

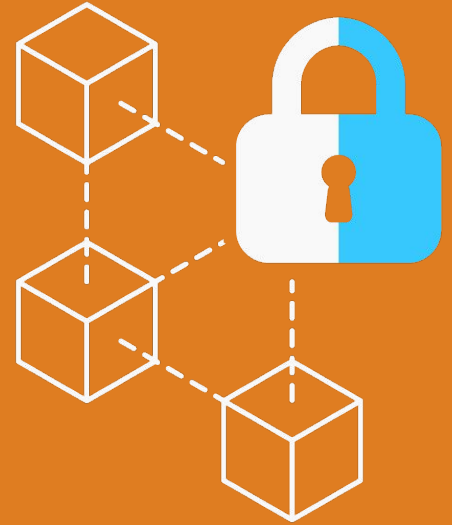
# indicio

**Security = Identity**  
**Identity = Security**

**Complete Zero Trust with  
Decentralized Identity**

Trevor Butterworth, Dr. Chase Cunningham, Will Groah

**V1.01 May 17, 2024**



# Overview

Zero Trust and Decentralized Identity emerged as responses to the escalating problems of data breaches and identity theft.

## Zero Trust

- Trust no one inside or outside a network security perimeter.
- Continuously verify for access to all network resources.
- Make access to network resources narrow.

## Decentralized Identity

- People hold and share data using verifiable credentials.
- No need for centralized databases to store personal data.
- Cryptography and digital signatures authenticate the source of the credential and indicate if it has been altered.
- No need for logins and passwords.
- Devices and apps can be bound with biometrics and liveness checks.

**By combining Zero Trust and Decentralized Identity,** a network can be certain of the identities of those trying to access its systems and can manage continuous verification in a maximally frictionless way.

**Blocker:** Security and identity teams often have different organizational responsibilities when a strong security posture means that identity and security are inseparable.

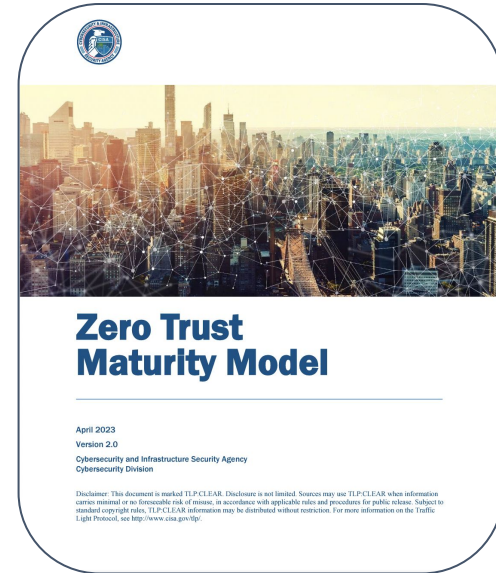
**Solution:** Implementing decentralized identity and verifiable credentials allow Zero Trust to be fully embraced, implemented, and extended.

**Recommendation:** Indicio Proven<sup>®</sup> is a complete, interoperable solution for decentralized identity and verifiable credentials that is quick to deploy, easy to scale, and works with any existing system.

# The critical challenges for Zero Trust

What happens if an employee or user's identity has been stolen or faked?

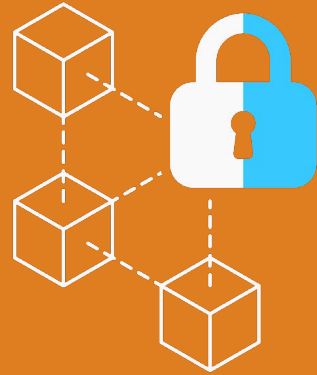
- Storing personal data in centralized databases for identity and access management puts masses of identity data at risk of theft.
- The reliance on email usernames and passwords as login credentials provides a constant route for phishing attacks
- Usernames, passwords, multi-factor authentication deliver poor user experiences when expectations are for contactless and seamless processes.
- All it takes is one user identity to be compromised to breach a security perimeter.
- Centralized identities are a permanent risk in any Zero Trust implementation.
- Only Decentralized Identity can provide the authentication needed for Zero Trust to be truly effective.
- Decentralized Identity can manage biometric authentication in a way that addresses challenge of generative AI.



