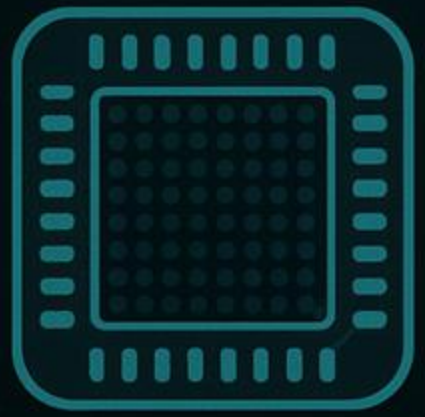


OBSIDIA

SECURITY AT THE SILICON LEVEL

Semiconductor Fraud - >$100B/yr

Counterfeit and tampered devices

Fabless – “Grey market electronics = revenue loss”

Wafer Foundries – “We see >5% losses annually from counterfeits”

Circuit Board Assembly – “Time and inventory are money – and we can’t go fast enough”

Contract Manufacturers – “Quality and supplier assurance are essential”

Application – “Failure means lost reputation and business – **even lives**”

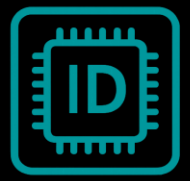
OBSIDIA

SECURITY AT THE SILICON LEVEL

(Based on OBSIDIA Customer Interviews)

OBSIDIA has breakthrough technology to safeguard the world's semiconductors.

Ultra-precise scanning detects even the smallest differences in chips, instantly identifying fraud.



Silicon watermarking embeds a unique, tamper-proof ID into every device at zero added cost.

Together, these innovations protect our digitally integrated society.

OBSIDIA
SECURITY AT THE SILICON LEVEL

Market Positioning

The Market is Cost, Cycle-Time and IP Sensitive

Spot checking is the status quo for authentication

- Expensive and time consuming
- No assurance for unmeasured parts

Secure Tracking through Process or Performance Data

- Time consuming, IP-Invasive, Data storage intensive

The Need is:

- **Free**
- Fast
- Agnostic
- Tamper Proof
- Stable
- Uncrackable

...and OBSIDIA delivers on all.

OBSIDIA
SECURITY AT THE SILICON LEVEL

Our Team

Founders

Erik Hosler PhD - CEO

GFS, PsiQuantum, xLight

Adam Wilson - CTO

Sphero, SO3 Technologies

Ari Block - CIO

Cellebrite, Siemens

Advisors

Greg Cardinale PhD

DARPA, Draper, MITRE

Darren Crum PhD

Purdue, NSWC - Crane

James Vedral PhD

KRI, Draper

Dick Butler

EMA

OBSIDIA

SECURITY AT THE SILICON LEVEL

Technology

Non-Linear RF Scanning

Intrinsic and Agnostic

Sensitive at Device Dimensions

Passive and Non-contact

Silicon Watermarking

Zero added Cost/Steps/Time

Device-Specific and Unique

Impossible to Spoof/Rev. Eng.

*Not required for initial OBSIDIA go-to-market.

Golden Reference Database

Established RF Signatures Across Customers

Zero-IP Risk to Customers

Exponential Value and Defensible Moat

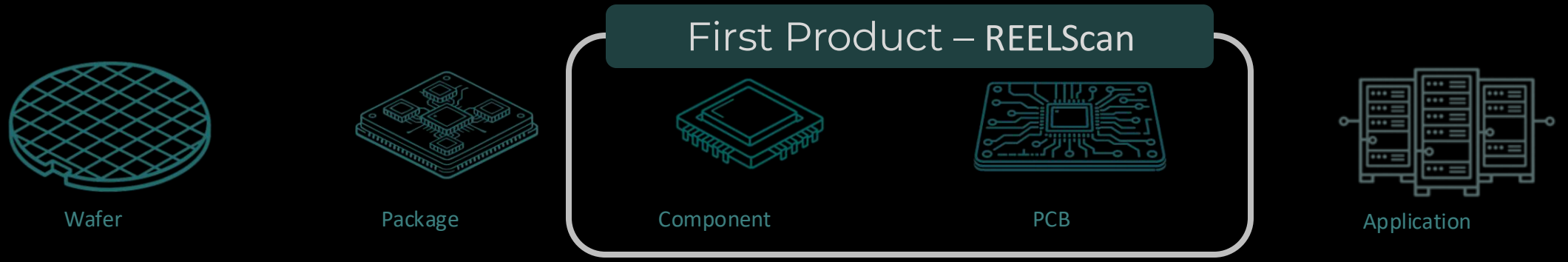
OBSIDIA pairs hardware system sales with scalable, high-margin recurring revenue from per-device authentication—driven by its proprietary golden-reference database.

