CUSTOMERS

**95%**

WORRIED ABOUT HOW THEIR SENSITIVE INFORMATION IS HANDLED

COMPANIES

**41%**

HAVE OVER 1,000 SENSITIVE CONSUMER FILES UNPROTECTED

# SECURE DIGITAL TRANSPORT

## A BUSINESS STRATEGY FOR TRANSPORTING SENSITIVE CONSUMER INFORMATION

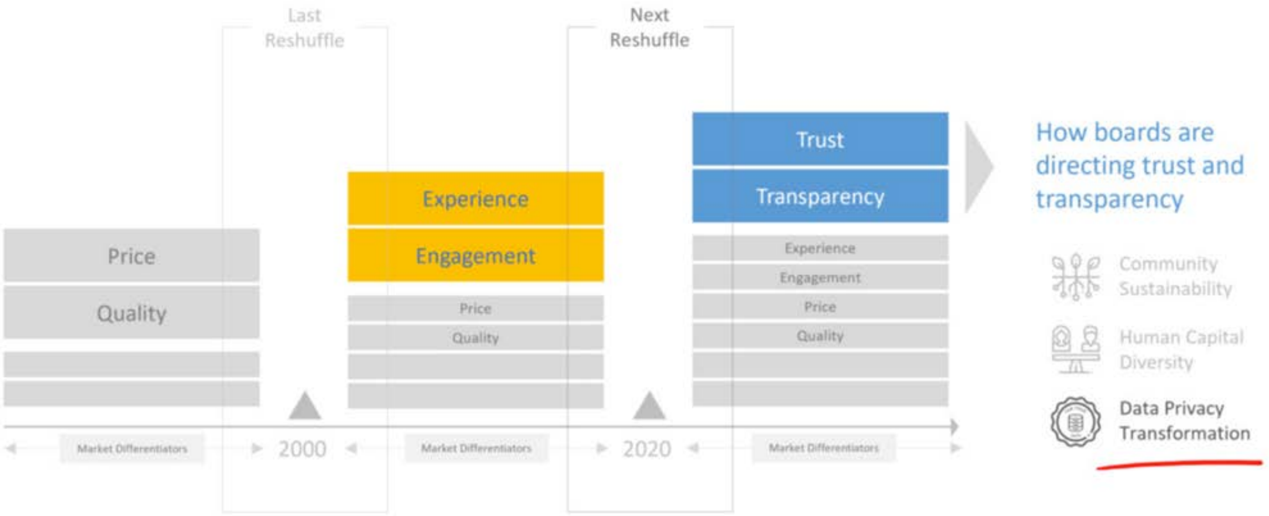
# SECURE DIGITAL TRANSPORT

Secure Digital Transport: is a segregated service to digitally transport and intelligently track data, enabling actionable logistics via a stateless environment where the connection between endpoints is dynamic and transactions are disposable. No external access is required to the endpoint delivery locations, endpoint storage locations are agnostic, leaving zero residual imprints.