The White House, through Executive Order (EO) 14028, 'Improving the Nation's Cybersecurity,' has pushed government agencies to adopt Zero Trust cybersecurity principles — [link](#).

# indicio

## What is Decentralized Identity?

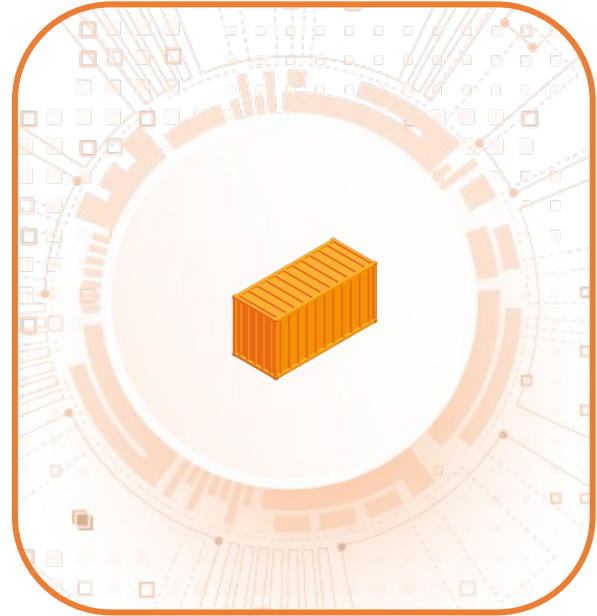


## Decentralized Identity is implemented using verifiable credentials

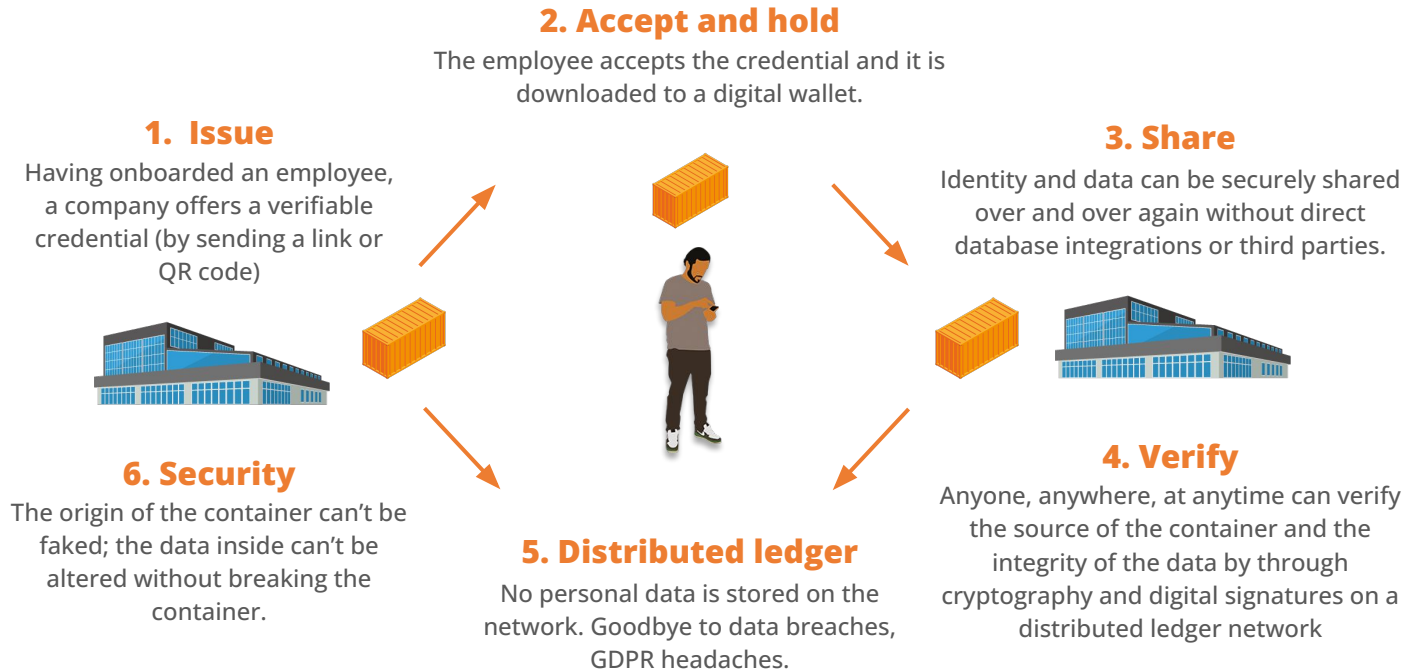
People, organizations, and devices can hold their own identity data by using verifiable credentials. And they can prove they own these credentials. This makes identity and access management more secure and more easily locked down as data doesn't need to be replicated everywhere.

