CLOUD ACCESS SECURITY BROKER (CASB)

HPS is a leading implementer of Cloud Access Security Broker Solutions.

Employees have increasingly gained access to a multitude of easy-to-use, flexible cloud services, many of which can be procured outside of IT control. Simultaneously, they have begun storing critical data and executing normal business processes in a way that has left the IT and security leaders tasked with protecting data and business processes blind. Enter CASB – a new category of security solutions aimed at securing both sanctioned and unsanctioned access to cloud services.

Our partnership with Netskope allows us to offer leading CASB technology to our customers. The Netskope CASB solution addresses the problem of protecting data across multiple cloud environments. This security solution is aimed at providing controls for all cloud services – both sanctioned and unsanctioned – granting IT visibility.

Our Netskope trained professionals will work alongside your team to address the challenges of a mobile and remote work environment. These now common environments can leave your information systems penetrable to security risks. We reduce these risks and provide cloud threat protection functionality for your systems.

HPS+CASB=Improved Security

Organizations are increasingly turning to CASB vendors, like HPS, to address cloud service risks, enforce security policies, and comply with regulations, even when cloud services are beyond their perimeter and out of their direct control. HPS is uniquely positioned to be your organization's systems integrator for cloud access security broker (CASB) solutions by offering an on-premises or cloud-based security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.

HPS team members are experts in CASB services. We have successfully completed implementations for public and private sector entities alike. We invite you to choose from our CASB rapid deployment programs or request a custom quote for your specific requirements.

HPS addresses the entire range of CASB services, including:

- Controlling activities in sanctioned and unsanctioned services
- Enforcing sensitive data polices in and en route to cloud services
- Enforcing policies based on Microsoft Active Directory groups or organizational units
- Detecting cloud activity anomalies like excessive downloads or shares across any service
- Monitoring and reporting on activity in regulated services for compliance purposes
- Enforcing policies remotely, including on mobile and in sync clients
- Mitigating risk against users with compromised accounts
- Finding and remediating threats and malware in your cloud services

SERVICES & FEATURES

THE FOUR PILLARS OF CASB

1: Visibility

Companies need visibility and control across both sanctioned and unsanctioned services. Rather than take an “allow” or “block” stance on cloud services, HPS will enable IT to say “yes” to useful services while governing access to activities and data within services. This could mean:

- Offering full access to a sanctioned suite, like Microsoft Office 365, to users on corporate devices.
- Enforcing a ‘no sharing outside the company’ policy across a category of unsanctioned services.

HPS will also help you get your arms around cloud spend by discovering all cloud services, reporting on what your cloud spend is, and finding redundancies in functionality and licensing costs.

2: Data Security

Accuracy comes from using highly sophisticated cloud DLP detection mechanisms, like document fingerprinting, combined with reducing detection surface areas using context such as user, location, and activity. When sensitive content is discovered in, or enroute to the cloud, a CASB solution enables IT administrators to control data ingress and egress points.

netskope

3: Compliance

As organizations move more of their data and systems to the cloud, they must ensure they comply with the many regulations designed to ensure the safety and privacy of personal or corporate data. HPS can help ensure compliance in the cloud whether you are a healthcare organization worried about HIPAA or HITECH compliance, a retail company concerned with PCI compliance, or a financial services organization needing to comply with FFIEC and FINRA.

4: Threat Protection

Organizations need to ensure their employees aren’t introducing or propagating cloud malware and threats through vectors such as cloud storage services, and their associated sync clients and services. This means being able to scan and remediate threats in real time, such as when an employee tries to share or upload an infected file or detecting and preventing unauthorized user access to cloud services and data.

Protect yourself against a host of cloud threats including malware and insider threats with cloud malware and threat capabilities that combine threat intelligence, static and dynamic malware analysis, prioritized analysis, and remediation of threats that may originate from, or be further propagated by, cloud services.