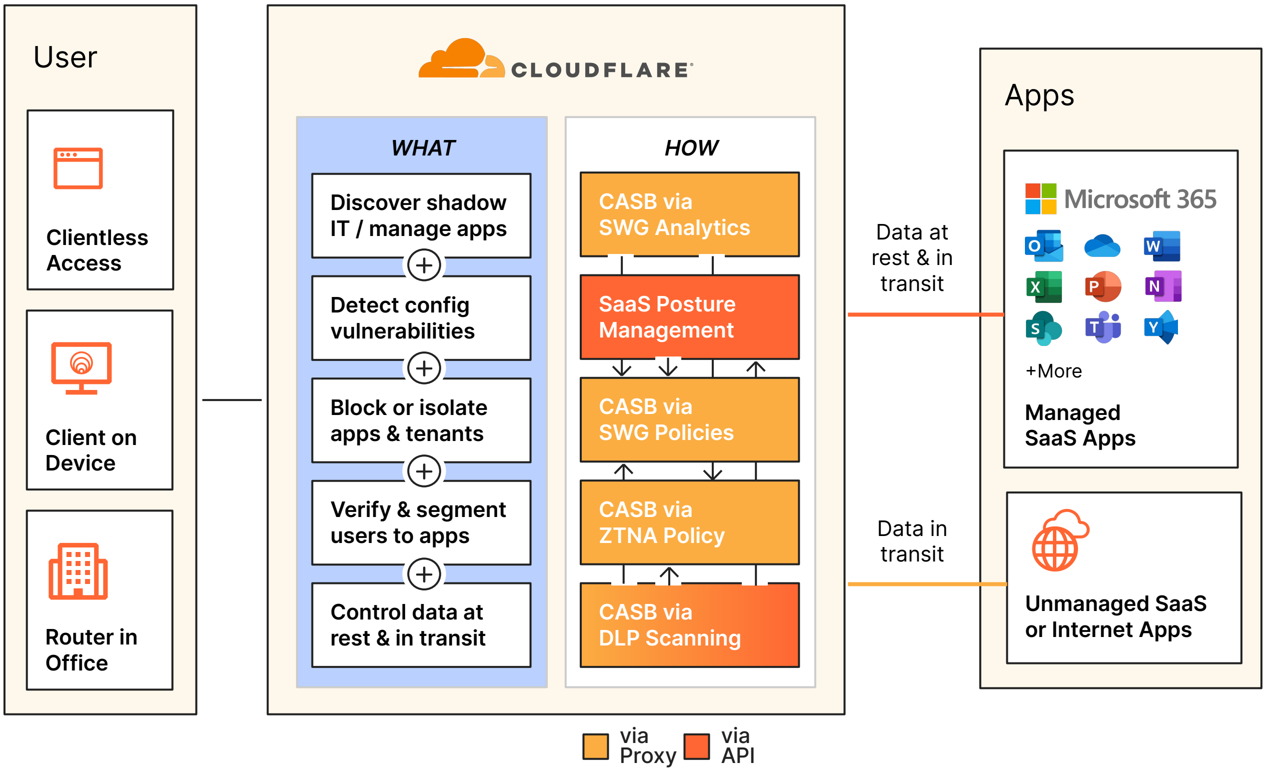
Cloudflare CASB removes these hurdles by providing extensive visibility across Microsoft 365 and other popular SaaS applications. This visibility enables organizations to quickly identify misconfigurations, exposed files, user access, and 3rd-party access.

Greater control over access and usage

SaaS applications operate outside of the corporate network, which can limit the amount of control over how employees use these applications. Cloudflare delivers greater control over SaaS applications to easily prevent data leaks and compliance violations. These controls include:

Tenant and data protection controls
Apply tenant controls to prevent users from accessing and storing data in the wrong versions of popular SaaS applications, either inadvertently or maliciously. Disable user actions (e.g. copy/paste, download/upload, print, etc.) to minimize the risk of data loss.

Shadow IT controls
Aggregate and automatically categorize all HTTP requests so that admins can set the status and track the usage of both approved and unapproved applications.



Stop data loss and exfiltration

Increase agility, not complexity for more data control

Maintaining a thorough inventory of sensitive data is harder than it seems and generally a massive lift for security teams. To help overcome data security troubles, Microsoft offers their customers data classification and protection tools. One popular option are the sensitivity labels available with Microsoft Purview Information Protection. However, customers need the ability to track sensitive data movement even as it migrates beyond the visibility of Microsoft.

With Cloudflare DLP, extend the power of Microsoft's labels to any of your corporate traffic in just a few clicks.

