Identity and Access Management Without RSA

Companies often attempt to provide a full-featured Identity and Access Management system with a patchwork of disconnected components. This leads to an inconsistent and poor user access experience – impacting business productivity – and opens the door to security risks, compliance violations, and audit issues.

**Access**
- NewUser
- FormerUser

**Applications**
- Joiner access takes too long, and is incorrect
- Access provisioning is manual and inconsistent
- Inconsistent access and authentication across applications

**Governance**
- Access provisioning is manual and inconsistent
- Inconvenient auth methods burden user
- Help desk overwhelmed by password resets

**Active Users**
- Customers
- Vendors
- Partners
- Employees

**Former User**
- Inconsistent access and authentication across applications
- No IT notification of Leavers, SaaS access retained
- No closed-loop Access Deactivation
- Role changes undetected

**Complex & ineffective Access Reviews, across few apps**

© Copyright 2015 EMC Corporation. All rights reserved.
RSA-Enabled Identity and Access Management

Identity and Access Management is governance-driven, supporting consistent policies and processes across the full range of users from employees to partners, vendors and customers. The result is a simpler, faster, and more secure experience, tailored to each user’s needs.

- **New User**
  - Automated and accurate provisioning
  - Joiners efficiently obtain appropriate access

- **Active Users**
  - Consistent access and authentication across applications
  - User role changes prompt automated remediation processes
  - Closed-loop Access Deactivation
  - User departures trigger automated access deactivation

- **Former User**
  - Efficient and effective Access Reviews for all key apps
  - Self-Service Help Portal

- **Applications**
  - NEWUSER
  - FORMERUSER
  - Partners
  - Employees
  - Customers
  - Vendors

© Copyright 2015 EMC Corporation. All rights reserved.