The complexity and number of logins employees must manage daily are increasing, resulting in frustration and lost productivity. In most organizations, employees are required to remember up to 20 passwords that need to be changed every 30 days based on password security policies. The time wasted entering, changing, writing down, forgetting and resetting passwords represents a significant loss in productivity and a significant cost to IT help-desk operations.

Key Benefits

- **Lower Administrative Costs.** Cut desktop administrative costs by up to 50% through centralized management.
- **User Productivity.** More than 85% reduction in time to information.
- **Security.** Improved identity assurance and 100% graceful sign-off.
- **Compliance reporting.** More than 75% reduction in fine-grained audit tracking costs.
- **Helpdesk cost reduction.** 35-45% reduction in IT helpdesk costs.
- **Leverage the best from VMware and IBM.** Long-term partnership and dedicated expertise to address customer needs.

Industry Challenges

Analysts estimate that the desktop virtualization market will grow to over $1 billion by 2015. While this solution simplifies the organization’s desktop implementation management processes and lowers the TCO of desktops in general, it does little to address the challenges and costs associated with managing the identities of users accessing the applications inside the virtual desktop. Also, this paradigm shift brings with it new security challenges, especially related to securing access to the virtual desktop and protecting the sensitive data and applications that are used inside it. Lastly, there’s an increasing need to address the regulatory and compliance challenges related to tracking application and data access inside the virtual desktop.

Solution Overview

IBM’s Security Access Manager for Enterprise Single Sign-On (SAM E-SSO) integrates with VMWare View™ to provide single sign-on and strong authentication to the virtual desktop increasing security. Users can now log into their PCs using a number of strong authentication factors such as fingerprints, smart cards, building access badges, etc. Once logged into their desktop, SAM E-SSO automatically signs them into their virtual desktop.

SAM E-SSO also provides single sign-on to all the user’s applications inside the virtual desktop. This increases user productivity and also helps reduce helpdesk costs associated with password resets, furthering reducing the organization’s TCO of desktops.
Secure and Simple Virtual Desktop Access

Solution Brief

The organization’s regulatory and compliance requirements, especially related to monitoring events such as application access and usage inside the virtual desktops can be satisfied using SAM E-SSO. The SAM E-SSO agent for virtual desktops collects audit information that can be used to generate detailed reports for compliance and chargeback accounting purposes.

Also available as a very easy to deploy and manage virtual appliance, SAM E-SSO provides substantially faster time to value and lower TCO to the organization.

Solution Components

VMware View
VMware View delivers desktop services from your cloud to enable end user freedom and IT management and control.

VMware View allows IT to simplify and automate the management of thousands of desktops and to securely deliver desktop as a service to users from a central location with levels of availability and reliability unmatched by traditional PCs. By delivering secure access to applications and data to any device, when and where the user needs it, VMware View provides end users with the highest levels of mobility and flexibility.

IBM Security Access Manager for Enterprise Single Sign-On
SAM E-SSO strengthens access to the virtual desktop and enables users to access all their applications inside the virtual desktop with a single strong password. This award-winning solution simplifies password management, protects information with strong authentication, and secures kiosks, shared workstations and roaming desktops. The solution also facilitates compliance with security and privacy regulations by leveraging centralized fine-grained auditing and reporting capabilities.

IBM Security Identity and Access Assurance
IBM Security Identity and Access Assurance helps organizations to protect data, users and applications by providing a comprehensive approach to identity governance, access management, and security assurance. It includes capabilities such as identity management, access management, and security assurance, which are essential for organizations to deploy and manage virtual desktops securely.

VMware Horizon Application Manager
VMware® Horizon Application ManagerT is a hosted management platform that centralizes IT control for end-user computing devices. Horizon gives end users access to Windows, SaaS and enterprise web applications across different devices while retaining control and visibility via policy-driven management. VMware Horizon Application Manager lets you provision and entitle secure access to end users, track SaaS license activity, and get usage reports.

Support & Professional Services

VMware offers enterprise-class support to all VMware View customers. For customers that require additional services, VMware also offers several professional services engagements on best practices and getting started with your VMware View deployment.

Support and Professional Services

FIND OUT MORE

VMware-IBM Alliance:

VMware View & Desktop Solutions:
http://www.vmware.com/solutions/desktop/

VMware Horizon Application Manager:
http://www.vmware.com/products/desktop_virtualization/horizon/

IBM Security Access Manager for Enterprise Single Sign-On:

IBM Security Identity and Access Assurance:
www-01.ibm.com/software/tivoli/products/identity-access-assurance/

Contact VMware
For information or to purchase VMware products, call 1-877-VMWARE (outside of North America dial +1-650-427-5000), visit www.vmware.com/products, or search online for an authorized reseller. For detailed product specifications and requirements, please refer to the VMware View documentation.