Reference Code: TA001481SEC
Publication Date: September 2008
Author: Alan Rodger

Butler Group
a Datamonitor Company

TECHNOLOGY AUDIT

Identity Management

IBM

BUTLER GROUP VIEW

ABSTRACT

IBM offers a range of products that address a very broad scope of requirements in the Identity and Access Management (I&AM) space, and positions these within its overall approach to security and service management, and on a platform of standards that pervades end-to-end. A number of differentiating, beneficial features are included, such as 'what-if' modelling (that simulates the effect of policy changes before they are enacted) reporting errors, or potential problems, and enabling these to be resolved before they affect live operations. Mainframe users benefit from a number of new products, extensions, and product integrations. Single Sign-On for enterprise users is provided by the recently-acquired Encentuate solution, and its integrations with other Identity Management products are newly released. Overall, IBM Identity Management constitutes an extremely high-quality basis for solutions to all enterprise I&AM needs that Butler Group can envisage, and can be deployed individually for point requirements or benefits.

KEY FINDINGS

- ✓ Breadth and depth across products that address a wide range of requirements.
- ✓ Excellent administration, reporting, and compliance features.
- ✓ Mainframe users' needs are addressed with integrated products.
- ✓ Policy simulation and 'what-if' modelling of changes aid management efficiency.
- ✓ Support for a wide range of standards across all products.
- ✗ Some further integration needed with newly-acquired Encentuate product (although much is already complete).

Key: ✓ Product Strength ✗ Product Weakness ⓘ Point of Information

LOOK AHEAD

Plans include enhanced identity governance through role modelling, role business design, and sign-off, and also enhanced management of highly privileged users. Strategic enhancements will aim towards the IBM vision of integrating identity management with service management functions such as incident management, as well as within the Tivoli security integration initiative.

FUNCTIONALITY

IBM's Identity Management capabilities are part of a wider group of software and services solutions – the IBM Security Framework, itself an element of IBM's Service Management Platform (which addresses the needs for visibility, control, and automation across enterprise IT platforms, including mainframes, and enables a lifecycle-oriented approach to these requirements). The IBM Security Framework addresses security governance, risk management, and compliance across the realms of people and identity; data and information; application and process; networks, servers, and endpoint devices; and physical infrastructure. Within this overall scope, Identity Management addresses requirements relating to people and identity, as well as application and process.

Product Analysis

IBM has a range of products that provide customers with a full range of capabilities to cater for identity and access management (I&AM) requirements, as follows:

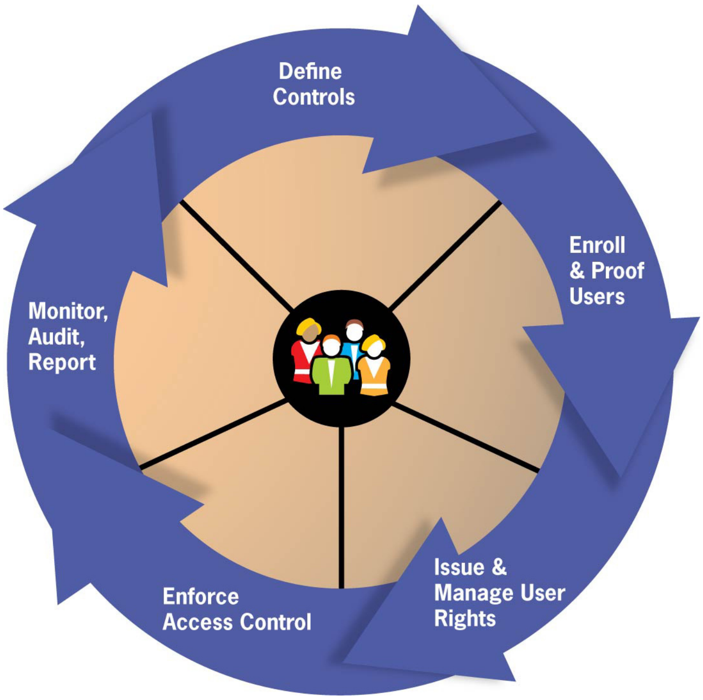
- IBM Tivoli Directory Server (TDS) is a scalable, standards-based identity data platform that interoperates with a broad range of operating systems and applications.
- IBM Tivoli Directory Integrator (TDI) can serve as a metadirectory, or data integration tool, synchronising or transforming identity information and other security information in real time across any relevant organisational sources.
- IBM Tivoli Identity Manager (TIM) provides identity management and provisioning relating to many types of logical assets (e.g. some databases and applications), network infrastructure (e.g. Cisco ACS), and access control systems (including those that are card-operated for building access). In all, it enables integration with a broad range of heterogeneous systems across multiple types of platform. A specialised edition for the Small to Medium-sized Business (SMB) market, IBM Tivoli Identity Manager Express (TIM Express), is also available – this provides identity management and user provisioning capabilities, optimised for rapid deployment and simplicity of use.
- IBM Tivoli Access Manager (TAM) for e-business (TAMeb) is a versatile solution for handling authentication and authorisation problems, which is primarily focused on Web-based applications, and can be implemented in varying forms from simple Web Single Sign-On (SSO) to more complex security infrastructure deployments.
- Encentuate, a solution acquired by IBM in 2008 which will be incorporated in, and integrated with, other elements of the TAM product family, and released as TAM for Enterprise SSO. Encentuate provides SSO for applications within the enterprise (normally termed Enterprise SSO), built-in integration with numerous strong authentication form factors and many common applications (as well as extensibility to further applications via a development toolkit), and session management for shared desktops.
- IBM Tivoli Federated Identity Manager (TFIM) provides the necessary framework to support standards-based, federated identity interactions between partners, with capabilities in the areas of Web (SSO), Web services security management, and federated provisioning.

- Tivoli zSecure, a product platform (gained from the acquisition by IBM of Consul) that delivers audit and administrative capabilities for mainframe security, including management of user credentials, and access rights (which it also enforces). It is also a foundation of IBM's Enterprise Security Hub mainframe solution, and integrates with mainframe security schemes such as Resource Access Control Facility (RACF), as well as with the mainframe editions of other IBM security products such as TIM and TFIM.

IBM's Identity Management solution is intended to support a process-based approach to I&AM (see Figure 1), and a 'trusted system of record', in that it can act as a single point in the enterprise where access privileges are defined, and enforced as policies throughout the target systems and assets. Unauthorised access to information resources can be prevented, and a single audit trail is provided for regulatory and audit compliance.

A notable feature is the breadth and depth of support for heterogeneous managed systems. IBM offers a wide variety of connectors for operating systems, directories, databases, applications, networks, and other infrastructure components. Pre-built adapters are provided, all of which support rich provisioning and compliance checking capabilities, and can be run either locally or 'agentlessly', within secure communication frameworks. Custom adapters can be built using TDI's graphical workbench.

Figure 1: A Process-based Approach to Identity and Access Management



Source: IBM

DATAMONITOR

Product Operation

TDS v6.2 is built on the DB2 database engine, in order to deliver high performance. IBM states that TDS is one of the first Open Group LDAP v3 certified directories, and that its development adheres very strictly to industry standards in order to maximise application support. It supports a number of features that increase administrator usability – for example, search results can be sorted and viewed as “pages”, and groups can be nested or dynamic (i.e. changes in a defined variable can automatically update the group profile). Its identity management features include role support, fine-grained access control, and entry ownership.

TDI v6.1 is for organisations that require integration of identity data from various repositories throughout the organisation (sometimes achieved by a metadirectory, in the I&AM market), and incorporates virtual directory capabilities. IBM states that TDI can implement very large, complex integrations, supporting hundreds of simultaneous synchronisations with enterprise-strength fault tolerance. The product has a development environment in which a drag-and-drop GUI allows customer definition of integration requirements.

