If a user or device becomes compromised, how can I automatically enforce additional layers of authentication to keep my organization safe?

SCENARIO:

As a division VP, I spend a good portion of my time traveling to visit the five offices I manage across the US, China, and Canada. I have access to highly sensitive information, so its important for me to protect my user identity. This proves much more difficult when traveling or connecting through public Wi-Fi. I need security that understands what's normal for me.

Microsoft 365 simplifies user access

Login to all my devices and apps with a single user identity

Scan my fingerprint or use facial recognition instead of a password

Prove its me by using Multi-Factor Authentication when I travel to a risky area or login from a new device

Change the actions I can take in cloud apps, if my user risk level increases

Get prompted to reset my password at next login, if my identity gets compromised

Shift admin privileges from "permanent" to "just in time" as proactive protection

Get automatic protection according to our identity protection policies, if my user credentials are for sale on the dark web

Avoid common passwords that could make me vulnerable to a brute force attack

Microsoft 365 Enterprise E5 provides holistic security across identity and access management, information protection, threat detection, and security management

Microsoft 365 Enterprise E5 includes powerful security tools that work together in different combinations to protect your organization in a variety of ways. These products come together to help protect user identities and manage access from any device or location:

Azure Active Directory	Windows Hello	Intune	Microsoft Cloud App Security	Azure Information Protection

Get complete, intelligent enterprise security

Test it yourself with a free trial, get serious with a proof of concept, or learn more at https://aka.ms//M365E5/Security

Microsoft