A verifiable credential is like a container that can seal any kind of digital information.

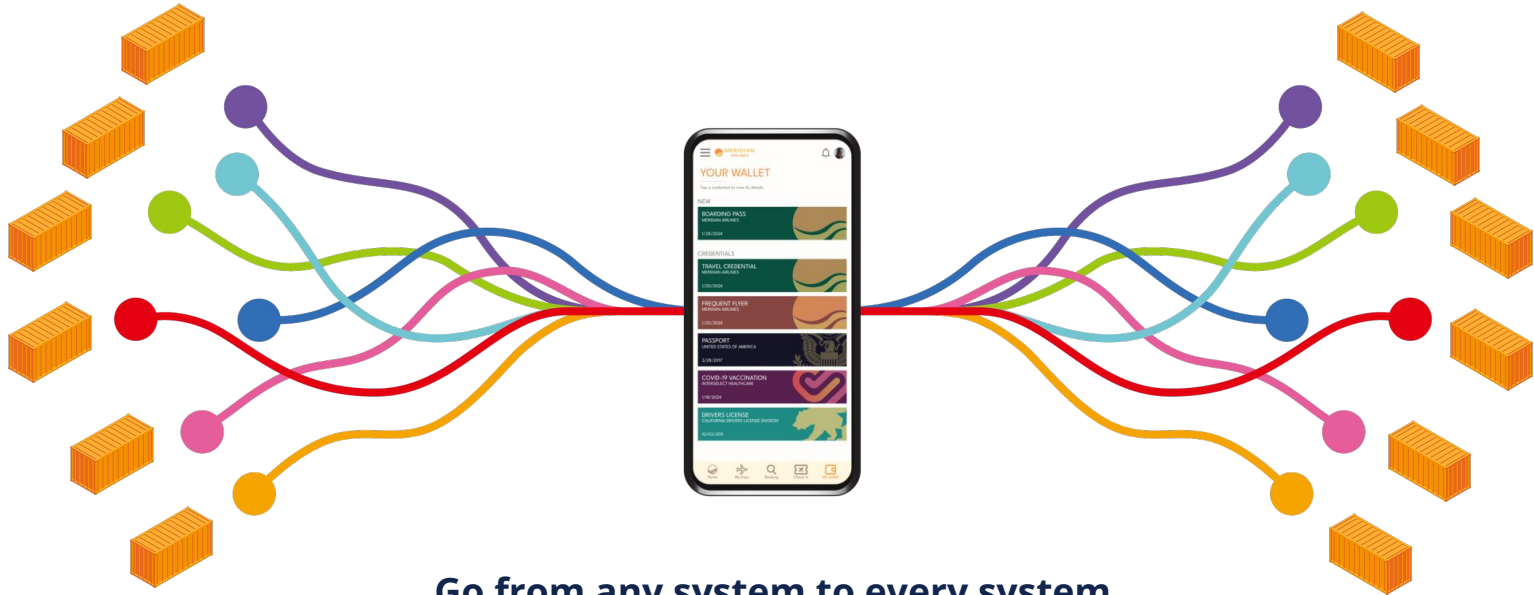
- The source of the container is always knowable.
- The contents of the container cannot be altered without breaking the seal.
- A trusted source means trustworthy contents.
- Decentralized identity makes trust portable.
- Portable trust enables immediate action, automated decision making
- Verifiable credentials are reusable — they can be programmed to expire, and they also can be revoked.