Extensively enhanced to v5.0, TIM provides a wide range of identity management features, including:

- Web-based self-service interfaces, with customisable look and feel, for end users (e.g. password reset and synchronisation) which have been extended to include request and approval for users’ membership of roles, and also provisioning needs.
- A role-based administration model for delegation of administrative privileges.
- A workflow engine for automated submission and approval of user requests.
- A provisioning engine to automate the implementation of administrative requests.
- Policy simulation, allowing modelling of security policy changes including ‘what-if’ scenarios, and reporting of issues such as conflicting roles so that these can be resolved.
- Business-friendly revalidation (sometimes termed attestation) of granular user access rights.
- Administration management features such as streamlined notification, bulk to-do items management, and task ownership and delegation.
- Broad out-of-the-box integration support for disparate applications and systems, and universal connectors for extending the management model to new and custom environments.
- Pre-defined reports on security policy, access rights, and audit events.

TIM is a J2EE application that provides an extensive range of Application Programming Interfaces (APIs) to provide extensibility, and uses IBM standard middleware as a basis for scalability, performance, and reliability. TDI (in addition to other pre-built agents) is used as the basis for adapters and connectors that manage user accounts on the systems managed by TIM: all adapters (with only one or two exceptions; e.g. RACF) operate ‘agentlessly’ (i.e. without remote management) or locally, and all communication across platforms is secured via Secure Sockets Layer (SSL). Policies are highly configurable, using advanced logic functionality within TIM based on JavaScript, and along with configuration can be made subject to version control, even via an external tool if required. Drag-and-drop workflow definition within TIM allows integration with other applications and workflow technology.

TIM Express provides similar capabilities to its enterprise-focused counterpart in the areas of password self-service; workflow-based provisioning requests and approvals; workflow-based revalidation of account access rights; and pre-defined reports. Since this product is targeted at the SMB market, IBM made a conscious decision to trade off some policy and configuration options in favour of a quick time to deployment. All TIM adapters will work with TIM Express.

TAMeb v6.1 centrally manages security and audit policy for enforcement points that can be placed as a proxy in front of Web applications, or through authorisation and authentication plug-ins direct into a Web server or application server environment. It can be used to control wired and wireless access based on identity, to applications and data. For authorised users, the product integrates with Web applications and servers to provide seamless access to applications and data across the extended enterprise, and to transactions with partners, customers, suppliers, and employees.

The user’s browser-based request for a resource is dealt with by a resource manager component of TAMeb called WebSEAL, which is resident on the Web server and responsible for applying security policy to resources. The policy enforcer component directs the request to the authorisation service for evaluation, and based on the result allows or denies access to the protected resources. Access Manager authorisation decisions are transferred using the TAM Credential, which contains a user ID, its group memberships, and selected user attributes.

The product provides facilities to allow custom authentication mechanisms to be added beyond those that it already supports. Authentication assertions can be communicated over HTTP, which makes it easier for organisations to integrate with external authentication services. A limited-use licence for TDI is included with TAMeb, providing options such as ‘directory chaining’ for user authentication. A session management facility enables user sessions to be tracked across enforcement points. This provides administrative benefits such as a single point from which to report on and manage user sessions, and the easier enablement of policy enforcement, which traverses any multiple routes that the user might have taken to access resources.

Policy import and export functions are included to simplify migration from test to production environments. Most types of resources, access control lists, and audit configuration can be exported to XML files, manipulated if required, and then re-imported into the same or a new environment. This is an additional option to prior methods (e.g. scripting), with the facilities combining to constitute a comprehensive set of policy migration options for security administrators.

TAMeb shares an architecture with other products within the IBM Tivoli Access Manager family, including IBM Tivoli Access Manager for Operating Systems (TAMOS), a policy-based access control system for UNIX or Linux operating systems that addresses the many system vulnerabilities surrounding super user or “root” accounts in these systems. Products within Identity Management use Tivoli Security Information and Event Manager (TSIEM) as a common integration point for auditing and logging. TSIEM is similarly used by other products, with the overall aim of providing a broader audit and compliance perspective. A new component called Tivoli Common Reporting (TCR) is being used in a similar way for reporting requirements, and TAM products are already integrated with TCR.

