**SOLUTION BRIEF**
CA Mainframe Security Management Solutions | September 2010

# how can mainframe security management solutions from CA Technologies help me simplify and unify security?

we can

ca technologies

**CA Mainframe Security Management solutions helps you reduce costs, facilitate new business opportunities, address regulatory compliance requirements, and mitigate security risks associated with users and their access to resources and applications.**

# executive summary

## Challenge

Security is a major concern for today's organizations. Without the appropriate security measures in place, someone could alter or destroy your valuable data, sell your company's secrets to your competitors, or invade the privacy of others. While mainframe security is generally considered more secure than other platforms, the creation of a more open infrastructure exposes the enterprise to unprecedented security threats.

## Opportunity

These concerns can be addressed through the deployment of a comprehensive and integrated mainframe security management solution. The CA Mainframe Security Management products help you reduce costs, facilitate new business opportunities, address regulatory compliance requirements, and mitigate security risks associated with users and their access to resources and applications.

## Benefits

Today, security is a fundamental business matter of mission-critical importance.  Mitigating risk while improving operational efficiencies and addressing compliance requirements through automation of security controls and more effective proof of controls is the primary benefit of CA Mainframe Security Management solutions. But equally important are business benefits such as reducing cost and improving efficiencies by automating and centralizing identity management, reducing risk by improving security for critical IT resources and information, and enabling greater business performance by improving competitive responsiveness, customer online experiences, and partner ecosystems.

## The CA Technologies advantage

CA Technologies continues to simplify and unify IT management and help you harness the potential of the mainframe platform while masking its complexity. For over 30 years, mainframe data centers have relied upon—and continue to rely upon—our Mainframe Security Management expertise to manage, protect and secure their environments, and CA Technologies is poised to lead the delivery of mainframe security management software for years to come.