# How a verifiable credential for employee access works in six steps



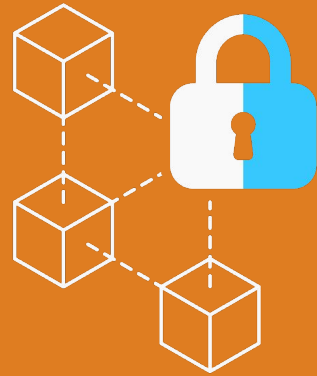
Verifiable credentials can be used to share data and identity across systems without the need for direct integration



**Go from any system to every system**  
**Act immediately on verified data and identities**

# indicio

Using Indicio Proven<sup>®</sup>  
for Zero Trust



## Indicio Proven® is the leading global solution for implementing a company's Zero Trust architecture using verifiable credentials

Quickly verify information about employees with tamper-proof verifiable digital credentials.

Manage employment status of contractors and gig workers no matter where they are located.

Revoke or reissue credentials if they expire, the employee leaves the company, or if a security issue is identified.

Credentials can also be used to simplify enrollment with external payroll and benefits providers.

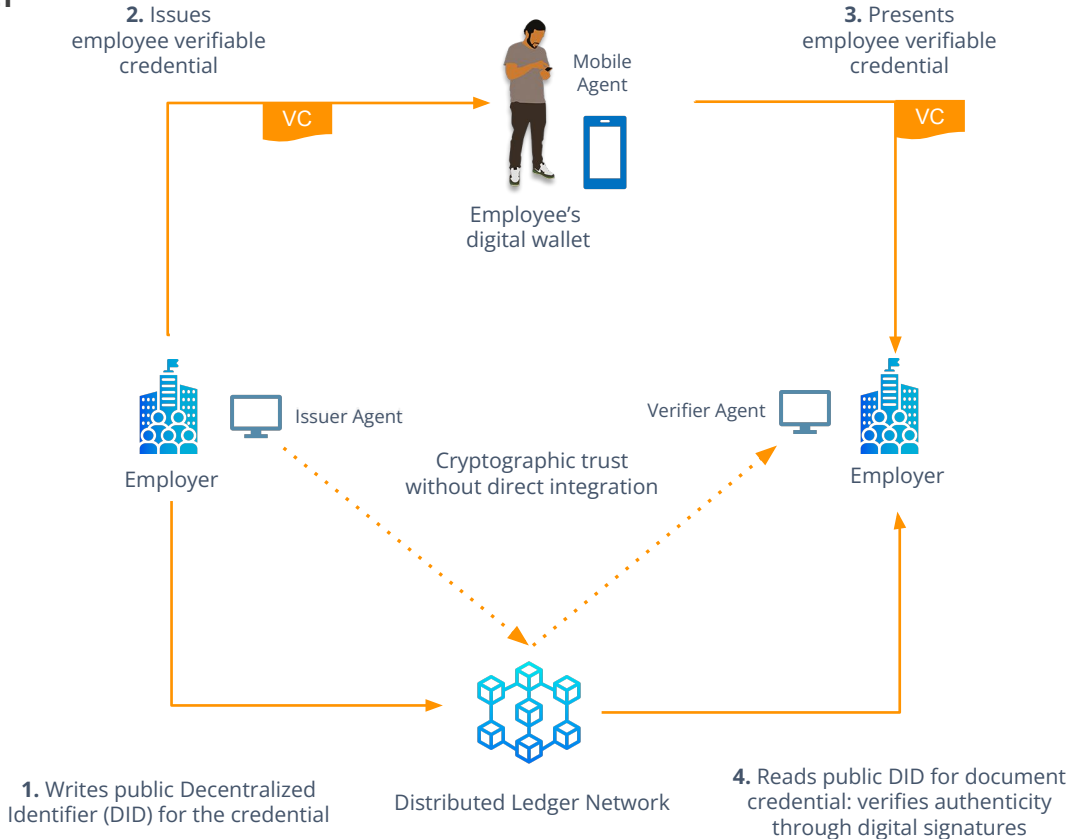
# 1. Verify every employee or user

Whether entering a facility, accessing a network resource, or a zoom meeting, a verifiable credential provides seamless, fraud-resistant authentication.

