Solution Brief

Zscaler for Microsoft Cloud App Security

Zscaler and Microsoft have joined forces to enable the secure adoption of cloud applications. The native integration of Zscaler's Zero Trust Exchange and Microsoft Cloud App Security provides the protection, visibility, and controls required to securely embrace the cloud.

Solution Overview

When applications resided in the data center, organizations built networks to connect their users to these applications and protected the network with a moat of security appliances. However, enterprise applications have rapidly been moving to the cloud to improve IT agility, advance innovation, improve productivity, and reduce costs.

One of the productivity benefits of cloud applications is that users can access them from anywhere. But if they use direct-to-cloud connections, as recommended, IT is left blind to this traffic and your organization may be at increased risk. On the other hand, if you force the traffic through centralized security controls before it can go out to its cloud destination, you undo the productivity and cost savings benefits you gained by moving your apps to the cloud. In the cloud world, the notion of providing security at the corporate network level is increasingly irrelevant.

Zscaler's Zero Trust Exchange sits in the cloud, between users and their applications, and provides full inline threat protection, data loss prevention (DLP), and cloud access control. Distributed in over 150+ data centers around the world, and peering with Microsoft in a large number of them, Zscaler brings security close to the user for complete protection and a fast user experience.

Zscaler and Microsoft have partnered to provide a closed-loop Cloud Access Security Broker (CASB) solution to discover and control cloud applications and shadow IT across all users, regardless of location or connection. Joint customers also receive a comprehensive risk assessment of all services and the ability to enforce policies to protect users and keep corporate data safe.

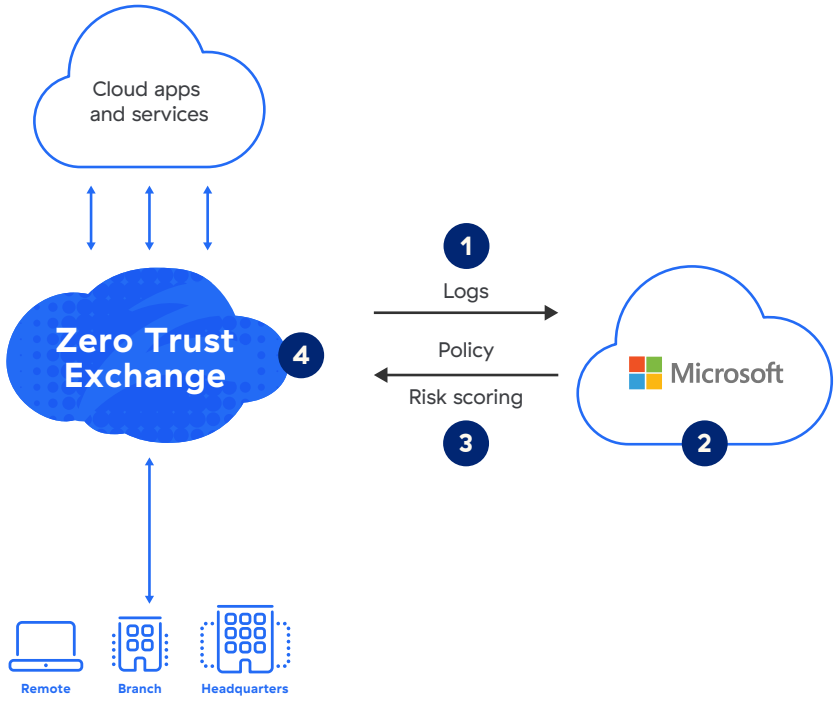
Zscaler Nanolog™ Streaming Service (NSS) streams real-time log data into Microsoft Cloud App Security, which uses the ingested logs to perform application discovery and classification into sanctioned, permitted, and unsanctioned applications. Administrators can define policy in Microsoft Cloud App Security for each of those categories, which are then enforced inline through Zscaler. This integration enables customer to:

- Enforce access control policies for sanctioned applications on managed/unmanaged devices (example: block the download of a Salesforce report to an unmanaged device)
- Securely enable the use of permitted applications with granular DLP policies (example: allow uploads to permitted GitHub repositories, while blocking uploads to others)
- Identify and control access to unsanctioned applications (example: block upload to PDF merging tool)

Integration Benefits

- **Gain control over cloud application access:** Unsanctioned applications defined in Microsoft Cloud App Security are automatically synced to Zscaler, where access is controlled inline for all users, on and off network.
- **Enhance visibility into shadow IT:** Applications discovered by Zscaler undergo a comprehensive risk assessment and investigation based on Microsoft Cloud App Security risk scoring.
- **Analyze cloud application usage:** Integration of Zscaler and Microsoft Cloud App Security management consoles allows administrators to investigate application usage by pivoting between consoles via UI links and easy-to-use actions and drill-downs.

Microsoft Cloud App Security is also used to identify applications for which access should be blocked for all users due to the risk associated with their use in compliance with customer policy. The list of restricted applications is then pulled into Zscaler via API integration and populates as “Microsoft Cloud App Security Unsanctioned Apps” under URL categories. In Zscaler, a policy can then be defined to block access to all Microsoft Cloud App Security Unsanctioned Apps, which is enforced inline. The closed-loop integration streamlines a process that would normally require multiple manual, repetitive workflows to export proxy logs to the CASB and then import configurations and blacklists back into the secure web gateway (SWG) for enforcement.



1. NSS log forwarding
2. Cloud app discovery and classification; Policy definition for cloud access
3. Policy pulled via API; Cloud App risk scoring
4. Inline enforcement of cloud access policy

The combined solution from Zscaler and Microsoft yields joint customers several benefits:

- **Better security:** Full inline inspection of all traffic from all users, on or off network, improves risk posture. Policy can be applied immediately to newly discovered applications.
- **Efficiency:** Native integration saves time and resources. After the initial setup, discovery and enforcement cycle, synchronization is automated without the need for human intervention.
- **Simplicity:** Automated integration requires no additional deployments or manual, repetitive workflows. Unified visibility on the management console exposes app risk info in a single location, improving the administrative experience

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world’s largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com