The Definitive Guide to Cloud Access Security Brokers

bitglass

Cloud apps like **Office 365**, **Salesforce**, and **Amazon Web Services (AWS)**, have enjoyed unprecedented mainstream adoption in the enterprise. However, security concerns continue to plague public cloud adoption. Many organizations are eager to migrate to the cloud, but need visibility and control to keep sensitive corporate data safe. In order to secure cloud, enterprises should adopt a comprehensive security solution that offers threat protection, data protection, identity management, and complete visibility.

Cloud access security brokers (CASBs) are a data-centric solution for securing data end-to-end, from any app to any device. While early cloud security solutions were focused on SaaS security, CASBs have evolved into comprehensive platforms that protect data across SaaS, IaaS, and private cloud apps. By intermediating or "proxying" traffic between cloud apps and end-user devices, CASBs offer IT administrators granular control over data access as well as deep visibility over corporate data—critical for organizations moving from internal, premises-based apps to the cloud.

> *"The forces of cloud and mobility fundamentally change how "packets" (and the transactions and data they represent) move between users and applications. This causes a need to adjust the list and the priorities of investment in security controls for any organization that is consuming cloud services. [By 2020] 85% of large enterprises will use a cloud access security broker platform for their cloud services, which is up from less than 5% today."*
>
> **—Craig Lawson, Neil MacDonald,**
> **Brian Lowans and Brian Reed, Gartner.**

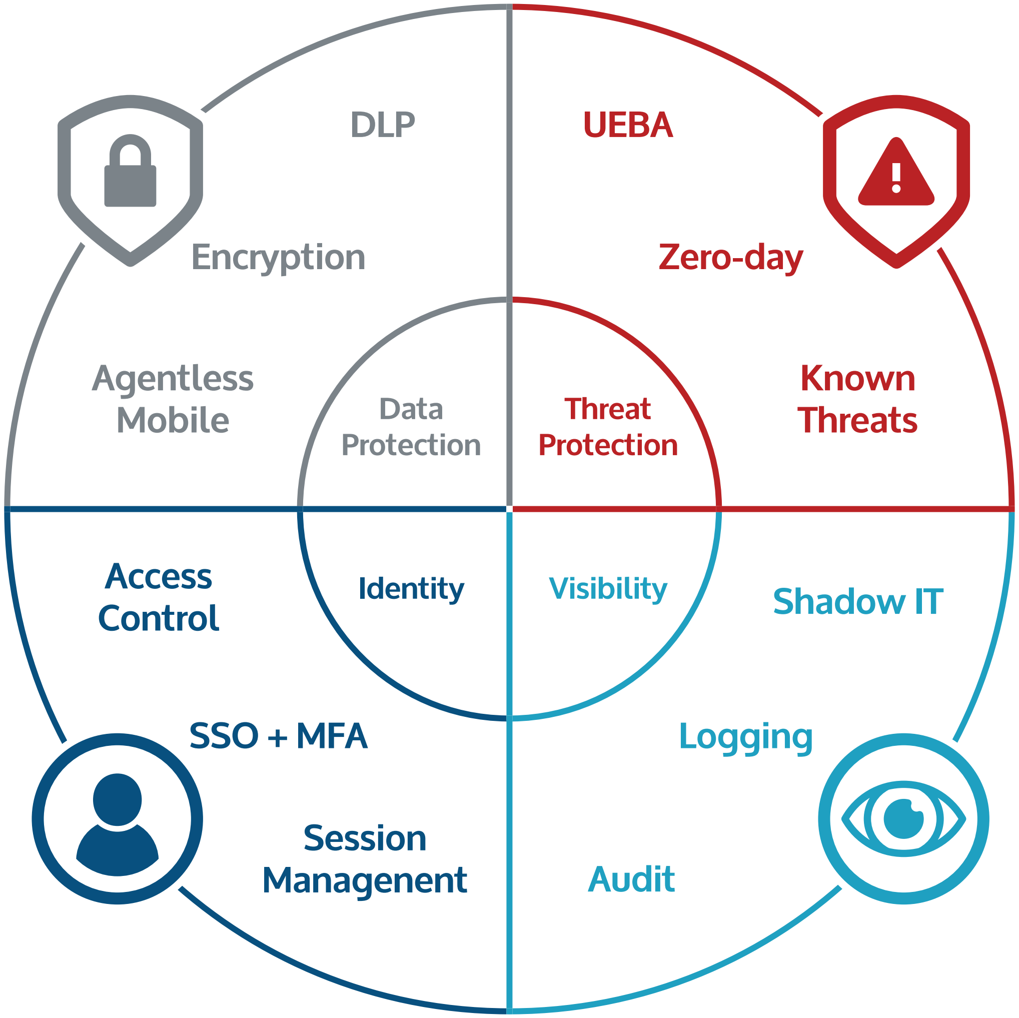
Limitations of Native Cloud App Security

