LICENSED FOR DISTRIBUTION

HOW TO EVALUATE AND OPERATE A CLOUD ACCESS SECURITY BROKER

08 DECEMBER 2015 | ID: G00292468

Analyst(s): Neil MacDonald, Craig Lawson

(http://www.gartner.com/home)

How to Evaluate and Operate a Cloud Access Security Broker

Summary

CASBs provide CISOs with a critical control point for cloud service visibility, security and compliance. Use Gartner CASB frameworks to support continuous cloud service discovery, adaptive access, verification, protection and the prioritization of CASB evaluation criteria.

Overview

Key Challenges

- Many enterprises lack a complete understanding of the cloud services they consume and the risks they represent, which makes compliance and protection difficult.
- Even when cloud services are known, most enterprises struggle to consistently verify compliance or the secure handling of sensitive data within and across these disparate services.
- Enterprises have no standardized way to detect whether (and when) compromised credentials or unmanaged devices are used to access cloud services.
- Cloud access security brokers provide a combination of access-centric and threat-centric capabilities, increasing the complexity of an evaluation.
- A large number of vendors have entered the CASB market with a wide variety of capabilities and approaches, confusing potential customers and blurring use cases.

Recommendations

Chief information security officers should:

- Use the Gartner CASB framework to structure their CASB strategies and evaluation criteria, including continuous cloud access discovery, verification and protection.
- Initiate CASB deployments with discovery/risk assessment ratings of the cloud services in use.
- Use the continuous visibility provided by most CASBs to help standardize on the best cloud services for the CISOs' organizations and to apply consistent security policies.
- Choose multimode CASB solutions that offer a variety of in-line and API-based visibility options.
- Extend sensitive data-monitoring processes to cloud-based services and look to integrate cloud data loss prevention with on-premises DLP efforts.
- Shortlist the security solutions they've already deployed, which may include CASB capabilities that meet their requirements, such as firewalls and secure Web gateways.

Strategic Prediction & Planning

By 2020, 85% of large enterprises will use a cloud access security broker solution for their cloud services, which is up from fewer than 5% in 2015.

Introduction

Cloud access security brokers (CASBs) provide information security professionals with a critical control point for the secure and compliant use of cloud services across multiple cloud providers. Many SaaS apps have limited visibility and control options. SaaS adoption is becoming pervasive in enterprises, which exacerbates the frustration of security teams looking for visibility and control.

In "Mind the SaaS Security Gaps," we described, at a high-level, four pillars of expected CASB functionality: visibility, compliance, data security and threat protection. As the market has become more crowded and the solutions have become more complex, clients evaluating CASB solutions need more detail for planning their CASB rollouts and executing their evaluations with more granularity. we then provide Gartner best practices for evaluating CASB solutions, which enterprise security leaders can apply.

Analysis

Achieve Cloud Service Visibility and Perform a Risk and Compliance Assessment

To understand the risks represented by the use of cloud services, enterprises need visibility into what cloud services are already in use, by which employee; the sensitivity of the data being handled; which devices are used to access that data; and from where it's accessed.

In almost all cases, even when enterprises feel they have a good understanding of cloud services use, unsanctioned (also referred to as "shadow IT" or "citizen IT") usage is taking place. To gain basic levels of visibility, an enterprise can turn to its Web proxy, firewall and domain name service (DNS) logs. Although this will have gaps (for example, when users are off-network), it is a useful way to gain visibility using existing log sources, from the existing tools.

For most organizations, this will be the first phase of a CASB deployment in which organizations need visibility. However if you ever ask a Chief Technology Officer (CIO) and ask him how many Cloud Services that they know and are monitoring, they probably will say 40-50. In fact there are a total of 10,000 different cloud platforms out there other than the common services like Google Drive, Dropbox and Sharefile. This is the problem, enterprises might be exposed to potential risks that they're unaware of — for example, if a poorly secured enterprise file synch and share services (EFSS) is being used. New cloud services are continually being introduced, and end users are constantly consuming cloud services outside the knowledge and management of the IT organization.

