Use case 1:



Legitimate employee attempts to log into corporate finance system from office in Sunnvvale, Calif., using work computer at 11 a.m. PST.

Upon access to risk-based authentication system:

User ID + Device Password + Fingerprint + Usage + Location + Login Äddress Context Trends

Current Pattern

Entered The companyissued laptop

and in line

with pattern



locations in

Sunnyvale.

line with

pattern

Calif., and in

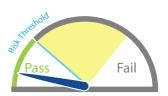
Legitimate





pattern

During working hours system and from 8 a.m. to in line with 5 p.m. PST and in line with pattern



Result:

Risk score assigned to attempt: Very Low

Criticality: Corporate Finance: High | Risk Threshold: Low

Outcome: Pass. User gets access to corporate finance system.

Use case 2:



Legitimate employee attempts to log in from LAX airport using work laptop at 7 p.m. PST and tries to access the list of company holidays stored on an internal benefits system.

Upon access to risk-based authentication system:

The risk-based authentication solution checks the attempt for:

User ID + Device Password Fingerprint + Usage + Location + IP Address Context Trends PIN

Current Pattern

Entered

issued laptop and in line with pattern

The company- Not one of Legitimate the standard locations of Palo Alto or Sunnvvale but close by geographically

Corporate holidays. working hours and Pattern is few times not in line a year with pattern



Result:

Risk score assigned to attempt: Medium

Criticality: Corporate Holiday Calendar page: Low || Risk Threshold: High

Outcome: Pass. User gets access to Corporate Holiday Calendar page.

Use case 3:

Upon access to risk-based authentication system:



Hacker attempts to log in from Shanghai at 3 a.m. PST and tries to access the designs for company's new product stored on an internal development server.

User ID + Device Password + Fingerprint + Usage + Location + IP Login Address Trends Context

Current Pattern



Unknown device and not in line with pattern



and from a

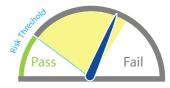
higher risk

location

Not one of Legitimate the standard locations of Palo Alto or Sunnvvale



Outside of working hours or access from home hours and not in line with pattern



Result:

Risk score assigned to attempt: Very High

Criticality: New Product Design Blueprint Repository: Very High | Risk Threshold: Very Low

Outcome: Initial test fails. Additional authentication is requested (e.g., entering one time code sent to the employee's phone). Since the hacker does not have access to this phone. additional authentification fails and access is denied. A legitimate user would be able to provide appropriate information and get access. Outcome: Fail.