Cloud app vendors like Google, Microsoft, and Amazon are motivated to secure their infrastructure and protect their applications from threats. Failure to do so can have a severe negative impact on their businesses. Denial of service attacks and large-scale infrastructure breaches are the types of security events that land cloud app vendors on the front page of the Wall Street Journal.

While cloud app vendors actively protect apps and infrastructure, securing data access and data on endpoints is the enterprise’s responsibility. Theft of user credentials, failure to comply with regulations, proliferation of malware, and data leakage due to improper controls all rest on IT. As such, IT must have a security solution in place to protect corporate data from the risks that fall outside the purview of SaaS and IaaS providers.

A Complete CASB

Cloud and mobile enable productivity and collaboration, but increase the risk of data leakage if not properly secured. A complete CASB provides threat protection, data protection, identity management, and visibility on any application, any device, anywhere.



Suppose "Felecia" works from home and uses a personal laptop to upload and download corporate files within Dropbox. Unbeknownst to Felecia, some of the trusted corporate files stored in Dropbox contain malware that can infect her personal and work machines. CASBs can prevent the upload and download of infected files within cloud apps, as well as scan for infected documents already in the cloud.

Threat Protection

User and Entity Behavior Analytics

Credential compromise renders many security solutions ineffective. When accounts are used by unauthorized individuals, there may be months of data exfiltration before the breach is noticed and addressed. Instead of responding after the fact, enterprises must adopt security measures that proactively monitor for anomalous user behavior. User and entity behavior analytics (UEBA) is a core component of any comprehensive CASB. UEBA generates baselines for user behavior in order to detect and respond to unusual activity in real time.

Malware

Malware and ransomware are major threats to data security. As cloud apps increase in popularity, they become more attractive to bad actors who use them as delivery vehicles for malware. Many CASBs are now incorporating malware detection and remediation into their platforms - enabling data scanning at upload and download via proxy, as well as data-at-rest scanning via API. However, as with endpoint protection suites, not all anti-malware is created equal. Traditional signature or hash-based malware detection can only defend against known threats, but AI-based scanning is effective for stopping known and zero-day malware.

Imagine that employee "John" uploads a file containing sensitive customer data to Microsoft OneDrive. John then shares the file to someone outside the company. A CASB will identify this risky external share and quarantine it for review by an administrator. Once the external share is deemed legitimate, the file is released from quarantine and the share is re-enabled.