Use the CASB to Select Appropriate Cloud Services

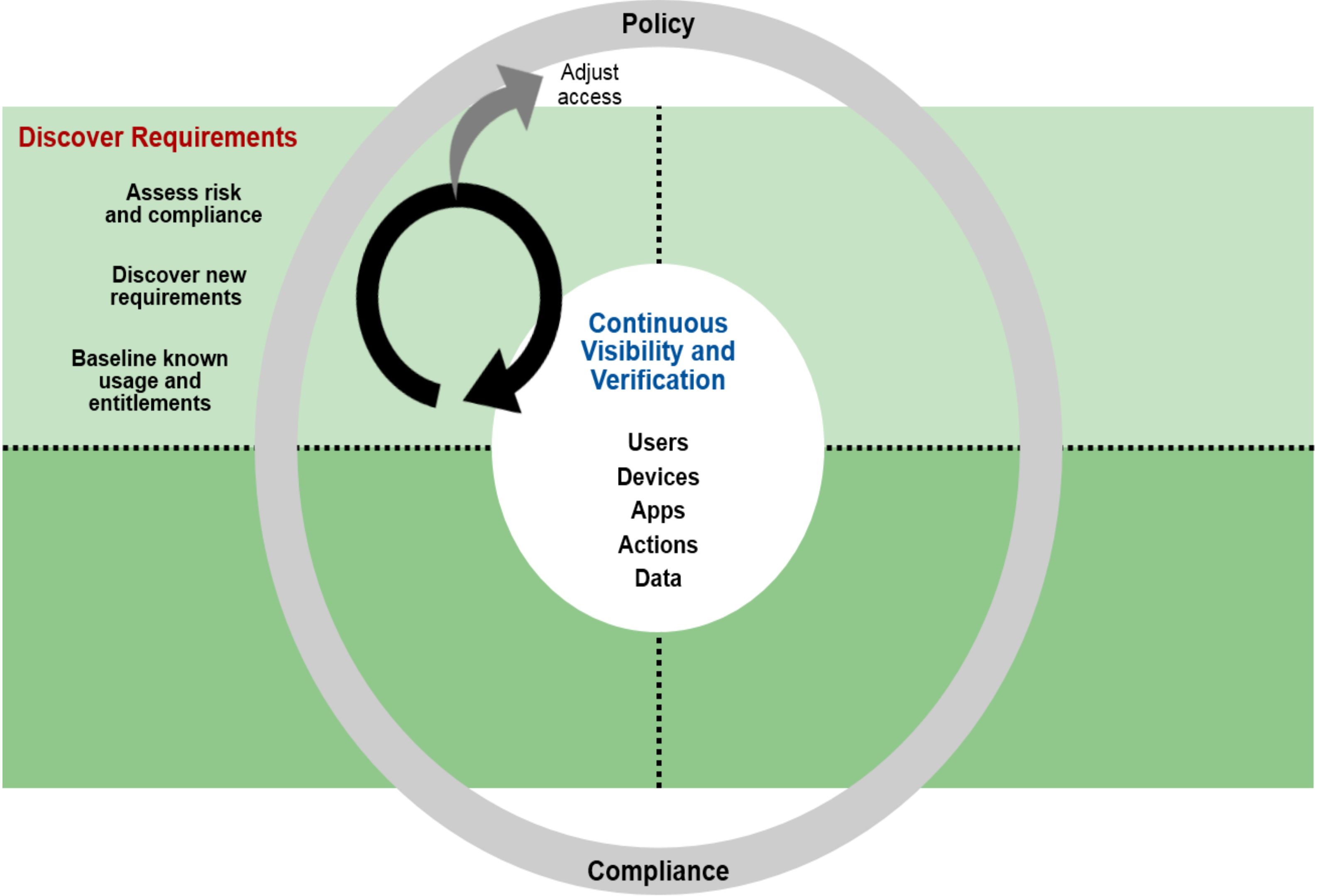
Enterprise goals for security and regulatory compliance are some of the more difficult enterprise requirement areas complicating the selection of cloud services. Although many SaaS applications have a similar look and feel, they differ significantly in ways that affect risk, and their risk considerations may change over time.

Enterprises need to continue to understand and verify the compliance and security posture of this cloud service. Leading CASBs have genuine intellectual property with their cloud service assurance databases. Maintaining and shadow IT discovery is not a one-time exercise and should be treated as a continuous process of discovering enterprise needs.

Typically, Gartner observes organizations adopting cloud services one category at a time. For example, a number of organizations have moved to adopt services such as CRM (e.g., Salesforce) and infrastructure as a service (IaaS; e.g., Amazon Web Services) and are now moving to consume cloud services for EFSS (Box) and productivity (Microsoft Office 365 or Google Apps for Work). When this happens, consider the credible options that are available, then allow the business to choose the best cloud service.

These starting points represent the typical first phase of most enterprise CASB deployments. They are represented in the upper left-hand corner of our CASB framework, which is built on a foundation of continuous visibility and verification (see Figure 1).

Figure 1. Discover Requirements


Policy
Adjust access
Discover Requirements
Assess risk and compliance
Discover new requirements
Baseline known usage and entitlements
Continuous Visibility and Verification
Users
Devices
Apps
Actions
Data
Compliance

Source: Gartner (December 2015)

Plan for Adaptive Access

To manage risk, enterprises are looking to CASB providers for the ability to apply real-time context to the decision as to whether a cloud service should be accessed — for example, restricting access based on the location, time of day or whether the device is enterprise-managed. Most CASB providers do not directly provide identity services; however, they must be capable of linking to enterprise and cloud identity repositories for the application of policy. Cloud services and all credible CASB platforms already provide built-in integration to leading cloud identification as a service (IDaaS) providers (see "Magic Quadrant for Identity and Access Management as a Service, Worldwide"), as well as providing support for Security Assertion Markup Language (SAML) and other identity and access management (IAM) open standards, as well as enterprise directory and identity systems. Some CASB solutions, such as IBM's Cloud Security Enforcer, [5] include integrated IDaaS capabilities. In both cases, the value added by a CASB is to apply additional context at the time of access and during the use of cloud services to make adaptive access decisions that can reduce the likelihood of unauthorized access to one of your accounts. This capability is especially critical for privileged accounts, such as administrative accounts of the cloud service. Examples include blocking access to a cloud service from an unmanaged or unhealthy device, blocking access from specific regions of the world or providing risk-based authentication capabilities.

