opensystems

WHITE PAPER

WHY CASB ALONE **ISN'T ENOUGH**

It's no secret that the traditional corporate perimeter is dead. Once upon a time, firewalls, IDS and AV were able to keep what was inside "in" and what was outside "out". But those nice, neat borders have been burst through thanks to the cloud.

open-systems.com

The cloud-based workplace gives employees the freedom to work wherever they want – to file reports from a café and conduct meetings from the beach. All the while users can use the application or website they want, what's called shadow IT, never having to worry about enterprise standards for security or compliance.

The cloud, shadow IT, and the end of the company "border" leaves network and security teams fighting new battles. Unapproved devices and unfettered access to all applications, sanctioned and unsanctioned, have led to a meteoric rise in security threats. Employees leaving their computers unattended while working at Starbucks. Downloaded movies and files infected with malware. Spear phishing targeting users and drive-by attacks leading users to picking up malware from the most unexpected places. All it takes is one careless person to click a malicious link to accidentally infect their entire network with ransomware or malware that compromises customer information.

As if that wasn't bad enough, General Data Protection Regulation (GDPR) has become a reality. The stakes are even higher with penalties for GDPR violations reaching up to four percent of yearly revenue. No wonder companies who previously might have overlooked employee use of the cloud are taking a harder line.

FIREWALLS AND TRADITIONAL SECURITY TOOLS ARE NO LONGER ENOUGH

So, what are your options? Some organizations attempt to secure their cloud infrastructure by blocking certain cloud application categories such as “personal storage”. Typically, such methods just drive users to look for alternative cloud applications undetected by the proxy. Block users from accessing Dropbox today and you might just find SugarSync on your network tomorrow. The resulting shadow IT environment has been responsible for a great number of corporate breaches.

Alternatively, some organizations choose to allow the use of cloud applications, while forcing users to sign disclaimers stating that they won’t share any confidential data with untrusted vendors. This “honor system” may not create shadow IT issues, but it does mean relying on one of the most unreliable factors in workplace security – the users themselves.

And although it may come as a disturbing surprise, some organizations grant their users unrestrained use of the internet (though few companies will admit it).

CASB SECURES THE CLOUD

Cloud Access Security Broker (CASB) fills this niche. A CASB sits between an organization’s premises and the cloud, acting as a gatekeeper by enforcing company security policies as users visit cloud applications and resources. While firewalls inspect layers three and four for threats and IPS checks for malware, CASB looks at the cloud application layer.

CASB provides four critical security functions:

- **Visibility:** It allows a comprehensive view of what applications are used by the users of an organization and provides a risk rating of how this application usage may affect the organization’s security.
- **Protection:** It adds proactive protection by helping security teams set and enforce access policies, prevent data infiltration and exfiltration.
- **Detection:** The increased visibility grants the ability to detect incidents by allowing security teams to locate sanctioned and unsanctioned use of cloud applications and detect anomalies.
- **Response:** Thanks to the enhanced level of visibility and control, teams can respond to events faster and with greater accuracy than previously.

To achieve those goals, CASB fuses together multiple security enforcement policies, such as authentication, SSO, credential mapping, encryption, and malware detection and prevention.

As such, CASBs provide better control and allow for deeper visibility and inspection of cloud services. They help security teams govern access and activities, secure and prevent data loss, replicate compliance controls and protect their organization from internal and external threats like ransomware and other forms of malicious code.

CASBs give security professionals a much-needed control point, granting visibility into all cloud applications that employees use, re-establishing the control and continuous visibility that has been lost due to the ever-eroding cloud perimeter.

CASB APPLIANCES ARE INSUFFICIENT

For all of their strengths, though, in-house CASB solutions face significant deployment challenges in today's business. To enforce security policies, CASB must be able to inspect and block traffic. With a single site and CASB sitting in-line of the default gateway, seeing all internet-bound traffic is relatively simple.

