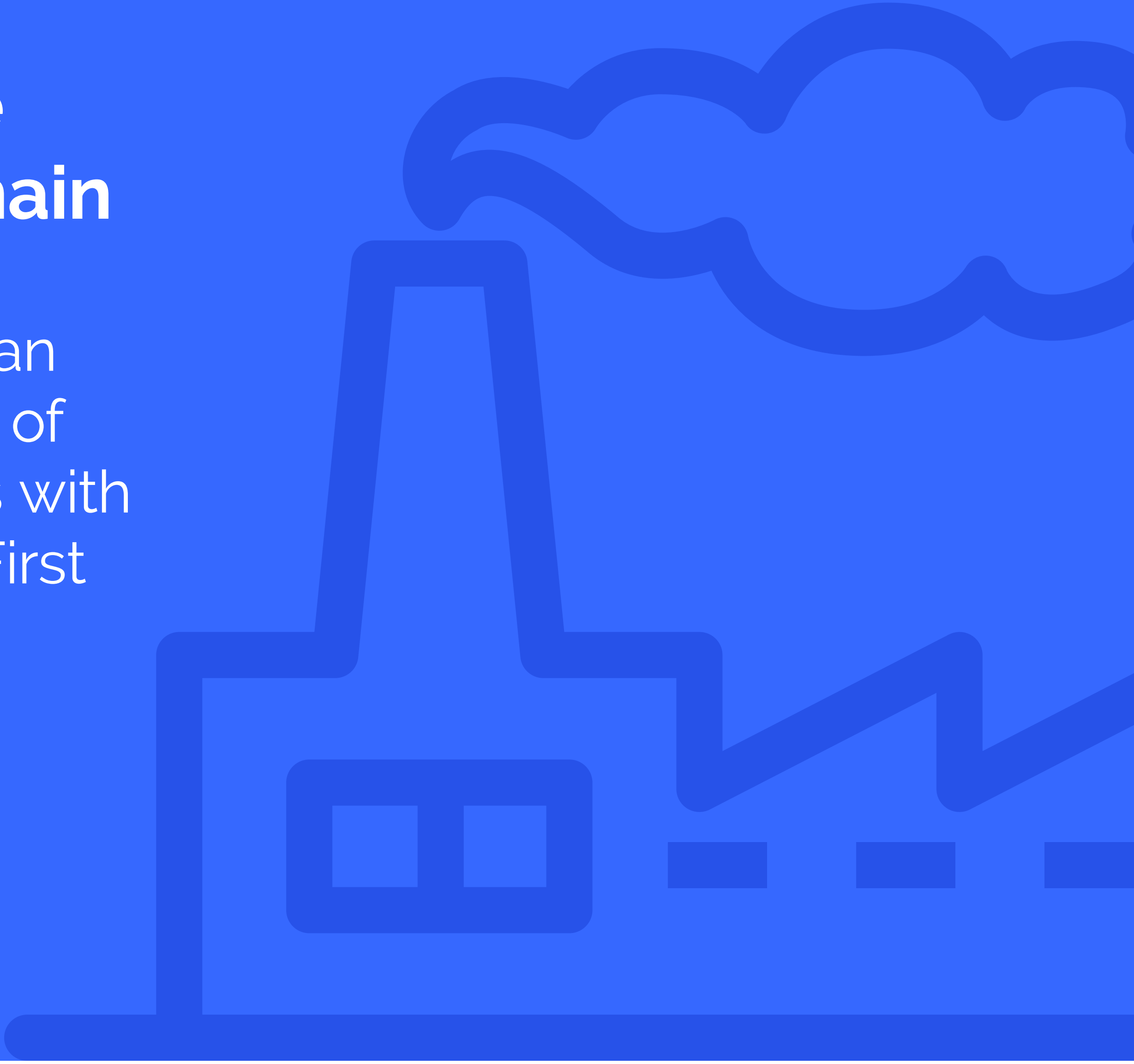
Transforming the Digital Supply Chain

How Manufacturers Can Overcome Limitations of Traditional Protections with a Data-Centric, User-First Approach



virtru

Table of Contents

The Promise of Digital Innovation vs. the Challenges of Physical Manufacturing

Digital workflows, cloud-based applications, and connected devices present unique challenges and opportunities for the manufacturing industry. Innovation is especially important for manufacturing: more advanced products and more efficient production and service models power differentiation and growth for years, yet failing to innovate puts the business at risk. All industries are facing similar obstacles, but manufacturers have the added challenge of aligning the potential of the digital world with the realities of the physical world. The nuts and bolts of a product have to come together in a complex physical supply chain, yet supply chain partners still expect rapid digital collaboration.