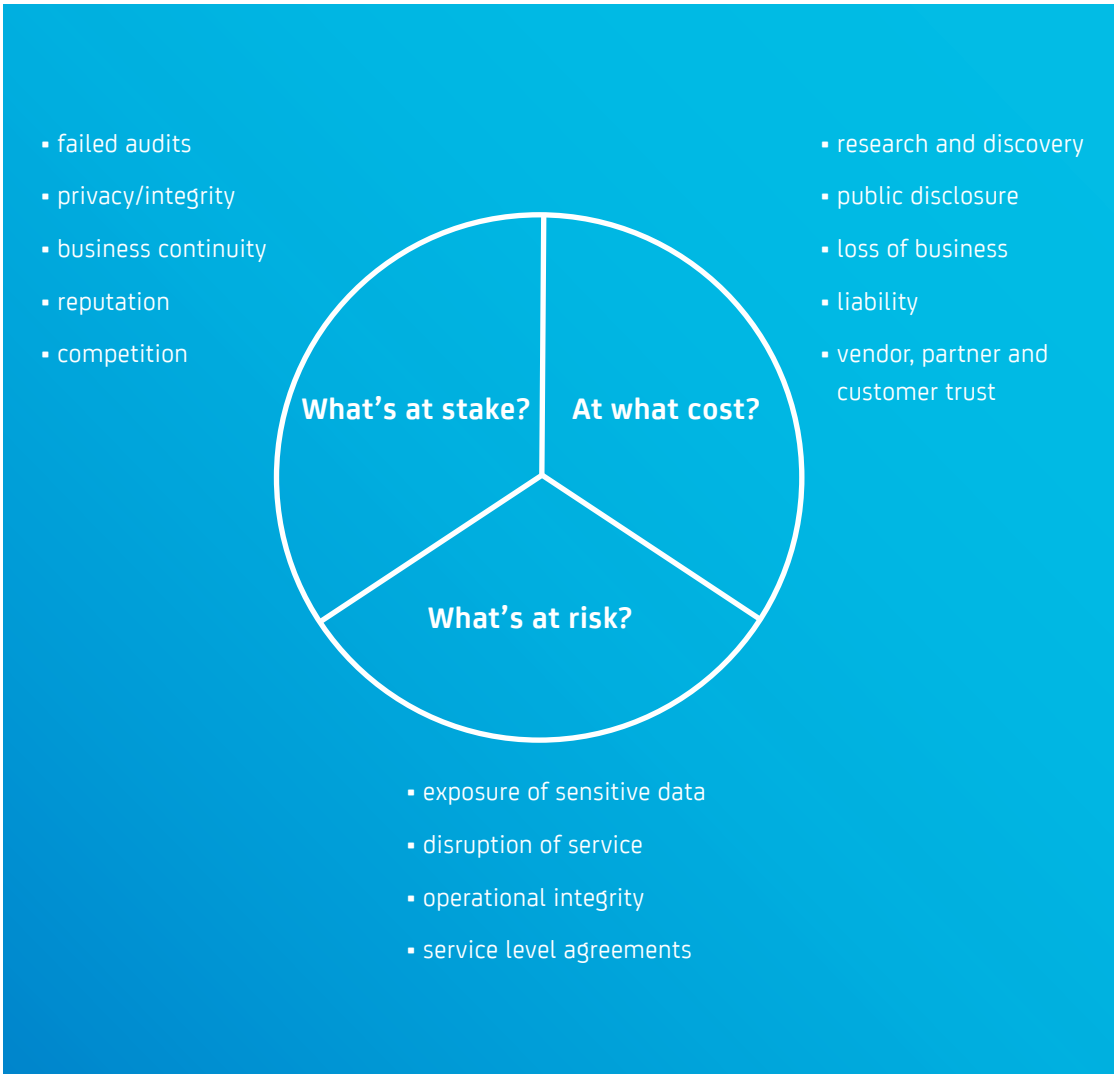
section 1: challenge

# Reduce risk, manage compliance, and grow your business

Security is a major concern for today's organizations. It is essential to make sure the right people have access to the right data. Without the appropriate security measures in place, you might find someone altering or destroying your valuable data, or selling your company's secrets to your competitors or someone invading the privacy of others. While mainframe security is generally considered more secure than other platforms, the creation of a more open infrastructure exposes the enterprise to unprecedented security threats. And without the appropriate processes and best practice guidance and tools it becomes costly and difficult to comply with relevant guidelines and regulations—leading to ineffective risk management and greater cost.

**Figure 1**
Cost of Doing Nothing

Without the appropriate solutions and tools it becomes costly and difficult to comply.



Many companies are still using mainframes today and are looking for ways to integrate the mainframe with their client-server networks, making cross-platform security essential. Most importantly, you must ensure continuous business operations by mitigating risk at virtually every level of your organization—all while maintaining budgets and achieving operational efficiencies.

Sound mainframe security management provides the foundation for effective security by ensuring all users have only the appropriate level of access rights to all protected resources, and that those rights are enforced appropriately. It helps lower administration costs by automating many system administration functions, as well as greatly enhancing regulatory compliance by automating your security controls and simplifying your compliance audits. Finally, it can enable business growth and help you solidify existing customer and partner relationships, as well as more effectively developing expanded relationships.

The key to effective security management solutions is to meet these challenges:

## Doing more with less

As businesses expand and evolve, they go through transformations. New applications are adopted and made available to employees, business partners and customers, which creates a plethora of digital identities and escalating administrative costs. Compounded by more security mandates on privacy and data confidentiality, IT administrators are burdened with additional access and auditing projects. Increasing demands on existing limited resources require greater efficiency.

## Mitigating risk

Managing users and their access is no longer a simple task in today's complex business environment. The definition of a user has expanded beyond the traditional enterprise user. Customers, suppliers and partners are now an integral part of an organization and thus require access to applications and data as well. Business partners require a trusted relationship to execute business transactions. Public-facing websites and business processes exposed via Web services must be provided. The complexity of identity management is further increased because it must have the capability and capacity to manage identities and security in different types of legacy and distributed systems and applications, including HR, ERP and supply chain management systems.

