Go beyond single sign-on with adaptive authentication

Make sure activity in your cloud accounts originates from authorized users with single sign-on and adaptive authentication. Automatically step up user authentication when high risk activity is detected or when confidential files are accessed with adaptive controls from an integrated CloudSOC and VIP solution.

For info on CASB and other integrations go.symantec.com/casb
Dynamically adjust authentication based on real-time threat risks

Trigger additional authentication for high risk users
Automatically require additional user authentication if a user’s ThreatScore™ in CloudSOC is elevated. A high ThreatScore indicates abnormal and potentially malicious user activity.

Protect sensitive content with multifactor authentication (MFA)
Automatically trigger multifactor authentication when a user tries to access sensitive files in cloud accounts.

Step up authentication for sensitive transactions
Automatically require additional authentication when a user performs specific actions in the cloud. For example, you can trigger additional authentication for users deleting folders, downloading files, or setting up a new virtual server.