Compliance and privacy are even more important against this backdrop. Multi-cloud environments that digital supply chain workflows rely on leave sensitive data at risk of exposure. All manufacturers have intellectual property (IP) within product specifications, industrial designs, and more. Protecting that IP preserves investments in R&D and ensures a competitive advantage. Meanwhile, heightened data privacy regulations add risks for steep noncompliance penalties if data is breached along the supply chain. In particular, manufacturers involved in the defense and military supply chain face very stringent requirements from regulations like the International Traffic in Arms Regulation (ITAR) for protecting technical data from access by foreign entities.

The demands of modern manufacturing operations reveal the inadequacies of traditional approaches to protecting data throughout the supply chain. This guide offers a close look at a fictional scenario based on real manufacturing use cases. It identifies key pain points associated with traditional data protection methods and uncovers how data-centric, user-first protections keep your innovation engine humming while your data stays private and compliant.

Inherent Cloud Risks for the Supply Chain

While the cloud transforms operations, it introduces substantial risks.

⚠ Across industries, organizations use an average of 78 different cloud-based applications every week. Yet security professionals are only aware of 38% of the applications known to IT administrators. Meanwhile, 23% of data stored in the cloud environments is accessible by the underlying cloud provider, which may violate compliance obligations. These inherent cloud risks are even more pronounced for manufacturing organizations with heightened privacy and compliance requirements.

SOURCE: Data Security & Privacy in The Digital Workplace

The Scenario: Partnering to Differentiate

Acme Manufacturing

Acme is a medium-sized manufacturer of hardware sensors with a wide variety of applications. The firm realizes that in order to sustain business growth, they must differentiate while transforming digital workflows to accelerate innovation and service delivery. After evaluating the Internet of Things (IoT) market, Acme decides to enter it by partnering with another manufacturer to enhance the connectivity of their sensors for incorporation into IoT apps and workflows.

Acme chooses Initech, a leading-edge manufacturer of sensor subcomponents that enable the collection of myriad data points (and associated metadata), including atmospheric temperature and pressure, water quality and levels, proximity of other connected devices, and much more.

The partnership begins right as Acme's head of sales identifies a lucrative government defense contract aligned with their new IoT product concept. Their joint bid is due in only 3 months, so both organizations are facing a tight deadline to develop working prototypes of their new IoT-enabled sensor.

The Massive IoT Opportunity

Manufacturers across the globe are entering the IoT market, which was valued at $212 Billion in 2018 and is **projected to experience 25.68% CAGR and reach $1.3 Trillion by 2026.**

SOURCE: Data Security & Privacy in The Digital Workplace

By 2028, IoT capabilities are projected to be embedded in over **15 billion endpoints.**

SOURCE: Scenarios for the IoT Marketplace, 2019, Gartner

The Use Case: External Collaboration with Supply Chain Partners via Email and Files

Acme has appointed Joe, Director of Product Development, to lead this joint development initiative, code name Project IDA.

Joe reaches out to Milton, his counterpart at Initech, to kick things off.

Pain Points with Traditional Approaches

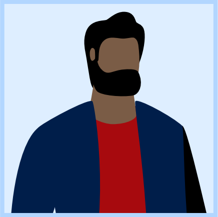
Joe needs to send Milton confidential documentation and an initial bill of materials for this new IoT sensor. Due to the sensor's government and defense applications, the documents contain ITAR technical data that must be protected with more stringent measures.

Acme generally uses Gmail and Google Drive for collaboration, in addition to on-premises file servers for more sensitive projects. Initech, meanwhile, has just migrated from on-premises Exchange to Office 365 and now uses Outlook and OneDrive, as well as on-premises infrastructure for sensitive data.

Joe decides the best immediate approach is to provision Milton a new account for access to Acme's on-premises file server. After some push back, Acme's IT team makes an exception to their security policies and creates Milton's account, but they limit Initech to only 1 new account for the whole project, to reduce security risk (and preserve their limited user licenses).

User Profiles

Joe - Director of Product Development at Acme



- 35 year-old hardware engineering leader.
- 10 years of experience at Acme overall, with 5 years of progressive management and operations experience and 5 years as lead engineer.
- Limited IT administration experience, but technically-savvy across a wide range of programs and platforms.

