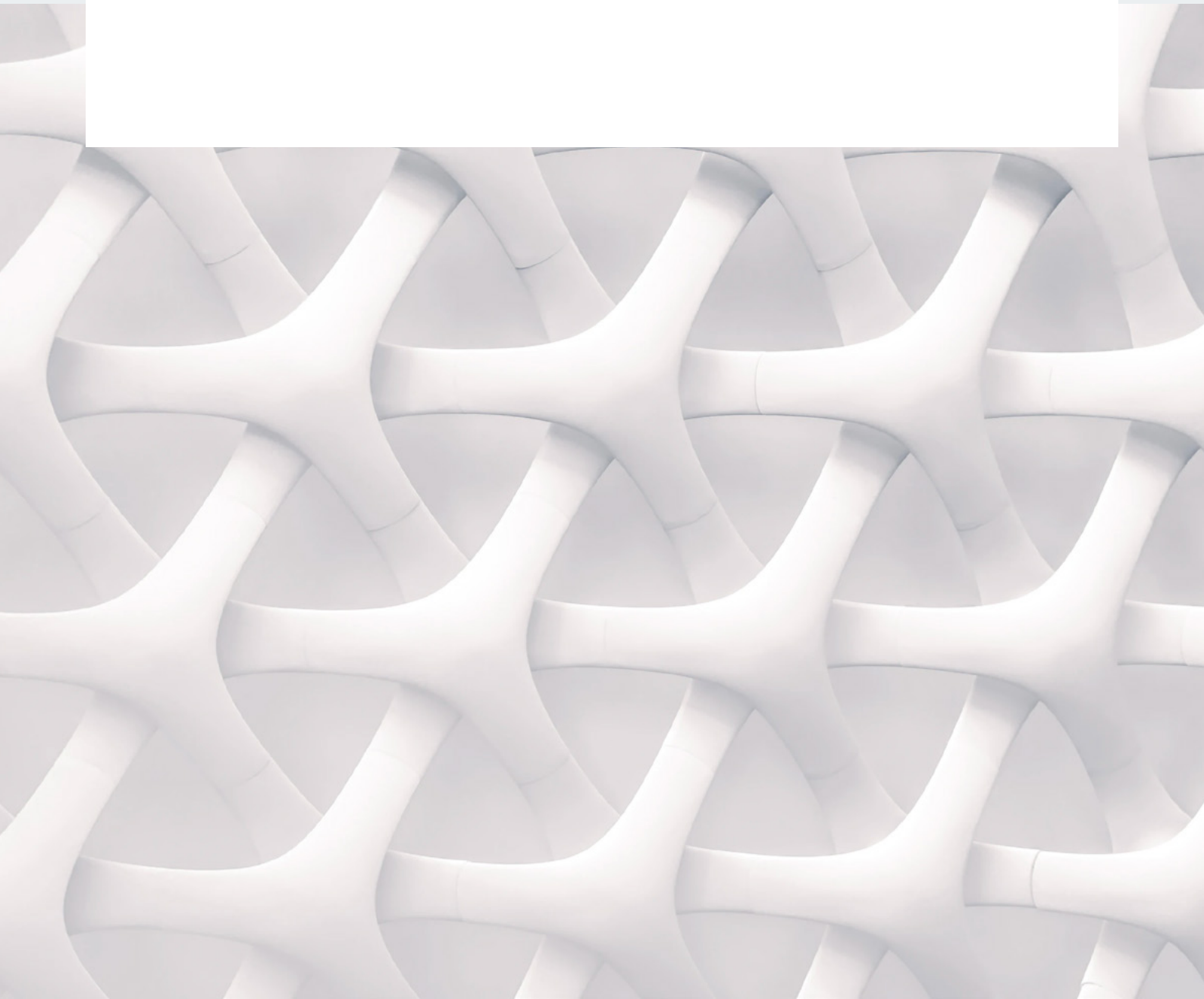
perimeter 81 | Office 365

Securing Office 365 with Perimeter 81 and Azure AD



Introduction

As digitalization and cloud adoption continues to increase combined with technology trends including bring-your-own-device (BYOD), the Internet of Things (IoT) and the proliferation of cloud-connected apps, the enterprise network security perimeter as it stands today is quickly becoming irrelevant.