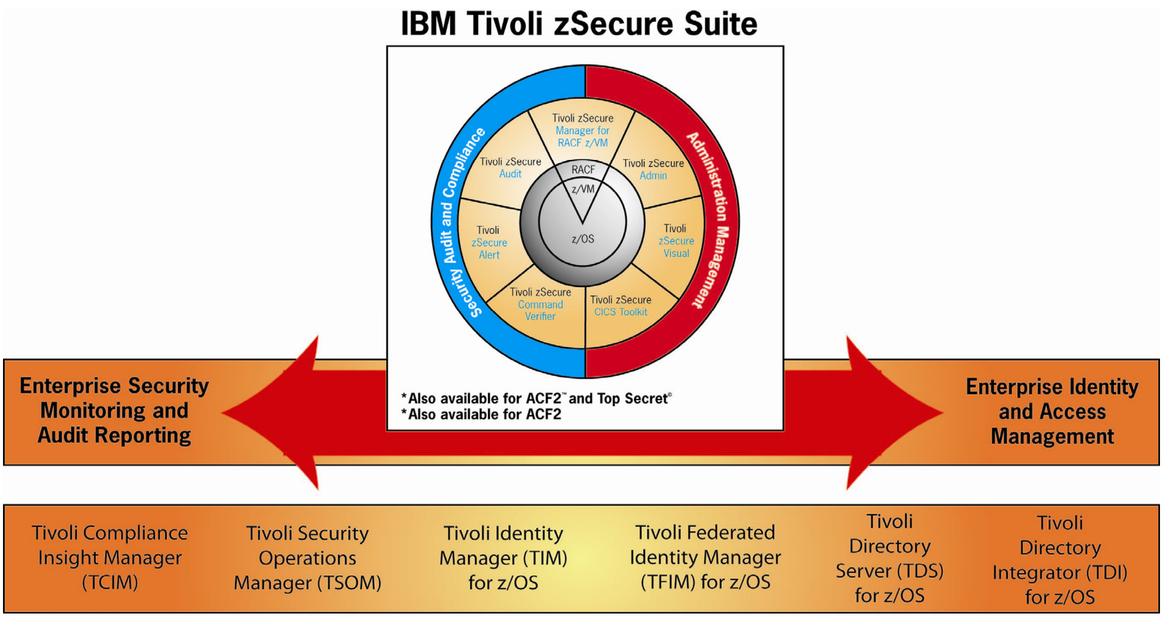
Encentuate provides SSO for enterprise applications, enabling the end-user experience to be simpler by eliminating the need to recall multiple user names and passwords (an approach which can also reduce the number of password reset calls to help desks). It can also improve security by minimising poor end-user password behaviour, and also by providing easier adoption of strong authentication form factors such as smart cards or biometrics, for which it provides integration out-of-the-box.

IBM expects to release a branded version in the third quarter of 2008 but, while integration with TAMeb and TIM are already available, Butler Group believes that IBM will need to integrate Encentuate with its other I&AM products in areas such as policy, over a longer period.

TFIM v6.2 has been enhanced to include management of users' access to assets using the OpenID and Higgins identity frameworks, and also Microsoft CardSpace. Extended integration with Microsoft .NET environments is incorporated, via a Kerberos token module, and with mainframe environments via visibility and auditing of RACF-based access. It also provides implementations of the SAML, Liberty ID-FF, WS-Federation, WS-Provisioning, and WS-Trust specifications for Federated SSO, and a single TFIM deployment can support all of these standards concurrently, as well as acting in different roles (e.g. identity provider, and service provider) concurrently, where applicable. In the Web services security space, TFIM provides a Secure Token Service (STS), as defined by the WS-Trust specification, as well as several modules for invoking the STS from IBM's WebSphere Application Server and WebSphere Web Services Gateway products. WS-Trust provides security token validation and mediation, user identity mapping, and partner key management services to Web service endpoints that implement the WS-Security standard. The federated provisioning components of TFIM provide an implementation of the WS-Provisioning specification. TFIM is a J2EE application, architected using a services model, which runs on IBM's WebSphere Application Server and also leverages TDS and Tivoli Access Manager.