This is not a new enterprise requirement. An easy way to think of this capability is that it is the functional equivalent of enterprise network access control (NAC) brought into the cloud era. Services can be accessed by anyone, anywhere, from any device connected to the Internet. CASBs such as NAC don't act as the identity store per se (this is usually Active Directory); however, they provide a level of assurance on the types of services that can be accessed from devices used, based on the user's profile.

Treat the Encryption and Tokenization of Data With Care

Several CASB solutions support the optional encryption and/or tokenization of data (at the field- or the file-content/object level), so that enterprises can meet the legal and regulatory requirements of their industries or countries. Implemented properly, data protection using encryption/tokenization, while the enterprise maintains control of the key/tokenization dictionary, can be a powerful way to protect sensitive data in the cloud. It can also prevent the cloud service provider from seeing it, if necessary, to satisfy compliance policy requirements.

Treat the Encryption and Tokenization of Data with Care

Several CASB solutions support the optional encryption and/or tokenization of data (at the field- or the file-content/object level), so that enterprises can meet the legal and regulatory requirements of their industries or countries. Implemented properly, data protection using encryption/tokenization, while the enterprise maintains control of the key/tokenization dictionary, can be a powerful way to protect sensitive data in the cloud. It can also prevent the cloud service provider from seeing it, if necessary, to satisfy compliance policy requirements.

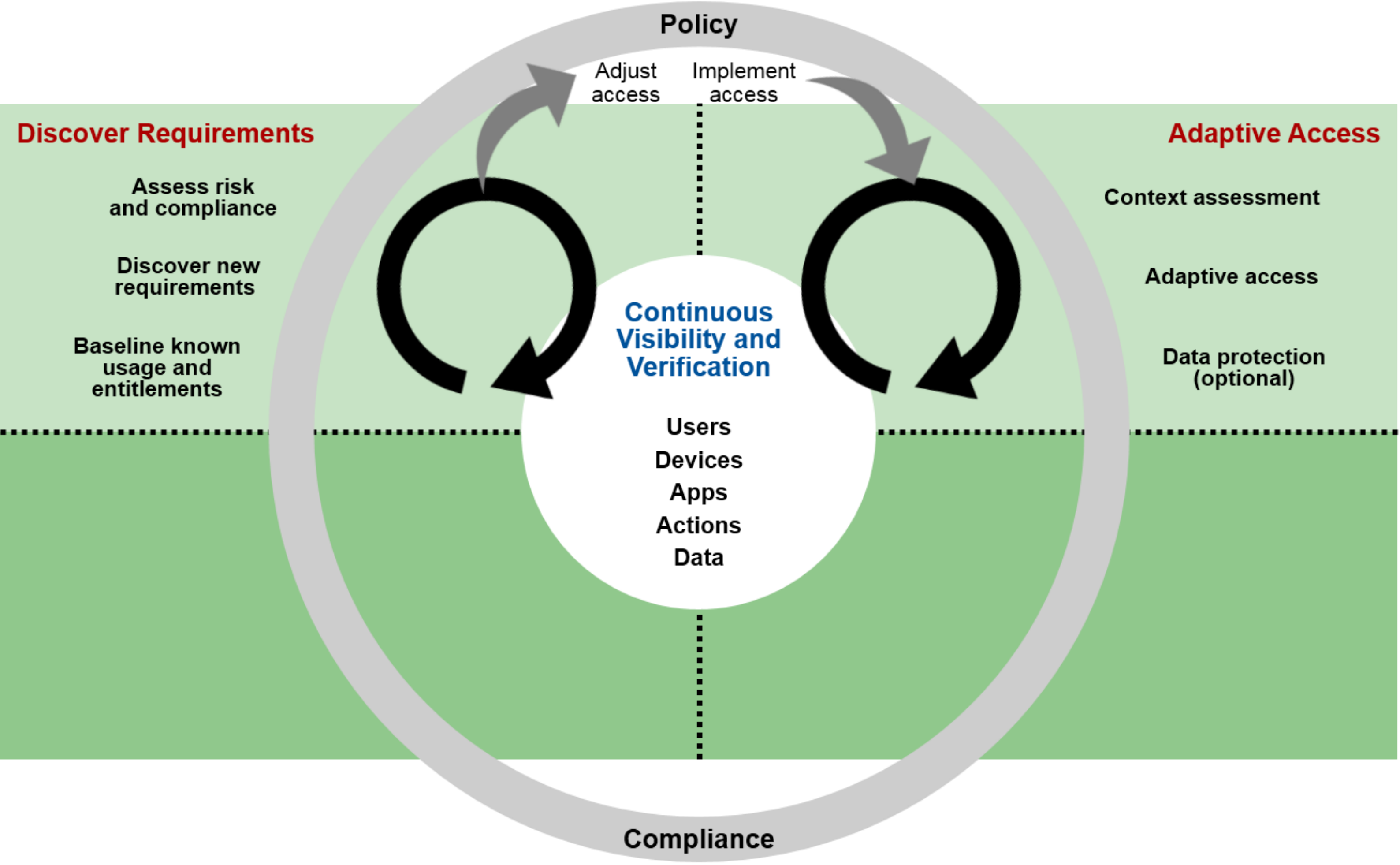
However, when implemented as an in-line proxy, this may create a single point of failure for the cloud service being accessed. If the CASB solution is down, access may not be possible, or, if accessible, the data may be unintelligible. Likewise, if the CASB mapping of the cloud service functionality is incorrect, due to a cloud service update, the CASB may effectively break the cloud service. More importantly, the encryption and or tokenization of data will often affect the end-user functionality of the SaaS application — specifically, search, indexing, sorting, numeric operations at the field level and functions such as document preview in an EFSS, if an object-level attachment is encrypted. Because of these issues, external cloud data protection should only be considered only when it is demanded by regulatory requirements. When this approach is used:

- Acknowledge and design for the limitations of encryption or tokenization performed outside the cloud service provider.
- Don't encrypt all SaaS data; choose only specific individual fields or files that are required to be tokenized or encrypted. In reality, too much tokenization/encryption can be as unhelpful to the business as not enough. Balance is the right approach here.
- Ensure that your CASB provider has close alignment with the cloud service it is protecting to ensure that changes in the cloud service are reflected in the CASB.

Emerging native cloud platform encryption services [6, 7] may be a better alternative for enterprises that are comfortable with the SaaS provider having access to the decryption keys (and the data being unencrypted in the memory of the cloud provider's servers) for short periods of time. In all cases in which data is encrypted, insist that customer-managed keys use an on-premises key management system or a cloud-based hardware security module (HSM) with tight control processes.

The need to provide adaptive access and optional encryption/tokenization is shown in the upper right-hand corner of Figure 2.

Figure 2. Adaptive Access


Policy
Adjust access
Implement access
Discover Requirements
Assess risk and compliance
Discover new requirements
Baseline known usage and entitlements
Adaptive Access
Context assessment
Adaptive access
Data protection (optional)
Continuous Visibility and Verification
Users
Devices
Apps
Actions
Data
Compliance

Source: Gartner (December 2015)

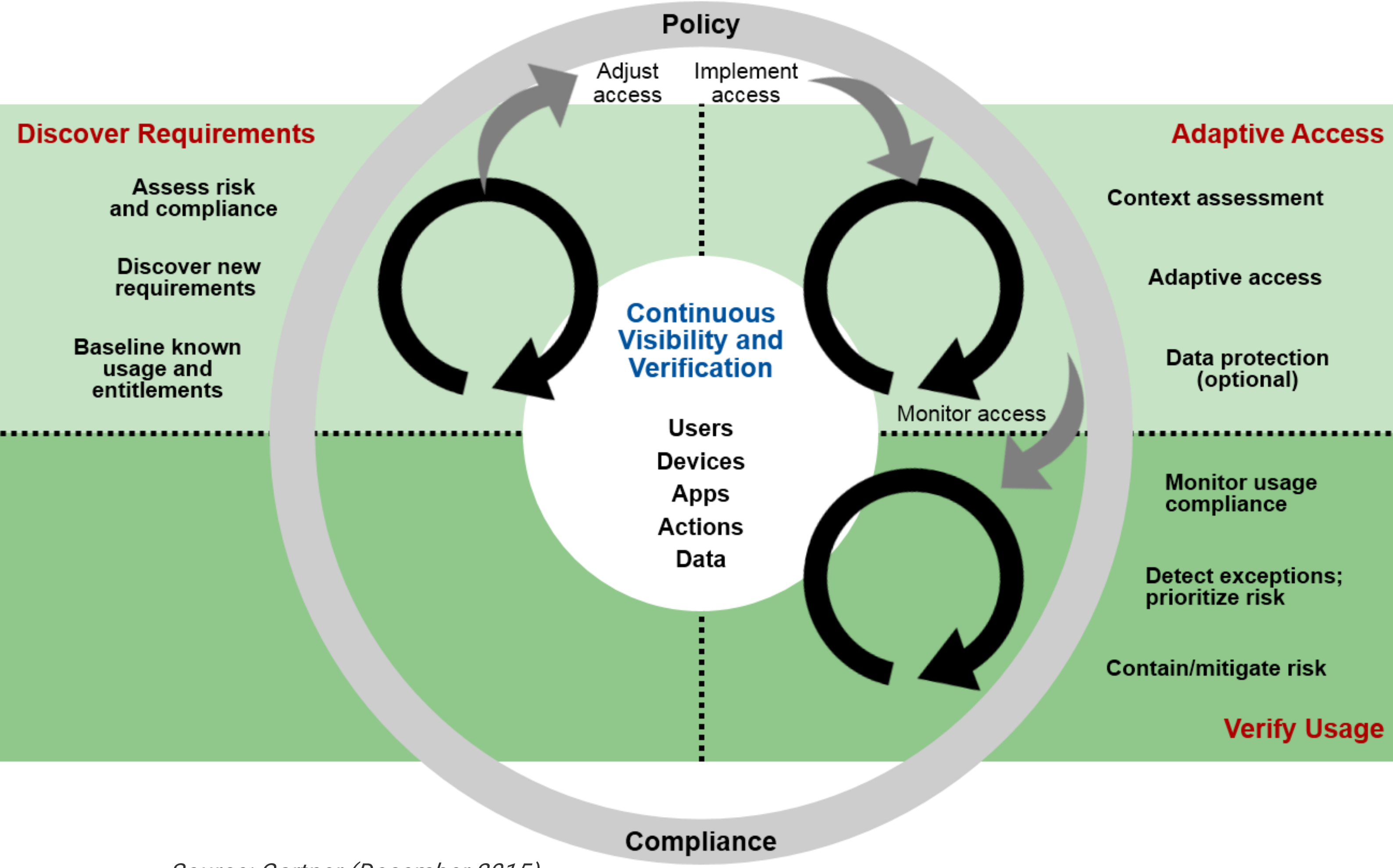
Continuously Verify Secure and Compliant Sensitive Data Usage

