

Protecting Sensitive Data and Resources Throughout the Organization

CA Security Management

Identity Lifecycle Management

Secure Web Business Enablement

Data & Resource Protection

Security Information and Compliance Management

Data & Resource Protection

CA Access Control

CA DLP (Data Loss Prevention)

CA Data & Resource Protection is a family of solutions that provides a proactive approach to securing sensitive information and critical systems without impacting normal business and IT activities. Data & Resource Protection provides data loss prevention functionality to protect the use of sensitive data across the organization. It also protects privileged access to systems, applications, and files by providing fine-grained access and activity entitlements.

This combined approach toward securing data from the insider threat helps organizations efficiently manage risk, protect sensitive information, and comply with both internal mandates and external regulations.

Overview

The number of data breaches and server resource issues continue to rise, and the resulting costs to affected organizations are significant and well documented. This trend is exacerbated by the current economic climate causing instability, turnover, and layoffs.

Insider errors and misuse are the primary source of these problems.

Companies need a proactive way to control and track privileged access to critical resources while controlling the activities end users can do with sensitive data.

Benefits

CA's solutions provide an efficient way to match an employee's access rights and data use capabilities to their specific job role. With robust controls that do not impede proper IT and business activities, this flexible, centralized approach can help your organization:

- Provide consistent server access security and prevent data loss
- Identify, analyze, and control stored data as well as data at the endpoint, the message server, and data on the network
- Comply with regulatory requirements and data privacy audits
- Report on security status and manage audit logs

The CA Advantage

CA's solutions are both proven and highly scalable. They can provide the right access and usage rights to the right people at the right time, while protecting your critical applications and data. CA offers all of this with the added benefit of detailed tracking and accountability to meet the needs of the auditors and compliance gurus.

CA is the only company that offers this important combination of identity management, server access control, and DLP capabilities.

As part of CA's vision for Enterprise IT Management (EITM), CA can help you unify and simplify your overall IT management.

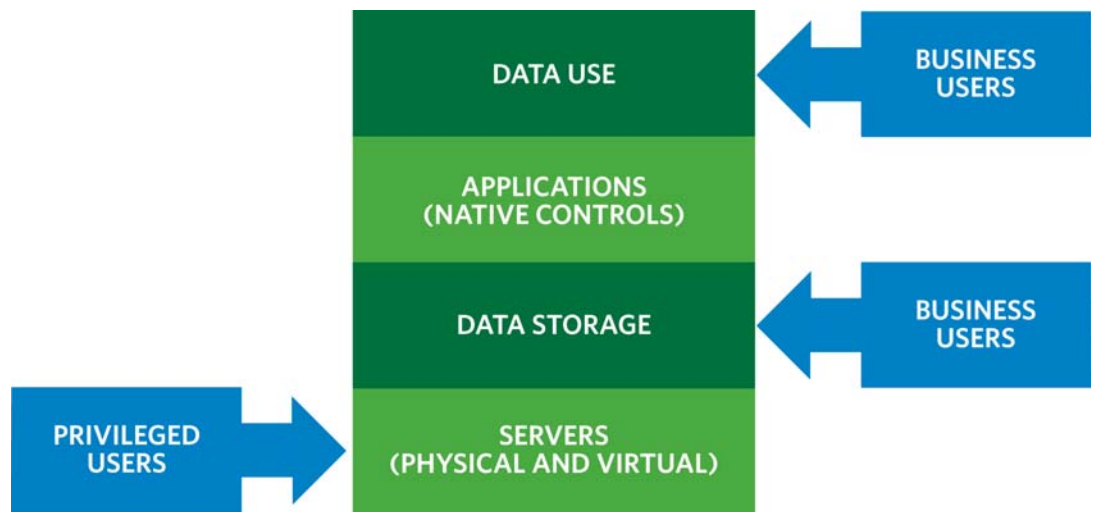
Address Multiple Layers of Data and Resource Security

When planning to secure IT resources and sensitive data, it is important to evaluate the areas of greatest exposure. While many applications have some form of security to control user rights, there are additional layers in the application stack, both above and below the application itself, that present many risks.

FIGURE A

Data needs to be secure for both business and privileged access.