Protecting enterprises and employees from malicious internet actors has become a battle where every access point and device or endpoint has become the new network perimeter. Today, identity and access management technologies that ensure zero-trust security are becoming critical as employees must access data and resources from not only within an enterprise but also from public cloud providers.

According to industry analyst firm Gartner, compromised identity credentials are a major factor in data breaches with the number of breaches, including identity-related fraud such as account takeovers growing rapidly[1].

"The number of identities for people, things, services and robotic process automation bots keep growing," says Gartner senior director Homan Farahmand. "And the walls between identity domains are blurring IAM architecture."

Because employees can now access their organization's resources from anywhere using many different devices, apps or services, legacy control policies that only focus on who can access a resource are becoming obsolete. To master the balance between strict security and employee productivity, IT admins must take a contextual view of identity by creating conditional access policies and user restrictions to protect data and employees.

Today, Microsoft Azure Active Directory Conditional Access has emerged at the foundational building block of how customers can implement a Zero Trust network approach. Conditional Access and Azure Active Directory Identity Protection make dynamic access control decisions based on user, device, location, and session risk for every resource request. It also combines attested runtime signals about the security state of a Windows device and the trustworthiness of the user session and identity to arrive at the strongest possible security posture.

These access policies control how and when specific authorized users can access corporate resources. Granular access considerations include user role, group membership, device health and compliance with Microsoft Intune for mobile device management (MDM)[2], mobile applications, location, and sign-in and works with any application configured for access with Azure AD.

Microsoft's complete Zero Trust security model includes capabilities from Microsoft 365: Windows Defender Advanced Threat Protection, Azure AD, Windows Defender System Guard, and Microsoft Intune.

1 https://www.gartner.com/smarterwithgartner/next-generation-trends-in-identity-and-access-management/

2 https://docs.microsoft.com/en-us/intune/protect/device-compliance-get-started

Zero Trust Security and Azure AD Conditional Access

Azure AD Conditional Access acts as the fundamental building block of Zero Trust security for Azure. When granting conditional access with Azure Active Directory Identity Protection access decisions are contextual meaning they are made based on user, device, location, and session.

All resource access requests are also based on runtime signals regarding user and device trustworthiness[3]. Conditional Access works with any application configured for access with Azure Active Directory.

Conditional Access policies control how users access corporate resources based on user role, group membership, device health, compliance, mobile application, location, or sign-in risk. Policies also help IT administrators decide whom to give access or deny access to and when, or control access with strict authentication technologies such as multi-factor authentication.

3 https://www.microsoft.com/security/blog/2018/06/14/building-zero-trust-networks-with-microsoft-365/

Azure AD Conditional Access and Federated Identity Management

Federated identity management (FIM) enables multiple enterprise public cloud providers or private network resources to grant resource access with encrypted and reusable identification credentials. This model of identity federation links a user's identity across multiple security domains with each supporting unique and different identity management systems.

When two domains are federated, the user can authenticate to one domain and then access resources in another domain without having to provide separate login credentials, thereby reducing redundancy and increasing worker productivity. Identity federation encompasses may large sets of user-to-user, user-to-application and application-to-application use cases with access from either a web browser or at the the service-oriented architecture level. *(Figure 1)*