## Enabling regulatory compliance

Enterprises are facing increasing challenges in meeting the requirements of governmental and industry regulations. Regulations covering IT security may have specific requirements related to the concept of knowing who users are, what applications and resources they are entitled to access, and what (and when) they actually did on their last access. Creating a set of automated and strong internal security controls related to user identities and their access can greatly ease the burden of meeting these requirements.

By meeting these challenges, organizations can identify and remediate inappropriate access rights, as well as ensure that your IT assets are appropriately protected. This brief will present the innovative solutions that CA Technologies provides for Mainframe Security Management, and highlight how these solutions can greatly simplify your compliance efforts, reduce your IT risk, and help you reduce your total IT costs.

section 2: opportunity

# Comprehensive mainframe security management solutions

CA Mainframe Security Management is a comprehensive, integrated solution that enables enterprises to make their business resources and IT assets open and available, while managing the digital identities of users, devices and applications accessing those resources and the underlying policies and processes that govern how those entities interact with the organization. It provides a robust and proven solution for protecting your IT assets across all platforms and environments within your enterprise. CA Mainframe Security Management products can provide the following important benefits:

REDUCED ADMINISTRATIVE COSTS AND IMPROVED EFFICIENCIES. Reduce your security administration and Help Desk costs, as well as improve the overall productivity of your user population. By centralizing the management of all user identities and their access rights, management of your security policies becomes easier, less error-prone, and significantly less costly.

IMPROVED ABILITY TO MANAGE REGULATORY COMPLIANCE. Provide your organization with tools that support effective regulatory compliance. These products provide strong security features that can help reduce the risk of security breaches, protect critical information, and facilitate IT auditing.

SEAMLESS INTEGRATION. With the mainframe now linked to other environments, CA Mainframe Security Management products provide both cross-product and cross-platform integration for security access control and administration.

UNIFIED SECURITY AND MAINFRAME MANAGEMENT. With the increase in security concerns and many new requirements for both mainframe and distributed platforms, CA Technologies believes unified management is a vital factor in maintaining comprehensive enterprise security and management.

## Maximize Your Investment with CA Mainframe Security Management

### Mainframe 2.0

CA Mainframe Security Management has adopted key Mainframe 2.0 features that are designed to simplify your use of CA Mainframe Security Management and enable your staff to install, deploy and maintain it more effectively and quickly.

- CA Mainframe Software Manager: The CA Mainframe Software Manager (CA MSM) automates CA Mainframe Security Management installation, deployment and maintenance and removes SMP/E complexities.
  - The Software Acquisition Service enables you to easily move product installation packages and maintenance from CA Support Online directly to your mainframe environment and prepare them for installation.

  - The Software Installation Service standardizes CA Mainframe Security Management installation, which includes a new, streamlined Electronic Software Delivery (ESD) method that allows CA Mainframe Security Management to be installed using standard utilities. This service also provides standardized SMP/E product installation and maintenance via APARs and PTFs, and simplifies SMP/E processing through an intuitive graphical user interface and an intelligent Installation Wizard.
  - The Software Deployment Service enables you to easily deploy CA Mainframe Security Management in your mainframe environment.
  - CA MSM Consolidated Software Inventory (CSI) updates and infrastructure improvements add flexibility to CA MSM processing of CSIs and enable CA MSM to more effectively utilize CPU and system memory.

- Installation Verification Program (IVP) and Execution Verification Program (EVP): As part of qualification for inclusion in the set of mainframe products released every May from CA Technologies, CA Mainframe Security Management has passed stringent tests performed through the IVP and EVP to find and resolve interoperability problems prior to release. These programs are an extension of CA Technologies ongoing interoperability certification initiative launched in May 2009.
- Best Practices Guide: This guide provides information on CA Mainframe Security Management installation, initial configuration and deployment to shorten the learning curve for staff that are responsible for the installation and management of this product.
- Health Checker: The Mainframe 2.0 Health Checker provides CA Mainframe Security Management Health Checks that execute under the IBM Health Checker for z/OS.