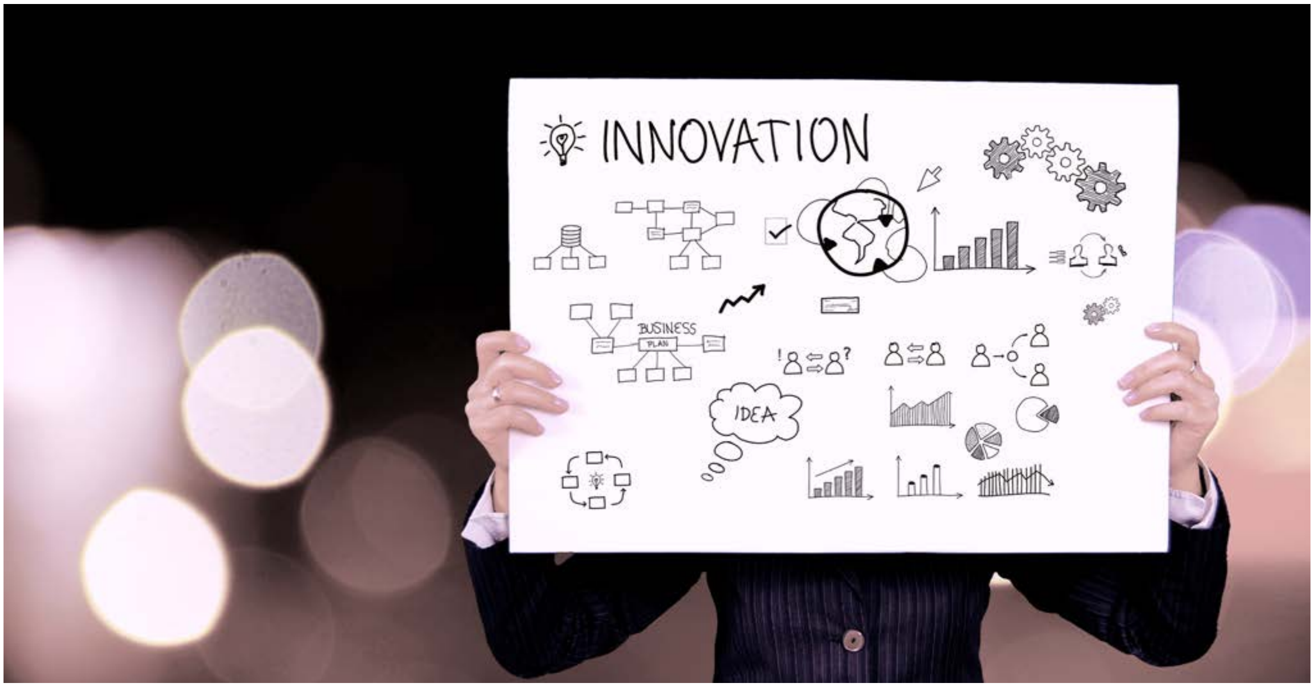
Secure Digital Transport is fundamentally a different way of thinking about data, the value of it, and how to transport it. It is difficult for most consumers and businesses to place a value on data, and so it often gets treated the same way as being either undervalued (or under classified) or overvalued (or over classified). Unlike physical documents, digital information has a tendency to be copied exponentially, and while this may be acceptable for things like family pictures which we would like to ensure are accessible from any device and shared as often as needed with friends and family, it is not appropriate for sensitive consumer information like PII, PHI, etc to be treated this way. Sensitive consumer data has real monetary value on the dark web for criminals, and the loss of it can have very negative consequences for consumers and businesses. Secure Digital Transport is a not just a technology. It is a business strategy for defining how sensitive data is transported.

# DATA PRIVACY IS THE NEW STRATEGIC DIFFERENTIATOR

With GDPR, numerous states in the US and other countries adopting similar privacy laws, there is a global adoption and heightened sense of awareness and urgency to protect sensitive consumer information. Within the first year (2018) of GDPR being in effect, companies like Facebook and Google were used as poster child examples to demonstrate that no business is immune from the responsibility they have of protecting consumer data. These companies and others are facing significant fines, congressional hearings and major lawsuits. Proactive companies have taken an offensive approach to data privacy and are using it as a strategic differentiator, thereby significantly reducing their liabilities while simultaneously increasing customer loyalty and market share.



# DISRUPTIVE INNOVATION AND PRIVACY



Disruptive innovation will continue to have a significant impact on privacy, for either good or for bad. Secure Digital Transport (SDT) is a positive force multiplier for privacy and analogous to Armored Transportation (i.e., Brinks). SDT is allowing companies to transport data and documents in and out of their systems without anybody ever having to log into those systems, all being accomplished with end-to-end encryption without pins, passwords, logins, accounts, apps or software to download. Furthermore, upon delivery the encrypted container and all the data within it evaporates. SDT is being referred to as a secure digital FedEx for data.

## Secure Digital Transport Three Core Features:

POINT DELIVERY SYSTEM

ENDPOINT STORAGE AGNOSTIC

ZERO RESIDUAL FOOTPRINT

# POINT DELIVERY SYSTEM

Point Delivery System: A segregated service to digitally transport data with end-to-end encryption via a stateless environment where the connection between endpoints is dynamic and transactions are disposable.