OBSIDIA

SECURITY AT THE SILICON LEVEL

OBSIDIA Semiconductors

- The semiconductor supply chain is vulnerable from the wafer fab to the application
- Each integration level poses unique security challenges – requiring tailored OBSIDIA solutions



Printed Circuit Board (PCB) assembly is the control point where counterfeit and tamper risk converge, making it the highest-leverage entry point for OBSIDIA

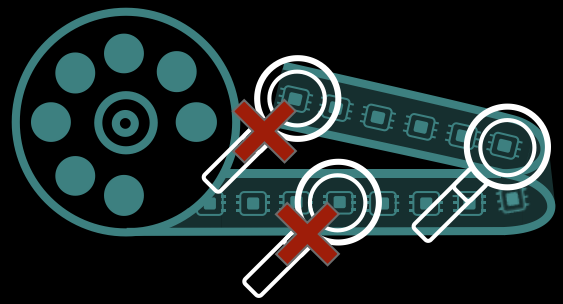
OBSIDIA's Value Proposition

Turning every semiconductor into a recurring revenue stream

Faster Cycle-Time

Same Day Verification

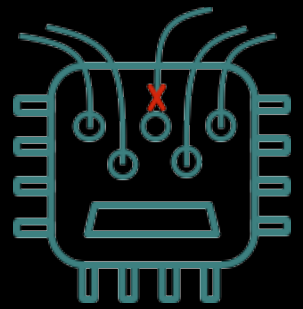
Reduced Rework



Less Overhead

No Validation Loss

>90% Cost Savings



Improved Quality

Trusted & Verified Supply Chain

Nonconformal Part Identification

Return Revenue

> 10% Sales Increase of Authentic Parts*

Measurement-based Remediation

*Based on Industry Losses

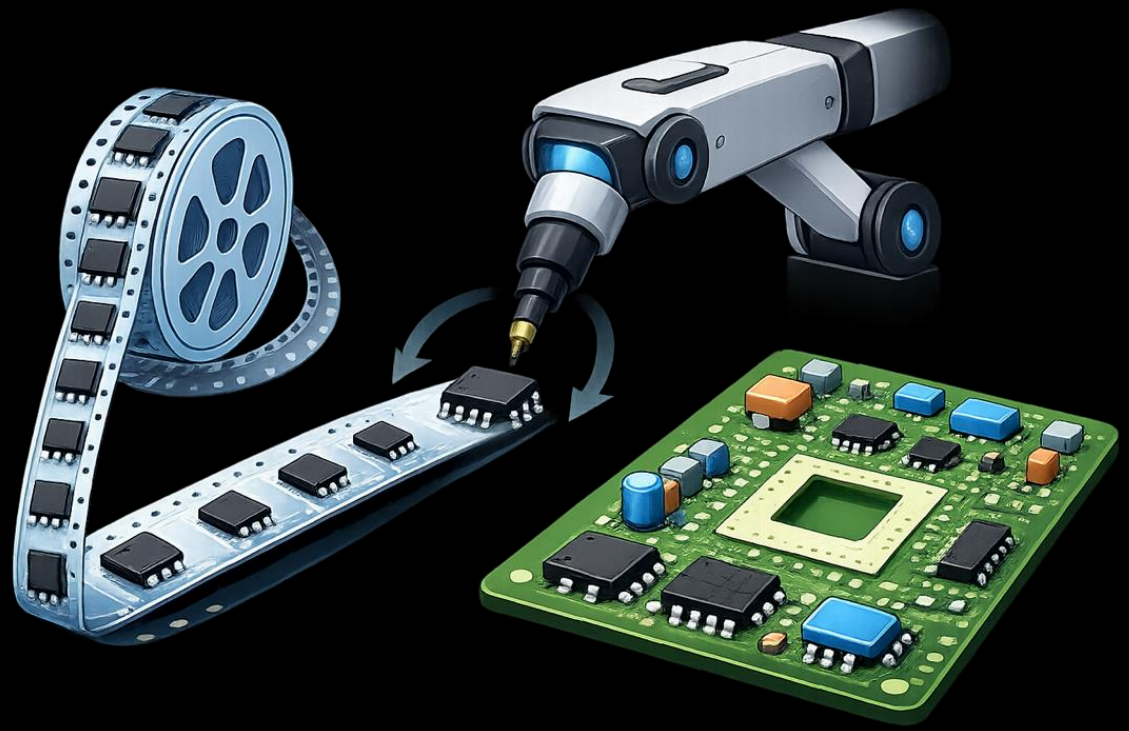
Why REELScan?

