IBM Identity and Access Management

As products go to market quicker and information flows faster than ever, employees, customers, and business partners need the ability to collaborate and access business data with more speed than ever before... when, where, and how they choose.

Identity and Access Management is key to the secure access of your organization's business assets, especially in today's era of compliance.

But traditional Identity and Access Management   takes a technology-driven approach to protecting against security threats and vulnerabilities. Multiple end point products often result in user data being stored and managed in multiple locations within an organization, and in users having multiple user ID's and passwords... creating silos of data, IT complexity, and redundant costs… and hindering business processes.

A business-driven approach to Identity and Access Management is a smarter approach. A business-driven approach keeps access to your data and technology convenient to business users to enhance productivity – without compromising security.

Business-driven Identity and Access Management   starts not with technologies and tactics, but with intelligence.

It begins with proper identification of business roles. Rather than try to apply technology against business roles, IBM looks at the business side of how your employees, customers, and business partners conduct business with your organization… and define business roles based on what your users are actually doing.

When you take a business-driven approach to secure four universal Identity and Access Management processes – provisioning, productivity, access, and audit – you align Identity and Access Management goals with your business objectives.

User provisioning tools support a business-focused view of roles and users, while automating the setup, removal, and management of user accounts.

Single sign-on and self-service for password resets give users productive access to your business, without overrunning your help desk with password reset calls.

Centralized access management allows you to consistently apply an access control policy across your entire business environment… reducing IT complexity and total cost of ownership.

Security information management, security event management, and privileged user monitoring allow you to monitor and report on user behavior across your entire infrastructure.

And Professional and Managed Security Services can help make your identity and access management program more successful by providing your organization with proven methodologies and approaches s

When you align Identity and Access Management goals with your business objectives, you give your employees, customers, and business partners the capabilities they need to create more value for your organization. You enhance compliance measures… and reduce security risks, IT complexity, and operational costs.

IBM's business-driven approach to Identity and Access Management is a smarter approach.

Only IBM delivers a breadth of security and compliance capabilities to address infrastructure, applications, information, people, and identities. Our extensive integration capabilities can secure access to all your business data and processes, while enhancing business productivity.

To learn more, contact your IBM representative or visit ibm.com/itsolutions/security.