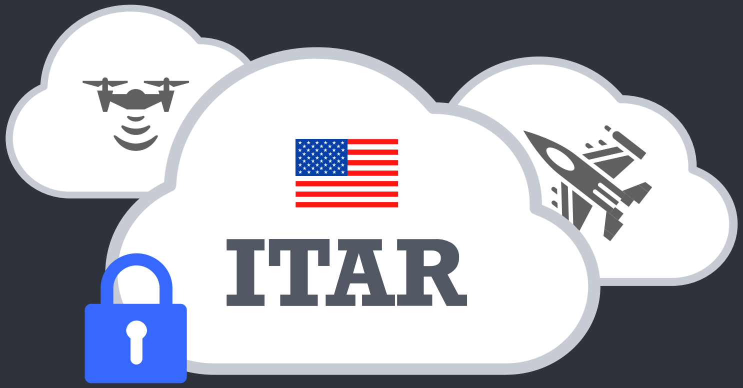
Milton - Senior Engineer at Initech

- 42 year-old hardware engineer and Army veteran.
- 10 years of experience working in the private sector as lead engineer across a range of manufacturing operations.
- Passionate about IoT devices and applications.
- Extensive administrative experience and deep knowledge of Microsoft Exchange and Office365 environments. Little to no experience with G Suite.

The International Traffic in Arms Regulation (ITAR)

ITAR is especially relevant for manufacturing firms, as it controls the export of manufactured defense items and related services and information in the interest of U.S. national security. ITAR closely regulates "technical data," or information needed for the development and manufacture of defense articles and services—such as firearms, aircraft, ground vehicles, and much more.

When non-U.S. persons obtain access to technical data, it is considered an "export" under ITAR. Without proper licensing, ITAR export violations can result in:



$500K

civil fines up to $500K

$100M

criminal fines up to $1M

10 years imprisonment

being barred from conducting any export business in the future

How the Users Feel

Joe is frustrated with the tradeoffs he faces in sharing these confidential files:

- Gmail and Google Drive facilitate internal collaboration on less sensitive projects, but they're not designed for ITAR compliance without added protections.
- Acme has an on-premise file server designed to keep confidential files private and compliant inside Acme's network—but not externally.
- Sharing without protections or additional controls risks noncompliance fines, and loss of Acme's precious IP.

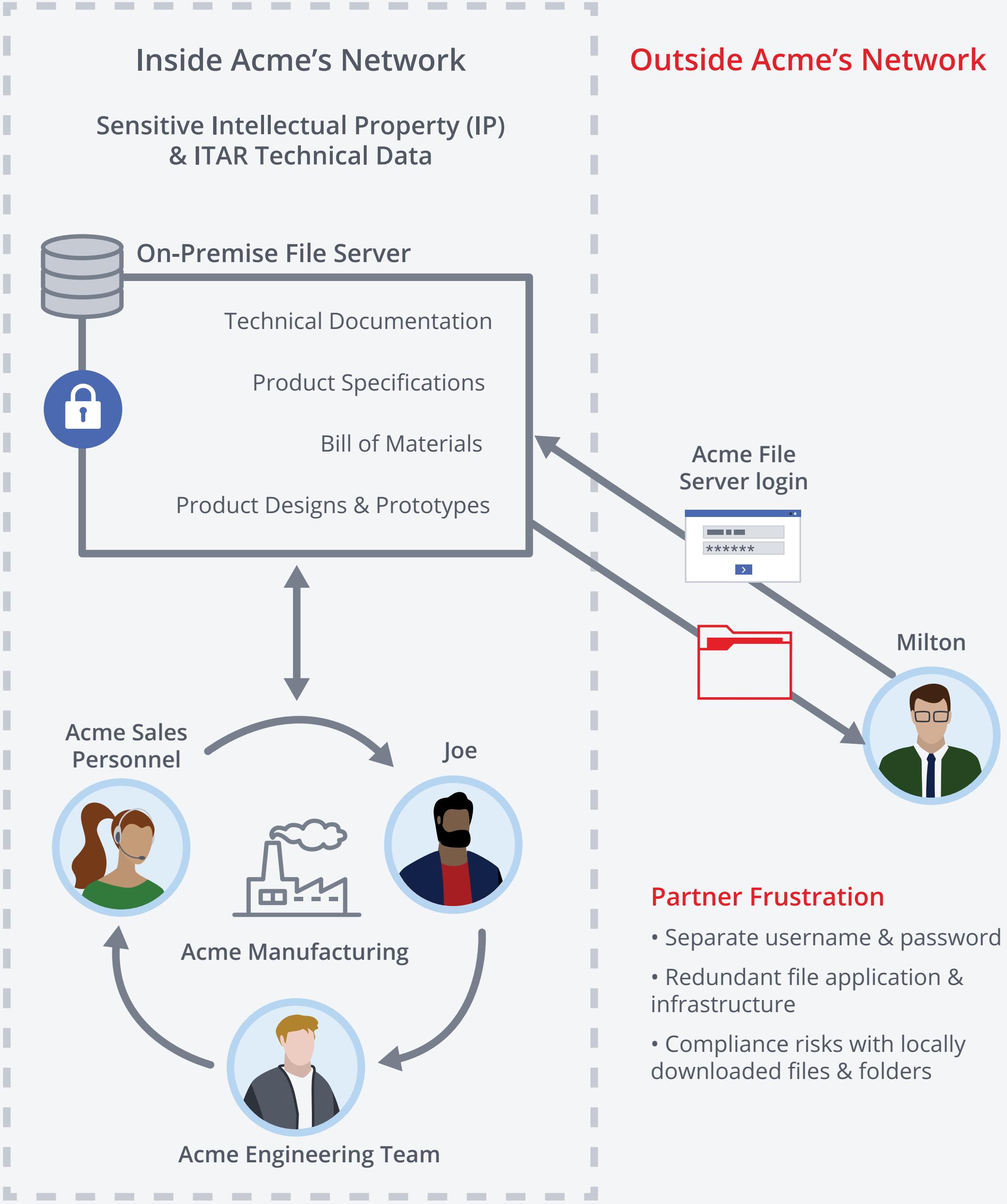
Milton feels frustrated and unproductive as these security measures and provisioning workflows waste time:

- Joe's delay in sending the documents sets back the project's kick off, costing them valuable time needed for their aggressive joint development and submission deadlines.
- Milton now has to manage a new account and learn a new workflow within Acme's file server, which is redundant with Initech's.
- Milton won't be the only Initech resource needed on the project, so Acme's decision to make him the only new account holder means Milton is now a bottleneck on development efforts.
- Milton has to consider sharing his new account credentials to facilitate collaboration vs. inherent ITAR compliance (and general security) risks in letting his team access his account.
- Milton anticipates the project will require a third partner, further down the supply chain, but dreads having to work through another provisioning workflow with Acme's IT team, taking even more time.

The Result

Neither organization will have control or visibility of project files as they collaborate on Project IDA, despite the secure on-premise server. As the submission deadline nears, the precious time lost is a point of friction between Initech and Acme. The Initech team prioritizes time-to-market over security and grows more careless as the bid deadline approaches—downloading files to desktops, sharing via email without end-to-end encryption, and using shadow IT to store the files within unknown environments that are not sanctioned by either organization.

Severe noncompliance and IP theft risks will continue throughout the project lifecycle. Even if they deliver the prototype and submit their bid on time, noncompliance penalties or stolen IP could easily wipe away any revenues gained from winning the contract.



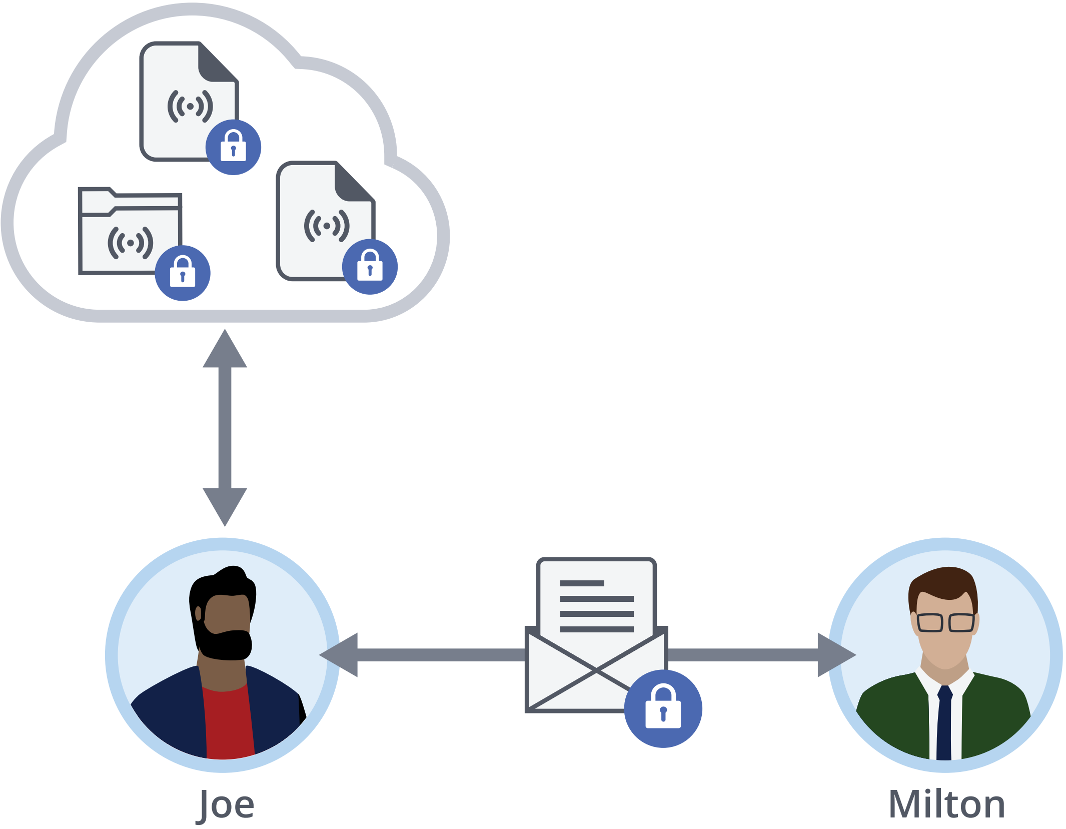
Partner Frustration

- Separate username & password
- Redundant file application & infrastructure
- Compliance risks with locally downloaded files & folders

A Better Way: The Data-Centric, User-First Approach

Virtru's email and file protections offer data-centric security via end-to-end encryption that prevents unauthorized access and enables persistent control and visibility. With data-centric security in place, protection, control, and visibility persist throughout the full lifecycle of the project, enabling more rapid collaboration workflows, without sacrificing security. Virtru's user-centric approach also ensures protections are embedded directly into Acme's G Suite workflows yet still protect files beyond G Suite, everywhere the file is shared.

Joe and Milton can now kick off the project immediately.

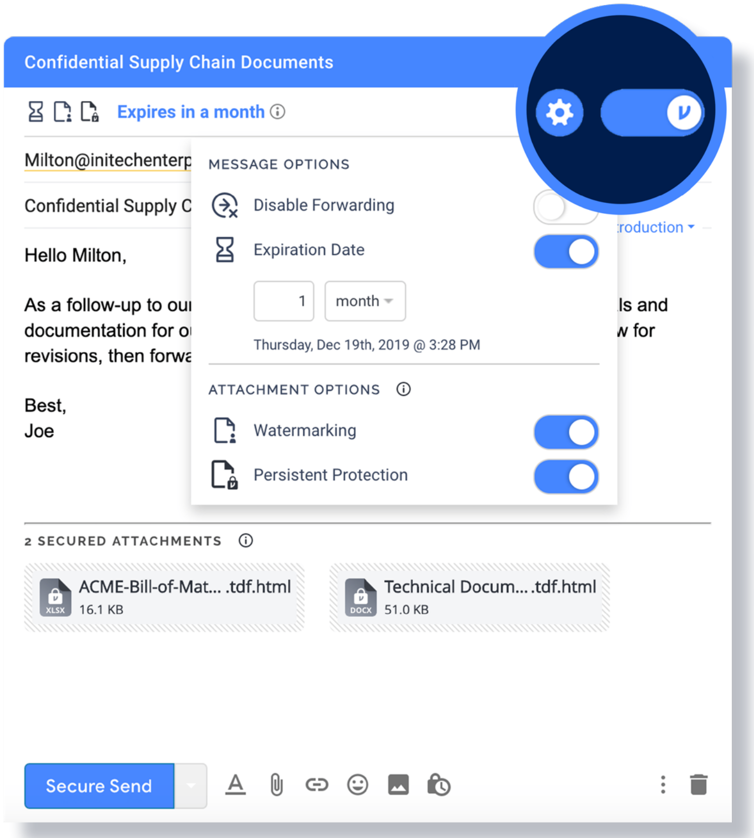


How the Users Feel Now

Joe feels EMPOWERED.

- Joe simply attaches the project files to a Gmail message and enables Virtru's end-to-end encryption to prevent access by any unauthorized party (including Google), ensuring ITAR compliance and IP protection.