## CA ACF2™ and CA Top Secret®

CA ACF2 and CA Top Secret provide leading-edge security for the z/OS, z/VM and z/VSE business transaction environments—including z/OS UNIX and Linux for System z. Built-in, comprehensive administrative and reporting tools, along with detailed event logging capabilities, simplify the management of users and their access rights. These solutions give you tools to monitor the effectiveness of your security policies and provide end-to-end security for the enterprise when deployed with other CA Technologies solutions.

| | |
|---|---|
| CA ACF2™ for z/OS<br><br>CA Top Secret® for z/OS | Deliver access control software for z/OS operating systems, which includes interfaces for CICS and IMS. Basic and advanced CA ACF2 and CA Top Secret mechanisms provide flexibility and control to help you monitor and adjust your security policies and accommodate virtually all organizational structures. Administrative tools, extensive reporting options, online monitoring and automatic logging capabilities accompany CA ACF2 for z/OS and CA Top Secret for z/OS, securing your environment while enabling comprehensive auditing and controlled sharing of data and resources. |

| | |
|---|---|
| CA ACF2™ for z/VM<br><br>CA Top Secret® for z/VM | Control access for z/VM operating systems, as well as to VM minidisks, CMS files, terminals, CP commands and diagnose instructions, and other types of user-defined resources—including applications and z/OS data sets. CA ACF2 for VM contributes Standard Security Facility (CAISSF) technology to the CA Integration Services (CIS), allowing centralized security administration and auditing through a single security facility. |
| CA Top Secret® for z/VSE | Establishes security controls for creating and accessing information for batch and online, and can enforce these controls at any desired level. The system can be tailored to fit perfectly in any size enterprise. This comprehensive solution for data and resource security gives you comprehensive control over virtually every resource in your data center by combining ease of use with the flexibility to customize security. |
| CA ACF2™ Option for DB2<br><br>CA Top Secret® Option for DB2 | Help you secure your DB2 resources. With a single-point centralized security strategy, it simplifies the complex process of managing access to critical DB2 resources, privileges and utilities. This access control solution also is designed to provide consistent security and logging, coupled with straightforward auditing and reporting. |
| CA Distributed Security Integration for z/OS | While the LDAP Server provides an interface to security services, it is limited to what the LDAP protocol supports. The CA DSI Server was created to provide the additional following functions while restricting access using native security scoping:<br>▪ CERT2UID - Maps a digital certificate to a user ID using the External Security Manager (ESMs). The digital certificate must reside in the ESM for this function to succeed.<br>▪ DATAPUT - Adds a certificate to the database and connects it to a key ring. If the specified key ring does not exist, an attempt is made to create the key ring.<br>▪ DATAREMOVE - Removes a certificate from a key ring. You can also indicate that the certificate should be removed from the database. For it to be deleted from the database, it cannot be connected to any other key rings.<br>▪ DELETERING - Deletes a key ring.<br>▪ GETPNL - Retrieves the groups associated with a LID. (This is CA ACF2 specific.)<br>▪ GETVER - Gets the product name and version of the ESM that is currently running.<br>▪ MAPUID - Maps a long user name to a short name or a short name to a long name using the ESMs.<br>▪ NEWRING - Creates a new key ring.<br>▪ PASSCHK - Performs user ID and password authentication to the ESM.<br>▪ PURGERING - Removes all certificates from an existing key ring.<br>▪ RESCHK - Performs a resource authorization check to the ESM.<br>▪ XEQCMD - Issues native commands to the ESM using the same native syntax as in TSO or batch. |
| CA LDAP Server for z/OS | This component provides a single interface for applications to request security services, including adding, updating and retrieving information—at no additional cost—to all customers who are current on maintenance of CA ACF2 and CA Top Secret for z/OS. It can be used to securely perform user authentication on behalf of business applications running on z/OS and other platforms connected through TCP/IP. You can leverage the existing information stored in your z/OS security solution and achieve mainframe-strength user authentication for applications throughout the enterprise by connecting to CA ACF2 or CA Top Secret via CA LDAP Server. |

