At a Glance
CA Top Secret® for z/OS provides innovative, comprehensive security for your business transaction environments—including z/OS®, UNIX® and Linux® on System z®—helping you realize the reliability, scalability and cost-effectiveness of the mainframe. CA Top Secret provides the Advanced Authentication Mainframe feature, system entry validation, resource control, auditability, accountability, administrative control, and SAF compatibility. In conjunction with distributed security solutions from CA Technologies, CA Top Secret provides mobile-to-mainframe enterprise class security and compliance management.

Key Benefits/Results

- **Strengthens security** and reduces risks across the enterprise.
- **Simplifies the tasks** associated with maintaining compliance.
- **Offers same day support** for new operating system releases and sub-system releases.
- **Improves efficiency** by providing streamlined administrative functions.

Key Features

- **Advanced Authentication Mainframe feature.** Requires users to successfully authenticate with two factors before logging in to mainframe applications.
- **Out-of-the-box, role-based access control.** Covers z/OS operating systems; interfaces for CICS, USS and IMS; and an optional add-on for DB2 for z/OS.
- **Flexibility and control.** Helps monitor and adjust security policies and accommodates virtually all organizational structures.
- **User-oriented architecture.** Focuses on the user to help reduce overhead, boost efficiency and enable better overall implementation.
- **Improved access control.** Externalizes USS file and directory-level security.
- **Controlled sharing and auditing of data and resources.** Includes administrative tools, extensive reporting options, online monitoring and automatic logging capabilities.

Business Challenges

In the application economy, the mainframe is at the heart of the data center and critical to the success of your business. With employees, partners, suppliers, and customers accessing sensitive data from multiple devices, identity has become the new perimeter. To protect sensitive information from hackers, companies must positively identify every user and device that requests access to their systems and data. User IDs and passwords used to be the key to identifying users, but now passwords alone have proven vulnerable to social engineering and simple hacking techniques. A successful multifactor identity management scheme is essential enterprise-wide, where users can be easily added and deleted as they come, go, and change roles within the organization.

Controlling access to content and resources goes hand in hand with identity management. Access control must be granular, role based, and continually updated to ensure that only the right people have the right access. Effective security requires consistent controls across systems and the organization—inconsistent policies increase risk and invite disaster.

Solution Overview

CA Top Secret is designed to protect your mainframe systems and data by controlling access to resources. The solution closely maps security to how you manage your organization by using a flexible configuration mechanism unique to CA Technologies that automatically associates users to one or more roles. CA Top Secret delivers out-of-the-box access control software for z/OS operating systems, which includes interfaces for CICS®, z/OS Unix (formerly known as OMVS) and IMS®, plus an optional add-on for DB2®. Additionally, CA Top Secret provides the Advanced Authentication Mainframe feature for RSA® SecurID® tokens at no additional cost to licensed customers. The mechanisms within CA Top Secret provide flexibility and control to help you monitor and adjust your security policies, and accommodate virtually all organizational structures.
Critical Differentiators
Because individual accountability is the key to effective information security, CA Top Secret allows you to decide which policies are relevant to your organization, and implements those structures. The product provides easy-to-use, role based administration functions that adapt to your organization’s structure and procedures to support your compliance with regulations and laws.

CA Top Secret delivers several options for you to separate security administration functions, providing different levels of administrative authority over your users and resources. The product can scope or limit privileges to discrete security functions, areas or resources. Users are protected by the built-in Advanced Authentication Mainframe feature for RSA® SecurID® tokens and consistent password policies enforced throughout your organization to increase information security.

CA Top Secret integrates with other solutions to provide comprehensive information security across your network and generates audit records for virtually any security-related event. The tool provides a comprehensive set of reports that enable you to view and analyze your security event information as well as limit the output of a particular report according to the privileges and restrictions of the specific user.

Related Products/Solutions
- **CA Top Secret Option for DB2 for z/OS**: Bring the powerful capabilities of CA Top Secret to the DB2 environment.
- **CA Data Content Discovery**: Locate unmanaged but regulated data on System z.
- **CA Auditor for z/OS**: Identify and control z/OS security exposures.
- **CA Cleanup for z/OS**: Automate continuous and unattended security file cleanup more easily.

Supported Environments
- **IBM z/OS**: any supported release through z/OS 2.2
- **IBM CICS Transaction Server for z/OS (CTS)**: any supported release through CTS 5.2
- **IBM Information Management System (IMS)**: any supported release through IMS 14.0
- **CA Common Services**: any supported release through CA Common Services for z/OS 14.1

For more information, please visit [ca.com/mainframe-security](http://ca.com/mainframe-security)