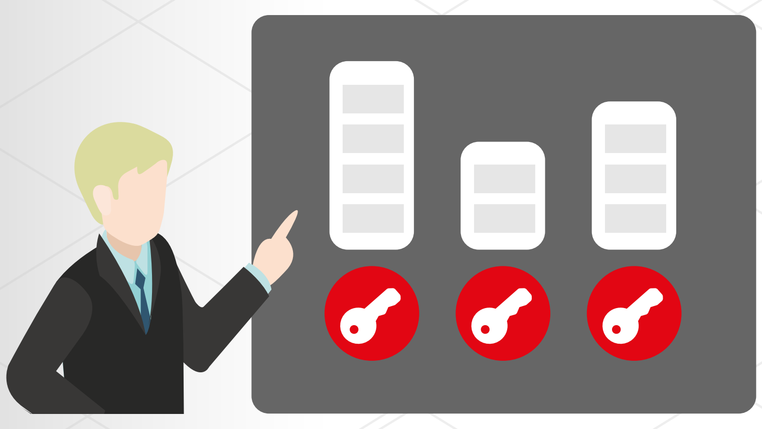
Day in the Life of a Security Admin

RSA

RSA SecurID Access: for any user, from anywhere, to anything. Deliver secure access to cloud, mobile, and traditional on-prem applications without creating roadblocks for users.

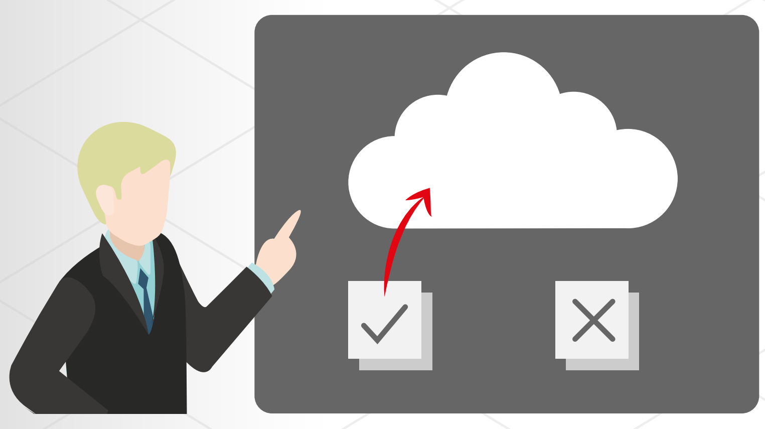
WITHOUT RSA SECURID ACCESS

BETWEEN A ROCK AND A HARD PLACE



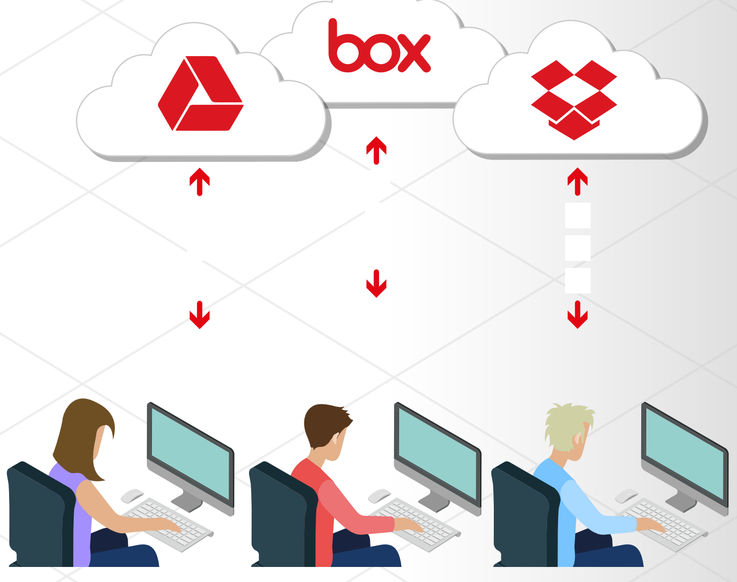
CISO Pressure: "Protect our data wherever it is"

With each new application, rules for access are set up in a silo. This means yet another username/password combination for the user and more separate policies for the admin.



CISO Pressure: "Reduce budget, use the cloud (but only if it's secure)"

For very sensitive data, IT is unable to take advantage of the cost savings and efficiency of the cloud because they think they can't secure it.



Line of Business Pressure: "Enable more users in more locations"

Because IT can't keep up, lines of business get frustrated, and actively circumvent IT rules with "Shadow IT" – they set up their own apps outside of IT's control.

Line of Business Pressure: "Enable more devices"

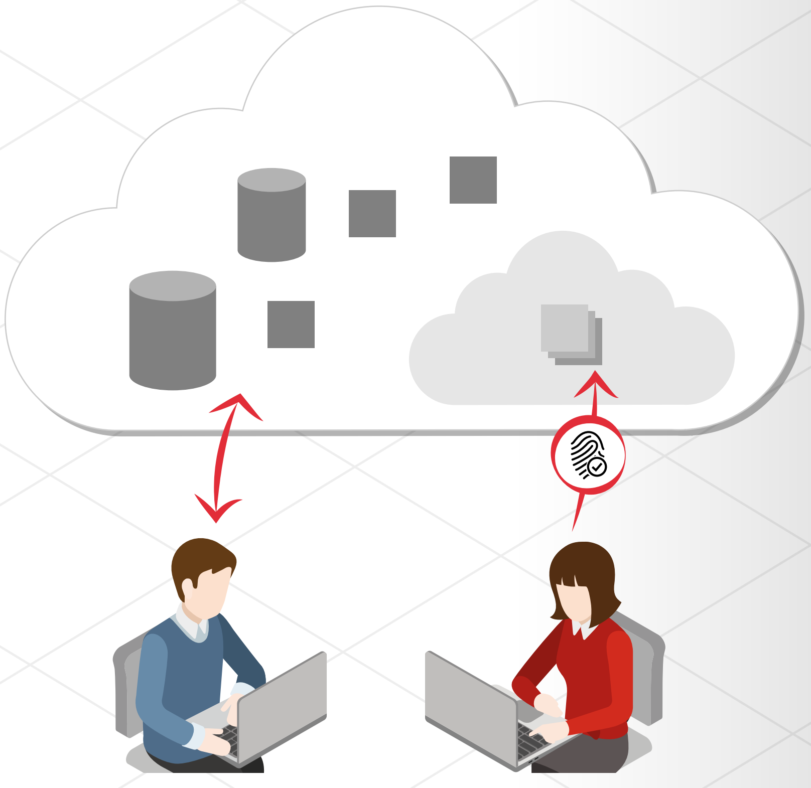
Without proper security, IT can't allow these devices – but line of business users adopt them anyways. They engage in "Rogue Access" – accessing data and content from unapproved and unmanaged devices.

WITH RSA SECURID ACCESS:

CONFLICT RESOLVED

CISO Gains Policy Compliance

The admin can now set precise security requirements directed by the CISO/CIO for each application. They can say "yes" much more often to requests for new cloud apps, because they are able to protect them appropriately.



Line of Business Gains Needed Flexibility

Line of business users can now take advantage of many cloud-based resources, and have access with 1 username/password combo (with occasional step-up authentication). It's now easier to follow IT guidance than engage in Shadow IT or Rogue Access.

Visit www.rsa.com/securidaccess to See if RSA SecurID Access is Right for Your Organization