SOLUTION BRIEF

Netskope with Microsoft

As your organization embarks on a transformational journey powered by Microsoft Cloud, use Netskope to deliver real-time protection to your users and data. Together, we deliver innovative, cloud-native solutions for data protection and threat prevention based upon the principles of Zero Trust.

KEY USE CASES

- **Protect data in the cloud:** Netskope integrates with Microsoft to provide comprehensive data protection that's consistently applied across Microsoft and third-party applications and instances.
- **Protect users from cloud and web threats:** Use Netskope and Microsoft for integrated threat protection and shared intelligence across the endpoint and the cloud.
- **Control user access to Microsoft and other applications:** Contextually enforce access controls to SaaS private applications using Netskope with identity management powered by Azure Active Directory.
- **Lightning-fast network access to Microsoft Cloud:** Use Netskope's NewEdge security private cloud to provide users and branch offices with lightning-fast access to Microsoft 365 and Azure cloud services from anywhere in the world.

THE CHALLENGE

As organizations transform their applications and workforces to take advantage of the cloud, the security team's visibility and protection is eroding. That's because traditional security was not designed to protect applications or users when either could lie outside of the traditional network perimeter. Consequently, companies are facing tremendous difficulty trying to stop emerging threats across an expansive attack surface.

Today, organizations must find ways to simplify their operations, deliver better protection, and improve the user experience. This can only be achieved by making technology choices that are designed to complement one another. Netskope and Microsoft's extensive strategic partnership helps security teams and end users work more efficiently by delivering integrated security solutions for Microsoft applications and endpoints.

NETSKOPE WITH MICROSOFT

Netskope and Microsoft together deliver modern, cloud-delivered protection for applications, users, endpoints, and data.

- Partnership: Netskope is a member of the Microsoft Intelligent Security Association, the Microsoft Networking Partner Program, and is a Microsoft Gold Partner.
- Technology Integrations: Our technologies complement each other and cover over 15 integration points.
- NewEdge Direct Peering: With direct peering with Microsoft at every NewEdge location, end users benefit from an exceptional user experience from anywhere around the world.

CAPABILITIES

PROTECT DATA IN THE CLOUD WITH MICROSOFT INFORMATION PROTECTION AND NETSKOPE DLP

To protect data in the cloud, organizations must continuously classify data stored in the cloud, check permissions and sharing policies, and implement controls that evaluate whether data movement is compliant with policy. This is especially difficult today, because the consistent enforcement of data protection policies must span a vast enterprise application landscape.

Netskope integrates with Microsoft to provide comprehensive data protection that's consistently applied across Microsoft and third-party applications and instances. Netskope works together with Microsoft Information Protection to protect data where it lives and where it moves. Microsoft Information Protection automatically discovers information stored within Azure and Microsoft 365, and applies workflows for data classification, labeling, and encryption. Netskope Data Loss Protection integrates with Microsoft Information Protection, providing seamless enforcement of data policies using the Netskope Security Cloud. Organizations can establish protections to make sure that the appropriate policies are in place to intercept accidental or malicious data movement to other cloud and web applications. These steps ensure that consistent real-time data protection measures are in place to keep data within managed instances, enforce consistent policies across other cloud applications, oversee user behavior to spot insider threats, and counter attempts to exfiltrate data.

Microsoft Information Protection integration operates bidirectionally, providing protection for data that originates outside of Microsoft applications. For example, Netskope AI/ML models detect sensitive data accidentally sent in unencrypted email and invokes Microsoft Information Protection to properly classify, tag, and encrypt the content in accordance with policy.

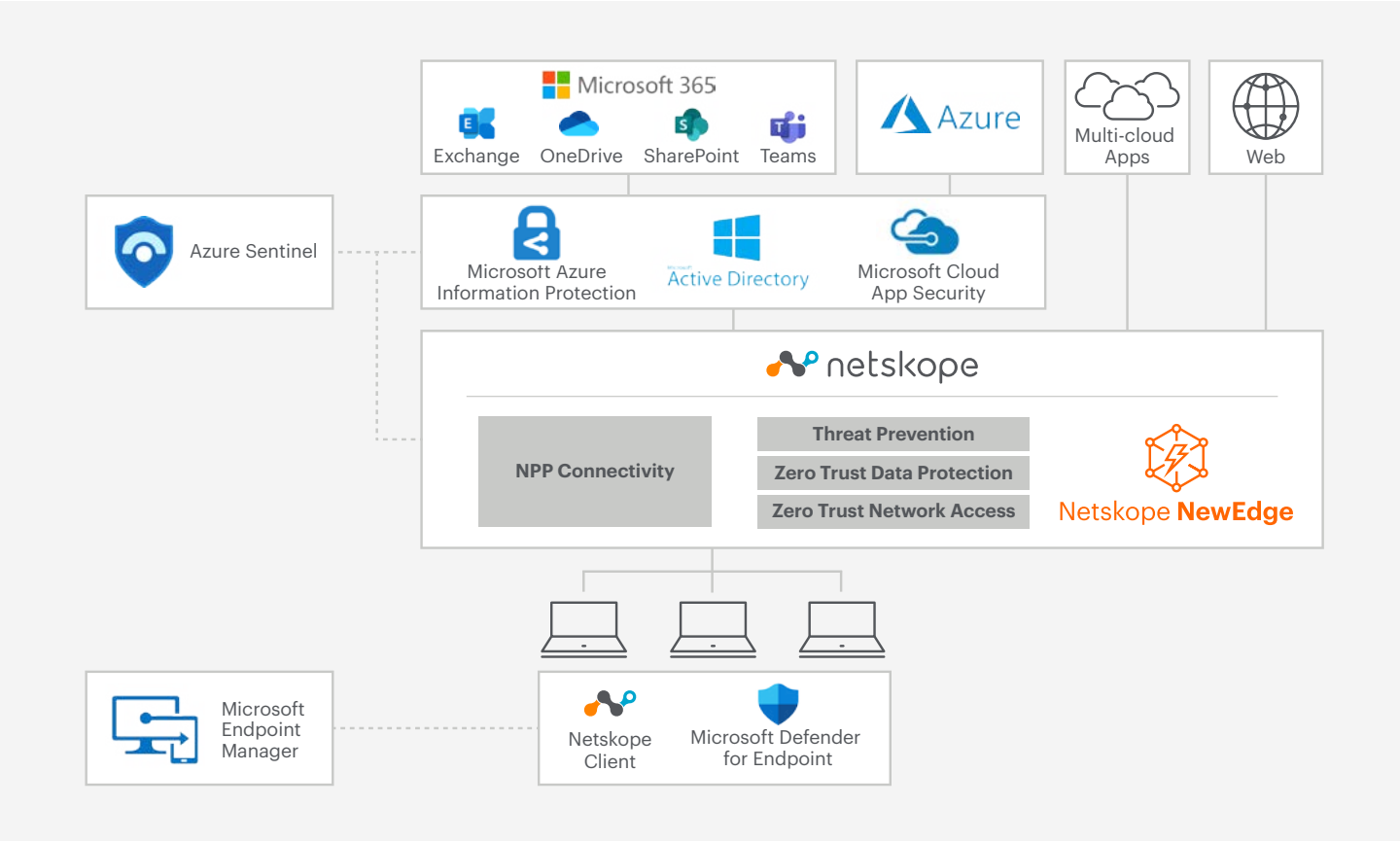
Netskope and Microsoft's extensive strategic partnership helps security teams and end users work more efficiently by delivering integrated security solutions for Microsoft applications and endpoints.

