LTS SECURE CASB

Secure data encryption and data protection

A cloud access security broker is software or tool or a service that sits between an organization's on premises infrastructure and cloud provider's infrastructure. A CASB acts as gatekeeper, allowing the organization to extend the reach of their security policies beyond their own infrastructure.

CASB plays important role in identity management. CASB helps in identity provisioning, identity de-provisioning and directory authentication

The Single Sign on Solution from LTS Secure is a unique authentication protocol designed by the experts at LTS Secure, which provides its users a unique dashboard that is a single sign on console, integrating all the active links to all their cloud-based applications. SSO not only strengthens the cloud security protocols, but also allows single sign on access to multiple users for easy IT monitoring. Single Sign On solution offers one-click access to all of the applications with one password.

A popular security option is two-factor authentication that CASB offers, which verifies the identity of users attempting to access stored data. Two Factor Authentication is in regular use, which means your customers won't be confused by it. It's a simple way to give them an added layer of security that doesn't detract from their experience of product or site.

HIGHLIGHTS

- Access Management
- Contextual Access Control
- Single Sign on
- Two Factor Authentication
- Identity Management
- Security Policies Enforcement
- Security Threats Protections
- Security Behavioral Analytics
- Data Loss Protection
- Pattern Based Fraud Detection
- Application Auditing
- Correlation Engine
- App Discovery Engine
- Data Encryption

Access Broker
- Single Sign-On (SSO)
- Two-factor authentication
- Access Management

Identity Management
- Identity Provisioning
- Identity De-provisioning
- Directory Authentication

Data Leaks
- User Behavioral analytics
- Data Leakage Protection
- Anomalous Alerting

Activity Visiblity
- Activity Monitoring
- Log Management
- Privilage Activity View

CASB provides context-based access control (CBAC), which is a feature of firewall software, which intelligently filters TCP and UDP packets based on application layer protocol session information. It can be used for intranets, extranets and internets.

The Cloud Access Security Broker (CASB) is an architectural concept of an over-sized security market category. Many of the pieces in the CASB model are necessary for coherent cloud security policy enforcement. Cloud Access Security Broker provides Security threat Protection and Security Behavioral Analytics. It protects the data and also helps in pattern based fraud detection.
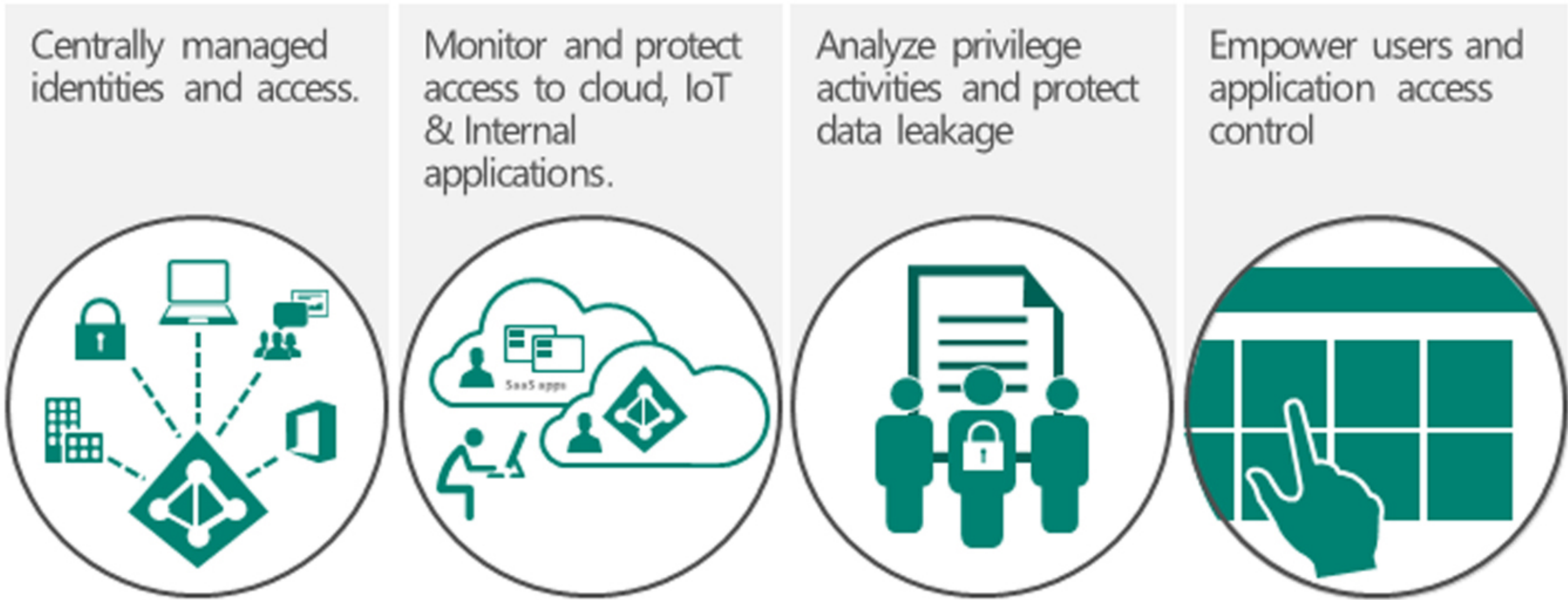
Application Audit discovers Shadow IT in use and provides risk analysis with intelligence on thousands of cloud services. With Audit you can monitor cloud app usage through intuitive dashboards and easily generate Shadow IT risk assessments on demand
The CASB correlation engine is an analytics tool that uses the logs on the firewall to detect actionable events on your network. The engine correlates a series of related threat events that, when combined, indicate a likely compromised host on your network or some other higher level conclusion.

Cloud App Discovery is a feature of CASB that enables you to discover unmanaged cloud applications being used by the people in your organization.

The main feature of CASB is data encryption, which protects the data loss or data breach.

Cloud Access Security Broker

| Centrally managed identities and access. | Monitor and protect access to cloud, IoT & Internal applications. | Analyze privilege activities and protect data leakage | Empower users and application access control |

LTS Secure

2