Data Protection

Data Leakage Prevention

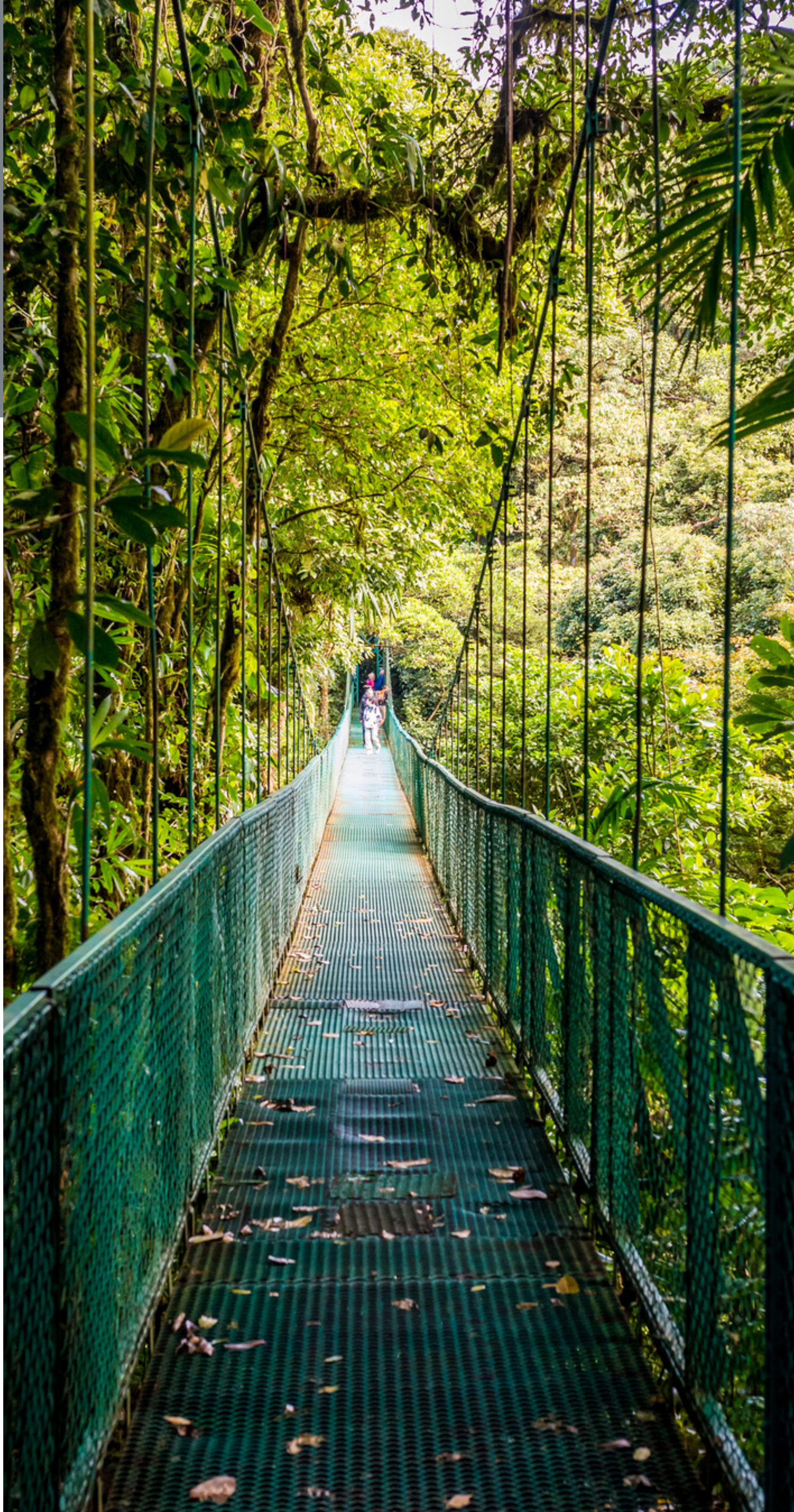
While traditional security solutions offer a limited range of policy actions, CASBs are context-aware and offer more flexibility in extending access and protecting data through proxies. With cloud data leakage prevention (DLP), CASBs can also scan and identify sensitive content at rest via API.

A lightweight policy action might be to allow a download, but embed watermarks within the file. More aggressive actions include redacting sensitive content or blocking a file from download altogether. These actions are particularly useful in risky contexts; for example, when a user attempts to download thousands of credit card numbers to a BYO device. Organizations must determine which protections they need and create policies accordingly.

Encryption

By encrypting cloud data, an organization benefits from public cloud functionality with private-cloud-level security. CASBs support field-level encryption for structured data, as well as file-level encryption for any app. In both cases, data is encrypted before upload to the cloud and decrypted at access when authorized by policy. Select CASBs offer "native" key management, but many also integrate with existing key management systems via the KMIP protocol.

The biggest challenge with cloud encryption is encrypting at full strength while preserving application functions like search and sort. Ensure that your CASB leverages industry standard encryption, 256-bit AES with 256-bit initialization vectors, and also enables full functionality.



"Chantelle" downloads sensitive corporate data to her personal iPhone in order to work remotely. A CASB can wrap data with DRM, requiring additional authentication before allowing her to view files. Additionally, she can be permitted to access the files offline, but only for a preset period of time. With an agentless CASB, this and more can be done without installing any software on mobile devices.