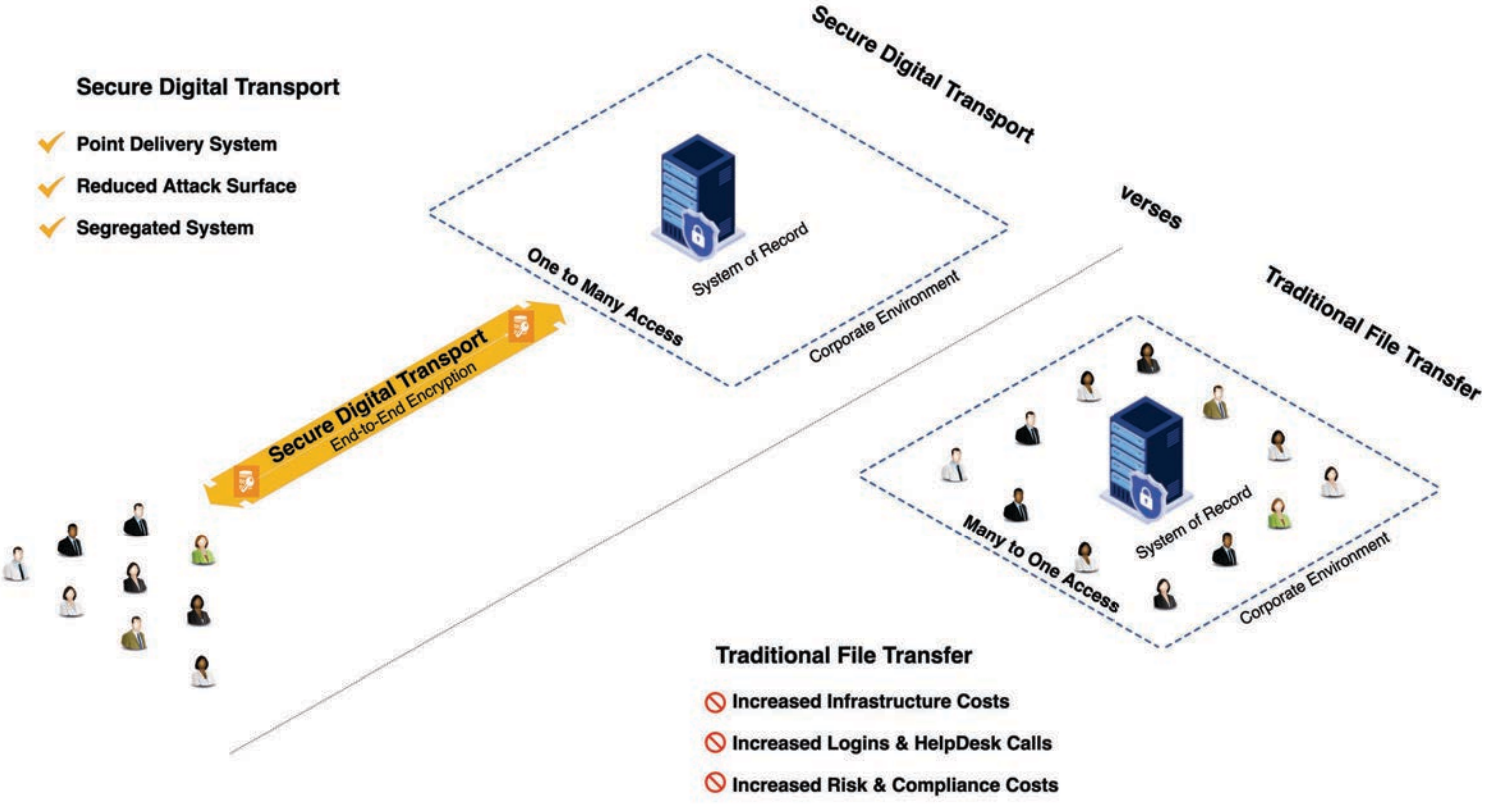
## Sending vs Sharing

The true need for sharing in a technological sense requires two or more parties on the same system at the exact same time for the simultaneous exchange of data. It's a true collaborative environment. Although that situation is needed, over 95% of the time when that sharing requirement was in place, nothing actually needed to be shared, only picked up or dropped off. Now because of SDT, "sending" is different. Sending removes one of the parties from the equation, and the party on the system utilizing SDT can remote collect and send to the other party without imposing that sharing requirement.

SDT enhances customer engagement experiences by reducing transactional friction. Companies who deploy SDT are able to transport data and documents in and out of their systems without anyone having to log into their systems. Asking consumers to log into portals is equivalent to asking them to drive to the post office to drop off a package. SDT providers have the ability to engage with consumers in the way they want (i.e. texting and instant messaging applications) with minimal friction. Having to download special apps or setup login accounts to access secure portals and emails which they may never use again, is simply not convenient and exposes consumer data to unnecessary risks.

SDT enables companies to ensure the highest levels of security and privacy while providing the highest levels of consumer convenience.

# POINT DELIVERY SYSTEM



**Secure Digital Transport**

- ✓ Point Delivery System
- ✓ Reduced Attack Surface
- ✓ Segregated System

**Traditional File Transfer**

- ⃠ Increased Infrastructure Costs
- ⃠ Increased Logins & HelpDesk Calls
- ⃠ Increased Risk & Compliance Costs