PROTECT USERS FROM CLOUD AND WEB THREATS WITH MICROSOFT DEFENDER, NETSKOPE NG SWG, AND CLOUD THREAT EXCHANGE

Today's cloud-enabled cyberattacks take advantage of blind spots in the traditional enterprise security stack. That's because cloud traffic does not always pass through perimeter controls. Even when it does, enterprise firewalls and proxies evaluate allow/block decisions based on the URL and are unable to distinguish between managed instances of an application and one that is under an attacker's control. As a result, organizations often lack the optics to identify applications, enforce security policies, and stop threats such as cloud-hosted phishing forms, command and control, and malware payloads.

Use Netskope and Microsoft for integrated threat protection and shared intelligence across the endpoint and the cloud. Apply granular, contextual instance-aware policies that discern cloud resources the enterprise manages, and the ones subject to additional access, inspection, and policy controls. Cloud threat intelligence shares threat feeds between Netskope and Microsoft, which powers real-time malware detection inline (Netskope Next Gen Secure Web Gateway), scanning malware in the cloud (Netskope CASB API and Microsoft MCAS) and on the endpoint (Microsoft Defender for Endpoint).

Deliver contextually rich alert and event data surfaced by Netskope into Azure Sentinel to facilitate incident response and investigations. This information enables security operators to tune the overall threat prevention architecture and reduce the end to end attack surface.



PROTECT ACCESS TO MICROSOFT 365 AND OTHER CLOUD APPLICATIONS WITH ZERO TRUST

Users need access to a number of different types of applications, including SaaS, web, and private applications in the data center and the virtual private cloud. Traditional network access controls and content inspection point products, such as VPNs, firewalls, and proxies were not designed to support today's application mix. This has been especially problematic for remote workers, because of the slow performance when hairpinning cloud traffic over VPN.

Netskope is a Microsoft Networking Partner, which makes the Netskope Security Cloud the ideal first hop for lightning fast, secure access to Internet-facing services and web pages. Netskope simplifies networking and security to enable the protection the organization needs with an unrivaled user experience.

Security teams can deliver simple, fast, and secure access to all applications using a single client deployable by Intune. Users automatically authenticate to Netskope Security Cloud using Azure Active Directory credentials for access to Microsoft cloud and other web applications.

- For SaaS and Web applications, Netskope Next Gen SWG provides inline threat and data protection from the Netskope Security Cloud without backhauling traffic back to an on-prem security appliance.
- For private applications in the data center and virtual private cloud, get secure Zero Trust Network Access using Netskope Private Access with integration with Azure Active Directory. Reduce exposure to risk and improve the user experience by eliminating remote access VPN. With Netskope and Microsoft, authorized users get application-level access without exposing servers to the internet.

"Offering our clients highly secure, highly-performant access to Microsoft 365 and other cloud applications means users have multiple options to protect data and prevent threats."

GARY MIGLICCO,
SECURITY STRATEGIST FOR SIRIUS

ACCELERATE NETWORK TRANSFORMATION WITH LIGHTNING-FAST NETWORK ACCESS TO MICROSOFT 365

Networking and security must work hand in hand to deliver optimal protection and an excellent user experience. However, congestion on enterprise networks and the rise in remote workforces have made direct to internet the preferred path to the cloud. Now organizations must find new ways to meet networking and security requirements to support today's application mix.

Use Netskope's NewEdge private security cloud to provide your users and branch offices with lightning-fast access to Microsoft 365 and Azure cloud services from anywhere in the world. NewEdge is a global high-performance, low-latency security cloud accessible from over 40+ cities around the world, with every location extensively peered with Microsoft. Netskope is a Microsoft Networking Partner and supports validated configurations using Microsoft 365 network connectivity principles

ABOUT MICROSOFT

Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.