| | |
|---|---|
| CA PAM Client for Linux for System z | Delivers user authentication and resource checking on Linux systems—at no additional cost—to all customers who are current on maintenance of CA ACF2 and CA Top Secret for z/OS. CA PAM Client support allows CA ACF2 for z/OS and CA Top Secret for z/OS to act as an authentication server for one or more Linux systems, eliminating the need for redundant security administration on a system-by-system basis. |
| CA Web Administrator for z/OS | CA ACF2 for z/OS and CA Top Secret for z/OS customers have had limited, text based, options for maintaining their z/OS security information. With the retirement of knowledgeable security administrators, customers are trying to maintain their systems using less experienced and/or non-mainframe personnel. Something is needed to help these new administrators accomplish what is needed in a faster and easier manner than reading the 1,000 page administrator guide and trying to determine the correct command syntax. The Web Administrator will provide a GUI—at no additional cost—to all customers who are current on maintenance of CA ACF2 and CA Top Secret for z/OS to help these new administrators. All administration is done in real time against live CA ACF2 and CA Top Secret. |

## CA Compliance Manager for z/OS

To stay abreast of today's challenges, organizations need to mitigate compliance risks by automating, applying policy controls and auditing in a continuous manner. CA Compliance Manager for z/OS can help your organization reduce the total cost of managing compliance.

| | |
|---|---|
| CA Compliance Manager for z/OS | CA Compliance Manager for z/OS provides your organization with a single source for information and events occurring within the mainframe environment—without the need for skilled mainframe staff and manual processes to extract data needed for compliance reporting and risk mitigation.<br><br>CA Compliance Manager for z/OS helps organizations address the following challenges:<br>▪ Scarce resources in the face of exploding compliance costs.<br>▪ Inability to adapt manual ad-hoc processes as the number of regulations continues to grow.<br>▪ IT staffs are overwhelmed with special requests for compliance-related assurances that require special skills.<br>▪ In-house procedures are inconclusive, time-consuming, error-prone, fragile, and not repeatable.<br>▪ Dire need for proactive tools designed to shorten the risk and threat management timelines.<br>▪ High demands on the time, resources and skills needed to prepare and respond to the increasing numbers of security audits.<br>▪ The need for a cost-effective, automated way to monitor, report, and investigate privileged user behaviors.<br>▪ Inability to provide assurances to auditors and management that effective controls are in place.<br><br>CA Compliance Manager for z/OS includes capabilities such as: change monitoring, event history, event warehousing, intuitive graphical user interface, real-time alerts, policy refinement, forensics and comprehensive reporting. |

## CA Cleanup

CA Cleanup provides easily automated, continuous and unattended security file cleanup by monitoring security system activity to identify security definitions that are currently unused.

CA Cleanup for ACF2™

CA Cleanup for RACF

CA Cleanup for Top Secret®

CA Cleanup solutions identify accounts unused beyond a specified threshold of time and generate commands to remove unused user IDs, entitlements, permissions, and profile and group connections that each user has but does not use. These solutions help effectively resolve the accumulation of obsolete and excessive access rights that otherwise occur within a security file over time, a key requirement for compliance with many regulations.

NOTE: CA does not provide legal advice. No software product referenced herein serves as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, standard, policy, administrative order, executive order, and so on (collectively, "Laws")) referenced herein or any contract obligations with any third parties. You should consult with competent legal counsel regarding any such Laws or contract obligations.

