The Move to Virtualized Infrastructures and Private Clouds

Organizations have been turning to virtualized desktop infrastructure (VDI) and private clouds for greater security, business agility, and cost efficiencies. However, to protect the integrity and confidentiality of data residing in their virtualized environment, whether streamed from the data center or accessed through a private cloud gateway, organizations still need to ensure that users are who they claim to be when accessing these solutions and infrastructure.

Obstacles to Securing Virtual Environments

Organizations wishing to secure access to their virtualized environments are confronted with several key challenges, namely:

> **Endpoint diversity**—Thin clients, zero clients, servers, and mobile BYOD devices that double for personal and corporate use all require a device-agnostic authentication strategy.

> **Password vulnerability**—Organizations gating their virtualized environments solely with a password jeopardize their information assets, and expose them to threat vectors such as phishing, social engineering, brute-force attacks, generic malware, password guessing, and credential theft.

> **Ubiquitous access**—While some organizations deploy their virtualized infrastructure within the enterprise firewall, others offer access to consultants or partners situated outside the corporate firewall (in the DMZ). This makes strong authentication crucial, as well as the ability to provision secure access remotely.

Key Benefits

> Enhanced security
> Frictionless authentication
> Reduced administration overheads
> Simplified compliance

> **Compliance**—To pass security audits and comply with regional, industry, and corporate governance regulations, enterprises need to demonstrate that they know who is accessing what and when.

> **Budgetary constraints**—To keep within their current budgets, in terms of both hard and soft costs, organizations may waive stronger access controls to their most valuable information assets and resources.

Simple, Strong Identity and Access Management from Gemalto

Gemalto’s Identity and Access Management Solutions deliver secure access to virtualized infrastructure:

> From any device, including thin clients, zero clients, and BYOD mobile devices

> To any VDI application, thanks to out-of-the-box integrations with Citrix, VMware, and AWS for a quick and easy deployment

> At any assurance level, via the broadest range of authentication methods
Gemalto’s Frictionless Management Strategy

Gemalto’s solutions reduce IT management overhead and simplify compliance through:

- Zero-touch user and token lifecycle administration, including auto-provisioning, updates, and revocation of permissions and tokens
- A single point of management for defining access policies once and enforcing them throughout your IT ecosystem
- Management by exception, achieved via real-time threshold-and event-based alerts
- A unified audit trail of all access events across on-premises, virtual, and cloud-based resources

Supported Authentication Methods

SafeNet Authentication Service is included in SafeNet Trusted Access. The combined solution supports a wide range of multi-factor authentication methods such as:

- OTP Push
- OTP Software
- OTP Hardware
- Pattern-based authentication
- Out-of-band via email and SMS text messages
- Password
- Kerberos

SafeNet Trusted Access Solution Advantages

- Effective risk management
- Balance convenience and security
- Universal authentication

Gemalto’s Identity and Access Management Platforms

- SafeNet Trusted Access
- SafeNet Authentication Service

About Gemalto’s SafeNet Identity and Access Management Solutions

Gemalto’s industry-leading Identity and Access Management solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy based SSO and universal authentication methods, enterprises can effectively manage risk, maintain regulatory compliance, gain visibility into all access events and simplify the login experience for their users.

To learn more about access management from Gemalto, visit https://safenet.gemalto.com/access-management/

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us
Follow Us: blog.gemalto.com/security