Most enterprises have a blind spot when sensitive data is stored in cloud services. The CASB platform should provide for continuous sensitive data monitoring — sometimes referred to as "cloud DLP" — through APIs or via in-line inspection. Here, the CASB solution should provide an understanding and a mapping of sensitive information flows — who, what, when where and why — even if no action is taken.

If the handling of sensitive data in a cloud service violates policy, the CASB platform should provide potential responses, including alerting the user, logging the event, and alerting an administrator or process/data owner. It should also allow blocking of the requested action — for example, not allowing certain content to be shared outside the organization and denying the ability to put personally identifiable information into a cloud service. Alternatively, the offending data may be encrypted or wrapped in a digital rights management (DRM) system for protection, or it could be quarantined in a file/folder for later review by an administrator or process owner.

The need to continuously monitor and verify sensitive data handling, as well as cloud activities and behaviors, is captured in the bottom right-hand corner of Figure 3.

Figure 3. Verify Usage



Source: Gartner (December 2015)

Investigate and Respond to Exceptions

Exceptions will be flagged in the access and use of cloud services that must be investigated. Because the core of any enterprise CASB strategy (and of the framework) is based on continuous visibility, this data must be available to a security analyst to investigate incidents that have been flagged, including in existing tools, such as security information and event management (SIEM). Leading CASBs are becoming increasingly sophisticated, enabling the exception response to be automated and making the data or process owners (and not IT) the primary escalation and action point for workflow.