CA Cleanup fully deploys within a day. Using CA Cleanup, you can:

- Identify and remove from individual users, entitlements and access groups no longer used.
- Identify entitlements (such as permissions and rules) actually used and create commands to remove those unused. This includes user-defined resources.
- Identify user IDs actually used and create delete commands for those unused. This is based on actual security usage, not reported "last-use" dates, which are often unreliable.
- Identify the IBM RACF Groups and Profiles that each ID actually uses and create the RACF Commands to remove those that are unused.
- Produce reports detailing both used and unused entitlements.
- Generate commands to enact or restore security cleanup.

When used with CA ACF2, you can identify active versus inactive logon IDs, rule sets and rules. This includes user-defined resource classes and NEXTKEY source and target rules. When used with CA Top Secret, you can identify active versus inactive ACIDS, permissions and profile connections. This includes user-defined resources and the *ALL* record. When used with IBM RACF, you can identify active versus inactive user IDs, profiles, permissions, group connections and IBM RACF resource groups. Permission use is tracked down to each specific access-list entry, whether discrete, generic or conditional.

## CA Auditor for z/OS

CA Auditor for z/OS (formerly eTrust CA-Examine Auditing) is an important tool that helps you manage compliance with the myriad of regulatory requirements that may govern your business and IT systems. Compliance is comprised of many things. It is about process and procedures—accountability for which is important when these govern your business processes. It is about change control and repeatable processes. It is about reporting and auditing. It is all these—and more.

| | |
|---|---|
| CA Auditor for z/OS | CA Auditor for z/OS is an industry leader in automated review and auditing for z/OS operating system integrity and verification. It provides important information about system security, integrity and control mechanisms, which are extremely difficult to obtain from other sources.<br><br>Traditionally, only experienced auditors and security specialists with a systems programming background could perform an extensive operating system review. Much of the work had to be performed manually or with utilities that were difficult to use. Even with the necessary data processing expertise, a z/OS review could take weeks or months to perform. In addition, the problem of what to do once the experts left always existed. In contrast, CA Auditor is a user-friendly solution that enables you to perform a system review—even if you do not have a systems software background.<br><br>CA Auditor helps identify and control security exposures, trap doors, Trojan horses and logic bombs that can destroy production dependability and circumvent existing security mechanisms. All of these exposures can exist in the form of improper or misused operating system code, supervisor calls (SVCs), exits, libraries, functions and facilities. Through the use of proficient system techniques and an English-language interface, information that is otherwise difficult or time-consuming to obtain can be instantly provided. In addition, CA Auditor identifies potential problems, makes suggestions and, with the dialog feature, answers your questions. |

## section 3: benefits

# Reducing IT security risk while improving operational efficiencies and addressing compliance requirements

The CA Mainframe Security Management solution provides a robust and proven solution for protecting your critical IT assets across your entire environment, delivering these important benefits to IT organizations of all sizes:

### Mitigation of security risks

CA Mainframe Security Management is designed to protect your critical IT resources by enabling only properly authorized users to access them, and only in approved ways. It also allows you to manage and analyze security event information to quickly identify and remediate potential security issues, including improper disclosure or use of sensitive corporate or customer information.

### Enhanced regulatory compliance

CA Mainframe Security Management products provide your organization with tools to support compliance with automated and centrally managed capabilities that help reduce costs while strengthening IT security controls. With comprehensive auditing, your compliance challenges become much simpler because you can provide proof of controls and validate to auditors the effective operation of your established security controls. CA Mainframe Security Management products also help

you automate your security compliance processes, so as to better manage compliance with your corporate or regulatory policies and to provide proof of compliance for easier and more efficient audits.

