

Is Your Legacy Access Control Software Working **For** You Or **Against** You?



Take a moment to test your assumptions and evaluate your risk.

Is the recruitment and training of highly-skilled security personnel an issue for you?

Problem: Legacy products require high levels of technical expertise to install, maintain and administer. People with the necessary skills are difficult to find. Many industry observers expect this situation to worsen in the future as people with mainframe skills leave the workforce. This may force some companies into the difficult position of having to choose between outsourcing their security administration or else living with the risk of unintended security exposures.

Solution: Deadbolt solves this problem by making it possible for existing administrators to be much more productive, while at the same time reducing the level of technical skills needed by new security personnel. This is possible because Deadbolt security administration is from a website, making it familiar to anyone who has used a PC to access the Internet. Not only is Deadbolt's website dramatically easier to use than the legacy product's interfaces, it is backed up by wizards, analysis functions, and integrated help facilities.

Would you be interested in reducing the cost of security?

Problem: Maintenance costs seem to increase without tangible benefit. Sometimes things which should have been part of the base product, e.g. DB2 support, wound up being marketed as separate or even third-party products. Cleanup and reorganization utilities, reporting facilities, even decent user interfaces, have become extra charge items for the legacy products.

Solution: Deadbolt directly reduces product costs through much better licensing arrangements and integration of all necessary security related functionality. No third party add-ons are required for Deadbolt, reducing the cost and complexity of installation security.

Are you satisfied with the capabilities of your security product?

Problem: Legacy products can be expensive to own and operate. Their architecture, based on dated proprietary technology, does not allow easy assessment of system overhead. They require significant levels of technical expertise to install and maintain. Their rigid architecture does not provide sufficient flexibility for many installations, requiring installations to resort to exits and local modifications to achieve the security protection

they need. Unfortunately, these exits may have been developed decades ago and the expertise to understand, maintain and extend these assembly language exits is quickly disappearing from the workforce.

Solution: Deadbolt uses a modern product architecture that supports industry standard interfaces and data formats. It uses a high performance caching structure and improved algorithms for access determination. Its DB2 relational database provides flexible, secure, and highly scalable storage for security information. Deadbolt installs with minimal impact, does not require exits, and allows major implementation changes without requiring a system IPL.

Are you concerned about the possibility of mistakes in security administration?

Problem: The risk of security exposures in mainframe systems has increased in today's highly interconnected environment. Legacy systems are too complicated for today's less technical security people to administer, increasing the chances of costly errors. Worse yet, decades of use may have turned the security permissions into a jumbled mess that few understand, resulting in a loss of control over the installation's data.

Solution: Deadbolt reduces the risk of costly errors through drop-down lists, selection boxes, radio-buttons, wizards, AJAX technology, and a number of facilities designed to "mistake proof" security administration. Deadbolt reduces the technical level required for effective security administration and makes existing personnel more productive. Deadbolt's web interface administration is dramatically easier to use than the competition's cryptic TSO-based "green screen" and line mode interfaces. Built-in autonomic functions will soon be available to analyze the security environment and offer suggestions for improving it.

Have you wanted to change security vendors but found the expense, time needed and risk involved in doing it was unacceptable?

Problem: Your legacy vendor relationship might be poor, but the cost of conversion is sky-high, will take months, maybe even years to complete, will require extensive retraining and then may not work in the end. All this presents an unacceptable level of risk for a marginal amount of reward, given that a change in legacy vendors provides little (if any) new functionality.

Solution: As a vendor, JME brings new passion, excellence, and world class expertise to security. As a product, Deadbolt provides breakthrough new facilities to make conversion fast, simple, cheap and above all, safe. And once converted, Deadbolt applies state-of-the-art technology to provide important new functionality designed to improve an organization's security capabilities.

If you need to consolidate security implementations (e.g., due to mergers, acquisitions, or data center consolidations), would you be interested in tools to help reduce time, cost, and most importantly, risk of error?

Problem: Mergers and acquisitions are a fact of modern corporate life. A company may find itself with multiple security systems as well as the third-party add-ons required to make these products usable. Aside from the ongoing maintenance expense, there are personnel training costs, corporate culture conflicts, coordination issues, and a level of complexity that gets in the way of effective security administration.

Solution: Deadbolt has the unique ability to protect an organization's investment in people and training. It's capable of supporting multiple legacy security perspectives, and doing so simultaneously. As a next generation product, Deadbolt includes the functionality missing from the legacy products, so expensive add-ons are unnecessary. Deadbolt's unique "poly" feature allows it to be added along side a legacy system and run in parallel until conversion has been completed, all but eliminating the risk of consolidation.

Could you use assistance from your security product in meeting your regulatory requirements, such as HIPAA, SOX, ISO 17799, etc?

Problem: The burden of regulatory compliance is growing at both state and national levels, as well as internationally. Sarbanes-Oxley (SOX) requires management to devise and certify a system of internal controls for financial reporting. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) adds stringent disclosure and access tracking requirements for medical data. GLBA mandates banking record confidentiality and integrity. ISO 17799 provides a set of security standards and requirements. Legacy products provide little or no help in meeting these regulatory demands. Huge fines and even jail sentences make compliance absolutely mandatory.