PCB assembly is an inflection point of manufacturing variability

Surface Mount Technology (SMT)

Components on Reel

Single Devices/Packages
&
Component Specific
RF signatures



Assembled PCB

Amalgamated Components
&
Unique RF
Signature Identifier

REELScan validates the authenticity and integrity of components prior to PCB assembly, ensuring an authentic product, traceable through its unique RF signature

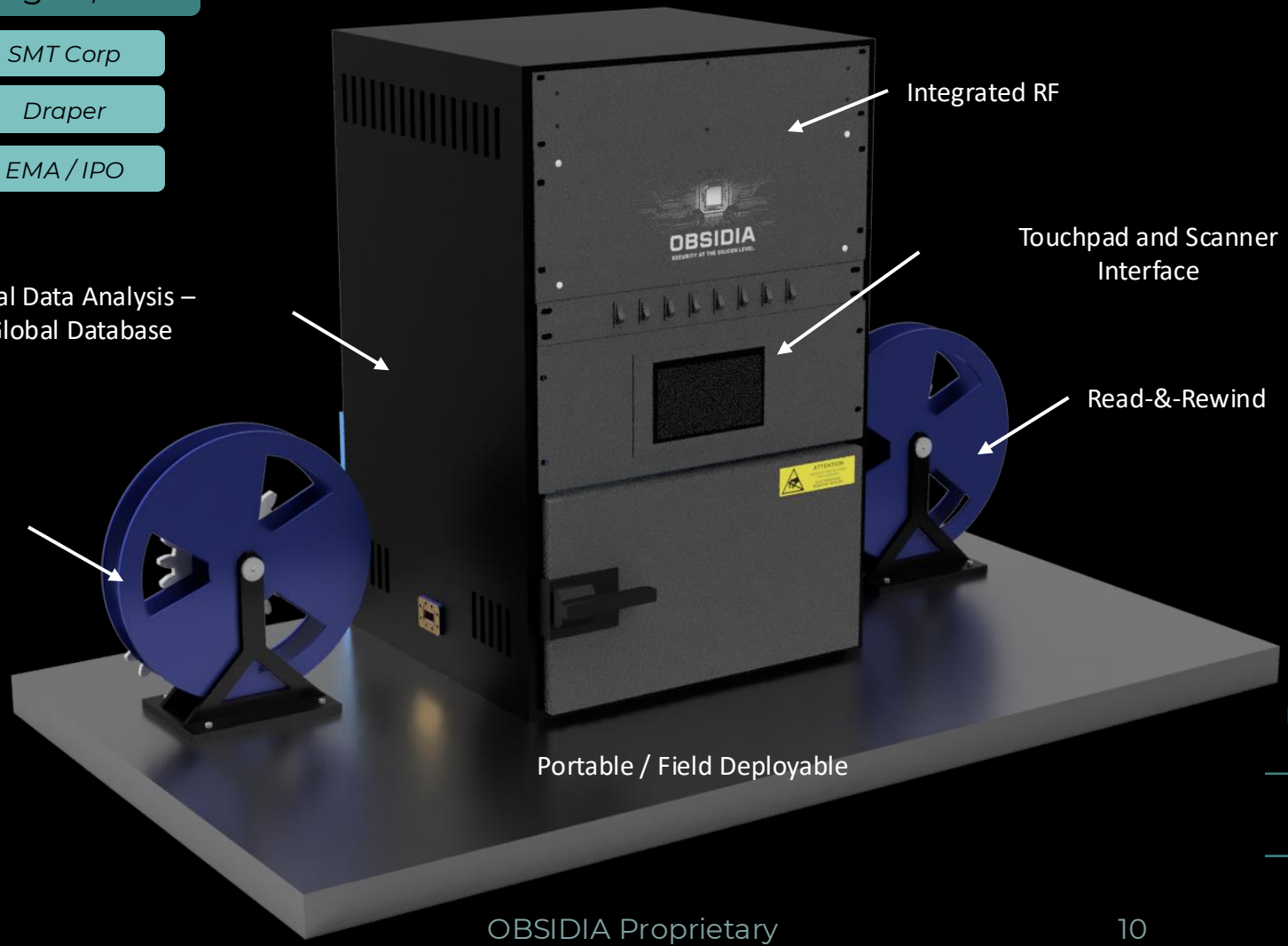
OBSIDIA
SECURITY AT THE SILICON LEVEL

REELScan Beta System

Partners

ParPro Technologies, Inc.