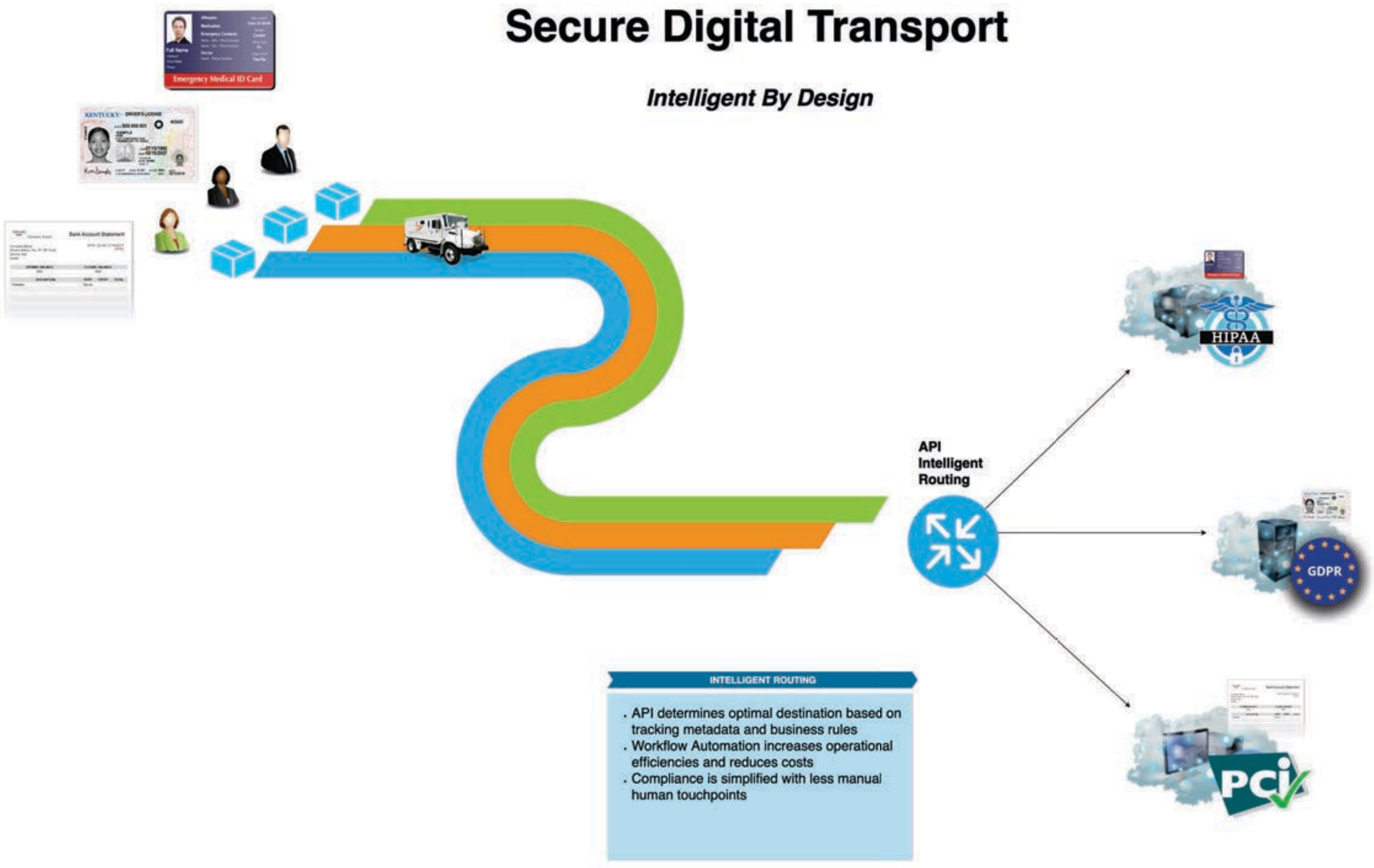
# ENDPOINT STORAGE AGNOSTIC

Endpoint Agnostic: The transportation system does not impose temporary or permanent storage limitations, and enables automated, intelligent routing of data (using tracking metadata) directly to the optimal location or System of Record (SOR).

In the early 2000s, numerous Managed File Transfer (MFT) vendors emerged to provide IT with a way to centralize B2B file transfers and address the deficiencies of legacy protocols like FTP (1971) and SMTP (1982), as well as new protocols like AS2 and ebXML. These solutions are typically on-premises hardware/software solutions which carry heavy upfront and on-going maintenance costs, typically require system integrators and consultants for implementation, and require additional IT staff for on-going support. While sometimes necessary for large enterprises with complex B2B file synchronization needs, it is often overkill for sending and receiving sensitive information with the consumer. In addition, these vendors often rely on a file sharing model in which all data is centrally located in a separate system on-prem or in the cloud. These systems themselves become High Value Targets for hackers and impose friction for users accessing them (logins, apps, etc). Although MFT technologies may solve one set of problems, they introduce an entirely new set of issues to contend with, while increasing costs and risks for the business and creating unnecessary friction for consumers.

With SDT, there is no need to maintain a master controller of encryption keys, passwords and routing information. The intelligence (tracking metadata) is embedded into each transaction and available indefinitely via an API call if needed for auditing or other purposes. This approach allows systems to intelligently route data from the consumer directly to the optimal location or System of Record (SOR), based on Technology/Infrastructure, Operations and/or Security requirements.

