Cloud Access Brokers: Bridging the Gap

What's a CASB?

- Cloud Access Security Brokers (CASBs) are either in-house network gateways or Security-as-a-Service (SecaaS) cloud offerings that inspect network traffic destined to the cloud, primarily for SaaS services
- These tools and services inspect all network traffic to determine whether sensitive data is being transmitted to the cloud, and apply various policies and security controls to protect the data or prevent it from being transmitted in the first place.

Whose Responsibility IS it?

"None of the provider entities have any obligation to verify that anyone using customer's account and password has customer's authorization"

"Customer is responsible for maintaining the confidentiality of its account and password and for restricting and granting access thereto"

"Customer is responsible and liable for all activities that occur under its account regardless of whether such activities are authorized by customer"

What We Want in a CASB

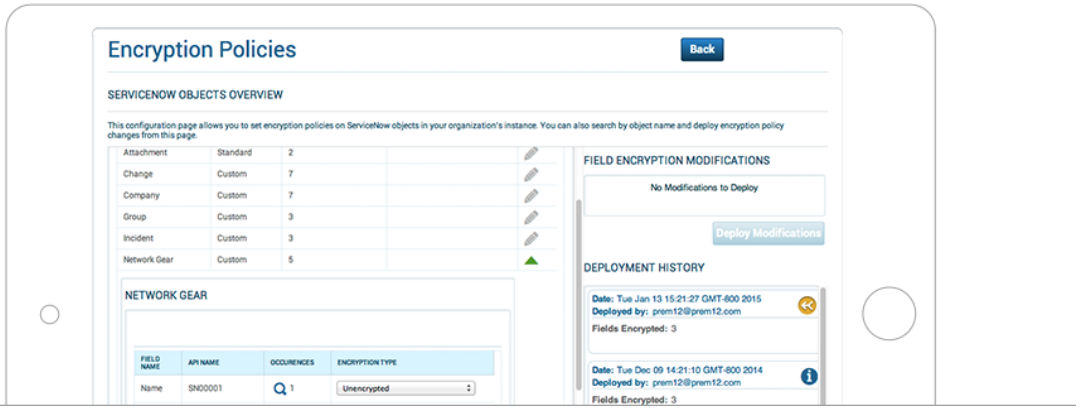
- All CASB platforms should provide the ability to:
  - Inspect network traffic
  - Apply customer-defined policies for controlling what data can go where
  - Apply some form of protective controls to the data as warranted.
- Some CASBs are integrated with significantly more cloud services than others, and may also have many more tightly integrated features.
- Enterprises should carefully evaluate the partnerships each CASB has when considering these products and services.

CASB Features: Visibility and App Identification

- CASBs originally were introduced to identify cloud applications in use, helping enterprises determine whether “Shadow IT” was occurring in the cloud.
- To that end, application and data visibility and cloud usage pattern profiling are still at the top of the list of features any CASB should have.
- CASBs identify cloud applications and data using a combination of URL inspection, traffic and protocol analysis, and data loss prevention (DLP) pattern matching.

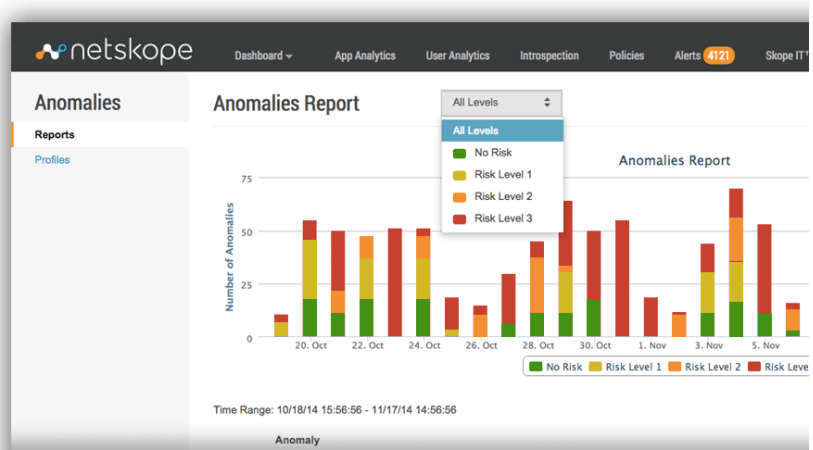
CASB Features: Data Protection

- Encryption and tokenization are the most common types of data protection controls available with many CASB providers
- Some CASBs will offer both.
- Enterprises should carefully evaluate key management capabilities and practices at any CASB where they intend to implement encryption and decryption of data.