Verifiable credentials are anchored to decentralized identifiers or "DIDs." DIDs refer to people, organizations, devices and allow identity to be decoupled from centralized registries, identify providers, or certificate authorities and be under the control of the DID owner.

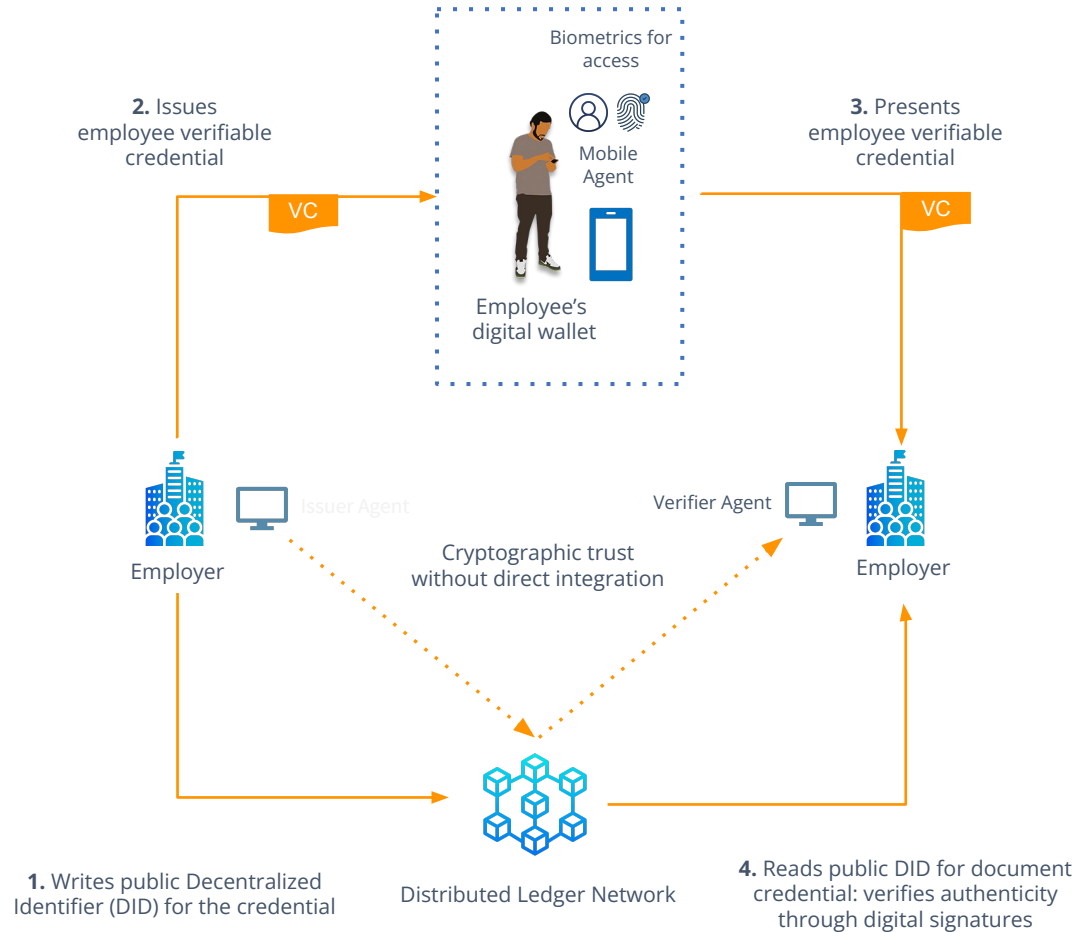
For more on DIDs and how they transform identity, see Indicio's [A Beginner's Guide to Decentralized Identity and Verifiable Data](#) and the [W3C DID specification](#).