# ENDPOINT STORAGE AGNOSTIC



Secure Digital Transport

*Intelligent By Design*

API Intelligent Routing

INTELLIGENT ROUTING

- API determines optimal destination based on tracking metadata and business rules
- Workflow Automation increases operational efficiencies and reduces costs
- Compliance is simplified with less manual human touchpoints

# ZERO RESIDUAL DIGITAL FOOTPRINT

Zero Residual Footprint: Items are temporarily stored during transport and then securely removed once delivery is confirmed. A single chain of custody between pickup and delivery points where duplicate copies are not created as part of the process.

Current means of digital transportation (fax, ftp, secure email, portals, etc.) inherently have an exponential data multiplication effect, resulting in “poisonous breadcrumbs” being left behind (residual digital copies). As seen in the diagram on page 9, most of these forms of digital transportation leave at least five (5) copies behind, typically unsecured. Imagine what would happen if an armored service provider like Brinks made multiple stops and left valuable goods along the away! They would not have been in business since 1859.

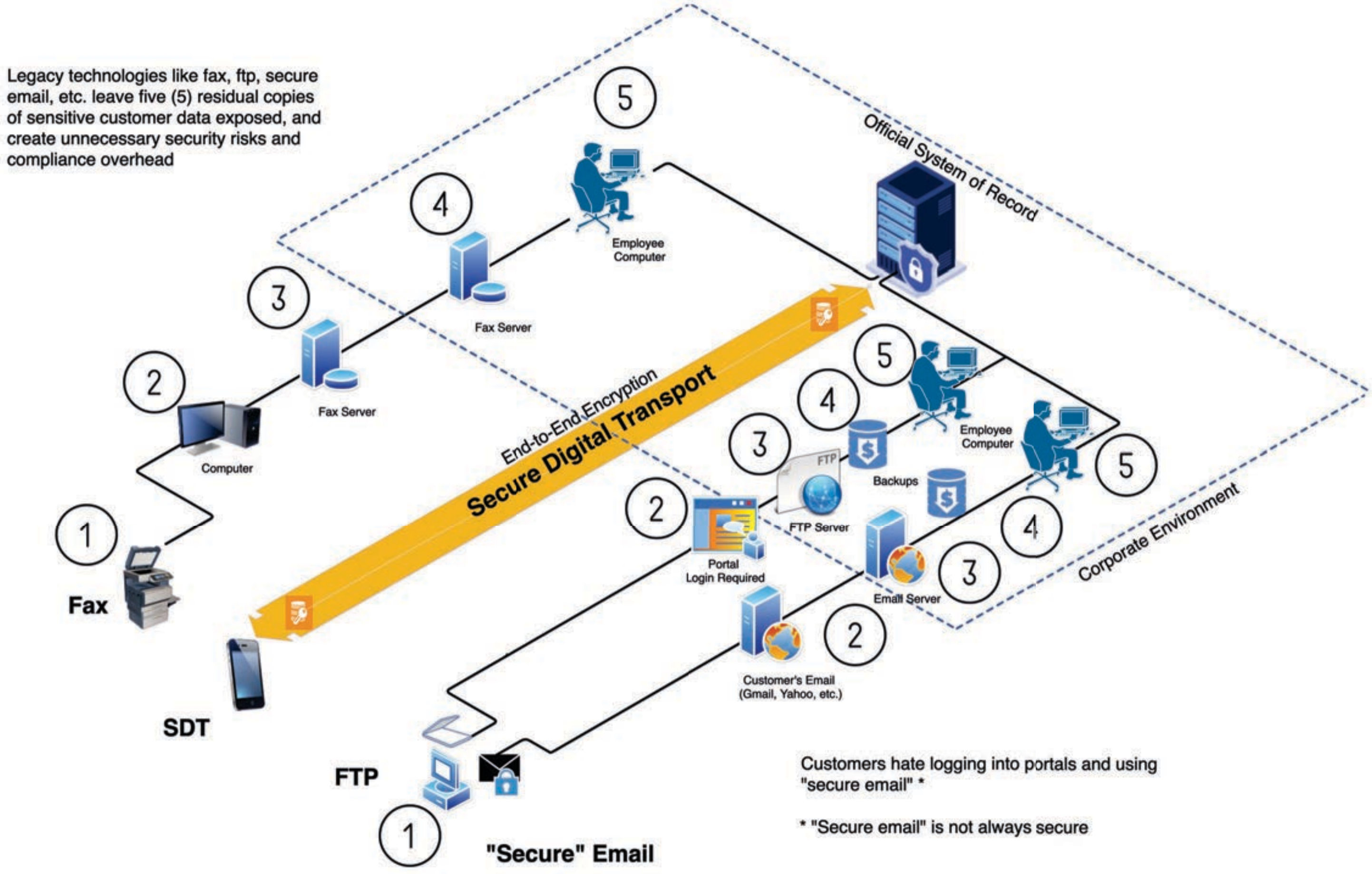
SDT providers deliver the same confidence and peace of mind for securely transporting sensitive digital information as Brinks does for transporting high value physical goods. Because SDT is transporting and not storing the data, there is minimal risk exposure from a security and compliance perspective.