- MetaMorph
- SMT Corp
- NSWC-Crane
- Draper
- KRI
- EMA / IPO



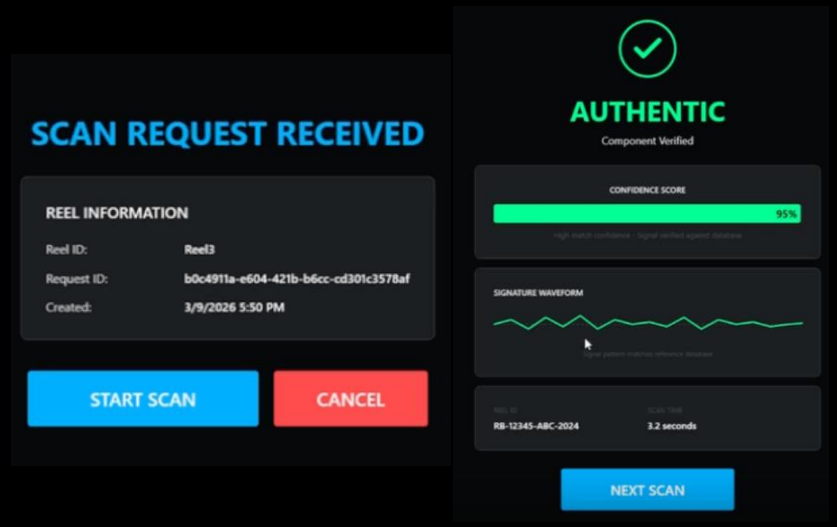
Key Specs

Component Measurement Time	<1s
Reel Load Time	< 10s
Cost Reduction	90%

OBSIDIA
SECURITY AT THE SILICON LEVEL

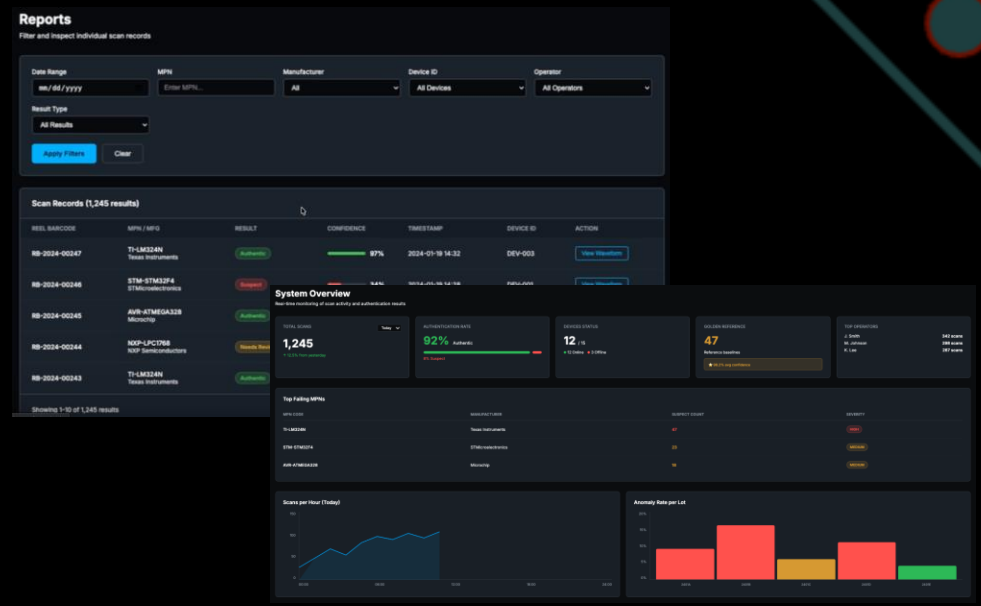
Customer Experience

Operator



- Minimal Interaction / High Actionability
- Fully Automated, Offline Deep-Dive Available
- Data Analytics Handled by OBSIDIA

Manager



- Fast Disposition and Remediation
- Full Inventory Tracking and Review
- Auditable Data and Analytics

Outlook + Ask

Customer Beta Site Launches OBSIDIA's Commercialization

April '26

NIST CRDO Review Validates Technology and Business Model

Expect - $34M Investment

Government Partnerships Established for Standardization

SEMI, NIST, DoT, DoW

DoW Pilot Programs Planned for Anti-Tamper / Anti-Counterfeit

Mission Systems and Data Centers

OBSIDIA is Seeking Co-Investment to Accelerate Commercialization

OBSIDIA
SECURITY AT THE SILICON LEVEL

Additional Information

OBSIDIA

SECURITY AT THE SILICON LEVEL

Counterfeit Electronics come in many different forms...

and COUNTERFEITERS hold the advantage.

OBSIDIA
SECURITY AT THE SILICON LEVEL

RECYCLED

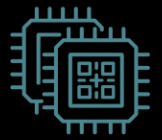
Part that has been reclaimed and then modified to misrepresent its authenticity or origin

REMARKED

Part from an authorized manufacturer which has had the legitimate part marking replaced with a forged marking

OUT-OF-SPEC / DEFECTIVE

Part that is identified as nonconforming by an authorized manufacturer, and then represented as conforming