DATA ACCESS LAYERS AND ASSOCIATED USERS



Below the application layer there are servers, both physical and virtual, that run critical application processes and store sensitive data. Because of the aggregated level of risk inherent on these servers, it is important to control who has privileged or administrative access as well as what data is stored on them. Anonymous and shared use of privileged or superuser accounts has led to an increasing number of damaging data loss and security issues in recent years. It is essential to limit the access rights of privileged users on these systems and to ensure accountability via detailed tamper-proof audit logs for all of their activities. It is equally important to know what data resides on these systems and whether or not that data is supposed to be there. To meet these challenges, organizations must reduce risk by eliminating shared accounts, enforcing fine-grained access controls for individual users, discovering where sensitive data resides, and auditing all activity.

While the previous consideration is a highly effective way to reduce the number of people that have access to critical processes and data, it does not provide a way to control what users, privileged or not, can do with that data.

Above the application and server layers there are business users that have access to sensitive data. Once users gain legitimate access to this data, many organizations have little or no control over what they can do with it. Typically, there are thousands of end users within a single enterprise with authorization access to some form of sensitive data as part of their normal job responsibilities. Organizations are now rushing to determine where critical information is used, where it is stored, and how it can be protected from misuse and loss. Most organizations believe that their own employees pose a more serious threat to data security, via either inadvertent or malicious behavior, than do outsiders.

Manual controls and multiple point solutions can help with these challenges, but this approach typically does not scale and is likely to inhibit normal business and IT processes. The best solutions add little to no undue burden on either IT or end users by enforcing server access rights transparently, with no change in the way privileged users access these systems, while scanning for sensitive data and taking corrective actions in real time.

CA's Approach to Data & Resource Protection

CA's solution for protecting server resources and sensitive data includes two products. CA Access Control provides fine-grained server access rights to support business and IT needs while reducing risks from over-privileged and shared accounts. It enforces segregation of duties and provides accountability by generating user based event data. CA DLP helps organizations understand where sensitive data is and how it is being used. It uses policies to control and rectify the inappropriate use of data at rest and data in motion.

Together, these products help companies reduce the risk of data loss while fulfilling audit requirements. With this set of solutions, an organization can:

- Provide the correct entitlements to users that access critical servers
- Find, classify, and enforce appropriate data use policies for sensitive data
- Enforce segregation of duties
- Facilitate secure audit and compliance efforts within an organization
- Use policy and entitlement reports to monitor security status

CA Access Control

CA Access Control secures servers by providing more granular entitlements for administrators and users across platforms than are offered by native operating systems. This ensures regulatory compliance through an unparalleled granularity of policy-based access control and enforcement that includes segregation of duties. CA Access Control helps limit who has access to specific systems and the resources that reside on those systems. It simplifies server access management by providing a single user interface to manage all of your server platforms. Its architecture easily scales to thousands of endpoints. Features include:

FINE-GRAINED CONTROLS Leverage more granular access control than native operating systems. Regulate access to resources, programs, files, and processes.

DYNAMIC POLICY MANAGEMENT AND AUTOMATED DISTRIBUTION Streamline policy deployment and management across the enterprise by allowing administrators to construct logical policy sets and deployment rules.

BROAD PLATFORM COVERAGE Neutralize platform differences and ensure all distributed servers are duly protected. These include Linux, UNIX and Windows platforms.

POLICY-BASED REPORTING Provide views of who has access to what resources across your distributed and virtual server environment.

PROTECTION AGAINST INTERNAL AND EXTERNAL THREATS Leverage capabilities such as stack overflow protection, registry protection, application jailing, and trusted application execution controls to help protect your servers from various forms of malicious activity or mistakes.

IDENTITY AUDIT TRAIL Track the interaction individuals have with protected resources.

CA DLP

CA DLP is a comprehensive and integrated set of products that help organizations manage the risk of uncontrolled information use and prevent data loss. It is a scalable, highly accurate, and cost effective offering that is designed to protect and control data-in-motion on the network and in the messaging system, data-in-use at the endpoint, and data-at-rest on servers and in repositories across the enterprise. CA DLP is a powerful data loss prevention solution that addresses risks on a wide range of control points while leveraging a single infrastructure and platform. Features include:

ACCURATE PRE-BUILT POLICIES Reduce the need to design policies and rules from scratch. Each policy was developed from real business use cases and can be used across a wide range of control points.