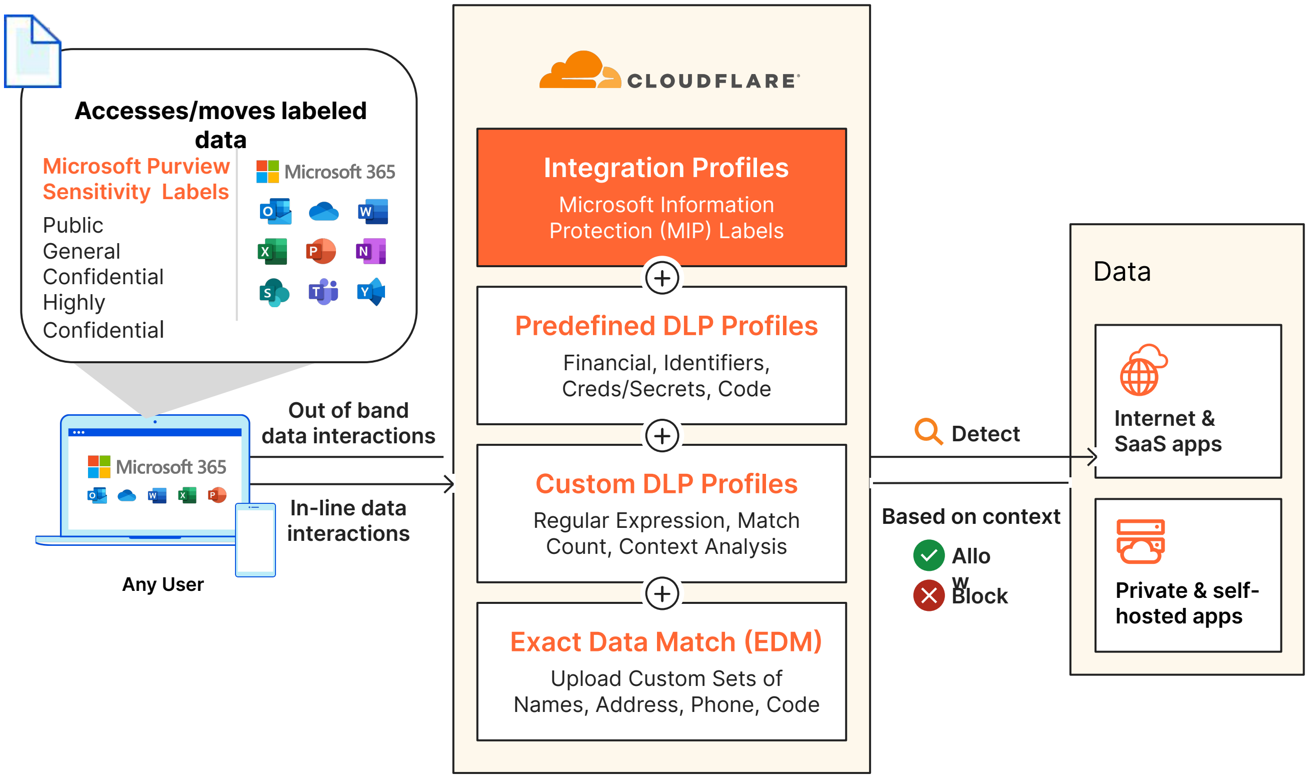
1. Integrate with your Microsoft account
2. Retrieve your sensitivity labels with CASB which automatically populates into DLP profiles
3. Build DLP rules to guide the movement of your confidential labeled data

Simplify regulatory compliance & safeguard IP

Data privacy regulations are becoming stricter and more expansive globally. But the explosive adoption of SaaS and cloud environments is leading to more personal data and code exposures. Cloudflare DLP reduces your risk of data breach by extending visibility and simplifying controls of your most sensitive data.

Regulated data controls
Quickly enable predefined DLP profiles to parse employee network traffic and block sharing of regulated data, such as PII, PHI, and other financial information (e.g., banking / credit card numbers).

Advanced customization for ever changing data
Apply granular controls to your other sensitive data types, such as secrets, code, credentials, and IP, by creating custom DLP profiles with context analysis and Exact Data Match.


Accesses/moves labeled data
Microsoft Purview Sensitivity Labels
Public
General
Confidential
Highly Confidential
Microsoft 365
Microsoft 365
Any User
Out of band data interactions
In-line data interactions
CLOUDFLARE
Integration Profiles
Microsoft Information Protection (MIP) Labels
Predefined DLP Profiles
Financial, Identifiers, Creds/Secrets, Code
Custom DLP Profiles
Regular Expression, Match Count, Context Analysis
Exact Data Match (EDM)
Upload Custom Sets of Names, Address, Phone, Code
Detect
Based on context
Allo
w
Block
Data
Internet & SaaS apps
Private & self-hosted apps

Composable, fully-integrated security

Building resilient operations depends not only on securing resources and infrastructure based on present conditions, but ensuring the ability to easily adapt and scale to future circumstances. By combining the power of Microsoft's cloud solutions with Cloudflare's Zero Trust platform, organizations can safely enable their employees to easily work from anywhere, without fear of costly breaches or disruptions.

No matter where an organizations are at in their cloud migration journey, Cloudflare can layer on protection as needed. Thanks to the composable nature of Cloudflare's Zero Trust platform, businesses can adopt and implement services at their own pace, based on their most critical needs and use cases.

Key takeaways for Microsoft customers

1

Increase value, not cost

Cloudflare enables greater consolidation and unified workflows with Microsoft that accelerate productivity while reducing overhead, manual tasks, and redundant features.

2

Drive seamless security

Cloudflare Zero Trust services complement Microsoft's cloud solutions to enhance their overall operational value while closing security gaps and exposure.

3

Improve resiliency

By simplifying and securing hybrid-cloud environments, Cloudflare and Microsoft can help your organization stay resilient, no matter what future circumstances arise.

Be more secure with Microsoft using Cloudflare One

Request a Zero Trust Workshop

Not quite ready for a live conversation?

Keep learning more about **Cloudflare's SSE & SASE platform**