MANAGED SOLUTIONS

Fact Sheet

CROWN CASTLE

Cloud Access Security Broker

Today's cyberattacks have become more advanced and sophisticated, with the focus shifting toward targeting individuals and end-users rather than just perimeter firewall devices. As a result, it's crucial for organizations to protect the most vulnerable and critical assets on the cloud—specifically, their data. To protect how sensitive data is stored, accessed and handled, organizations need a cybersecurity solution that covers all aspects of zero trust approach to avoid unauthorized access, data leaks, account takeovers and other malicious insider threats.

Cloud Access Security Broker (CASB) can be added to your Secure Remote User solution, enhancing visibility, detecting and assessing shadow IT and mitigating risks from unauthorized cloud apps. It employs automated risk level assignments and identity-based policies that reduce the risks of insider threats and accidental data exposure.

CASB provides organizations like yours better application controls that allow your administrators to customize security policies based on user roles, devices and locations, enabling dynamic protection against evolving threats.

The challenge

IT teams face significant challenges while improving their overall security posture. These include:

1. **Keeping remote workers and distributed teams secure**
   There has been a surge in employees accessing sensitive data and resources from a variety of geo-locations and devices (laptops, PCs, mobile phones, tablets). Threats and attacks can originate from those devices, leaving it up to the IT teams to properly identify whether a user is logged in from a valid device/location.
2. **Gaining visibility into application activities**
   Traditional perimeter devices lack the sophisticated features that provide granular visibility into application activities and identify risky traffic based on ongoing transactions. This lack of visibility can make it difficult for IT teams to:
   - Identify the type of application and actions the users perform.
   - Discover shadow IT applications at the organization level.
   - Apply effective controls based on different contexts.
   - Detect modern risks and threats as well as malicious actors.
3. **Preventing data loss and allowing compliance monitoring**
   To ensure sensitive data isn't accessed or leaked by unauthorized parties, organizations need to implement monitoring and restriction mechanisms that can scan, detect and prevent unauthorized access and other data exfiltration activities on the fly. Without the right partner, this may be a daunting task, as data can reside on multiple cloud platforms where users can access it from anywhere and from any device.
4. **Creating and implementing unified security policies**
   As new tools and solutions flood the market, IT teams are tasked with managing an ever-expanding ecosystem of applications, each with its own configurations and controls—leading to fragmented security management that makes it harder to detect and respond to potential threats. A unified security policy should span and apply actions based on users, geo-location, device-compliance status, application actions (like, upload, download, etc.) and data type across the whole organization, regardless of where the user accesses the data. Without a centralized security policy framework, you may struggle to maintain compliance with industry regulations and standards, which can result in significant security risks that can compromise sensitive data and assets.

How it works

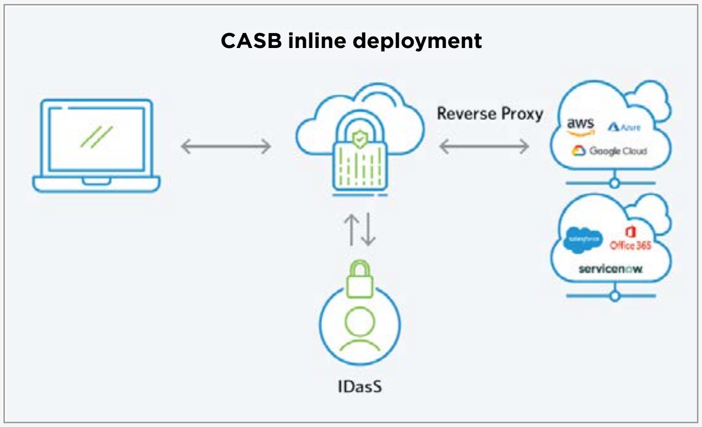
CASB is a value-added feature available to our Secure Remote User solution—and is deployed between our SASE gateways and cloud applications and/or internet. It's an intermediary broker between an end-user and the cloud, where the CASB engine gains visibility into cloud application usage—including encrypted TLS/SSL traffic—and applies differential treatment access controls for datain motion.

