AKM CYBER CORP

AUTOMATING CYBERSECURITY

AKM Cyber Corp.

Scalable Cyber Security from Endpoint to Enterprise

Best, True, "Zero Trust Architecture" (ZTA)

CEO: Bart Shields,	bart@akmcyber.com,	+1 (951) 522-3540 (USA)
COO: Bill Basser	bill@akmcyber.com,	+1 (931) 302-7397 (USA)
VP Engr: Larry Butler	larry@akmcyber.com,	+1 (817) 771-4684 (USA)
Advisor: Bruce McIndoe	bruce@mcindoeriskadvisory.com,	+1 (410) 320-4513 (USA)

7000 Columbia Gateway, Suite 150 Columbia, MD 21046

What is the Problem we are Solving?

AKM CYBER CORP
AUTOMATING CYBERSECURITY

Traditional Security is Expensive, Complex, Difficult to Deploy & Maintain, and gets more Expensive and Difficult every year!!!

- **Existing Security Methodology (based on 30+ year old, Public Key Infrastructure) is Expensive, Complex, and Requires a huge learning curve to deploy and maintain.**
- **Though PKI technology has evolved since the 1980s, its implementation and management can still be daunting.**
- **A significant reason is the complexity involved in managing digital trust through PKI certificates.**
- **As the digital ecosystem expands, companies must address scalability, security, and operational challenges.**
- **Overconfidence in an organization's capacity to manage PKI often leads to vulnerabilities.**
- **The solution is NEVER replacing PKI, it is ALWAYS adding more security layers to PKI, thus increasing the complexity, thus, increasing the threat surface, thus increasing the need for expensive cybersecurity personnel (which are always in short supply), thus increasing the likelihood of a breach.**
- **PKI based systems require significant digital footprint and processing capabilities.**

Traditional Security Problems Solved by AKM

AKM CYBER CORP
AUTOMATING CYBERSECURITY

Traditional Security Problems	AKM Solution
❑ Legacy Systems (w/Outdated Technology)	❑ Small footprint with minimal processing overhead
❑ Complex and Interconnected Networks	❑ Physical network agnostic, simplified architecture
❑ Large Threat Surface	❑ Limited threat surface exposed only during OEM factory configuration
❑ Difficulty with Integration of IT and OT	❑ Secure tunnels logically isolate each ATR
❑ Increasing Complexity	❑ ATRs enable intuitive, contextualized grouping
❑ Limited Security Controls	❑ Designed to prevent most common threats
❑ 88% to 95% of all Breaches are a result of Human Error	❑ One-time Configuration “One and Done”
❑ Difficulty Supporting Long Lifespan of Devices	❑ Autonomous operation

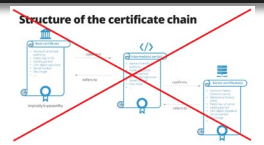
What is Autonomous Key Management (AKM)?

- **AKM is a 'Zero Knowledge' digital asset-centric cryptographic cybersecurity framework** that prevents most cyber risks from occurring in the first place.
- **AKM eliminates the need for many of today's remediation-oriented 'Band-Aid' solutions**.
- **AKM operates autonomously** and can be applied to concurrent virtualized groupings of users, devices and digital assets. Each grouping is referred to as, an AKM Trust Relationship (ATR).
- **AKM is highly resilient to quantum computers and human error**, and far more flexible, administratively efficient, and cost-effective than todays standard PKI + TLS protocols.

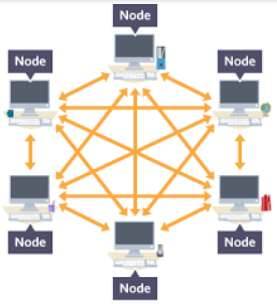
Autonomous Key Management (AKM) = **Crypto Key Management System (KMS)** + **Secure Communication Protocol**

Autonomous Key Management (AKM) Value Proposition?

- No External Certificates



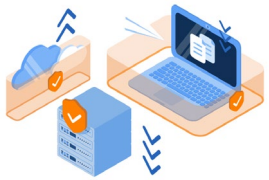
- True End-to-End Security for both Point-to-Point and Multipoint-to-Multipoint Networks



- Encrypted Data-in-Motion and Data-at-Rest

- Does NOT reinvent the Wheel – work within existing cybersecurity frameworks.

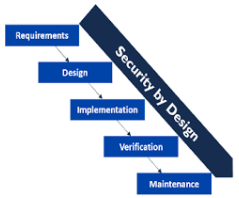
- Authentication and Integrity Monitoring



- Quantum Resilience – No Secrets are ever exposed

- Less Complexity, Lower Costs, Easier to Manage, More Secure

- True Security by Design



- Simplified Zero Trust Architecture

Where are We Going?