CASB Features: Threat Protection

- Many CASBs are now able to monitor traffic for indicators of malware and compromise by looking for anomalous behavior and known command and control signatures.
- Attackers may hijack cloud service accounts or try to access data stored in cloud service provider environments, and a CASB should ideally detect these unusual patterns of access.

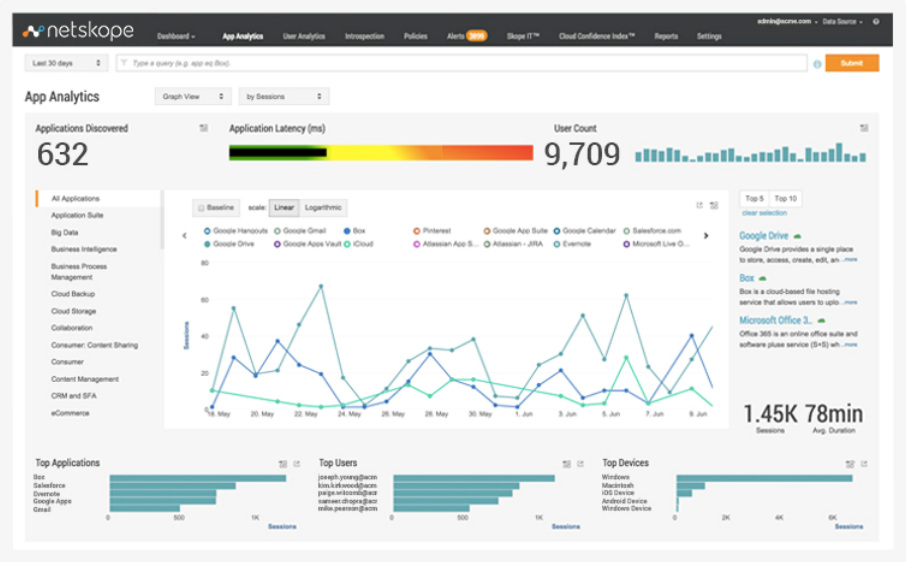


CASB Features: Access Controls

- As many cloud services are tied to internal user directories like Active Directory, controlling access to cloud services and data through role-based access policies is another core element of protection.
- Ideally, the CASB will offer simple and native integration with internal user directories or cloud-based identity services.
- Strong access controls and authentication to the CASB console and configuration should also be available, and a mature offering should have:
  - Role-based access for administrators
  - Multi-factor authentication to the console
  - Strong logging and audit trails for monitoring use of the CASB services.

CASB Features: Dashboard Metrics + Reporting

- All CASB tools should provide an easy-to-use dashboard that offers a variety of reporting options.
- All CASB providers should offer a set of “canned” reports that detail user activity, data detected and/or protected, malicious traffic detected and blocked, etc.



CASB Features: “Nice To Haves”

- **Integration with network malware sandboxes**. Some CASB services can integrate with on-premise or cloud-based malware sandboxes
- **User behavior timelines**. For organizations looking to assess patterns of user behavior with cloud services, often for detection of compromised accounts or fraud, some CASBs have begun offering behavioral analytics and visualization tools
- **In-house threat intelligence teams**. Some providers offer additional threat intelligence services and data feeds that can augment the core data and user monitoring capabilities.
- **Cloud service reputation ratings**. Some CASB vendors also monitor cloud service providers’ activities and reputation, and can inform customers of any changes at a cloud service provider that may be deemed risky.