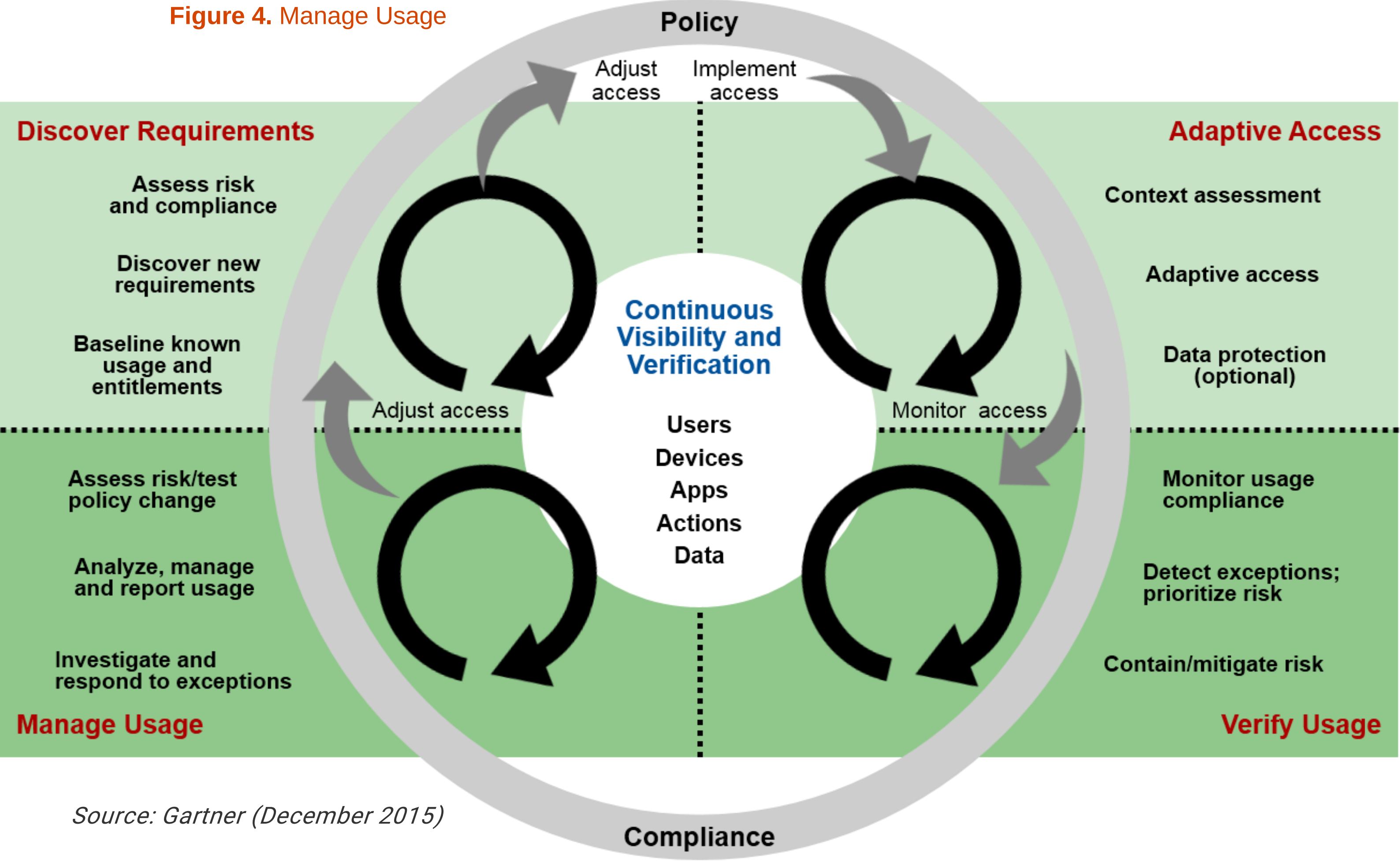
As a best practice, information security teams should focus on the exceptions, rather than on complete involvement with the specification of every possible control. The goal of the enterprise should not be to lock down and control cloud access at an extremely granular level. Rather it should focus on the access that matters (to sensitive data and applications from unmanaged devices) and use continuous monitoring and visibility as a compensating control for locking down and blocking access entirely. Risk is acceptable; unmanaged or unseen risk is not.

Manage Usage

In addition to managing exceptions, the rich amount of cloud services usage data can be analyzed and used to better manage cloud use. For example, to enable an operations or security analyst to visualize overall usage and activities, as described previously, business unit application owners should also be able to view this data and make intelligence-driven decisions as to access and licensing. Ideally, the CASB platform provides visualization capabilities to visualize and understand trending, as well as highlighting overlicensing or underlicensing situations. In addition to the native management console, the event data stream should be exportable to enterprise SIEM systems for analysis and compliance reporting. If policy changes are considered, the CASB solution should provide the ability to proactively model the impact and risk of making the change before the change is implemented.

The ongoing need to support the security analyst, operations analyst and business unit power to investigate cloud usage exceptions and manage cloud use is captured in the bottom left-hand corner of Figure 4. This completes the continuous adaptive security architecture for CASB solutions.

Figure 4. Manage Usage



Policy
Adjust access
Implement access
Discover Requirements
Assess risk and compliance
Discover new requirements
Baseline known usage and entitlements
Adaptive Access
Context assessment
Adaptive access
Data protection (optional)
Continuous Visibility and Verification
Users
Devices
Apps
Actions
Data
Adjust access
Monitor access
Assess risk/test policy change
Analyze, manage and report usage
Investigate and respond to exceptions
Manage Usage
Monitor usage compliance
Detect exceptions; prioritize risk
Contain/mitigate risk
Verify Usage
Compliance

Source: Gartner (December 2015)