The distributed ledger provides keys and schemas for instantaneous cryptographic validation of the credential.



## 2. Validate devices

Liveness and biometric checks implemented during credential issuance control access to both the employee's device and their digital wallet.

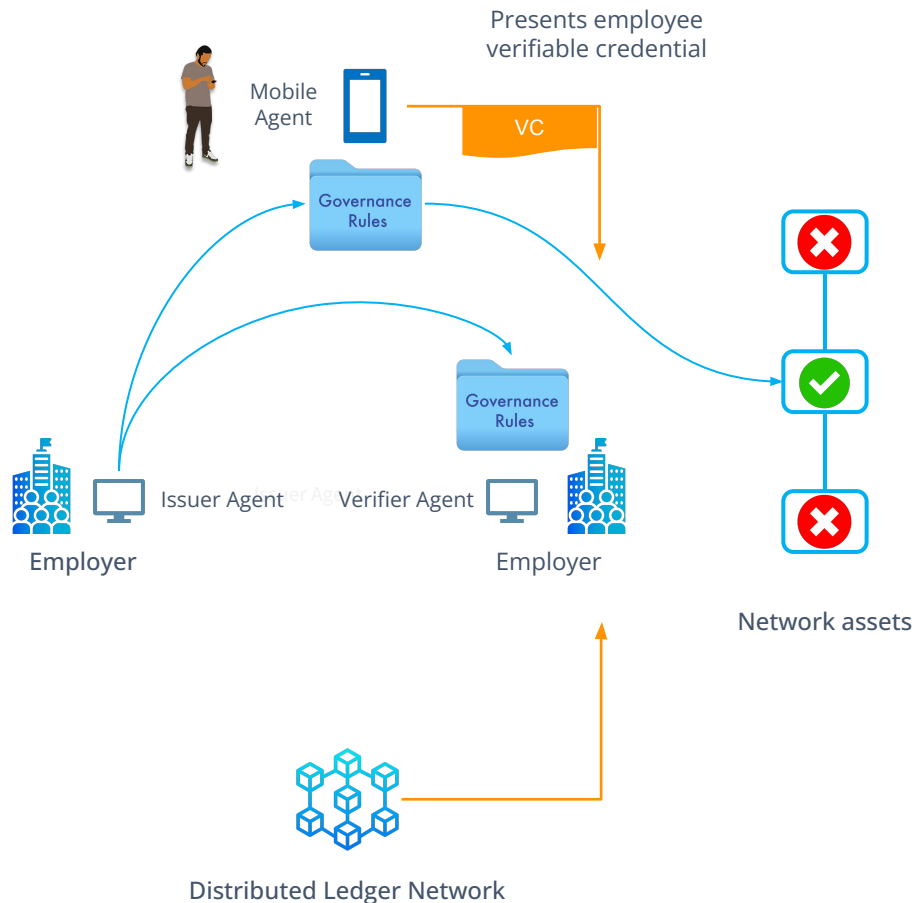


### 3. Limit access (and automated decision making)

Access and micro segmentation can be managed in different ways. Use different credentials for different employees or use governance rules published and stored in the verifier agent software to control specific access points.

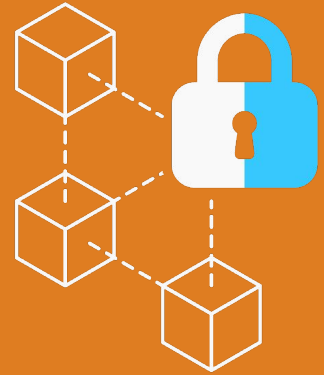
Indicio Proven<sup>®</sup> comes with a governance editor for writing governance rules and a governance interpreter for operationalizing them.

This means that information flows and decision-making can be automated.