Tivoli zSecure Suite (currently at v1.9.1) is the centrepiece of a number of identity- and security-related capabilities that serve organisations that are mainframe users. Its products with most relevance to I&AM are IBM Tivoli zSecure Admin and IBM Tivoli zSecure Visual, which both enable complex mainframe security mechanisms to be administered without encountering as much complexity as via native management systems. IBM provides editions of many of its Identity Management products that connect to the mainframe (TIM, TFIM, TDS, TDI can run on z/OS or zLinux, and TAMeb on zLinux), allowing central administrators to connect to the mainframe for routine, enterprise-wide administration (see Figure 2).

Figure 2: Tivoli zSecure Suite, and Other Mainframe Security Capabilities (including I&AM)


IBM Tivoli zSecure Suite
Security Audit and Compliance
Administration Management
Tivoli zSecure Manager for RACF z/VM
Tivoli zSecure Audit
Tivoli zSecure Admin
Tivoli zSecure Alert
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
RACF
z/VM
z/OS
*Also available for ACF2™ and Top Secret©
*Also available for ACF2
Enterprise Security Monitoring and Audit Reporting
Enterprise Identity and Access Management
Tivoli Compliance Insight Manager (TCIM)
Tivoli Security Operations Manager (TSOM)
Tivoli Identity Manager (TIM) for z/OS
Tivoli Federated Identity Manager (TFIM) for z/OS
Tivoli Directory Server (TDS) for z/OS
Tivoli Directory Integrator (TDI) for z/OS

Source: IBM

DATAMONITOR

Product Emphasis

IBM offers a range of excellent products, each of which have great strengths of maturity, and richness in features. With recent enhancements, IBM has added particular value to mainframe users, allowing I&AM in these environments to be more integrated with the equivalent in organisations' distributed environments. The acquisition of Encentuate adds a sophisticated enterprise SSO solution to IBM's I&AM portfolio, but at this early stage some work remains to integrate the Encentuate product with IBM's existing products. Across all of the products, IBM provides integrations with a range of systems and applications that would meet the great majority of enterprise requirements, and commendably uses industry standards throughout.

DEPLOYMENT

Although TDS uses a DB2 platform, no DB2 technical skills are required to deploy the product. The database platform enables TDS to achieve very high scalability, proven to tens of millions of users, and it can support up to dozens of master copies of the directory, and groups as large as hundreds of thousands of users. With its latest release, TDS offers a free LDAP Proxy Server optimised for massive scalability (up to hundreds of millions of users), as well as fault tolerance and very high write performance. TDS runs on Linux, z/OS, AIX, Windows, Solaris, and HP-UX distributed servers, and in the future will run on i5/OS (from that product's first release). It is the default directory for Tivoli, WebSphere, and AIX products, and hence some IBM customers will already be licence holders.

TDI does not require a database environment, but runs in a Java runtime environment. It is tested for AIX, Linux, Windows, Solaris, HP-UX, and z/OS systems, and can integrate data from a diverse range of platforms, e.g. telephony exchange equipment.

TIM supports user bases of at least 1.5 million in some customers' deployments, across thousands of managed systems. It is available on AIX, Linux, HP-UX, Solaris, and Windows platforms. IBM states that average implementation timescales are three to eight months, including re-engineering related business processes.

While TIM Express leverages the core engine of TIM, IBM has made substantial changes to better suit the needs of SMBs, which typically do not have the resources to deploy traditional identity management products. This variant has best practices templates designed to accelerate deployment, and IBM states that it can be installed in under two hours. TIM Express operates on a single server, is available on Windows and Linux platforms only, and is restricted by licensing to a maximum of 5,000 managed users. All TIM integration adapters work with this edition, with a large variety included as basic (LDAP, Solaris, Red Hat Enterprise Linux, SuSE Linux, AIX, CISCO ACS, Informix, Oracle database, Sybase database, Tru64 UNIX, RSA Authentication Manager, SQL Server, Lotus Notes, Active Directory, Novell Netware and HP/UX), and an additional charge for each required beyond these.