Companies can significantly reduce their risk and scope of compliance by using SDT, instead of exposing a company’s entire environment to stringent regulations like PCI, HIPAA, GDPR, and FERPA.

"The Healthcare industry has a multifaceted problem with mail, in both electronic and printed form. The industry is not immune to the same illnesses we see in other verticals such as the very common scenario of phishing emails sent to dupe users into clicking and entering their email credentials on a phony site. The freshly stolen login information is then used to access the user’s cloud-based mail account, and any patient data that is chilling in the Inbox, or Sent Items, or other folder for that matter is considered compromised – and its disclosure time."

- Verizon 2019 Data Breach Investigations Report

# ZERO RESIDUAL DIGITAL FOOTPRINT



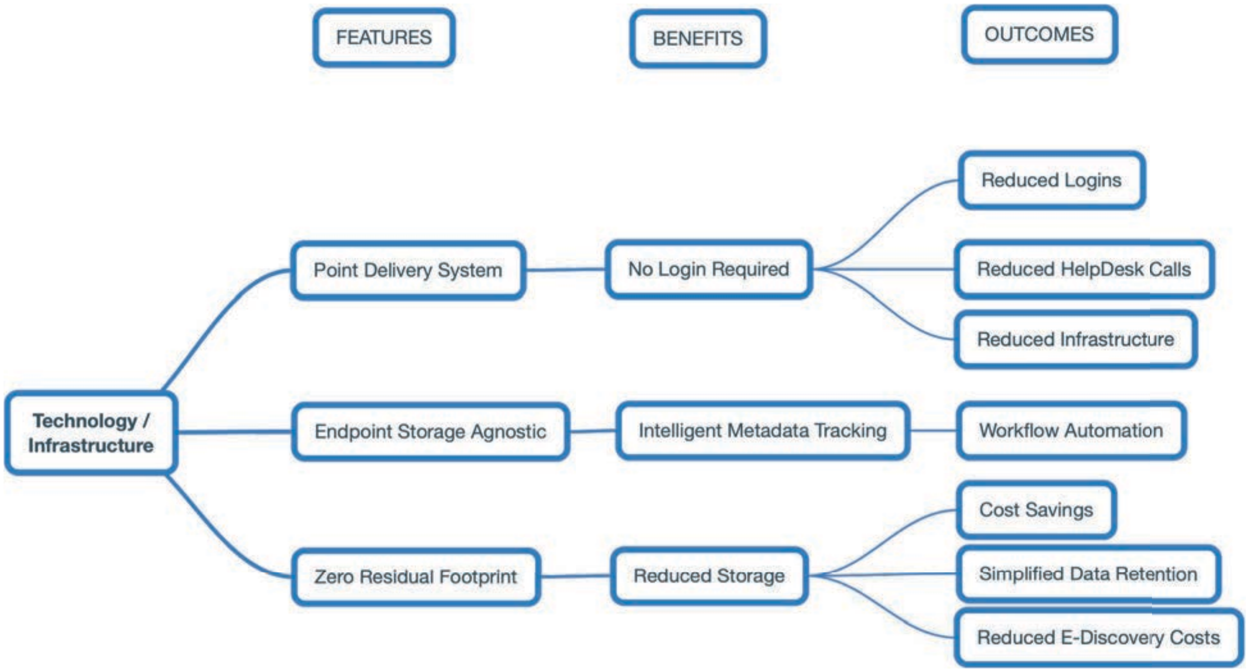
Legacy technologies like fax, ftp, secure email, etc. leave five (5) residual copies of sensitive customer data exposed, and create unnecessary security risks and compliance overhead