Data Protection

Agentless Mobile

Data must be protected across all devices, including unmanaged mobile assets. Because employees often reject cumbersome, agent-based EMM solutions, organizations are now taking an agentless approach to mobile security. Agentless CASBs can protect data on any mobile device without harming user privacy or device functionality—this is done via secure transmission, content-aware DLP, and device controls.

Organizations supporting BYOD also face the threat of lost and stolen devices. Agentless CASBs are capable of enforcing device-level security policies on any mobile device—functionality that has historically only been possible on managed devices. These CASBs can require the use of a PIN or passcode, enforce session management, and more.

Tools like mobile device management (MDM) often support the remote wiping of data on mobile devices. However, IT administrators are typically hesitant to use this capability for fear of deleting users' personal data and facing legal action. Fortunately, select CASBs enable agentless selective wipe so that IT can ensure that corporate information is deleted without harming personal data.

Employee "Jacob" typically logs into cloud applications from his managed corporate laptop inside the corporate network. Over the weekend, Jacob gets a new smartphone and decides to log in to multiple company cloud apps from the device. A CASB will recognize the device as new and take Jacob through additional authentication steps in order to validate his identity.

Identity

Secure Authentication

Identity management is a core component of any complete CASB solution. Whether through a native identity and access management (IAM) solution or integration with existing IAM infrastructure, CASBs facilitate secure authentication across all cloud apps. This type of integrated solution provides simple provisioning of accounts, a streamlined user experience with single sign-on, and involves less operational overhead than integrating separate standalone components.

Secure authentication, often necessary to achieve regulatory compliance, can drastically reduce the attack surface that hackers can use to access corporate data. Multi-factor authentication, for example, requires a user's password and access to a physical token in order to allow a login. When suspicious logins are detected, CASBs can automatically step up to multi-factor authentication. Similarly, automated session management monitors user activity and can force users to reauthenticate in order to prevent account hijacking.

Access Control

Contextual access control in a CASB governs where and how employees can access corporate data. Granular policies can be defined based on access method (browser or native app), device (managed vs unmanaged), location (by country or IP address range), and more. Organizations can block, allow, or provide intermediate levels of access to apps and sensitive data based on a user's identity and access context.

Imagine employee "Annie" uploads a corporate file to an unsanctioned cloud app—the standard shadow IT problem. In isolation, this action isn't necessarily indicative of a breach. However, if the data were uploaded to an unsanctioned cloud app immediately after the device contacted a known malware server, then it is fairly likely that the upload was a breach. CASBs can evaluate cloud apps by risk and quickly analyze multiple events to identify potential breaches.