Threat Intelligence and Heuristics

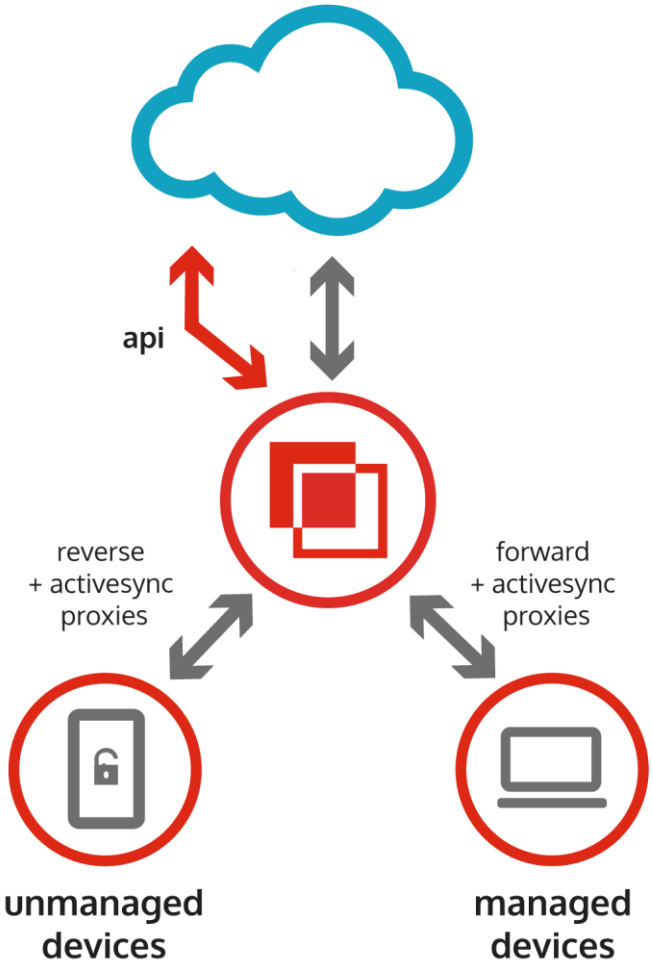
- SaaS attack vectors are different from traditional security attacks
- Governance and security features must be combined with threat intelligence and heuristics
- What's normal usage for one organization may be different for another
- Who is accessing SaaS applications?
- Where are they coming from?
- What are "normal" patterns of access and behavior?

CASBs: Key Considerations

- Select the right deployment modes, gain visibility into cloud usage
  - Some CASBs are integrated with other cloud services
  - Gateways? SecaaS?
- Begin with out-of-band controls, i.e. govern data at rest
  - DLP and monitoring
- Enable in-line prevention controls for specific use cases
  - Blocking content or layering encryption on data and connections

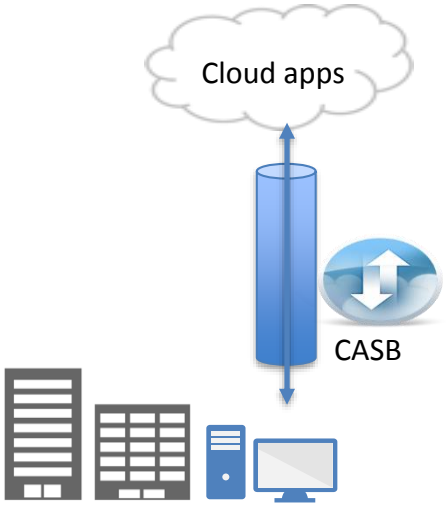
CASB and Mobile

- Demand for BYOD continues to rise
- MDM solutions do not always address cloud apps and allowed
- IT must securely enable access to frequently used SaaS apps



Selecting The Right Architecture

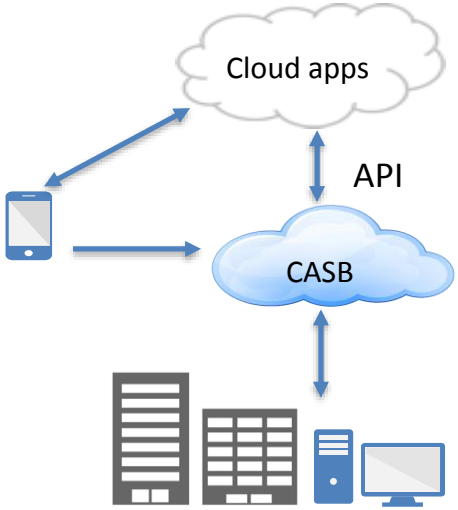
Legacy approach



"Endpoint" agent and forward proxy approach

Managed device, managed network

Cloud-centric approach



and Reverse Proxy

Any app, user, device, network

CASB Deployment

- Phase 1: Out-of-Band
  - Leverage cloud APIs
  - Detect shadow cloud and policy violations
- Phase 2: In-Band Prevention
  - Implement proxy gateways or access control APIs
  - Access based on IP, location, device, user or role
  - Also able to block specific content or behaviors
- Phase 2+
  - Refine and implement policies