Customers hate logging into portals and using "secure email" *

* "Secure email" is not always secure

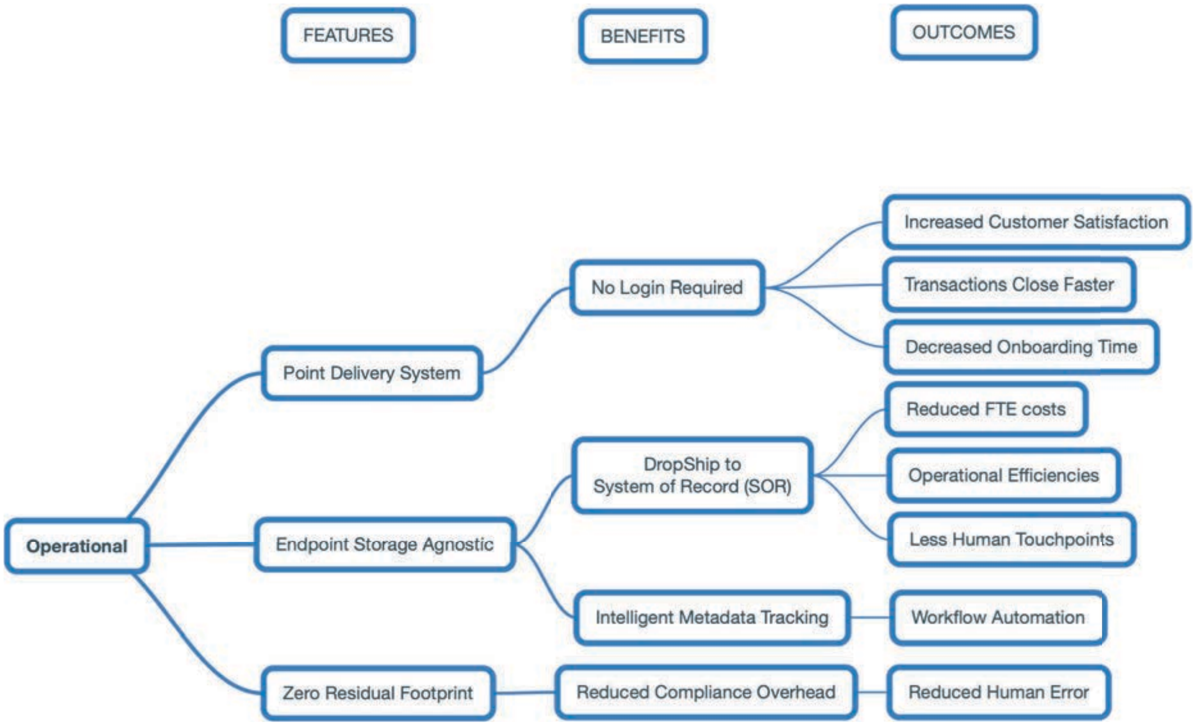
SDT = No PINS, Passwords or Logins

# TECHNOLOGY / INFRASTRUCTURE SDT BENEFITS



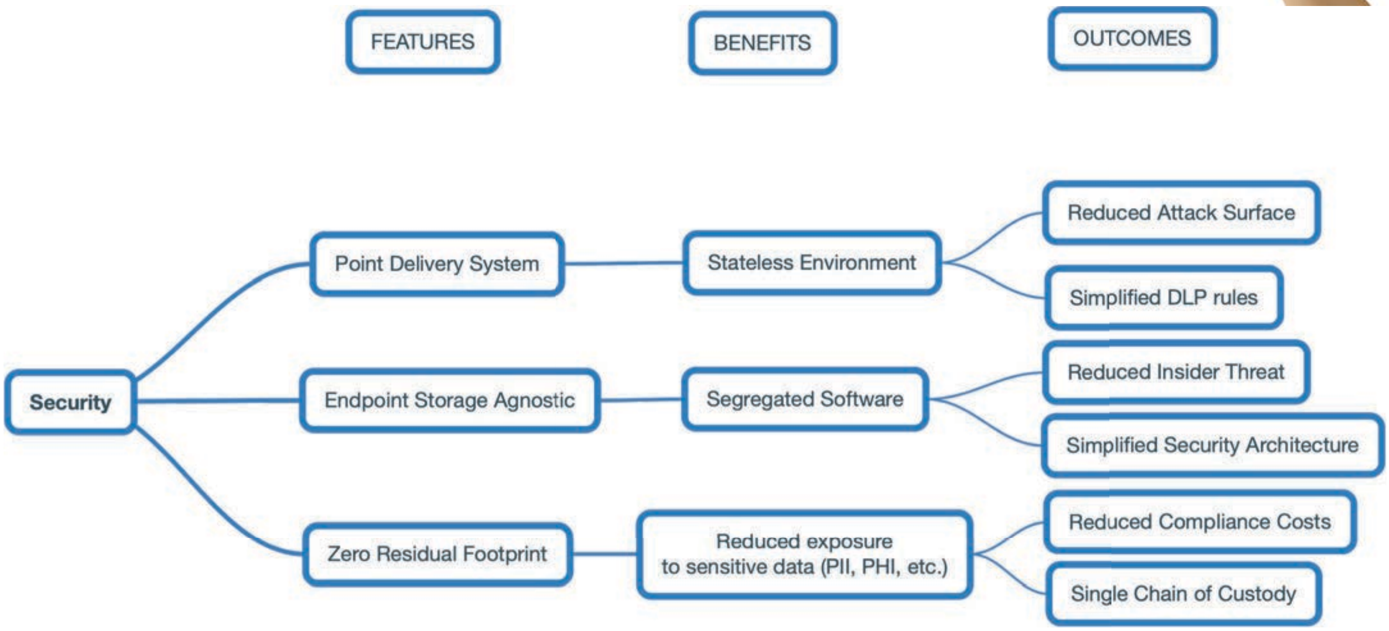
For CIOs and CTOs, the primary benefit of SDT is simplification. Because consumers are not logging into systems, logins are significantly reduced and subsequently HelpDesk calls are as well, thereby reducing overall IT costs including infrastructure. In addition, because sensitive data is only stored in the official System of Record and not on employee desktops and random file shares, overall data retention is simplified and E-Discovery costs can be significantly reduced.