It integrates seamlessly with our Advanced Threat Protection (ATP) feature, enforcing robust security policies and safeguarding cloud app use and data. It provides AI-driven threat detection, behavioral analysis and anomaly detection to identify and prevent malicious activities targeting cloud services.

Flexible deployment

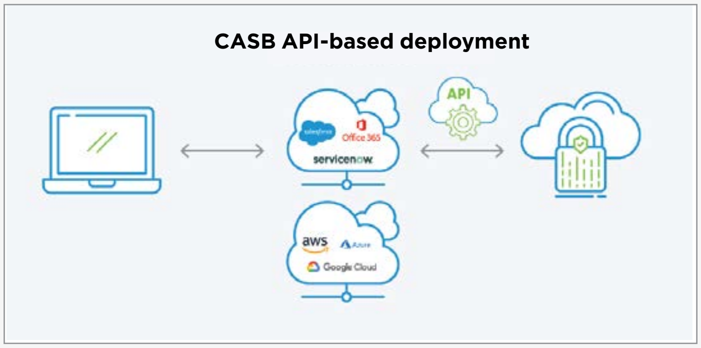
There are two forms of CASB deployments: : Inline and API-based.

Inline deployment



Inline deployment positions CASB directly in the traffic path between user devices and cloud apps, enabling real-time monitoring and policy enforcement. Because traffic reaches CASB before the cloud application, inline deployment is ideal for analyzing data in transit and taking preemptive action (e.g. blocking a file from being uploaded, etc.). Inline deployment can be configured via forward or reverse proxy.

API-based deployment



API-based deployment is an out-of-band deployment where CASB is not in the flow of traffic. Instead, it connects directly to cloud apps via APIs, providing ultra-granular, application-specific controls without interfering with live traffic. Because CASB is not in the traffic path, action is taken in near-real-time via API. This approach is ideal for:

- Enforcing policies for both managed and unmanaged devices.
- Protecting cloud apps that use certificate pinning.
- Conducting scheduled scans and post-incident forensic analysis.
- Ensuring continuous monitoring and enforcement of data-at-rest security policies.

Deployment mode	Ideal for
Inline – forward proxy Requires SASE client on endpoint devices	› Analyzing data in transit and taking preventative action (e.g. blocking a malicious file from being uploaded) › Managed devices
Inline – reverse proxy Requires integration with an Identify Provider (IdP)	› Analyzing data in transit and taking preventative action (e.g. blocking a malicious file from being uploaded) › Unmanaged devices (but can also support managed)
API-based Not in the direct flow of traffic	› Analyzing data at rest (e.g. scheduled scans, post-incident forensics) › Securing certificate-pinned apps › Managed and unmanaged devices

Key Benefits

Enhanced network security

We work with you to maximize security, keeping you safely connected across all your locations and wherever your employees work, with an average uptime of 99.999%.

Optimized performance and reliability

Easily view how users are accessing and experiencing services, no matter where they are. IT teams can see and fix problems before users notice them, manage user expectations around performance, or give tips on how to improve their experience.

Greater performance visibility

We provide detailed monitoring, sharing performance metrics for all segments between a user's device and the app they're accessing. Instead of siloed views from multiple tools, admins get a single, unified view.

Simplified network management

With end-to-end visibility and control through a single pane of glass, we make it easier to manage security policies and monitor threats across your network. Our dedicated experts work closely with your team, providing a best-in-class turn-up process and around-the-clock service for your trouble tickets, helping you operate at maximum efficiency.

Why Crown Castle?

Our unique, nationwide portfolio

With approximately 90,000 route miles of fiber, we own and operate one of the largest and densest fiber networks in the country with a presence in 23 of the top 25 US markets.

Our proven track record

In our 30+ years of experience owning and operating network assets we've seen it all and we're always ready to adapt to changing network trends.

Our deep expertise

We've worked with nearly every industry so we understand your unique opportunities and challenges and can tailor solutions to meet your goals.

Our solutions

We have your networking and security needs covered. Visit our infrastructure solutions page to learn more about our suite of solutions and how they can solve your toughest challenges.

CROWN CASTLE

Crown Castle owns, operates and leases approximately 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. This nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service—bringing information, ideas and innovations to the people and businesses that need them.

For more information, please contact 1-888-898-6336 or visit **CrownCastle.com**