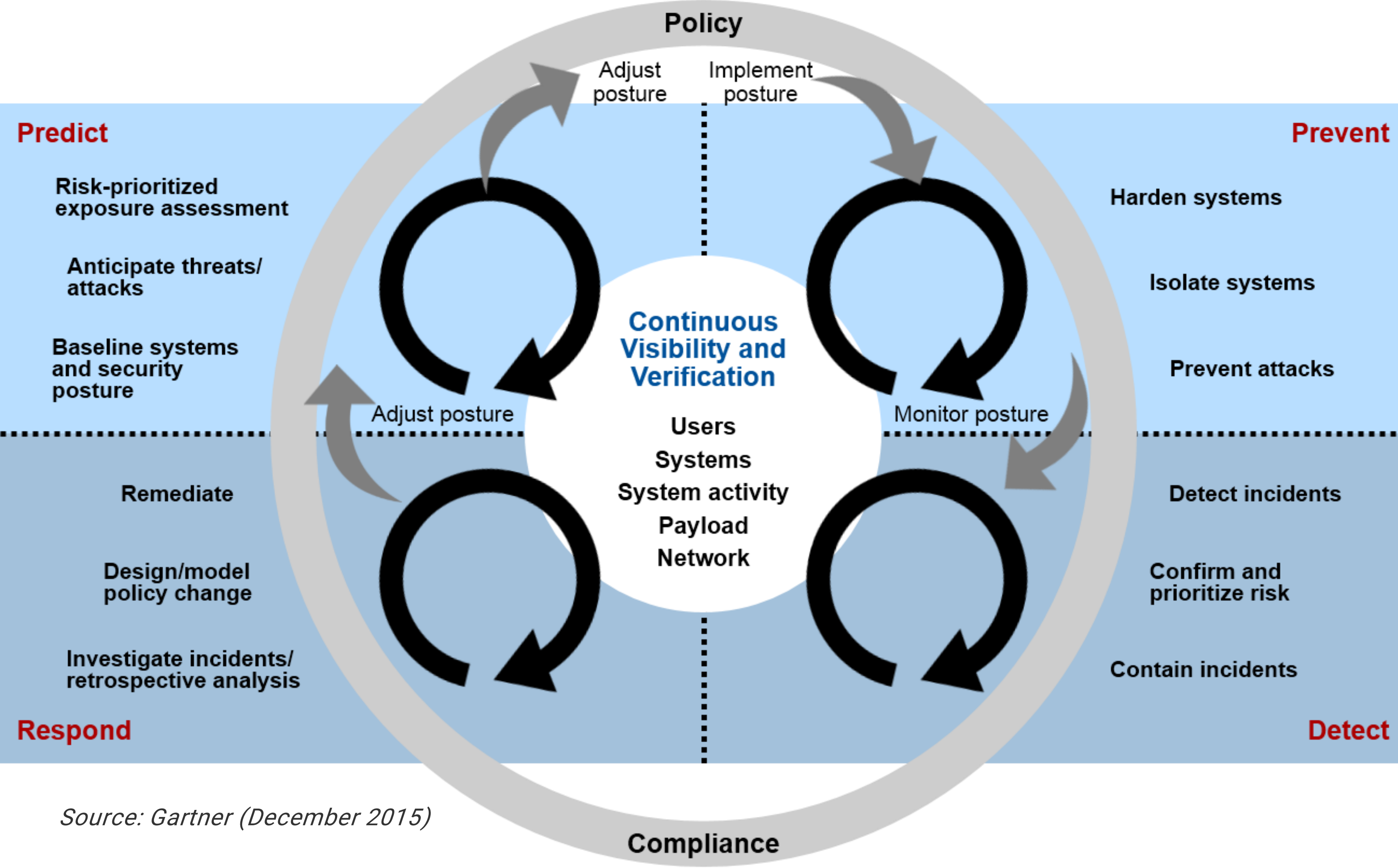
Make Threat Protection an Integral CASB Capability

The CASB architecture we've discussed to this point has been "access centric" — cloud services discovery, access, monitoring and management. However, we haven't discussed threat protection as a core capability to be evaluated when selecting a CASB solution (which we believe is a pillar of CASB capabilities). This is critical, because cloud services reside outside traditional enterprise security protection, such as intrusion prevention systems (IPSs) and anti-malware scanning. Furthermore, phishing of employees and the resulting hijacking of endpoints and accounts, has become one of the most common causes of security failure in the enterprise. Threat protection is exacerbated by the public cloud, because more services are externally accessible; however, less information is available on what your users are doing ("Everything You Know About SaaS Security Is Wrong").

Threat protection refers to a set of capabilities that provide prevention, detection, response and anticipation of threats to the enterprise when cloud services are used. To evaluate the threat protection capabilities of a CASB, enterprises can directly apply the Gartner Adaptive Security Architecture (see"Designing an Adaptive Security Architecture for Protection From Advanced Attacks"). This framework serves as complementary, threat-centric way for enterprises to design for a continuous and integrated approach for threat protection capabilities within a CASB solution.

Like the access-centric architecture of Figure 4, the heart of the threat-centric architecture of Figure 5 is based on continuous visibility and verification.