## Reduced administrative expense and improved efficiency

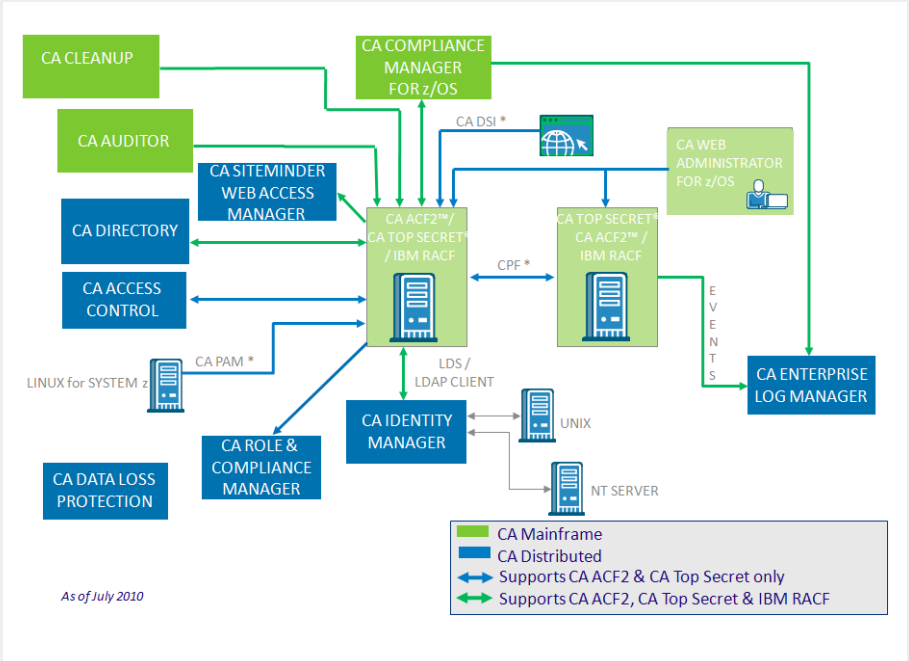
CA Mainframe Security Management products can help automate many of your key IT administrative processes, especially those related to managing user identities and access rights. Along with automated filtering and analysis of security log information, these capabilities can bring significant administrative efficiencies, thereby reducing your overall IT costs. They can also help to improve user and management productivity, since less time has to be spent in manual processes.

## End-to-end integration

CA Mainframe Security Management products provide comprehensive capabilities, and take integration to an unprecedented level, providing your organization with user identity administration, provisioning and access management that operates across virtually all your enterprise platforms. The figure below illustrates the functional areas of CA ACF2 and CA Top Secret and their integration into your IT infrastructure.  Note: modules or components can be purchased and deployed separately.

**Figure 2**
Comprehensive security management—from the mainframe to the web.

Integration points to and from CA ACF2, CA Top Secret and IBM RACF.



## section 4
# The CA Technologies advantage

Mainframe Security products from CA Technologies are integrated components of the comprehensive Security Management solution set that, enables customers to easily manage and protect IT assets across all platforms and environments. By leveraging this end-to-end Security Management solution, organizations can centralize user identity administration, provisioning and access management across the enterprise to improve IT efficiency, reduce IT costs and enhance user productivity. This solution also enables security administrators to view consolidated cross-platform security events for enhanced auditing and compliance and faster response to security risks and incidents.

To optimize the performance, reliability and efficiency of your overall IT environment, you need to tightly integrate the control and management of distinct functions, such as operations, storage, and lifecycle and service management, along with IT security and identity and access management capabilities. CA Mainframe Security helps provide a consistent and secure solution across your entire IT environment, including emerging technologies that you might adopt in the near future.

CA Technologies has been a leader in IT management for over 30 years, has over 1000 security customers, and is committed to continuing to bring innovative security capabilities to them. We have a large and dedicated group of security experts who know how to make security deployments successful, and help our customers achieve very quick time-to-value.

## section 5
# Next steps

If you're finding that:

- You need to strengthen security...
- You are struggling with the costs and effort required for compliance with relevant industry and regulatory requirements...
- Your budgetary pressures are demanding greater efficiencies in your administrative functions...
- You are concerned about potential risks and need to enhance auditing capabilities...

...then take a look at CA Mainframe Security Management solutions. When combined with other CA Technologies solutions, you can achieve end-to-end control to help your organization address business and compliance requirements across the enterprise. Visit us at ca.com/mainframe/security today.


CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and physical to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies' innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com



2842