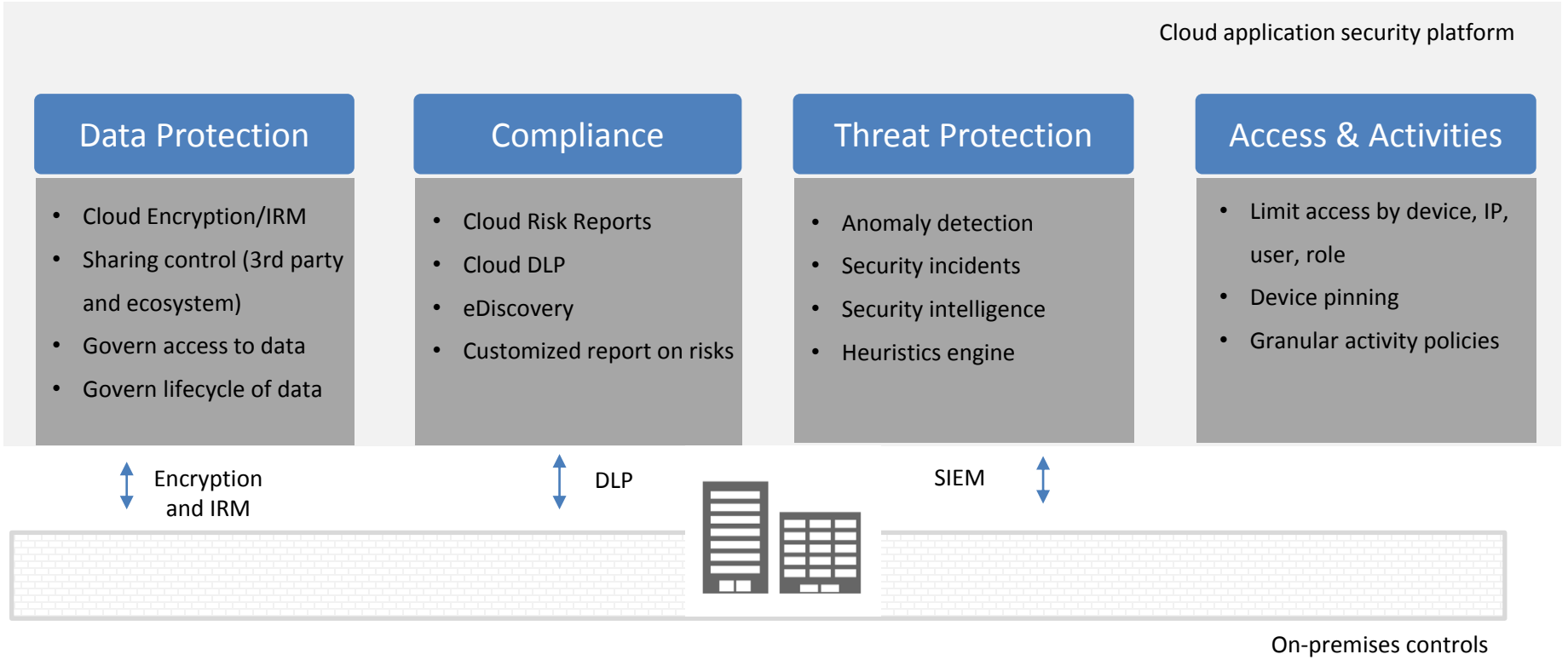
SaaS Security Requirements

Goal	Requirements
Visibility	Visibility into users and activities, devices, data in the cloud
Data Protection/Data Leakage	Protection of data when it is stored, processed and transported in the cloud
Access Control	Limiting access from unmanaged devices, preventing illicit access, locking down admin access for cloud deployments
Compliance	Compliance with regulatory mandates for IP, PII, PCI, PHI and legal eDiscovery requests
Detection and Response	Detecting compromised accounts/systems and identifying anomalous behaviors in the cloud

Vetting the CASB

- Ensure your CASB cloud/infrastructure supports the following:
  - Security controls and independent audits
  - Availability and SLA requirements
  - Penetration Testing
  - Certifications

CASB: The Complete Picture



Wrapping Up

- CASB services primarily focus on monitoring cloud usage and protecting data sent to the cloud
- CASBs are rapidly emerging to become more fully featured platforms that offer preventive, detective, and response controls.
- When evaluating CASB services, organizations should focus on compatibility with cloud service providers, as well as user and data inspection and protection features
- Implementing a CASB service should not require a major architecture overhaul, nor should it require significant manpower to maintain