- Using Virtru's granular access controls, Joe also:
  - Sets an expiration date for 3 months from now, after the length of the project.
  - Adds watermarking, which puts any recipients' name across the background of the file to deter them from leaking it.
  - Applies persistent protection, which keeps the file private and compliant even beyond the initial email to personal desktops, cloud content collaboration platforms, network drives, and more.
- With these granular controls, Joe can add both Milton and a skilled junior engineer at Initech as recipients, without burdening his IT team with new account provisioning workflows.
- Throughout the course of the project, Joe maintains ownership of the file, and can always adjust the access controls as collaboration needs evolve (for example, disabling forwarding beyond the initial collaborators).



Confidential Supply Chain Documents

Expires in a month

Milton@initechenterp

Confidential Supply C

Hello Milton,

As a follow-up to our ls and
documentation for o w for
revisions, then forwa

Best,
Joe

MESSAGE OPTIONS

Disable Forwarding

Expiration Date

1 month

Thursday, Dec 19th, 2019 @ 3:28 PM

ATTACHMENT OPTIONS

Watermarking

Persistent Protection

2 SECURED ATTACHMENTS

ACME-Bill-of-Mat... .tdf.html 16.1 KB

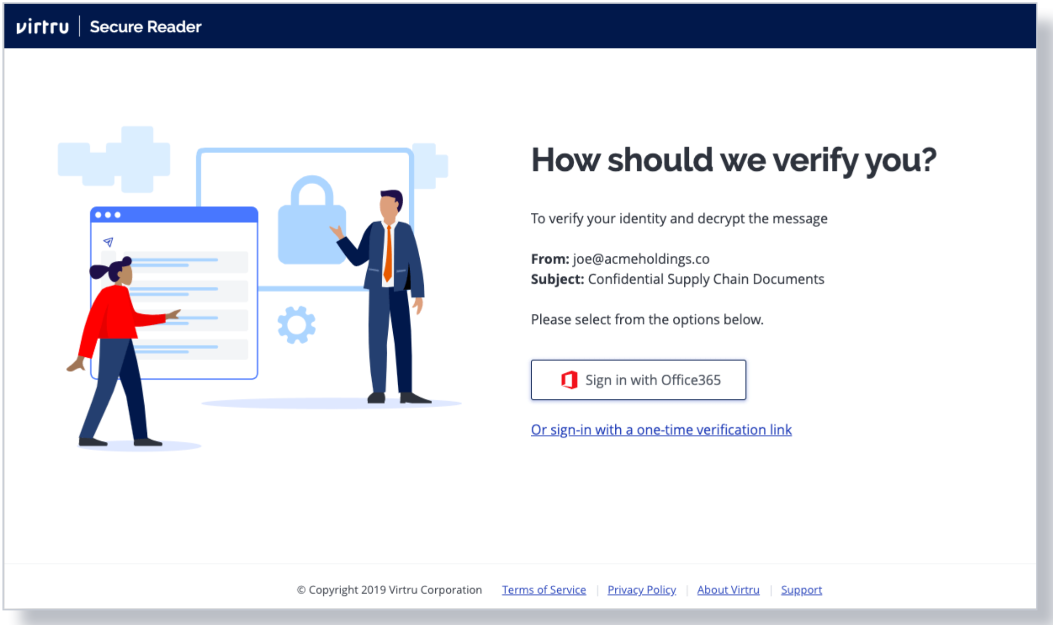
Technical Docum... .tdf.html 51.0 KB

Virtru's easy end-to-end encryption protects confidential, regulated project files as soon as they're attached to the Gmail message.

How the Users Feel Now

Milton feels CONFIDENT his team can deliver on the project's aggressive engineering timelines:

- Milton uses his existing workflows and applications for secure collaboration:
  - He doesn't have to create a new account to access the project files. He uses his existing Initech account within Office 365 to authenticate and access the files via the Virtru Secure Reader.
  - Milton can download the project files for storage in his engineering team's existing joint development network drive folder.
- Milton can add a third supply chain partner team to the project, simply notifying Joe of the needed personnel so Joe can grant secure access to project files.



How should we verify you?

