Skyhigh Security

WHITE PAPER

The Benefits of a Dedicated Cloud Security Platform

A comparison of Microsoft CASB and Skyhigh Security CASB

Table of Contents

1 A comparison of Microsoft CASB and Skyhigh Security CASB

3 Multi-platform requires comprehensive security

4 Skyhigh's Security Service Edge

6 Why customers choose Skyhigh Security over Microsoft

9 Skyhigh Security Customer Perspectives

9 Discover Skyhigh Security for your business

Your corporate environment extends beyond O365, Teams, and OneDrive

Many businesses are drawn to the efficiency, scalability, and innovation provided by Microsoft's Office and Azure platforms. At their core, these platforms are powerful IaaS/PaaS cloud computing services which enable companies to achieve technology and business goals better and faster than ever before. Because of this, many organizations have also purchased additional services such as cybersecurity in a single, convenient, commercial bundle. While providing basic security capabilities for the Microsoft environment, organizations have also recognized the benefits of a broader cloud migration strategy. In this multi-cloud SaaS environment, organizations have found that this bundle is insufficient to provide the necessary protection relative to other best-of-breed offers in the marketplace.

Multi-platform requires comprehensive security

Point products vs platform add-ons

At one end of the spectrum, offering the widest support of applications, is the point product. Security is either provided by the application itself or by a 3rd party which is purpose-built to provide security for a specific threat. If there were only one or two applications, this might be acceptable, but when there are dozens or hundreds of applications this is nearly impossible to manage.

On the other end of the spectrum is a platform add-on. For example, Microsoft, AWS, and Google each offer security solutions to help customers secure applications built on their platforms. These solutions follow a PaaS-type pattern where the platform provider gives customers the ability to do almost anything. At the same time, very little is complete out of the box and customers are left to integrate and configure these on their own using PowerShell, scripting languages, regular expressions, and other complex tasks. Not only will security teams need the know-how to build and code the rules, but they also need to replicate them across the different platforms.

Purpose-built CASB / SSE / SASE

Between the extremes of point products and platform add-ons is a single cloud platform that abstracts away the underlying complexity of different cloud and SaaS platforms sometimes called a CASB, security service edge (SSE), or even secure access service edge (SASE). This approach provides a consistent security operations experience across different cloud and SaaS applications. Executives should consider these purpose-built solutions as a balance between simplicity and flexibility.

Executives should strongly consider choosing a purpose-built Security Solution to provide the right balance between simplicity and effectiveness.

Skyhigh's Security Service Edge

Skyhigh's Security Service Edge is a collection of integrated, cloud-centric security capabilities that facilitate safe access to websites, cloud, and applications. The Skyhigh Security portfolio converges security services including Secure Web Gateway, Cloud Access Security Broker, and Zero Trust Network Access into a single, cloud-native framework. This integrated approach supports the digital business transformation and workforce mobility, while minimizing the impact on security performance, complexity, and cost.

One of the key components of Skyhigh Security's portfolio is the CASB product. From its beginnings as an answer to Shadow IT, CASB has grown to include functionality that can be described in terms of four pillars: Visibility, Compliance, Data Security and Threat Protection

Visibility

Large businesses may have any number of employees accessing many applications in many different cloud environments. When cloud usage is outside the view of IT, enterprise data is no longer bound by the company's governance, risk, or compliance policies. To safeguard users, confidential data, and intellectual property, a CASB solution provides comprehensive visibility into cloud app usage, including user information such as device and location info. The cloud discovery analysis provides a risk assessment for each cloud service in use, allowing enterprise security professionals to decide whether to continue allowing access or whether to block the app. This information is also useful in helping shape more granular controls, such as granting varying levels of access to apps and data based on an individual's device, location, and job function.

Compliance

While businesses can outsource all their systems and data storage to the cloud, they maintain responsibility for compliance with regulations governing the privacy and safety of enterprise data. Cloud access security brokers can help maintain compliance in the cloud by addressing a wide variety of compliance regulations such as HIPAA, as well as regulatory requirements such as ISO 27001, PCI DSS, and more. A CASB solution can determine the areas of highest risk in terms of compliance and provide direction as to what the security team should focus on to resolve them.

