

Ensure secure, compliant use of cloud applications

DXC Managed Cloud Access Security Broker

Gain visibility and control of sanctioned and unsanctioned cloud applications across your enterprise.

Benefits

- Understand the current usage of cloud applications
- Engage your organization on the appropriate use of software as a service (SaaS)
- Identify anomalous and potentially malicious behavior by understanding user activity
- Scan files stored in sanctioned cloud applications for violations of company policy or compliance criteria

As IT infrastructures and applications migrate to cloud-based alternatives, traditional security monitoring solutions lose visibility and control. Your users have access to free, cloud-based collaboration and file-sharing applications, which may violate or circumvent your organizational security controls and policies. This issue is particularly prevalent in organizations with mobile workforces.

“Shadow IT” — a term used to describe the use of computing resources and applications that are not sponsored by or under the control of an organization’s IT department — bypasses traditional security controls and policies. This leaves your organization vulnerable to the misuse of applications while increasing your risk of regulatory violations and data exposure.

To secure sensitive data stored in cloud applications, you must:

- Identify which cloud applications employees are using and how they are using them
- Determine appropriate applications to meet business needs
- Sanction required services
- Enforce company or regulatory requirements

Identify violators and threats to security

Managed Cloud Access Security Broker from DXC Technology protects sensitive data by identifying cloud applications being used in your organization, determining which applications should be sanctioned, and creating and enforcing security policies through continuous monitoring and threat analysis. This approach to managing cloud security access prevents attackers or disgruntled employees from exposing or disseminating confidential company information. Additionally, it ensures compliance with regulatory requirements by demonstrating your adherence to security policies.

Secure sensitive data while complying with regulations

DXC Managed Cloud Access Security Broker continuously monitors and analyzes the use of sanctioned cloud applications and rapidly responds to incidents and compliance violations in real time.

This protects confidential company information from violators who threaten your organizational security and ensures that important regulatory requirements are met.

Control and visibility of threat detection, response and hunting activities guard against takeover attempts and data destruction while defending service infrastructure integrity. This approach minimizes risk of exposure, damaging attacks and hefty noncompliance fines. Your company also gains the proven security expertise required to define and implement the right data protection strategy.

Why DXC?

- **First to market.** An industry innovator for 50+ years, DXC is the first IT services provider to offer managed cloud access security broker services.
- **Superior data science.** Our managed service leverages threat telemetry and data from multiple sources for unrivaled behavior analysis.
- **Best-in-class threat detection and remediation.** Leading encryption and data loss prevention technologies fuel DXC's fast, accurate threat detection and remediation.
- **Flexibility and scalability.** Cloud applications are continuously changing. DXC responds with a flexible solution that is easily scalable.
- **Comprehensive cloud security.** With 24x7 monitoring across a network of Security Operations Centers (SOCs) on five continents, DXC delivers end-to-end protection of cloud applications through proven threat detection, analysis and response services.

Find a solution that fits perfectly

Managed Cloud Access Security Broker provides a suite of security tools that support the discovery and protection of cloud-based applications.

These tools feature options for every organization:

- A shadow IT risk assessment provides your organization with a clear view of the cloud applications being used. This information is critical when building a tailored solution.
- Your organization may already know which cloud applications are in use but requires further understanding of how those apps are being used and what data is stored in them.

You can accomplish this objective by using application APIs or hosted gateway solutions to monitor sanctioned applications.

Gain control and visibility

DXC helps you know which cloud applications are being used and who is using them.

This enables your organization to:

- Gain control and visibility over the use of key web applications
- Minimize risk of exposing and disseminating confidential company information
- Reduce over-sharing of sensitive content

- Comply with regulatory requirements by demonstrating adherence to security policies
- Define a data protection strategy for securing additional cloud applications and services
- Build a strong relationship with a trusted security expert that understands your business and offers sound advice

Take the next step to proactively safeguard your digital enterprise

Schedule a consultation with DXC experts who can conduct a comprehensive risk assessment of your security posture and an in-depth analysis of the results.

Your organization will gain a systemic view of all cloud applications currently in use.

A subsequent deep-dive session with DXC solidifies the strategy for continuously monitoring and managing user activity and enforcing usage policies on sanctioned and unsanctioned cloud applications.

Contact us at www.dxc.technology/contact_us to find out how to leverage DXC's security expertise to build the right protection strategy for your business.

Learn more at
www.dxc.technology/mcasb