Visibility

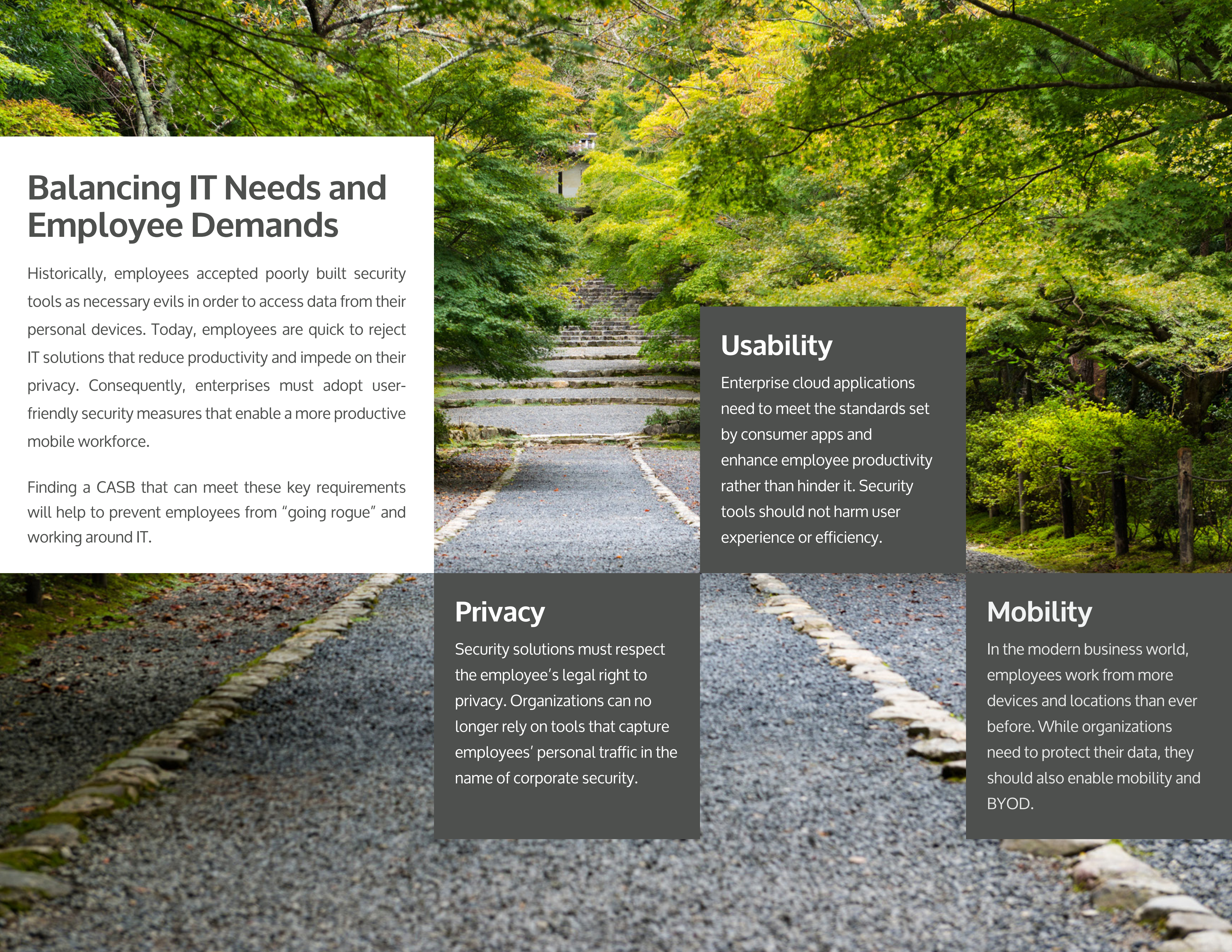
Shadow IT

Data exfiltration is a major concern for enterprises, particularly when destinations include malware command and control sites, anonymizers, TOR networks, and unsanctioned cloud applications. While blocking unsanctioned cloud apps may sound like the right strategy, employees will often work around this by using different apps or networks—demonstrating the need for a data-centric approach to security.

CASBs offer discovery services that analyze proxy or firewall data to scrutinize web traffic. Destinations associated with known malicious activity can be identified in order to remediate high risk endpoints and users. Unsanctioned cloud apps (shadow IT) are classified according to risk so that organizations can decide what to block and what to safely enable through a CASB.

Logging and Audit

CASBs provide detailed logs with information on all cloud app transactions, including downloads, logins, and more. Additionally, CASBs can track application-specific behaviors like contact database downloads in Salesforce and external file-sharing through Box. CASBs typically generate logs in human-readable form, allow for search and filter functionality, and integrate seamlessly with SIEMs and other security operations tools and workflows.



Balancing IT Needs and Employee Demands

Historically, employees accepted poorly built security tools as necessary evils in order to access data from their personal devices. Today, employees are quick to reject IT solutions that reduce productivity and impede on their privacy. Consequently, enterprises must adopt user-friendly security measures that enable a more productive mobile workforce.

Finding a CASB that can meet these key requirements will help to prevent employees from "going rogue" and working around IT.

Usability

Enterprise cloud applications need to meet the standards set by consumer apps and enhance employee productivity rather than hinder it. Security tools should not harm user experience or efficiency.

Privacy

Security solutions must respect the employee's legal right to privacy. Organizations can no longer rely on tools that capture employees' personal traffic in the name of corporate security.

Mobility

In the modern business world, employees work from more devices and locations than ever before. While organizations need to protect their data, they should also enable mobility and BYOD.