To verify your identity and decrypt the message

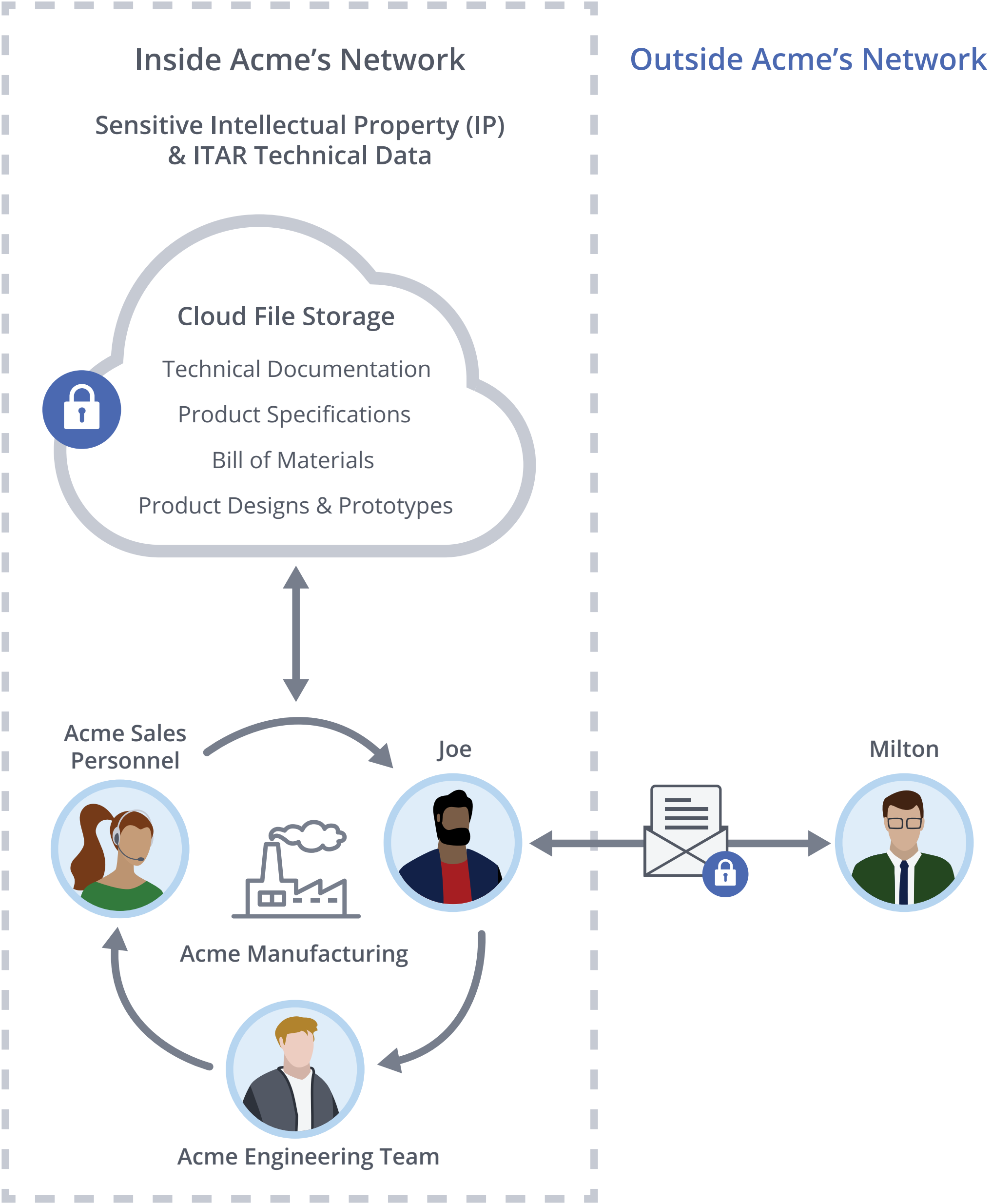
From: joe@acmeholdings.co
Subject: Confidential Supply Chain Documents

Please select from the options below.

Or sign-in with a one-time verification link

© Copyright 2019 Virtru Corporation | Terms of Service | Privacy Policy | About Virtru | Support

Virtru's user-first approach to collaboration enables easy access using existing accounts and credentials.



Inside Acme's Network

Outside Acme's Network

Sensitive Intellectual Property (IP) & ITAR Technical Data

Cloud File Storage

Technical Documentation

Product Specifications

Bill of Materials

Product Designs & Prototypes

Acme Sales Personnel

Joe

Milton

Acme Manufacturing

Acme Engineering Team

The Result

Instead of feeling frustrated and powerless at the beginning of the project, both Joe and Milton hit the ground running by securely sharing the initial project files, and any other confidential files used throughout joint development. As new personnel are added to collaboration workflows, Milton can reshare the file, while Joe has control to approve or deny access requests. Impacts to Initech and Acme's existing user workflows are minimized by Virtru's user-first approach.