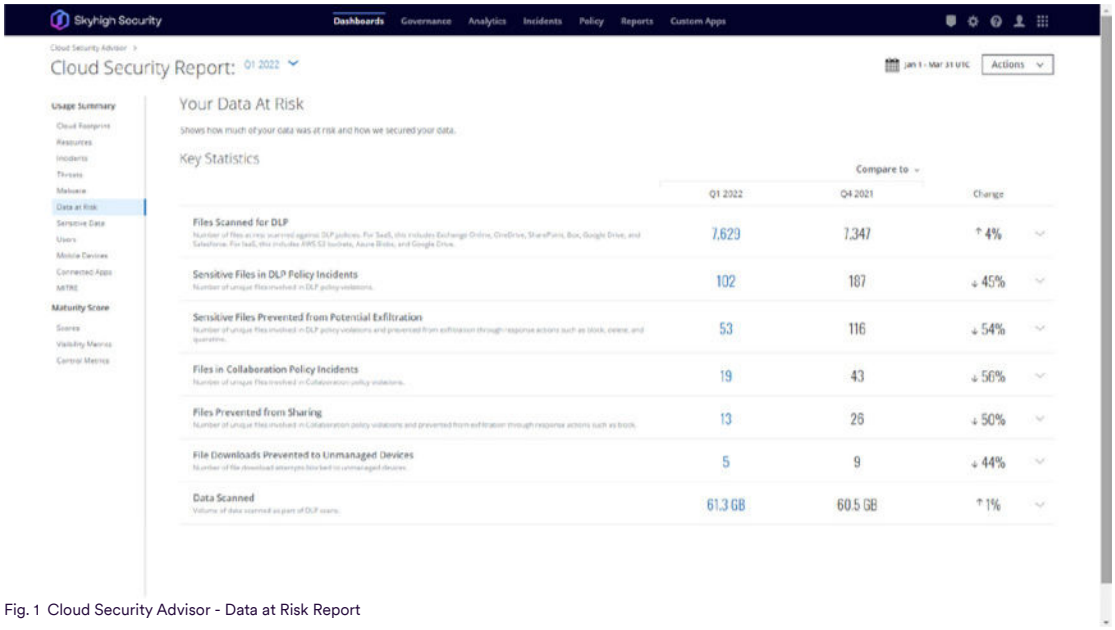

Fig. 1 Cloud Security Advisor - Data at Risk Report

Data Security

Cloud adoption has removed many of the barriers preventing effective collaboration at a distance. As much as the seamless movement of data can be of benefit, though, it can also come at a tremendous cost for businesses with an interest in protecting sensitive and confidential information. While on-premises DLP solutions are designed to safeguard data, their ability to do so often does not extend to cloud services and lacks cloud context. The combination of CASB with sophisticated DLP allows IT the ability to see when sensitive content is traveling to or from the cloud, within the cloud, and cloud –to-cloud. By deploying security features like data loss prevention, collaboration control, access control, information rights management, encryption, and tokenization, enterprise data leaks can be minimized.

Threat Protection

Whether through negligence or malicious intent, employees and third parties with stolen credentials can leak or steal sensitive data from cloud services. To help pinpoint anomalous user behavior, CASBs can compile a comprehensive view of regular usage patterns and use it as a basis for comparison. With machine learning-based user and entity behavior analytics (UEBA) technology, CASBs can detect and remediate threats as soon as someone attempts to steal data or improperly gain access. To protect against threats coming from cloud services, the CASB can use capabilities such as adaptive access control, static and dynamic malware analysis, prioritized analysis, and threat intelligence to block malware.

Cloud adoption has removed many of the barriers preventing effective collaboration at a distance... it can also come at a tremendous cost for businesses with an interest in protecting sensitive and confidential information.