CLONED

Reproduction of a part produced by an unauthorized manufacturer without approval or design authority that replicates an authentic part

TAMPERED

Modification of a part with the intent of representing another part or for malicious intent such as sabotage, malfunction, or espionage

Market Opportunity

TAM

Spend on Security Features in Electronics Devices, Specifically Semiconductors

SAM

Critical Sector Applications, including Data Infrastructure, Government, Aerospace, and Automotive

SOM

> 5% Direct Market Capture by 2030

OBSIDIA
SECURITY AT THE SILICON LEVEL

OBSIDIA Foundations

Spectroscopist & Engineer

Lithography Processing

SILMarq

Stochastic Fingerprint Tech

Reel Scan Prototype 1A

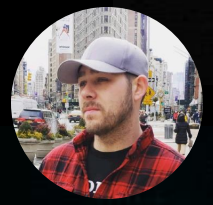
Customer Beta Alignment

OBSIDIA Vetted

TODAY

April, 2025

Manufacturing



DARPA Phase II SBIR

Fingerprint Test w/ KRI

RFMetrix

Analytics

Signal Processing & AI/ML

Sphero Counterfeiting Losses ($$M)

OBSIDIA
SECURITY AT THE SILICON LEVEL

Formation

Competitive Technology Analysis

Technique	Description	Touchpoints	Fast	Tamper-Resistant	Stable	Discoverable	Cost
PUF	Electrically Testable						
Chip Marking	Physically Written ID						
X-Ray	Spot Checking						
X-Ray	Full Chip Read						
Visual	Spot Checking / All Parts						
Electrical	Circuit Variations						
Tear-Down	Destructive Discovery						
Zero-Trust	Transport Security						
Database	Tracking-only / Blockchain						
Active RF	Powered Device EMI						
OBSIDIA	**REELScan**						
OBSIDIA	**SILMarq**						

Meets Security Requirements