Discovery of Shadow IT with Microsoft Cloud App Security

The rise of cloud-based services has led to a significant increase in productivity for organizations. While it allows IT to outsource operations and makes collaboration among end users much easier, it also allows organizations to be much more flexible in adapting to new market conditions. As a result, users continuously find new cloud services to support their work process, ahead of IT support.

Our data shows that an average of 1,181 cloud applications are used in large enterprises today, while >60% IT isn’t even aware of, leading to large numbers of Shadow IT in organizations and introducing security and compliance risks.

Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) solution that enables you to identify, assess and manage the cloud apps used by your organization and establish a lifecycle management approach for your cloud services.

“Using Cloud App Security as a magnifying glass, we gain amazing visibility into our SaaS environment, giving us the confidence we need to deliver on our digital workplace transformation,” says

- Yasir Khan, Head of IT Infrastructure at Nakilat

Lifecycle Management for a secure adoption of cloud apps

Enabling seamless Discovery in Microsoft Cloud App Security is the first step in creating a sophisticated lifecycle management approach, to ensure that your organization securely accesses cloud apps and services. Leverage the breadth of capabilities to identify which apps are being used in your organization, assess their potential risk and enable continuous monitoring to take immediate action when new cloud apps are discovered.

© 2018 Microsoft Corporation. All rights reserved.
Streamlined Discovery by integrating with Windows Defender ATP

Microsoft Cloud App Security uniquely integrates with Windows Defender Advanced Threat Protection (ATP) to enhance the Discovery of Shadow IT in your organization. It provides a simplified roll out of Cloud Discovery, extends the capabilities beyond your corporate network, and enables machine-based investigation.

Microsoft Cloud App Security leverages Windows Defender ATP to collect traffic information about the cloud apps and services being accessed from IT-managed Windows 10 machines – covering client- and browser-based apps. This seamless integration does not require any additional deployment and gives admins a more complete view of the cloud app- and services usage in their organization.

“Onboarding WDATP data in MCAS was a breeze, just flip the switch in the portal and go”
- DevOps Infrastructure Engineer

How it works

Windows Defender ATP is an integrated part of Windows 10 Enterprise. To leverage the existing sensors and send traffic information to Microsoft Cloud App Security, you need to enable this integration via a simple toggle in the Windows Defender Security Center. Once activated, Windows Defender ATP continuously logs resource usage and reports it back to Microsoft Cloud App Security, with signals shared via the Microsoft Intelligent Security Graph.

Microsoft Cloud App Security will then leverage the traffic information from Windows Defender ATP’s log store to surface all relevant details in the Discovery Dashboard and provide relevant insights for discovered apps, users, IP addresses and a new, machine-centric view.

Admins now have visibility into the cloud apps that are being accessed, on and off the corporate network. In addition, they will be able to see how many and which devices are accessing each one of the apps that are discovered.

Integration Highlights

Discovery beyond the corporate network
Discovery of cloud apps accessed from managed Windows 10 machines, regardless of the network.

Ease of deployment
All it takes is a simple checkbox in the Windows Defender Security Center to enable the new Discovery integration.

Machine-based Discovery
Analyze your findings on a machine-basis to get a granular insight into the apps accessed from specific machines.

Deep dive investigation in Windows Defender ATP
Continue your investigation in the Windows Defender Security Center for more granularity and visibility into all the different behaviors on a suspicious machine.

© 2018 Microsoft Corporation. All rights reserved.
Integration Architecture

Windows Defender ATP enables Discovery beyond the corporate network for Windows 10 machines. To ensure that all devices in your organization are captured, a hybrid deployment with a traditional log collector deployment against your firewall or proxy, in combination with the existing Windows Defender ATP integration will provide you with complete insight.

On its own, Cloud App Security analyzes logs from your network using logs you configured for automatic upload. This native integration enables you to take advantage of the network transactions Windows Defender ATP observes and monitors and utilizes them for Shadow IT discovery across the Windows machines on your network. To enable you to perform Cloud Discovery across other platforms, it’s best to use both the Cloud App Security log collector, as well as the integration with Windows Defender ATP to monitor your Windows 10 machines.

Prerequisites:
✓ Microsoft Cloud App Security
✓ Windows Defender ATP
✓ Windows 10 October 2018 Update

Microsoft Cloud App Security
Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that gives you visibility into your cloud apps and services, provides sophisticated analytics to identify and combat cyberthreats and enables you to protect your data and control how it travels.

Windows Defender Advanced Threat Protection
Windows Defender Advanced Threat Protection (ATP) is a unified endpoint security platform for protection, detection, investigation and response. Windows Defender ATP protects endpoints from cyber threats; detects advanced attacks and data breaches, automates security incidents and improves security posture.