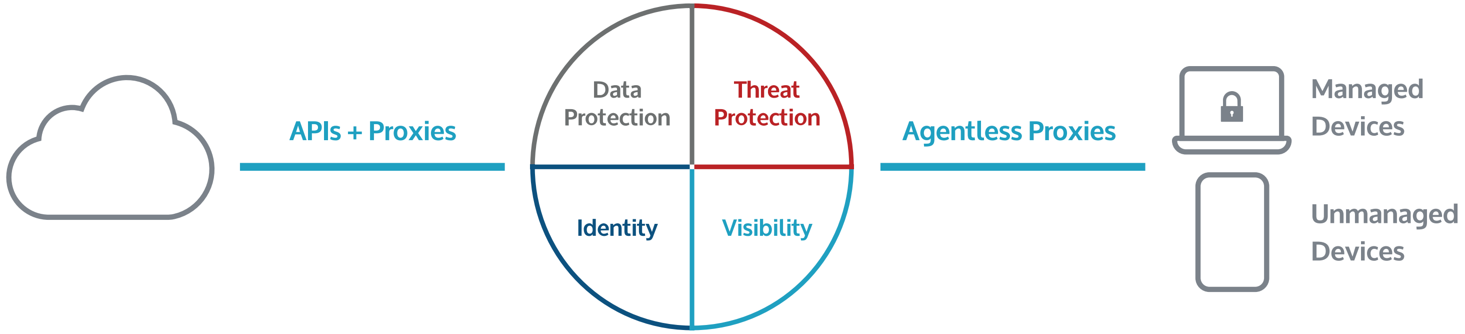
CASB Technology

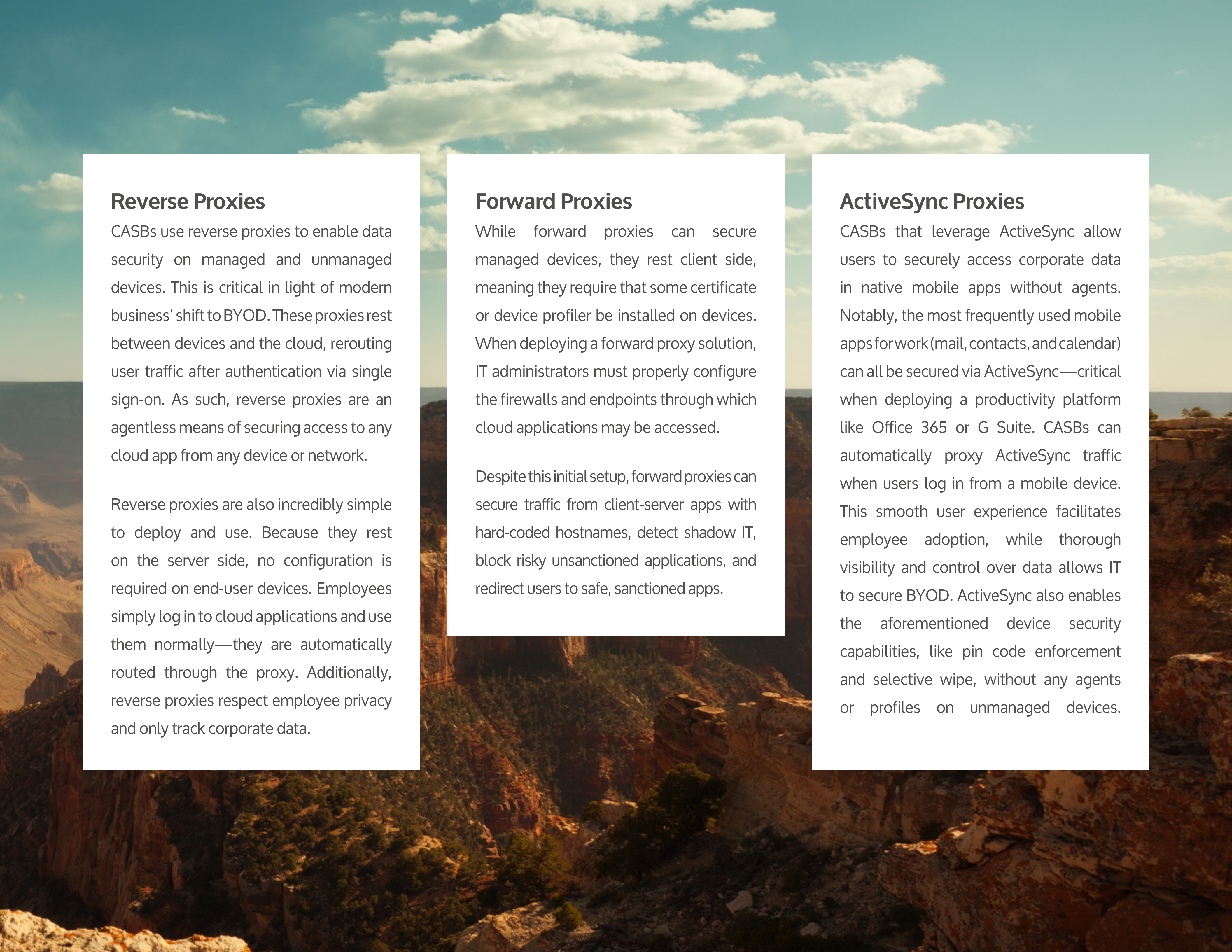
Most CASBs rely upon a combination of proxies and APIs to provide real-time control and visibility. Inline control on unmanaged, managed, and mobile devices is enabled through reverse, forward, and ActiveSync proxies, respectively. APIs, while not real-time, grant control over backend functions like external sharing.