Solution: Deadbolt has a number of features designed to help installations achieve regulatory compliance. It provides built-in access permission documentation and integral ownership designation. It also provides an installation the ability to assign security and reporting categories to Protected Health Information (PHI), Personally Identifiable Information (PII), and other critical data. Deadbolt maintains comprehensive statistics and audit trails for the access and usage of resources under its protection. It also generates email and SMS alerts to data owners and security personnel for events involving critical resources.

Should emergency access procedures be an integral part of a security product?

Problem: In the real world, emergency access must occasionally be granted in order to deal with unexpected operational problems. Regulatory requirements recognize this, but dictate that emergency access must be authorized, controlled, and restricted to only what is necessary for problem remediation. Legacy products require third-party add-ons to achieve this capability and may still not meet all necessary documentation and reporting requirements.

Solution: Deadbolt provides an integrated “Passkey” facility, which allows emergency access to take place in a controlled fashion with full accountability. Approval for emergency access can be pre-defined and documented, before a crisis occurs. Subsequent activation of Passkey privileges will automatically generate a security event, triggering appropriate notification of security personnel.

Would you be willing to evaluate a security product if it provided help in “cleaning up” your existing security environment?

Problem: Vulnerability to unrecognized security exposures is a constant threat in some installations. Years of patches, maintenance and turn-over of personnel may make it extremely difficult to know exactly who can access which resources. This is particularly true when exits and local modifications have been made to the security software. Even when the “what” for specific security permissions can be unambiguously determined, the “why” has probably long since been lost. Add-on products address some of these deficiencies but introduce problems of their own, including increased cost, complexity, maintenance and support.

Solution: Deadbolt can be added to an existing system without disturbing the legacy security product. Automated conversion routines map the legacy product’s security files into Deadbolt’s relational database where they can be analyzed and documented. Deadbolt’s autonomic analysis functions are also designed to identify obsolete user IDs, access permissions, and perform a number of “clean up” functions. Deadbolt can also discover hidden implicit security policies. Running in “poly” mode, Deadbolt observes the legacy security system’s behavior and reports any differences from what it would do based on the explicit security permissions. This allows assessment of the impact of exits and local modifications in the legacy product.

Would online tools for monitoring security permissions be useful in your installation?

Problem: Auditors are quick to recognize the business risk from inappropriate and/or obsolete security permissions. Installations must monitor security policies on an ongoing basis to remain protected and prevent surprises at audit time. Legacy security products don't provide tools to track security permission usage and effectiveness. Third party "add-on" products are necessary to add these features, resulting in increased complexity and expense.

Solution: Deadbolt automatically tracks which Access Control Entries (ACEs) are being used to determine access, so unused ACEs can be highlighted and eliminated, and if the access is being journaled, which specific ACE provided the access permission. To further aid in achieving effective protection and reduce the likelihood of audit issues, autonomic analysis functions will be made available in Deadbolt to assess the adequacy and appropriateness of current security permissions.

Is minimizing the possibility of adverse impact from changes in your security product's software important to you?

Problem: z/OS system security and availability may be impacted by the implementation of untested changes to the legacy security system software. These products lack a mechanism for testing changes prior to placing them into production. This presents an unacceptable risk from "mission critical" system software that can literally put down a data center.

Solution: Using its unique "poly" feature, a second copy of Deadbolt can be brought up and run alongside the production Deadbolt for testing new code or large changes to the security database. As when running poly Deadbolt to monitor legacy systems, a test version of Deadbolt could monitor the production version and report any differences in security permissions. Once it is validated, the test version can be promoted to production without any requirement to IPL. Deadbolt lowers the risk of software change and maintenance by its ability to allow the verification of product changes prior to placing them into production.

Would you be interested in reducing the risk of unintended consequences from changes in security permissions?

Problem: Untested security permission changes may result in security breaches or denial of access to legitimate users, both raising the possibility of major business impact. Although certain legacy products do have a simulation-style "test command", it's very limited in functionality and doesn't allow proposed security changes to be fully evaluated in a production environment prior to implementation.

Solution: Deadbolt provides unique testing facilities for security permission changes. Although it provides a robust simulation environment for asking "what if" questions, Deadbolt also allows proposed changes to Access Control lists (ACLs) to be safely evaluated against the real production environment. This is done with automatic monitoring and reporting of any differences in access that the proposed ACL would introduce. This allows validation of access permission changes before they are implemented. No similar capability exists in the legacy products.

Can your security be improved through better follow-up of incidents?

Problem: Inadequate legacy tools make follow-up difficult. Security breaches and incidents may "fall through the cracks" and not receive adequate investigation and remediation. Special powers given for emergency access (Firecall support) may not receive adequate documentation, approval or review. Security department service requests may be difficult to plan, report and schedule, resulting in inefficient usage of department personnel and resources.