DATA CONTROLS AT THE ENDPOINT Analyze user activity at the endpoint as files are copied or moved to removable media such as a USB storage device.

DATA-IN-MOTION PROTECTION Protect the network perimeter by analyzing and taking action on information in email, IM, Web (HTTP), FTP, and many more protocols.

DATA-AT-REST DISCOVERY Gain visibility into data-at-rest and prevent access to, or the inadvertent exposure of sensitive information.

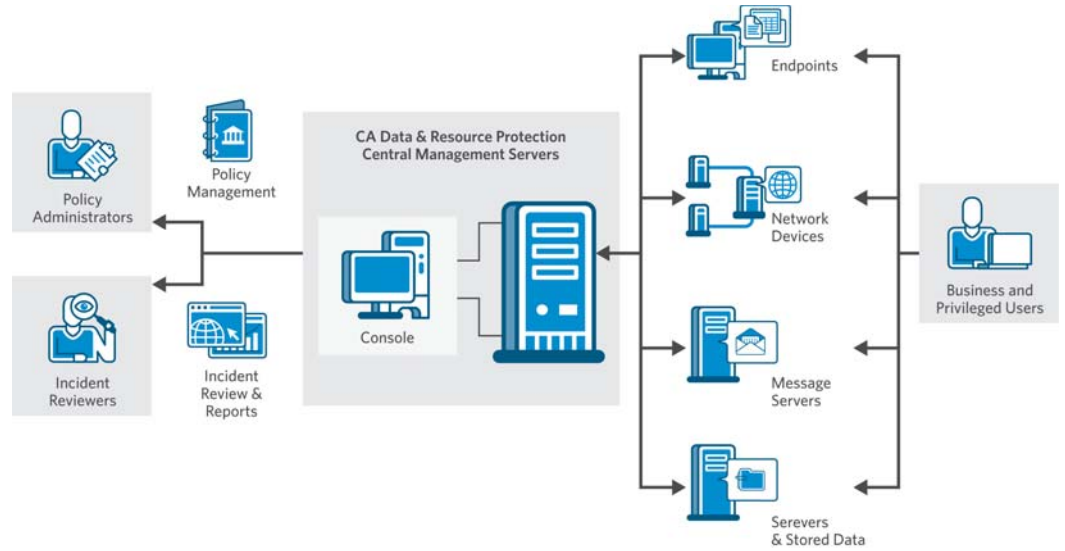
CENTRAL PLATFORM Scale to accommodate the needs of small, medium, and large organizations while protecting and controlling data across the enterprise.

SECURE REVIEW AND REPORTING Use a comprehensive review workflow with event routing, one-click escalation, one-click approval, pre-built response templates, audit trails, and the ability to add free-form comments to incidents with open issues.

FIGURE B

CA Data & Resource Protection Logical Architecture — Business Users utilize the infrastructure and Privileged Users manage the infrastructure.

CA DATA & RESOURCE PROTECTION LOGICAL ARCHITECTURE



CA Security Management Integration

CA Identity Lifecycle Management

Identity-driven data and resource protection enables real-time control over information based on role, user, group, and location. By understanding and tightly controlling who is involved with the activity, the solution can make the most accurate assessment as to the intent of the activity. This approach enables organizations to control information and asset usage without impeding normal business or IT flow. Integrating with identity lifecycle management solutions allows the organization to leverage identity intelligence and become more effective in their data and resource protection strategies.