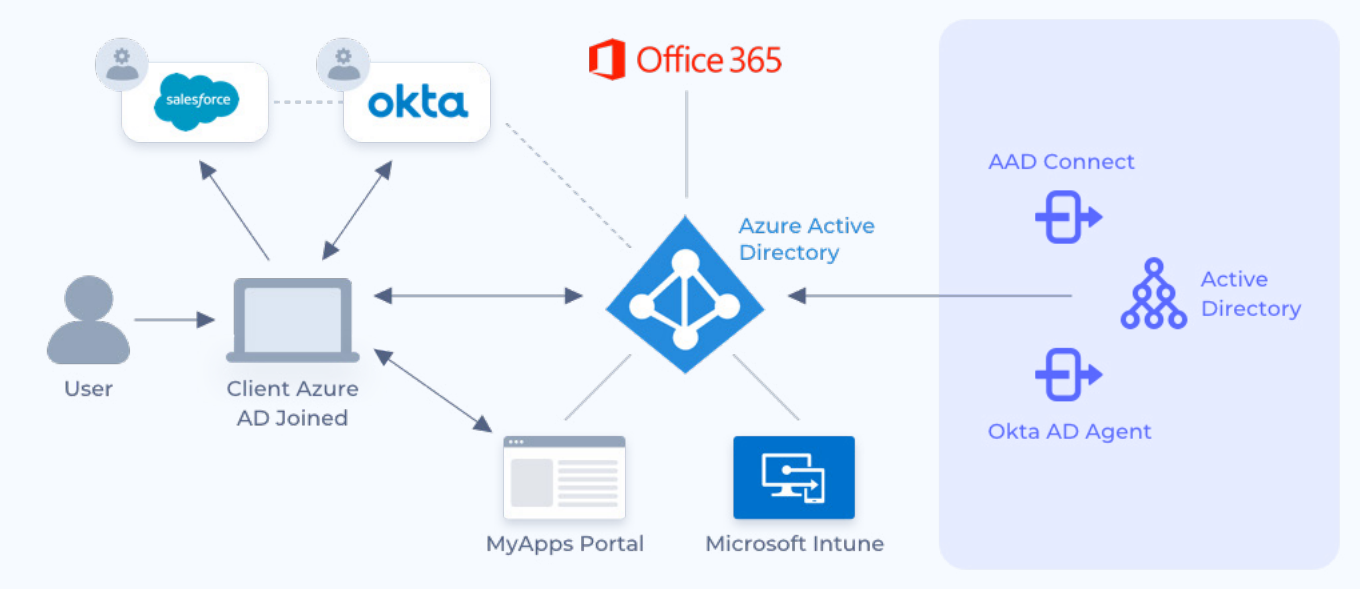


Figure 1

Azure AD Conditional Access is applied before access is granted to the application the user is accessing. When using federated authentication with Azure AD, a trust relationship is established between users and resources. Conditional Access policies with Azure AD federated authentication then support policy decisions that are applied to user sign-ins or additional federation services to sign individual into applications or network resources.

When the configured conditional access policy requires multi-factor authentication, Azure AD redirects to the federation service after the user has signed in. Azure AD then handles policy requirements such as device compliance or other contextual security signals.

Perimeter 81 for AWS

To implement a ZT security architecture combined with Azure AD Conditional Access and Office 365, IT managers must isolate resources within their IT infrastructure in the form of micro-segmentation and connect Perimeter 81 with Office 365 by white-listing any private IP obtained from Perimeter 81 *(Figure 2)*.