Solution: In addition to real-time alerts through email and SMS messages, Deadbolt integrates an incident reporting and tracking system into its administration website. The website assigns incident numbers, provides problem escalation, and allows security personnel to document findings. Deadbolt documents the activation of emergency access usage (Passkey feature) and provides online ad-hoc analysis of security information from its relational database.

Should a security product provide built-in documentation, analysis and tracking of its security permissions?

Problem: Poorly documented legacy system access permissions may result in inappropriate access being granted to users and a negative potential business impact. Regulatory compliance cannot be achieved without adequate documentation.

Solution: Deadbolt provides a built-in facility for documentation of everything under its control, including all the security permissions specified for resources. Deadbolt allows free-form text descriptions to be associated with users and resources, as well as incidents and events. Integrated documentation is the key to being able to understand the rationale for security decisions over the passage of time. It provides continuity to the security department as personnel change and provides documentation of intent and purpose for regulatory compliance.

Does your company have international security requirements?

Problem: Today's corporations operate around the world in a 24/7 environment. Different markets may have different languages and traditions for displaying data, such as the European style for specifying dates versus the one used in the States. Unfortunately, the legacy security products were originally designed for usage in English-speaking North America. As a result, adapting them to function in a global economy has been difficult to say the least, creating no end of problems for international users.

Solution: Deadbolt was designed from the beginning to be a global product, providing multiple ways of displaying dates, numbers and other locally sensitive information. Its internal architecture not only supports other languages, but other alphabets and character sets as well. For example, Deadbolts web interface administration can display English words and Chinese characters simultaneously, a major advantage for international companies operating in multiple markets.

Would online, real-time security analysis and reporting improve your organization's security posture?

Problem: Legacy products lack the flexibility to report even the limited information they have about users and resources in ways that support dynamic security analysis techniques. Furthermore, security event data is only journalled to the System Management Facility (SMF). Reports are restricted to rigid "canned" formats or difficult to master report writers that hamper an organization's ability to respond to emerging threats and problems in a timely manner.

Solution: Deadbolt uses a relational database for storing both security permissions and security events. The power and flexibility inherent in a relational database allow the storage and analysis of far more data than the proprietary file structures of the legacy products. Deadbolt's web interface administration allows online user-customizable report layouts, multiple sort sequences, selection filters, even built-in graphics support for problem analysis, all in real time. But because it is also important to archive data for historical use, Deadbolt also provides full SMF journaling.

Are you satisfied with the performance and usability of your security system in multi-system environments?

Problem: Legacy products utilizing proprietary synchronization schemes for multiple security systems are limited in scope and may have performance and consistency issues. They may also require licensing multiple copies of the security software for effective use in a Sysplex and don't integrate well with the enterprise.

Solution: Deadbolt employs a security kernel, backed up by a high performance cache system for each LPAR to be controlled. Most access decisions can be made without reference to its security database, which is implemented using a DB2 relational database on z/OS platforms. DB2 utilizes the z/OS System Coupling Facility to maximize performance in Sysplex environments, allowing the sharing of a single security database. Deadbolt utilizes open source and industry standard interfaces to allow its planned extension to the enterprise.

Would you like to reduce the costs of security help desk services?

Problem: Routine security help desk activities, such as resetting forgotten passwords, changing phone numbers, etc., can add up to significant expenditures of time and money. Worse yet, this kind of activity diverts security personnel from their primary mission of protecting the installation. Legacy products do not address this area, leaving users to seek third-party solutions, (where and if available).

Solution: Deadbolt's administrative website architecture provides for easy and secure self-service of routine functions such as resetting forgotten passwords. A sophisticated challenge-response system will be used to identify authorized users and reset their password using their web browser, freeing up security personnel for more productive use.

Would you be willing to consider a new security product if it encompassed both mainframe and distributed systems?

Problem: Legacy systems cannot be extended into the enterprise. Their proprietary architectures prevent migration to other platforms, locking them into the mainframe and preventing enterprise-wide consolidation and control of security.

Solution: Deadbolt was architected from the beginning to support the multi-platform enterprise. It was coded in a portable programming language and uses a relational database instead of mainframe specific file structures, to allow porting to other platforms and systems. Deadbolt uses DB2 for its z/OS implementation because of its stability, high-performance and EAL 4 certification. Since DB2 UDB is available on other platforms, Deadbolt will easily integrate with the enterprise, setting the stage for a consolidated approach to security.

Would you be interested in mainframe-style security for the enterprise?

Problem: In spite of all their other positive attributes, many installations find UNIX and Linux do not provide sufficient granularity and flexibility for effective access control of multiple applications shared between multiple groups and users. Nor do these systems provide adequate security administration facilities for managing multiple systems across the network, forcing users to administer security on a one-at-a-time basis.

Solution: The planned enterprise version of Deadbolt will provide mainframe-style access control flexibility for user authentication and resource control on these systems. Deadbolt's administration websites will provide consolidated administration and reporting of security for these distributed systems. For the first time, security will have a common look and feel for both mainframe and distributed systems, providing installations with better security with significantly lower costs of administration.

