

## Business Value with CA

**“By using CA’s mainframe security products, we can more easily ensure that only authorized users have access to critical data and that unused user IDs and access rights are deleted from the system. We can also easily generate reports to demonstrate compliance with a wide range of Federal regulations including FERPA (Family Educational Rights and Privacy Act), the Privacy Act of 1974, Gramm-Leach-Bliley and HIPAA.”**

**Joanne Kelly,**

Sr. Information Security Analyst, Consultant,  
Boston University



# Boston University

Boston University Uses eTrust® CA-Top Secret® Security and eTrust® Cleanup to Achieve Regulatory Compliance

### Customer Profile:

(August 2006)



Boston University  
Boston, MA  
**bu.com**

### Industry:

Education

### Annual Revenue:

1.5 Billion

### Employees:

8000

### CA Products:

- eTrust® CA-Top Secret® Security for z/OS
- eTrust® Cleanup for CA-Top Secret® Security

### CA Advantages:

- Efficiency
- Stability
- Reliability
- Services/Support

## Institution of Higher Education

Boston University — independent, coeducational, and non-sectarian — is an internationally recognized institution of higher education and research located along the banks of the Charles River and adjacent to the historic Back Bay district of Boston. With more than 30,000 students from all 50 states and 135 countries, it is one of the largest independent universities in the United States. For over 150 years, Boston University has anticipated the changing needs of its students while serving the greater needs of society.

## Regulatory Compliance Challenge

Every university is increasingly challenged by today’s hostile data security environment and the need to meet expanding regulatory requirements, even as the free interchange of ideas and scholarly information remains fundamental to its mission. Meeting compliance regulations, such as FERPA (Family Educational Rights and Privacy Act), GLBA (Gramm-Leach-Bliley) and HIPAA (Health Insurance Portability and Accountability Act), in a timely manner is critical for all such organizations, and this is what Boston University is facing today. Boston University needs to ensure that it is not only meeting these regulations, but protecting the integrity of its data and minimizing disruption to its IT flow. Hence, the right tools are needed to administer security from a central location and to ensure that internal procedures and policies are in place to maintain compliance efficiently and effectively.

## The CA Solution

Boston University has been using eTrust® CA-Top Secret® Security (eTrust CA-Top Secret) for over 20 years. “It’s easy to manage and administer, is very dependable, support has been top notch,” says Joanne Kelly, Sr. Information Security Analyst at Boston University. By using eTrust CA-Top Secret, Boston University is able to secure its data center with ease. eTrust CA-Top Secret fully protects the institution’s information assets and helps monitor the effectiveness of its data, assets and security policies. eTrust CA-Top Secret will also help the university with cross platform security, which is another initiative currently being worked on.

### Key Benefits:

- Provides security and integrity of systems and information
- Maintains individual accountability
- Offers flexible structure to match their organization
- Designed for ease-of-use and effective administration
- Provides unparalleled auditing, reporting and monitoring

### Key eTrust CA-Top Secret Security Features:

- Comprehensive security
- Inclusive user management
- Data and resource management
- Auditing and monitoring
- Separation of administrative functions
- Administration diversity

### Key eTrust Cleanup Features:

- Identifies unused logon ids and accesses
- Reports on activity at any time
- Generates commands for removal
- Creates recovery file for deleted logon ids and accesses
- Identifies active rules versus inactive rules allowing you to combine accesses
- Supports multiple security databases in synchronized environments

### Key Business Processes:

- Protecting data and assets
- Meeting Compliance Regulations
- Administer security from a central location
- Minimal disruption to IT flow

### IT Environment

- z890 250 with z/OS 1.4
- z/VM 5.1
- z/Linux SuSE 9.2
- Two production LPARs, two test LPARs and one z/VM LPAR running on an IFL hosting 7 Linux Guests

Boston University is also using eTrust® Cleanup for CA-Top Secret® (eTrust Cleanup). eTrust Cleanup provides an immediate and substantial response to help with obsolete, unused, redundant and excessive access rights, thereby improving security control, risk compliance, ease-of-audit and performance. eTrust Cleanup also provides the ability to restore users and access rights that were unintentionally removed.

eTrust Cleanup helps mitigate Boston University's risk by tracking, reporting on and eliminating obsolete or inappropriate mainframe users and access rights. "eTrust Cleanup works like a shadow, we do not even know that it's running. It's great for our compliance requirements, and it takes minutes vs. the hours it used to take to clean up security files," says Joanne Kelly. With eTrust CA-Top Secret and eTrust Cleanup, Boston University has complete control over every resource in the data center from one central location, helping it to meet compliance issues and feel safer about its systems.

## Meeting Federal Regulations

By using eTrust CA-Top Secret Security and eTrust Cleanup, Boston University can more easily:

- Ensure that only authorized users have access to critical data
- Ensure that unused user IDs and access rights are deleted from the system
- Generate reports needed to demonstrate compliance with a wide range of federal regulations

eTrust CA-Top Secret is essential to setting up role-based security. eTrust CA-Top Secret allows Boston University to set up file permissions that are more intuitive to its mainframe users and that can be administered from a central location. "Once you have the mainframe architecture, once you put the permissions in place, they're there, and they're working," Joanne said. eTrust Cleanup is also used on the system, and Joanne indicated that it doesn't use up much CPU, but rather just "sits back" and monitors the security system. eTrust Cleanup helps Boston University with regulatory compliance issues, since "I can easily go back and determine which user accessed what file."

## Providing Tangible Business Value

eTrust CA-Top Secret Security and eTrust Cleanup provide:

- Strong automated internal controls that simplify the management of users and their access rights for the z/OS environment
- Comprehensive reporting and auditing capabilities required to maintain compliance with regulations such as HIPAA, FERPA, GLBA, etc.
- Protection of mainframe data sets from unauthorized access
- Automatic identification and removal of obsolete, unused and rogue user IDs and access rights
- Risk mitigation
  - Ensure you know who has access to what
  - Ensure privacy of confidential user data
  - Audit all user access, so as to report alterations to data and database objects

CA's mainframe security solutions help ensure the integrity and security of critical business assets which reside on the mainframe, enabling customers to reduce risk and demonstrate compliance with regulations while streamlining core user administration tasks. Also, the CA Mainframe Security Support and Development teams truly show CA's commitment to the mainframe and service. In regard to Return on Investment (ROI), Joanne states, "The products have paid back their cost many times over."

[For more information, visit ca.com.](http://ca.com)