Data-centric security enables fast, secure collaboration on Project IDA, giving Acme and Initech confidence that they'll deliver the project on time, without risking IP theft and noncompliance penalties in the process.

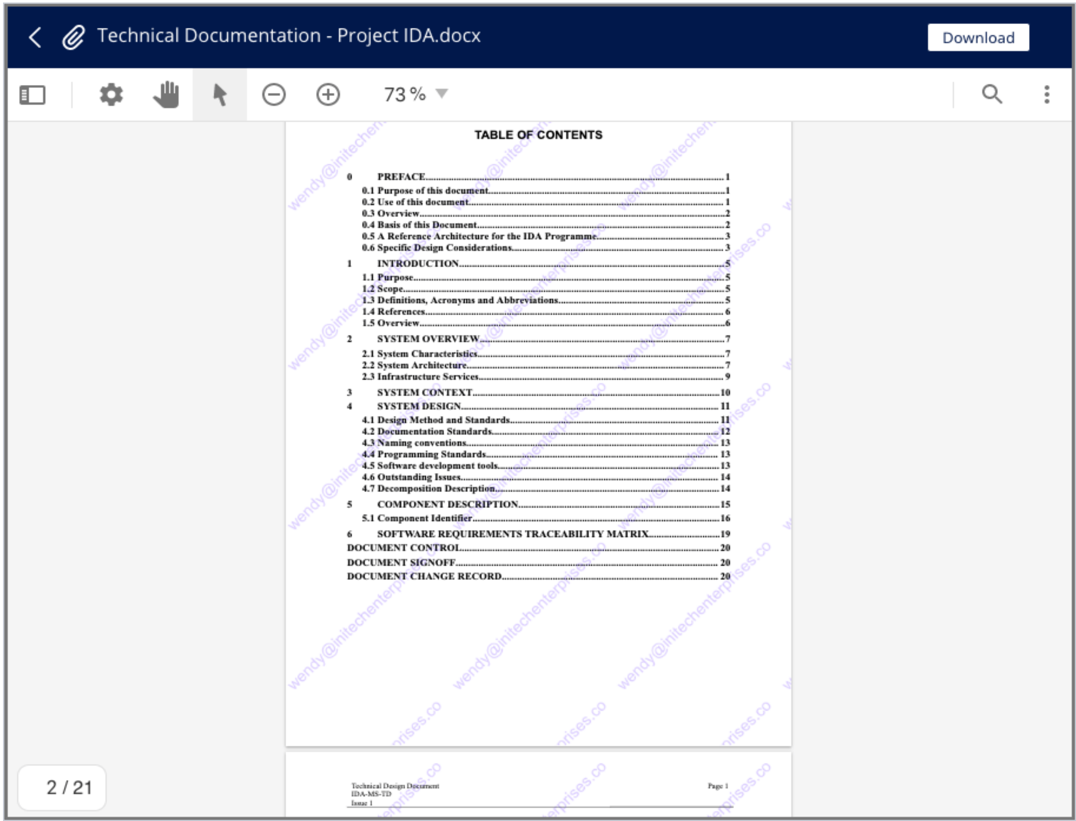

Technical Documentation - Project IDA.docx
Download
73 %
2 / 21
wendy@initechenterprises.co

TABLE OF CONTENTS

Technical Design Document
IDA-MS-TD
Issue 1

Page 1

The Virtru Secure Reader gives collaborators seamless access, while the file owner maintains control with persistent protection and watermarks that prevent leaks.

Security as a Competitive Advantage

Digital transformation brings plentiful opportunities to manufacturing organizations, but it also carries significant risks for privacy, IP protection, and compliance. As Acme's experience illustrates, traditional methods of protection don't support the dynamic, rapid collaboration workflows for manufacturing innovative products, leaving users frustrated and development timelines at risk.

Combining data-centric protections with a user-first approach to security gives manufacturing organizations a clear competitive advantage. IT and security teams can empower users with secure collaboration workflows that enable quick development of new products, while protecting sensitive data throughout the supply chain to reduce the risk of IP theft and noncompliance fines.

If your organization is interested in learning how Virtru can help modernize your operations, contact us to see how easy it is to keep your digital supply chain private and compliant. virtru.com/contact-us

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 20,000 organizations trust Virtru for data security and privacy protection.

Visit virtru.com or follow us on Twitter at @virtruprivacy.

virtru