Figure 5. CASB Adaptive Threat Protection Using Gartner's Adaptive Security Architecture



Policy
Adjust posture
Implement posture
Predict
Risk-prioritized exposure assessment
Anticipate threats/ attacks
Baseline systems and security posture
Prevent
Harden systems
Isolate systems
Prevent attacks
Continuous Visibility and Verification
Users
Systems
System activity
Payload
Network
Adjust posture
Monitor posture
Remediate
Design/model policy change
Investigate incidents/ retrospective analysis
Respond
Detect incidents
Confirm and prioritize risk
Contain incidents
Detect
Compliance

Source: Gartner (December 2015)

The similarity between Figure 4 and Figure 5 is by design, because information security is dealing with the requirements of enabling secure and compliant access (Figure 4), while simultaneously keeping threats out (Figure 5). This is especially true with the consumption of cloud-based services, where traditional enterprise control points have difficulty acquiring the visibility necessary to apply policy. Ideally, CASBs bring the different domains of "letting the good guys in" and "keeping the bad guys out" into a single, integrated solution leveraging the continuous visibility and verification at the heart of both models. The overlap and inclusion of CASB threat-facing capabilities in other traditional, threat-facing product classes (e.g., network firewall, IPS and SWG) means that not all CASB capabilities will require point solutions or stand-alone products. For example, several SWG vendors are adding CASB capabilities.[9,10,11]

Applying Gartner's Adaptive Security Architecture to CASB solutions, the following are best practices for evaluating CASB threat protection capabilities.

The Prevent Phase

- Select a CASB provider that integrates with single sign-on (SSO) tools (or provides its own capabilities) and enterprise directories and can block access to a given cloud service from devices that appear to be compromised, regardless of whether they are sanctioned or employee-owned.
- Require CASB providers to scan file-based payloads (for example, a file being uploaded or downloaded from an EFSS) for malware, using a reputable, third-party, anti-malware engine or a cloud service.
- Evaluate your SWG and firewall solutions as potential providers of CASB capabilities, if they can provide sufficient visibility via logs, proxy, in-line or API, and their capabilities meet your project requirements. [9,10,11]

The Detect Phase

- Favor CASB providers that can integrate with leading on-premises or cloud-based network sandboxing solutions (see "Market Guide for Network Sandboxing") for deeper inspection of payloads beyond signatures.
- Require CASB providers to integrate with third-party threat intelligence feeds as a way to help detect cloud sessions to and from suspicious IP addresses, the handling of suspect files and so on.
- Require CASB providers to export their monitoring and event logs in syslog format (or, better yet, native integration) for ingestion into a SIEM or centralized logging systems.
- Favor CASB providers that include embedded user behavior analytics capabilities to identify malicious insiders and/or compromised user credentials, based on analysis of the user's behavior and activities within cloud-based services.

The Response Phase

- Select a CASB provider that supplies an investigation console where the full cloud services usage event tracking can be accessed. Ensure that it can provide a risk-prioritized view of suspicious or suspected malicious activities for a SOC analyst.
- Favor CASB solutions capable of providing a visual way to navigate a user's timeline of events as they interact with a given cloud-based service and that allow full exploration of the cloud services a user has accessed — for example, if a user leaves the company answering the question, "What cloud services and activities within these cloud services has the user performed during the past month?"

The Predict/Anticipate Phase

- Favor CASB providers that maintain their own proactive cloud threat research laboratories, actively research vulnerabilities and attacks on cloud service providers, [12, 13] and can use this intelligence to protect their CASB customers by recommending policy changes.
- Favor CASB providers that enable you to benchmark your own cloud services use patterns, as well as security and compliance settings against your peers in the same industry.
- Favor CASB providers with rich cloud service databases that enable you to anticipate (or predict) which cloud services should not be selected for sanctioned use in the first place, regardless of how well the CASB can provide overlay security controls for that service.

Bottom Line

As enterprises increasingly demand cloud services, information security teams need a control point for the secure and compliant use of cloud services that simultaneously address the need for secure access and threat protection. CASBs provide this control point. However, the market for CASB capabilities is rapidly developing, as enterprise needs emerge and industry consolidation occurs. Thus, limiting contracts to one or two years is recommended. Use the framework provided in this research to prioritize among the large number of features and architectural approaches being offered. Because no CASB buyer can fully anticipate everything they will want to do with a CASB, use this framework to identify CASB solutions and platforms that provide the needed enterprise capabilities today, as well as the vision and flexibility to address future requirements.

Evidence

[1] Palo Alto Networks

[2] Web Gateway

[3] Cloud Services Report

[4] Microsoft Azure

[5] IBM Cloud Security Enforcer

[6] Box Enterprise Key Management

[7] Salesforce Shield

[8] Symantec Data Loss Prevention

[9] Blue Coat Acquires Perspecsys

[10] Blue Coat to Acquire Cloud Security Vendor Elastica

[11] Zscaler Cloud Application Visibility and Control

[12] A New Zeus Variant Targeting Salesforce.com — Research and Analysis

[13] Severe Office 365 Token Disclosure Vulnerability — Research and Analysis

References: http:/www.gartner.com/doc/reprints?id=1-2X9IFXT&ct=160128&st=sb

For more information please contact CHASSasia Pte Ltd

Phone: (+65) 62129191 Email: Enquiry-SG@CHASSasia.com