Why customers choose Skyhigh Security over Microsoft

Microsoft offers a basic CASB solution which they position as “free” when bundled into their enterprise license agreements. In general, this is sufficient for Microsoft office productivity applications such as O365 and IaaS solutions like Azure, but it does not have the broad feature set to scale to other applications.

There are two key differences between Skyhigh Security’s CASB and Microsoft’s CASB for protecting data in the cloud.

Consistent Cloud Security

DLP for data in motion and at rest

Skyhigh Security supports scanning and classifying data both in motion and at rest. For instance, a single DLP policy can apply to a file being uploaded to a personal cloud service, to a file being shared via OneDrive, or to a file being emailed through Outlook. That same DLP policy can also apply to data at rest in Azure, AWS, and even Exchange mailboxes. This provides customers with assurance that information stored in the cloud meets today’s security standards.

While Microsoft Information Protection will help many companies secure newly created Office documents, it neglects the data that already exists. This leaves customers with no way to ensure that current policies are being complied with as Microsoft cannot apply DLP policies against data at rest for most services, including its own Exchange or Azure storage.

Multiple Instances of Cloud Apps

Skyhigh Security supports multiple instances (tenant) of cloud applications and treats them as separate entities. This means customers have a choice whether to apply the same or a customized security policy for each instance.

Microsoft Defender for Cloud Apps does not support multiple instances of Office 365. This could seriously limit your ability to apply security to M&A targets or take on sensitive or government projects that require isolated tenants.

Complete coverage for non-Microsoft IaaS and SaaS

Skyhigh Security has an extensible framework that works with a large list of IaaS and SaaS services that continues to grow. Skyhigh Security utilizes APIs published by these services, to not only scan for configuration and data security problems, but also to help customers streamline remediation of any issues. For example, Skyhigh Security can automatically limit improper permissions on a file share or quarantine a file with sensitive data on many platforms. Additionally, Skyhigh Security supports manual remediation of security incidents using a consistent workflow.

In contrast, Microsoft´s solution provides limited remediation options for non-Microsoft platforms, either manually or automatic. In other words, security teams can be alerted of potential problems but cannot do anything about it without logging into an additional console. This makes incident management a much more burdensome and expensive process that could lead to costly outcomes.

Discover and manage Shadow IT (unsanctioned cloud applications)

Skyhigh Security's portfolio includes a fully featured forward proxy which secures access to the web, provides DLP controls, and provides granular controls to cloud services. This solution uses standards-based proxy technology, so it works with Windows, Linux, mobile devices, and just about everything else.

In contrast, Microsoft's solution to Shadow IT is to block access to sites using Windows Defender. This capability is limited as organizations need more granular activity controls such as letting users access some instances of an application or allowing certain operations but not others. For example, with Microsoft's solution you cannot control access to other Office365 tenants or permit read-only access to personal cloud services.

Also, because Microsoft's solution only works for Windows, any Shadow IT policies you create for Windows Defender will need to be duplicated in another solution to cover non-Windows devices, mobile devices, etc.

Efficient Security Operations

Skyhigh Security has been built from the ground up with security in mind which means that its dashboards, reports, configuration, and incident workflows will be familiar to security professionals. The product works in the way security professionals expect it to without the need for multiple dashboards, heavy customization, PowerShell, scripting, etc. Skyhigh Security's efficient incident management capabilities make it easy for administrators to manage data incidents in CASB, with detailed information about the context around the match, allowing them to take responses quickly depending on the incident risk, and reduce the corporate risk.

Centralized policy management

Skyhigh Security provides a single console to manage everything from secure web access, to DLP, to posture management (SSPM, CSPM).

On the other hand, Microsoft requires four separate consoles to manage different aspect of CASB:

1. In-line policies in Azure AD Conditional Access console
2. DLP sensitive data classifiers in Purview Compliance console
3. Other CASB policies in Microsoft Defender for Cloud Apps console
4. SSPM from Microsoft 365 Defender console

This means that Microsoft administrators will have to spend additional time jumping from one console to other to make policy configurations and troubleshoot.