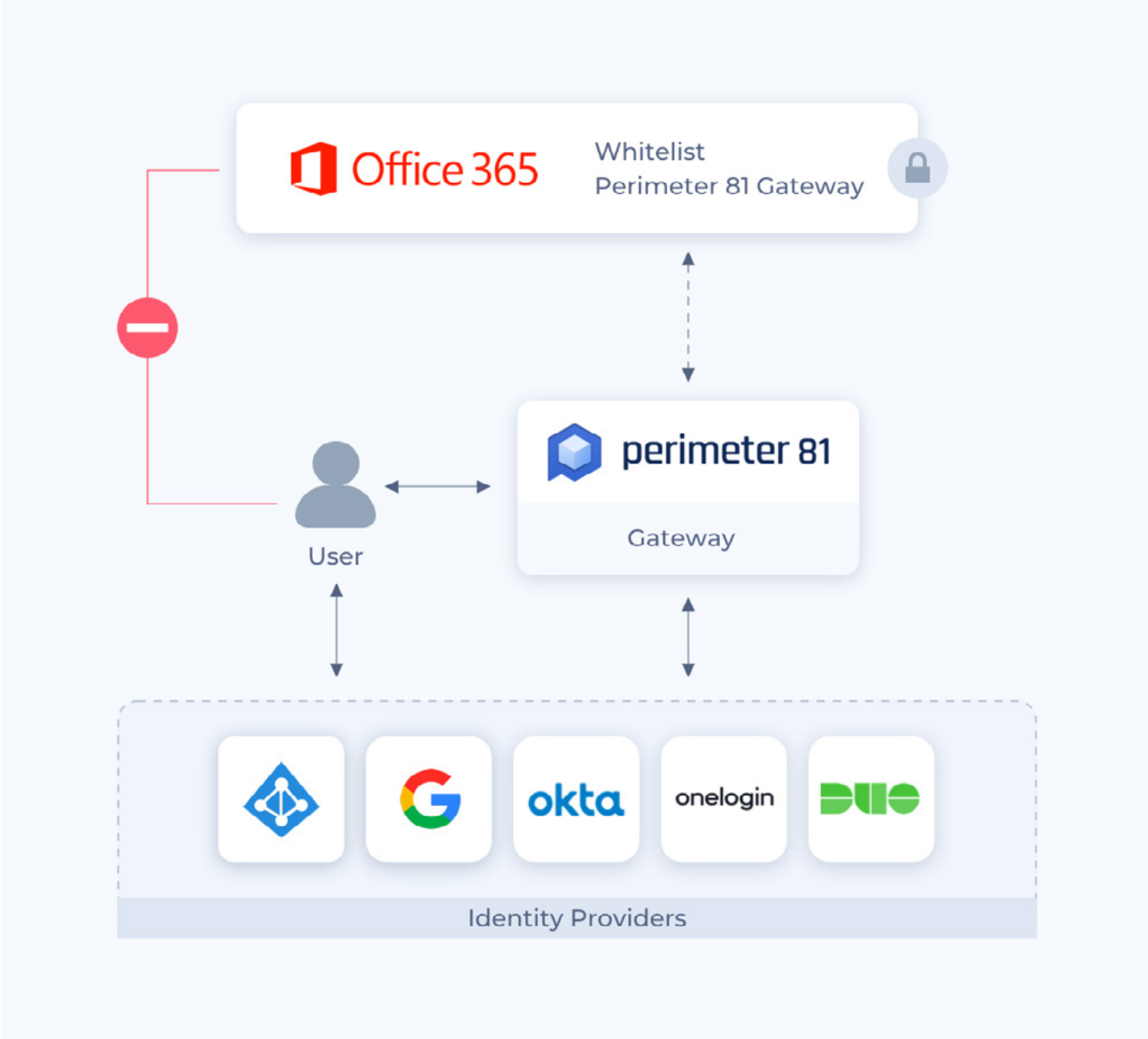


Figure 2

Forrester Research recommends dividing network resources at a granular level, allowing organizations to tune security settings to different types of traffic and create policies that limit network and application flows to only those that are explicitly permitted. This network micro-segmentation approach allows security teams the flexibility to apply the right level of protection to a given workload based on sensitivity and value to the business.

Utilizing a ZT security model, Perimeter 81's encrypted, closed network security solution quickly and easily secures access to on-premise and cloud resources, as well as web applications, through it's authentication service. With a single management console, Perimeter 81 offers user-centric and adaptive, policy-based network access to on-premise resources, SaaS applications and cloud environments; interconnectivity among cloud environments and different network branches; and fully audited agentless access to web applications, SSH, RDP, VNC or Telnet.

Perimeter 81's Multi-Regional feature also allows enterprises to deploy private encrypted gateways in multiple locations, so IT administrators can create custom closed networks to best serve international branches and remote employees with low latency and high availability.

Mobile employees are protected with Perimeter 81's Single Sign-On native client applications that can be used on any Windows, Mac, iPhone and Android devices. Perimeter 81's innovative Automatic Wi-Fi Security also shields all data by automatically activating protection when employees connect to unknown or untrusted networks.

With centralized control and identity management integrated into the Perimeter 81 management platform, employees and groups can easily be added to corporate network resources and cloud environments with secure policy-based resource access. Detailed activity reports provide insight into resource and bandwidth utilization while active connection and session information can be monitored. Finally, all company data passing over any network is secured with 256-bit bank-level encryption and routed through a dedicated private gateway concealing a company's actual IP address with an IP mask.

About Perimeter 81

Perimeter 81 is a Zero Trust Network as a Service that has taken the outdated, complex and hardware-based traditional network security technologies, and transformed them into a user-friendly and easy-to-use software solution — simplifying secure network access for the modern and distributed workforce. Perimeter 81 serves a wide range of businesses, from midsize to Fortune 500 companies, and has established partnerships with the world's foremost integrators, managed service providers and channel resellers.

Contact Us

www.perimeter81.com

sales@perimeter81.com

Request a Free Demo

Connect with Us




Blog

perimeter 81