However, with multiple locations, enterprises face several architectural challenges. Locating a CASB at every location is impractical and bringing all traffic back to the CASB for inspection adds latency to internet sessions. Companies can use a CASB reactively to identify past policy violations. But besides the fact that such an approach puts IT at the disadvantage, configuration is also more complex as local firewalls and other security tools at the various locations must be configured to forward their logs to the CASB for analysis. Enterprises must still incur the costs of in-house security expertise for analyzing the CASB alerts and resolving any violations.

CASB SERVICES PROVIDE A PARTIAL SOLUTION

CASB cloud services address these challenges. There's no traffic backhaul, messy configuration, and IT can proactively block violations. The CASB service operates as a reverse proxy, inspecting traffic after it leaves the customer premises. All internet and cloud traffic is sent to the local point of presence (PoP) of the CASB cloud service, inspected, and either flagged, blocked, or forwarded to its destination.

While a CASB cloud service addresses many of the challenges of running a CASB appliance, alone it's not sufficient. It must be used in tandem with a secure web gateway (SWG), firewalls and other IT controls. The enterprise is left with trying to integrate the cloud service with its existing security infrastructure, often an impractical and impossible task. If security functions are not tightly integrated, management will become even more complex. This will cost organizations dearly in terms of visibility, because context will be spread across multiple platforms.

THE COMPLETE WEB PROTECTION PLATFORM

What's needed is a not just a CASB service but a service with complete web protection, managed and maintained by security specialists who can take over the load of security architecture integration. Such a complete solution provides full "radar" with threat protection to cover what's coming in from the web and a management layer to handle the configuration, integration, and event analysis needed to make the solution work. More specifically, a complete web protection platform will:

- **Easily ingest data from proxies:** You must have someone who can handle the import of all security logs into the CASB.

- **Decrypt SSL traffic:** Just having access to all the logs alone is not enough. You need to do "man-in-the-middle" decryption to be see what's inside the SSL traffic.

- **Provide deep visibility into user activity:** The CASB should allow you to see what your users bring in from the web, such as an unauthorized Dropbox account or other unsanctioned tools. APIs do the work, independent of the user. The APIs monitor SharePoint and OneDrive, looking for data that should not be there, such as credit card numbers and personal ID information or corporate documents that are publicly shared.

- **Include rule filtering:** The CASB should let you filter whatever rules you choose to specify. For example, if confidential documents are labeled with metadata, they can be blocked from being shared outside the organization without authorization. This can be accomplished using data leakage protection (DLP) to scan the text of the documents, searching for specific data elements.

- **Block applications from a central console:** This is not common, since there can be many false positives and it requires careful management. Most companies have not been successful, since you have to block all access to that app, such as Google Drive, which would clearly upset users. The technology is not proven yet without false positives in this application.

CASB deployment: practical recommendations

Start with an out-of-band solution to focus on detection and response, while building the baseline for an enforcement policy of cloud usage. This can either be on-prem or in the cloud, but it does not matter in terms of performance. If you don't have any specific compliance issues, the cloud is a better option as it scales well and is highly available by default.

Decide if your primary target is enforcing security policies on your cloud apps, which is often enough for many organizations (in which case you would need to use the reverse proxy method), or if the primary target is preventing use of any unsanctioned cloud apps (in which case you would need a forward proxy). This second option takes about one to two years for the typical organization to implement and by then, many CASB vendors will have changed their worldwide coverage of cloud PoPs, thus alleviating any performance concerns.

Once you start deploying the active components of your CASB solution (not just passive monitoring), you will experience issues like false classifications or needed whitelists for some applications. This isn't very different from any new deployment and should not be considered a problem. Troubleshooting and change management, which is a core part of the managed CASB service with complete web protection and adjustments, should be implemented in very short order.

Open Systems is a groundbreaking cybersecurity company delivering an experience way beyond expectations. Our obsessive care for our clients' businesses has led us to reinvent how cybersecurity is delivered to fit today's mobile, cloud-based world. Our team, based in North America, Europe, and Asia, consistently provides crazy good cybersecurity to leading organizations all over the world.

Learn more at open-systems.com | Approved for public use.