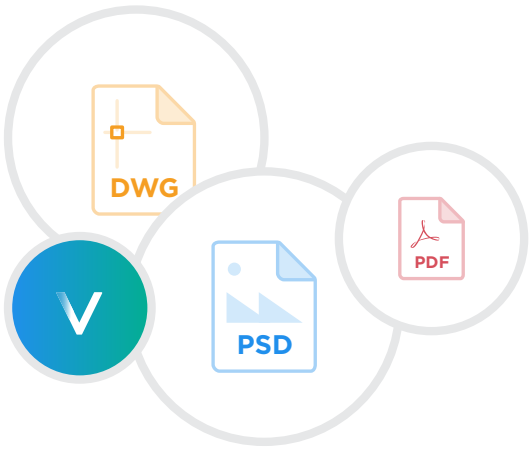
VERA

CHECKS AND BALANCES:

PROTECTING CORE IP WITH CONTEXT-DRIVEN AUTHENTICATION

A Fortune 100 engineering and manufacturing firm builds high performance aircraft, advanced jet engines, and engineers superior world-class aviation equipment. Behind every product are decades' worth of R&D, proprietary billion-dollar designs, and valuable product specifications. Securing IP is not only a company-wide, board-sponsored initiative, it's their mission-critical competitive advantage.



The Challenge:

The company had two big challenges.
First, as a multinational company, the business creates and shares thousands of sensitive product designs with internal employees, temporary contractors, and external vendors all over the world. How could they prevent competitors from ever getting their hands on their R&D? For the company, that's priority #1.

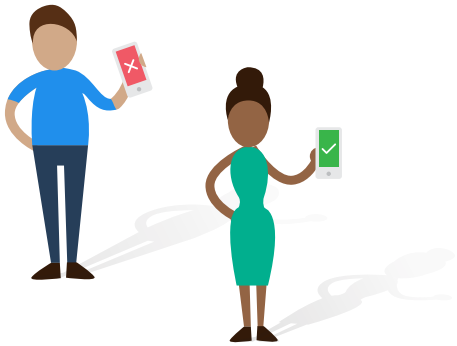
Second, the company had highly confidential strategic plans that required an additional layer of security to ensure only authorized personnel could access it. To solve this challenge, they set out to identify the data and require a second layer of authentication without adding yet another tool to the firm's tech stack.

Vera: Data-Centric Security with Dynamic 2nd-Factor Authentication

The company had tried other methods of securing its intellectual property, everything from Data Loss Prevention (DLP) to application-specific password protections, but none of these could protect data when it mattered the most. Once proprietary designs were shared beyond the company's borders, were copied by employees or downloaded by partners, the security team couldn't provide auditing or the assurance that data hadn't traveled to the wrong people.

With Vera, the company now automatically secures IP across all corporate systems (including Box, SharePoint Online, local SMB drives, and PLM systems), and controls how others use sensitive documents throughout their entire life cycle. Vera's always-on, dynamic data protections let them enforce usage rights like blocking copy and paste, preventing printing, and auto-expiring content in real-time.

Moreover, the firm uses Vera's policy-driven two-factor authentication to protect its most highly-classified information. Based on the sensitivity of a document, where it's been stored, and who has access, Vera automatically requires an additional authentication factor to confirm they're the right party to access sensitive data.



The Results:

The engineering firm can now track and ensure only authorized parties can access unreleased strategic plans, and can confidently confirm identity, access, and permissions with a context-sensitive second factor. And, Vera seamlessly integrates with their existing identity and multi-factor authentication providers to prevent intellectual property, strategic planning, and private financial data from ever falling into the wrong hands. There's no better way to keep your checks in balance.