

DEADBOLT™ Explorer

Cross-platform security-definition reporting and analysis

DEADBOLT Explorer gives you intuitive, web-browser access to the security information associated with users and groups of users, in concert with the resources they can access. This security insight may span all Windows, UNIX, and z/OS nodes in the enterprise. *DEADBOLT Explorer* scans the nodes in your network, discovering the security attributes for resources and how individuals, user IDs, and groups have access to those resources. Sources of information for *DEADBOLT Explorer* include basic system security information, file systems, databases, directories, sudo, and additional third-party applications that have internally defined user IDs, groups, resources, and sharing.

Why DEADBOLT Explorer?

- Do your security auditors, compliance officers, and helpdesk personnel know who has access to your data, what type of access they have, and what facility grants them that access?
- When employees leave, is deprovisioning their user IDs from systems AND applications well understood?
- Do you have a central repository which combines security information from your decentralized Windows, UNIX, and z/OS systems, as well as directories, databases, and other third-party applications?

More DEADBOLT Explorer highlights

- Display a consolidated view of resources and the owners of the resource from across your enterprise.
- Import existing knowledge bases that contain individuals, user IDs, groups, and resources.
- Find enterprise-wide conflicts in user ID and group definitions and perform remediation on demand.
- Access Explorer from anywhere using a web browser, and create custom reports using built-in wizards.

Combine security information across the enterprise

DEADBOLT Explorer is unique in that it combines security information from the standard security products on Windows, UNIX, and z/OS systems into one central repository. Explorer can also combine information stored in LDAP-accessible directories (like Active Directory), databases (users, grant/revoke, and so on) and other third-party applications (including sudo, cvs, svn, apache, web applications, PeopleSoft SAP, and many more) into its repository.

Tie individuals to user IDs, groups, and resources

DEADBOLT Explorer matches real people by name to the user IDs assigned to them, as well as to their group memberships. The scan phase matches a user ID to an individual, assigns a confidence level to the assignment, and enables you to accept or modify the inferences Explorer has drawn—including resource ownership and the departments inside your organization that are most likely responsible for those resources (such as sysadmin, DBAs, HR, and others). User IDs not associated with a person are easy to find as well, thus aiding in provisioning and deprovisioning of user IDs. Explorer also gives you a view into resources and how an individual, a specific user ID, or a group of users gets to a resource and the type of access they have to those resources; a must for your compliance officers!

Import existing data

You may already have some of the information *DEADBOLT Explorer* collects stored in your own data repository. Explorer can import existing data, making it easier to match user IDs, groups, and departments with individuals. Explorer's ability to import your existing repositories accelerates the initial acceptance phase.

Find conflicts and optionally perform remediation

DEADBOLT Explorer identifies conflicts such as one user ID that is being used by two different individuals on two different systems, UNIX UIDs that are not consistent across the enterprise, and groups defined with too much authority. At your request, Explorer can also resolve the conflicts that it finds.

Build custom and ad-hoc reports

With *DEADBOLT Explorer*, you can create reports without learning a programming language or involving your IT department. Built-in wizards make it easy to create both standard and one-time reports. You can save definitions and run reports on demand or on a schedule that you define. Output can be viewed online, printed, exported to a spreadsheet or PDF file, or e-mailed to addresses that you specify.

About JME Software

JME Software is delivering a new generation of tools and applications for managing, monitoring, securing, and automating 21st-century heterogeneous IT infrastructure. JME solutions are designed to simplify the management of systems, networks, and applications across the entire enterprise. All JME products are built on a common Web 2.0 development framework, provide a consistent browser-based user interface and integrate with a full suite of ITIL-compliant applications. With SOX and regulatory compliance central to enterprise IT, all JME products deliver specific support for IT compliance and governance initiatives.