# indicio

Take the next step in Zero Trust  
with Decentralized Identity



## Zero Trust + Decentralized Identity = digital transformation

Decentralized identity technology removes the Achilles heel of centralized identity from Zero Trust and it provides an efficient, effective, and easily implementable way to meet the need for continuous authentication.

In “completing” Zero Trust, decentralized identity also allows Zero Trust to be extended beyond network security — to see everything as a continuously evolving system of overlapping networks sharing verifiable data through verifiable identities.

People, companies, organizations, government agencies, and connected devices can all be continuously verified and hold and share verifiable data.

Indicio Proven's® award-winning technology is the choice of global enterprises who need flexible, interoperable, and powerful verifiable data and identity solutions that will work with any system and at any scale. Contact us to learn more, see a demo, workshop your path to getting the most out of Zero Trust and Decentralized Identity.

“The ability to confidently and continuously authenticate identity and data realizes the original vision of the internet and brings us to the next stage of the web — an open digital landscape for people and organizations to connect, trust, and prosper.”

— Heather Dahl, CEO, Indicio

## Resources

Want to understand the basics of Decentralized Identity? Check out Indicio's [A Beginner's Guide to Decentralized Identity and Verifiable Data](#)



Dr. Chase Cunningham — “Dr. Zero Trust” writes for the Indicio Blog on [Decentralization and the Future of Enterprise Security](#). Also, listen to — [Dr. Zero Trust's Podcast](#)



**Key Indicio articles on Decentralized Identity, Zero Trust, and enterprise security.**

[Zero-Trust Practices with DIDComm - Indicio](#)

[How Verifiable Credentials Can Handle the Threat of Deepfakes in KYC - Indicio](#)

[The Indicio Proven Blueprint for Creating a Trusted Data Strategy](#)

## About the Authors



Trevor Butterworth is a co-founder of Indicio and Vice President of Communications & Governance. As part of his communications portfolio, he serves as chief writer and managing editor for Indicio's written content and communication, including presentations, website content, blogs, and white papers. His focus is both on explaining the technology to non-technical audiences and envisioning how it can be used to drive innovation.

He is the author of Indicio's Beginners Guide to Decentralized Identity and co-author of Indicio's position paper, "A Trusted Copilot: Using decentralized identity to manage an AI virtual assistant."

Trevor Butterworth is a co-founder of Indicio and Vice President of Communications & Governance. As part of his communications portfolio, he serves as chief writer and managing editor for Indicio's written content and communication, including presentations, website content, blogs, and white papers. His focus is both on explaining the technology to non-technical audiences and envisioning how it can be used to drive innovation.

He is the author of Indicio's Beginners Guide to Decentralized Identity and co-author of Indicio's position paper, "A Trusted Copilot: Using decentralized identity to manage an AI virtual assistant."

Trevor is also responsible for Indicio's governance, Indicio Network's governance framework, and ensuring Indicio meets its corporate responsibilities as a public benefit corporation. He also works on developing governance for Indicio's customers. He is also on the Stewards Governance Committee of the Velocity Network.

Prior to Indicio, Trevor was a consultant to the Sovrin Foundation, and Director of Research at Cynja.tech. He was the founding Executive Director of Sense About Science USA, a nonprofit which developed innovative and collaborative projects on communicating the complexity of scientific and statistical evidence with, among others, the American Statistical Association, the Annals of Internal Medicine, The Broad Institute, Caltech, Harvard, MIT, Rockefeller University, Nature, and the Library of Congress.

He was a consultant to the American Statistical Association, and to Cornell University, where he provided communications support to the machine learning and evidence analysis element of CERES 2030, the flagship project for the United Nations' Sustainable Development Goal to achieve 'zero hunger' (SDG 2), which was supported by the Bill and Melinda Gates Foundation and BMZ Germany.

As a journalist, he has written for numerous publications, including the Financial Times, the Wall Street Journal, the Washington Post, the Atlantic, Forbes, Newsweek, and Vox. He has presented at many conferences and events and institutions, including the Ford Foundation, Hyperledger Global Forum, the US National Academy of Sciences, and the UN World Data Forum.