# OPERATIONAL SDT BENEFITS



For COOs and CFOs, SDT provides direct ROI through cost savings and operational efficiency gains. By leveraging tracking metadata intelligence, the business is able to implement workflow automation to reduce manual human efforts and associated errors. This results in decreased onboarding times for new customers, transactions closing faster and overall increased customer satisfaction and retention.

# SECURITY SDT BENEFITS



Security

| FEATURES | BENEFITS | OUTCOMES |
|---|---|---|
| Point Delivery System | Stateless Environment | Reduced Attack Surface<br>Simplified DLP rules |
| Endpoint Storage Agnostic | Segregated Software | Reduced Insider Threat<br>Simplified Security Architecture |
| Zero Residual Footprint | Reduced exposure to sensitive data (PII, PHI, etc.) | Reduced Compliance Costs<br>Single Chain of Custody |

For CISOs, SDT is a Swiss army knife which can be used multiple times throughout the business to improve the overall security posture and enable business transformation. Since SDT is a stateless and segregated environment, the company's overall attack surface is reduced, thereby simplifying the security architecture and reducing overall risks. By reducing exposure to sensitive data, insider threats are also reduced and more easily detected by simplified DLP rules. Since SDT minimizes manual human touch-points and provides a single chain of custody, compliance attestation is also simplified.

# A Note to CISOs

We know that being a Chief Information Security Officer is not easy. New threats, regulations and technologies are constantly emerging, and because security impacts all areas of business, it's difficult to prioritize what's really most important. SDT is not just another point security technology or an additional layer of defense. It is a paradigm shift in how businesses engage consumers and handle their most sensitive data. It's a strategic enabler for the entire business.

**Common challenges facing most CISOs**
Let’s face it, most CISOs share the same challenges of never having enough budget for the people or technology they feel is needed to adequately protect the organization. In most organizations, security budgets are considered to be "just another expense required to do business” and are difficult to demonstrate quantifiable ROI. The term “defense in depth” typically translates to “expense in depth” for many CFOs who find it frustrating to quantify the value of cybersecurity.

**A paradigm shift in security economics**
A CISO should spend 20% of their most valuable investment on thinking and investing strategically in the business as opposed to keeping up with (researching, testing, implementing and maintaining) the newest security technologies which provide minimal (if any) improvements in risk mitigation to the business?

**What would this look like?**
Forward thinking CISOs use their most precious commodity (time) to understand what is really important to the business and are champions of disruptive security innovation that also drives business transformation. These CISOs will be considered invaluable internal consultants by the business and will be consulted with early and often on major decisions impacting the business. From strategy of new products and services to mergers and acquisitions, these CISOs will truly “have a seat at the table” while most of their peers will not.

**CISOs using SDT as a strategy to enhance security are automatically enabling business transformation, and the smart ones do it without increasing their own budgets!**

# ABOUT BOTDOC

Botdoc is a Secure Digital Transport provider.

Botdoc provides a streamlined and secure process for transporting data and documents with end-to-end encryption, without pins, passwords, logins, accounts, apps or software to download. Furthermore, upon delivery the encrypted container and all of the data is securely erased. The API allows data to be transported directly in and out of the official system of record without anyone needing to login, making systems more secure, while transactions close faster with less human touch-points.

Every major system roadmap will include Secure Digital Transport in the next 3-5 years. A market-shift is already underway and Botdoc is pioneering what SDT is today and what it means in the future.

Join the movement today!

https://botdoc.io

BOTDOC·iO

GDPR COMPLIANT

AICPA SOC SOC2 CERTIFIED

HIPAA COMPLIANT

PCI DSS COMPLIANT

FERPA COMPLIANT

PRIVACY SHIELD CERTIFIED