TAMeb supports both proxy and server plug-in models for authentication and authorisation. For larger-scale deployments most implementations use the proxy model, which has benefits including a simple, centralised server management model, and also provides added protection as users cannot access protected Web servers until they have undergone authentication. The proxy model also enables new authentication methods, to be added more easily, as changes are abstracted from enterprise systems. Both this and the TAMos, product have achieved Common Criteria EAL 3 certification.

The WebSEAL Web server proxy component of TAMeb is usually deployed on a separate server within the DMZ, to provide protection for back-end resources. All software components required are included in the price. TAMeb integrates with RACF on z/OS (or can run via a plug-in) to accommodate customers with that platform requirement, and it can run on the following industry-leading server platforms:

- IBM AIX® on IBM RISC System/6000®.
- Sun Solaris on Sun SPARC.
- Microsoft Windows® 2000 Advanced Server.
- Microsoft Windows 2003 Standard Server and Enterprise.
- HP-UX.
- United Linux® including SuSE Linux Enterprise Server.
- Red Hat Enterprise Linux for Intel®, S/390, and zSeries.
- zLinux.

The Encentuate product's server element runs on Microsoft's Windows 2000 Server or Windows 2003 Server platforms. IBM Tivoli zSecure is intended to be sited in a mainframe environment. The IBM products as a whole run on a very wide range of platforms, and the list of their integrations with target environments is too extensive to be covered in detail in this document, but its size and depth is a significant strength in terms of value to customers.

The TFIM server runs on AIX, Linux, HP-UX, Solaris, and Windows platforms. The supported Linux platforms include Red Hat and SuSE Linux offerings on zSeries. Due to its loose coupling between TFIM and the applications it provides SSO for, TFIM can be used to provide federated SSO to Web applications hosted on legacy systems, or security token mediation and identity mapping services to XML gateways protecting Web service applications hosted on legacy systems. The product can also achieve user-level integration via an STS with RACF using RACF Passticket, or via TDS running on z/OS.

Typically, customers' implementations rely on a mix of home-grown expertise, and services resources from either System Integrators (SIs) or IBM. General knowledge on installing middleware and expertise around security or audit and compliance is helpful in tailoring implementations to specific needs. Implementation times vary widely due to the different types of environment and complexity levels, but generally solution deployments are a number of months in duration. As policy definition takes up a significant portion of the time spent in deployment, customers with a security policy already defined will generally benefit from reduced timescales for their implementation programme.

IBM offers training in various delivery formats on all of the products, as well as an extensive range of online resources such as datasheets, product documentation, and Redbooks.

PRODUCT STRATEGY

IBM contends that securing Web and Service Oriented Architecture (SOA) applications requires a lifecycle approach from architecture design stage, through to the operations environment. The company offers solutions across this range of needs, including elements of its Rational tools (which address requirements, design, development, testing, and post-deployment assessment), WebSphere Business Modeler, and Service Management solutions (TSIEM, which monitors user activity in real-time and reports compliance, and Tivoli Security Policy Manager, which can manage and enforce security policies across heterogeneous environments).

TDS and TDI are included when customers purchase TIM, TAM, or TFIM. TDS is bundled with WebSphere Application Server and Portal Server, and AIX; TDI with IBM Workplace, IT Service Management offerings (via the Tivoli Change and Configuration Management Database), and Tivoli Compliance Management solutions.

TAMeb is one of a number of products in the Access Manager family. The other products provide equivalent access management and control functionality (which can be integrated with TAMeb via the Policy Server) relating to application servers, messaging systems, integration solutions, and Linux, UNIX, and RACF-based systems.