Trevor attended Trinity College Dublin (BA honors, M.Phil) Georgetown University, and Columbia University's Graduate School of Journalism (M.S.), where he received the Sevelon Brown Award. He was a visiting fellow at Cornell and an adjunct assistant professor for science communication in the department of Immunology at Trinity Biomedical Sciences Institute at Trinity College Dublin.

## About the Authors



Will Groah, is an Indicio board member, advisor, and investor, and plays a key role in shaping/supporting the company's evolution and delivering shareholder value. Supporting Indicio's board and executive team, and with the additional role of representing Indicio's preferred investors, he helps guide and support the company's executive team and the company's strategic vision.

Will is an experienced entrepreneur, advisor, private investor, and board member. With only \$1,000, he founded Technica Corporation, a U.S. defense and intelligence company, which he grew to over 300 people and \$150M in revenue before exiting. He served in all phases of the company in various board and executive roles, including Managing partner, COO, CFO, and CIO. He directly hired the first 50 people and all C-Level executives, created all company department operations, wrote and won all of the company's first, major, multi-year, multi-million dollar proposal submissions, and created and developed services and product divisions, employee and channel partner programs and team cultures.

As a private angel and LP investor/scout supporting several venture funds and networks, Will extends his expertise to a variety of ventures in FinTech, AdTech, SportsTech, health, and other companies aiming to improve national interests. Will is especially interested in companies contributing to Florida's economy and communities and in U.S. companies that have global reach capabilities through information technology, including decentralized technology, AI, AI/computer vision, and cyber security architectures, and which are aimed at addressing significant market challenges. His active involvement in helping companies define investable problems, create new categories, and foster partnerships enriches his contributions to Indicio, bringing a diverse perspective and innovative solutions to the company's core mission.

Will supports Indicio's team by providing operational insights and advisory in specific business areas, including brand story marketing, category design, data monetization, technology business management, business and partner development, as well as serving as a mentor for early career staff.

## About the Authors



Dr. Chase Cunningham is a retired Navy Chief Cryptologist with over two decades of experience in Cyber Forensic and Analytical Operations. With a wealth of technical expertise, advanced education, and many certifications, he offers a profound understanding of cyber operations and forensic analysis.

Having served extensively within highly technical and operationally demanding environments at institutions like the NSA, CIA, FBI, and other government agencies, Chase honed his skills through hands-on engagement in cyber forensics, analytics, and both offensive and defensive cyber operations.

Driven by a steadfast belief in the inherent human right to cyber security and online safety, Chase advocates for proactive measures to negate adversaries' exploitation of perceived weakness. He champions immediate action and continual improvement in combating cyber threats.

Chase has had the privilege of collaborating with industry luminaries throughout his career, witnessing firsthand the transformative potential within the cybersecurity landscape. His diverse project portfolio spans the spectrum of cyber security, with a particular focus on enhancing the business side of the field. Conversations with satisfied clients attest to the game-changing impact of his expertise and guidance.

Chase has maintained a robust online and social presence and is dedicated to disseminating truthful insights and knowledge to those eager to learn. He ardently seeks opportunities to empower businesses and individuals to bolster their safety, security, and efficiency.

Eager to engage in discussions surrounding Zero Trust, cyber security, or cyber warfare, Chase welcomes dialogue with anyone willing to lend an ear to his wealth of experience.

# Version history

## V1 published 05-07-24

### V1.01 published 05-17-24

P2: Edit on date of emergence — Zero Trust emerged in early 2000s; decentralized identity emerged around 2016.

P5: Edited to remove suggestion that organizations can do away with any kind of account systems for employees.



**James Schulte**

VP of Business Development

[james@indicio.tech](mailto:james@indicio.tech)

+1.765.437.7305

**Hiroshi Matsui**

VP of Business Development & Customer Success

[hiroshi.matsui@indicio.tech](mailto:hiroshi.matsui@indicio.tech)

+1.415.694.3365