Cloud-based productivity suites like Office 365 and G Suite can be accessed via the web, thick clients, and on any device that supports ActiveSync. As such, a complete CASB must use a combination of proxies and API integrations to secure data in any app, any device, anywhere.

API Integration

Cloud access security brokers leverage APIs for additional visibility and control over data stored in cloud apps. Within any app that provides access via an API, CASBs can crawl all files, or select files, to identify sensitive data and threats like malware. In turn, this informs the placement of controls around data so that organizations can govern sharing and access more effectively. Advanced data protection capabilities can also be implemented via API. For example, DLP actions like redaction and watermarking can be taken on cloud data at rest.





Reverse Proxies

CASBs use reverse proxies to enable data security on managed and unmanaged devices. This is critical in light of modern business' shift to BYOD. These proxies rest between devices and the cloud, rerouting user traffic after authentication via single sign-on. As such, reverse proxies are an agentless means of securing access to any cloud app from any device or network.

Reverse proxies are also incredibly simple to deploy and use. Because they rest on the server side, no configuration is required on end-user devices. Employees simply log in to cloud applications and use them normally—they are automatically routed through the proxy. Additionally, reverse proxies respect employee privacy and only track corporate data.

Forward Proxies

While forward proxies can secure managed devices, they rest client side, meaning they require that some certificate or device profiler be installed on devices. When deploying a forward proxy solution, IT administrators must properly configure the firewalls and endpoints through which cloud applications may be accessed.

Despite this initial setup, forward proxies can secure traffic from client-server apps with hard-coded hostnames, detect shadow IT, block risky unsanctioned applications, and redirect users to safe, sanctioned apps.

ActiveSync Proxies

CASBs that leverage ActiveSync allow users to securely access corporate data in native mobile apps without agents. Notably, the most frequently used mobile apps for work (mail, contacts, and calendar) can all be secured via ActiveSync—critical when deploying a productivity platform like Office 365 or G Suite. CASBs can automatically proxy ActiveSync traffic when users log in from a mobile device. This smooth user experience facilitates employee adoption, while thorough visibility and control over data allows IT to secure BYOD. ActiveSync also enables the aforementioned device security capabilities, like pin code enforcement and selective wipe, without any agents or profiles on unmanaged devices.

Wrap-up

Cloud access security brokers are quickly emerging as a must-have solution for organizations looking to secure cloud and mobile. CASBs bridge the gaps that cloud app vendors leave to enterprises to solve—they enable threat protection, data protection, identity management, and visibility. To protect sensitive corporate information, organizations need to adopt a comprehensive solution that can secure data on any app, any device, anywhere.

Bitglass, the total data protection company, is a global cloud access security broker and agentless mobile security firm based in Silicon Valley. Bitglass' solutions enable real-time, end-to-end data protection, from the cloud to the device. The company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

Try it for Free

For more information, visit www.bitglass.com