The main focus of IBM’s recent major enhancement to Identity Management has been in the following areas:

- User provisioning is intended to be more intuitive for business users, and faster to deploy for administrators or integrators.
- Directory services are intended to be more robust, to support demanding performance requirements, such as arise from business- and government-to-consumer applications.
- Easy implementation options are provided for federated identity, and key lifecycle management, requirements.
- Common reporting is implemented across I&AM products (except those that are newly acquired).
- More insight is used within Identity governance, and privileged user management, capabilities.

The approach to licensing and other payments varies across the product range, as follows:

- For TDS, the cost is US$10,000 per processor plus annual maintenance.
- For TDI, the cost is US$16 per value unit (i.e. user, most commonly), for the entire package (runtime and development environments, administration management console, connectors, and parsers, etc.) plus an annual maintenance fee.
- TIM, TAM, and TFIM can be purchased on a per-user basis, or per-processor, with volume discounts where applicable.
- TAM-ESSO is purchased on a per-user basis, with volume discounts where applicable.
- All IBM software is subject to a customer discount scheme. Maintenance and support must be purchased annually at 20% of the licence cost, which also affords access to any upgrades.

COMPANY PROFILE

IBM was founded over 80 years ago, and is the world's largest information technology company in terms of revenues from enterprise markets. Drawing on resources from across IBM and key business partners, IBM offers a wide range of services, financing, solutions, and technologies. The company had over 386,000 employees at the end of 2007, and is represented throughout every area of the populated world. Table 1 is a summary of the company's financial performance in recently completed years:

Table 1: Financial Details

Year ending 31 December	2007	2006	2005
Revenue (US$ billion)	98.8	91.4	91.1
Change on Previous Year (%)	8.1	0.3	(5.6)
Total Net Income/(Loss) (US$ billion)	10.4	9.5	8.0

Source: IBM DATAMONITOR

Tivoli was founded in 1989 and acquired by IBM in 1996 – its company name is now one of five major brands within the IBM Software Group, offering software products that undertake business application management; server, network, and device management; storage management; and security management. IBM acquired DASCOM in 1999, whose IntraVerse product formed the basis for TAMeb. In 2002, IBM purchased Metamerge for its metadirectory product, which formed the basis of what is now TDI. Later that year, IBM purchased Access360, whose former product (enRole) is now the basis of TIM, for which IBM now has over 800 customers. IBM completed the acquisition of Consul in 2007, and that of Encentuate in March 2008.

SUMMARY

IBM's product offerings cover all bases across the range of I&AM requirements, and demonstrate considerable strength and depth from end to end. The addition of an Enterprise SSO product, in Encentuate, fills a former gap in the IBM portfolio, and with one of the more up-to-date solutions of that type. The company has also focused on enhancing I&AM's integration with customers' mainframe environments. Consistency of excellence throughout the products, and in addressing advanced requirements such as federation, and extreme scalability and performance needs, mark IBM as having a prominent position amongst the leadership in this market – likewise does the vision of I&AM fulfilling an integrated role in the context of broader security, and service, management. IBM is one of the few vendors with sufficient breadth to bring such a vision to fruition.

Table 2: Contact Details

IBM Tivoli in UK
Sefton Park
Bells Hill, Stoke Poges
Bucks
SL2 4HD
UK
Tel: +44 (0)1753 780000
Fax: +44 (0)1619 764481
www.ibm.com/tivoli

IBM Center of Operations for Tivoli Software
11301 Burnet Road
Austin, TX 78758
Texas
USA

Tel: +1 877 TIVOLI1 (in the US)
Tel: +1 512 436 8000 (outside US)

Source: IBM DATAMONITOR

Headquarters
Europa House,
184 Ferensway,
Hull, East Yorkshire,
HU1 3UT, UK
Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Butler Direct Pty Ltd.
Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000,
Australia
Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

Butler Group
245 Fifth Avenue,
4th Floor, New York,
NY 10016,
USA
Tel: +1 212 652 5302
Fax: +1 212 202 4684

For more information on Butler Group's Subscription Services please contact one of the local offices above.

Important Notice

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.