Streamlined incident response

Skyhigh Security has a unified system for detecting, prioritizing, and managing cloud security incidents. For customers who already have a SIEM and/or SOAR, Skyhigh Security provides standards-based support for easy integration.

Microsoft has multiple consoles so that incidents can be difficult to find or prioritize. While all of these integrate fairly well into Microsoft's own SOAR solution (Sentinel), this comes at an additional cost and increases the hazard of vendor lock-in.

In addition, Microsoft's automated responses for their own products can work in ways that are unexpected or ineffective. For example, a Microsoft-native policy which restricts the sharing of sensitive data can take up to a day to trigger, long after most recipients will have downloaded the data. In contrast, a similar Skyhigh Security policy would take effect in real time, eliminating any opportunity for data leakage and addressing issues before they become serious problems.

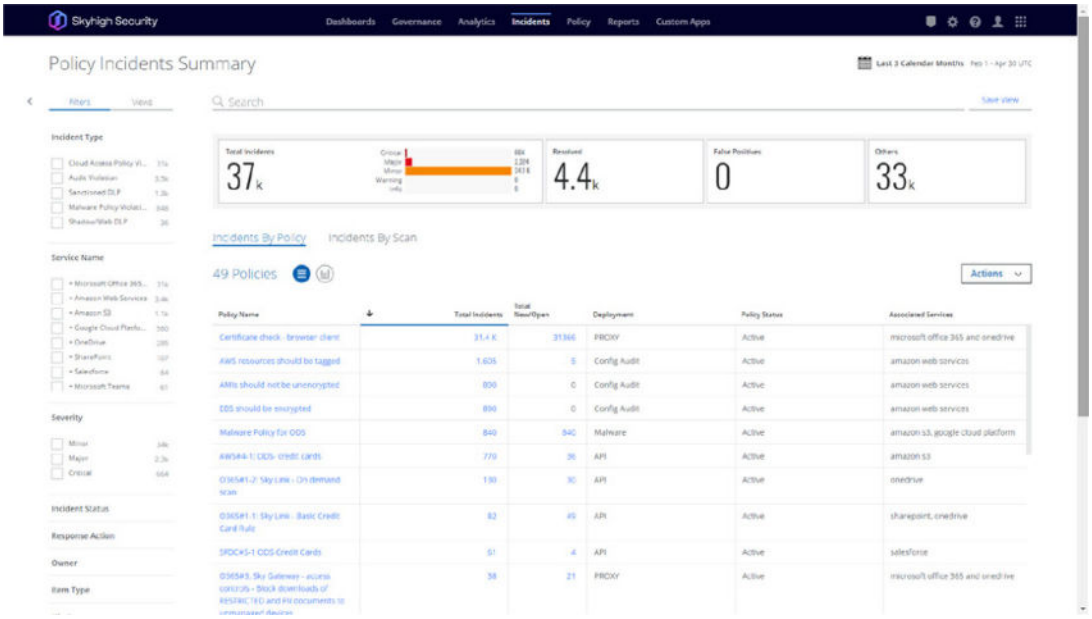

Fig. 2 Policy Incidents Summary

Skyhigh Security Customer Perspectives

Skyhigh Security was named a 'Customers' Choice' in the Gartner® Peer Insights™ 'Voice of the Customer': Security Service Edge 2022 report. The Gartner Peer Insights Customers' Choice is based on feedback and ratings from end-user professionals who use the Skyhigh Security portfolio.

Skyhigh Security achieved an overall rating of 4.7 out of five with 200 verified customer reviews, achieving the 'Customers Choice' distinction across more segments than other vendors, including Microsoft, in the report.



Discover Skyhigh Security for your business

Skyhigh Security goes beyond securing data access—it secures how sensitive data is used. We extend the security control point beyond the network to the data itself. As it moves across the web to SaaS applications, cloud applications, and platforms. We protect it with a single policy that moves with your data instead of being tied to each access technology. Our easy-to-use, integrated platform enables organization-wide data protection, streamlines data security operations, and reduces complexity.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2023.
March 2023