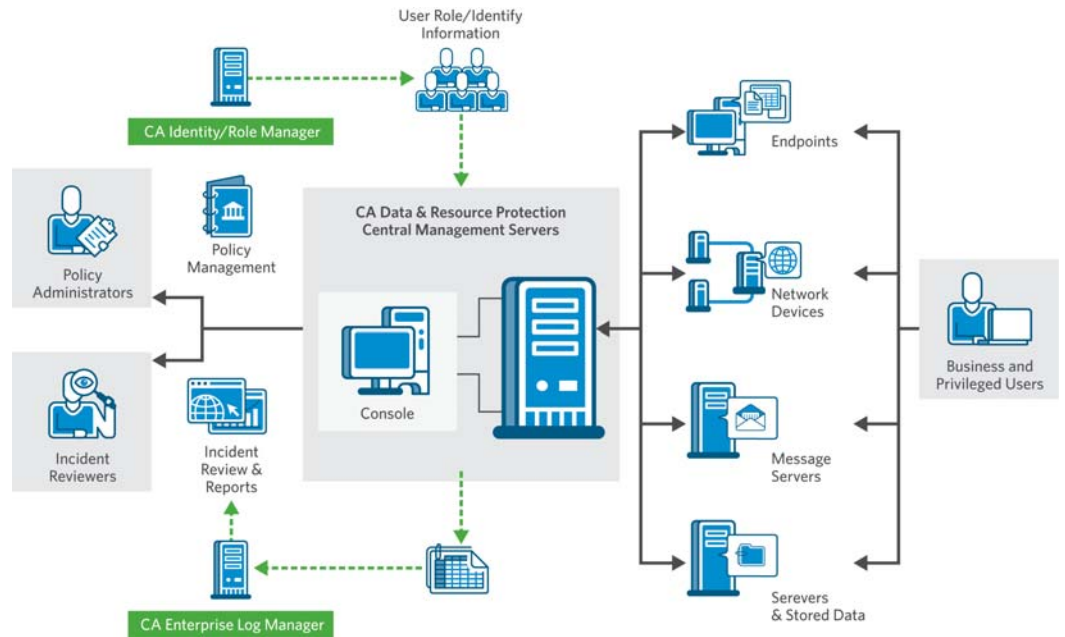
CA Security Information Management

CA Enterprise Log Manager addresses regulatory compliance objectives by centralizing, aggregating, and storing security event data from across the enterprise and facilitating efficient analysis and reporting of that information. It collects data from both CA Access Control and CA DLP, as well as other sources, including operating systems, applications, network devices, security devices, mainframe, identity and access management systems, Web services, and more. By using its federated search and multidimensional log analysis capabilities, IT organizations can quickly investigate user, data, and resource access activities.

FIGURE C

CA Data & Resource Protection Integration.

CA DATA & RESOURCE PROTECTION WITH INTEGRATIONS TO OTHER SOLUTIONS



Conclusion

Consistent, accurate, and effective protection and control of information across the entire enterprise is critical. The CA Data & Resource Protection solutions deliver this protection and control. Organizations using these products can realize many benefits.

- Facilitate user management, reduce down-time and sensitive data loss, and comply with regulatory requirements
- Prevent the intentional or inadvertent misuse of information across the enterprise
- Educate end-users about proper information use
- Ensure compliant behavior for communications and the use of sensitive data
- Accelerate time to value by leveraging proven, highly accurate pre-built policies

The CA Data & Resource Protection solutions empower you to protect data and systems while significantly reducing the administrative costs associated with managing diverse environments. This powerful security layer delivers the platform for the three organizational value propositions listed below.

IMPROVE REGULATORY COMPLIANCE Easily create, deploy, and monitor secure access and data use policies across your environment in support of a variety of data privacy and protection rules including HIPAA, PCI, SOX, GLBA, the EU Data Protection Directive, and J-SOX. Automatically and securely collect and retain auditable records and generate customizable reports to prove the effectiveness of these controls in response to audits and requests from specific regulatory bodies.

MITIGATE RISKS Protect your sensitive information and applications by segregating duties, providing “need to know” access, and defining alerts for specific events thereby minimizing insider and external threats. Reduce the risk of unintended server access or data loss due to inadvertent or malicious activities.

REDUCE COSTS Simplify the management of both server access and data use policies with centralized administration. Reduce the time and resources required to create, deploy and monitor security policies across your environment. Automate the log management process with seamless aggregation of audit data across systems.

To learn more, and see how CA software solutions enable other organizations to unify and simplify IT management for better business results, visit www.ca.com/drp.

CA (NASDAQ: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

MP337770309

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