AKM CYBER CORP
AUTOMATING CYBERSECURITY

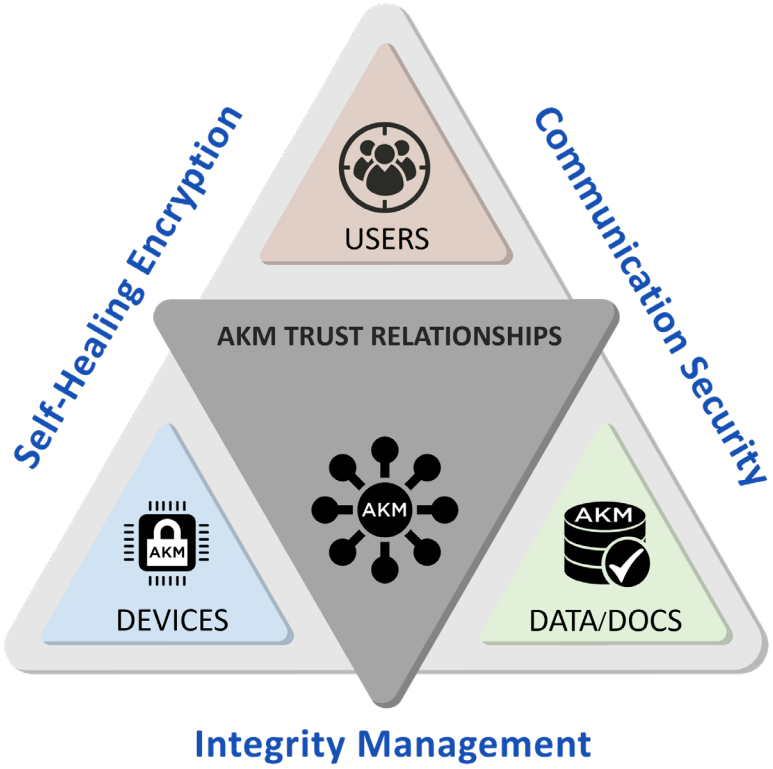
Seed Phase Products

- **AKM Endpoint Module -** Pre-Integrated, AKM Endpoint SDK in Tamper Resistant COTS-based Hardware Module ($400 per Endpoint Module). This is the direct productization of our AKM Endpoint MVP that is due to be released in January of 2025.
- **AKM Endpoint SDK** for ease of development or legacy integration ($10/endpoint for SDK lifetime license + yearly maintenance and support after year one). This is an OS agnostic version of what goes into our AKM Endpoint Module.
- **AKM Management Module to configure AKM Network** in Tamper Resistant COTS-based Hardware ($2,000 per Management Module).

Series A Phase Products

- **AKM Configuration Backend & Root-of-Trust Module** in Tamper Resistant COTS-based Hardware ($5K per Backend/RoT Module)
- **AKM Object Oriented Windows Management Console** – Windows-based Console enables IT personnel to easily configure AKM Security Network on either Management Module or Root-of-Trust Module ($2.5K per Management Console seat)
- **AKM Zero-Trust HSM Plug-In Module in M.2 Form Factor for Additional Security in laptops and embedded hardware** – Tamper Resistant COTS-based Hardware. Installs in M.2 slot to provide a Hardware-Based Zero Trust Architecture, enabling HSM to HSM direct communication with zero chance an infected host device could compromise HSM ($1K per Module)

Understanding AKM a Little Deeper



1. Turns any physical (connected) or virtual (digital) asset into an **AKM Protected Asset (APA)**, issuing each a unique AKM-ID
2. Configures APAs into **any number* of AKM Trust Relationships (ATRs)** of any type, scale, or structure, with each representing a unique AKM Trust Relationship
3. Each ATR concurrently operates its own **pre-configured, contextualized security rules** while being 100% cryptographically isolated from every other ATR
4. Once configured, each independent **ATR autonomously manages itself**.
5. In addition to configuration, the **AKM Management Module** can monitor and collect heuristic data and potentially **self-heal an ATR** in case of an attempted breach.
6. An extension of the AKM Endpoint SDK, the **AKM Asset Integrity Management (AIM) (i.e., an asset-monitoring service)** can also be enabled.

** Up to the implementation-specific limit.*

Market Opportunity

AKM CYBER CORP
AUTOMATING CYBERSECURITY

The **OT Cybersecurity Market** is expected to be $84.2 by 2032

Almost 4X what it is today (~$21.5B)

Reasonable Expectations for TAM, SAM, and SOM are:

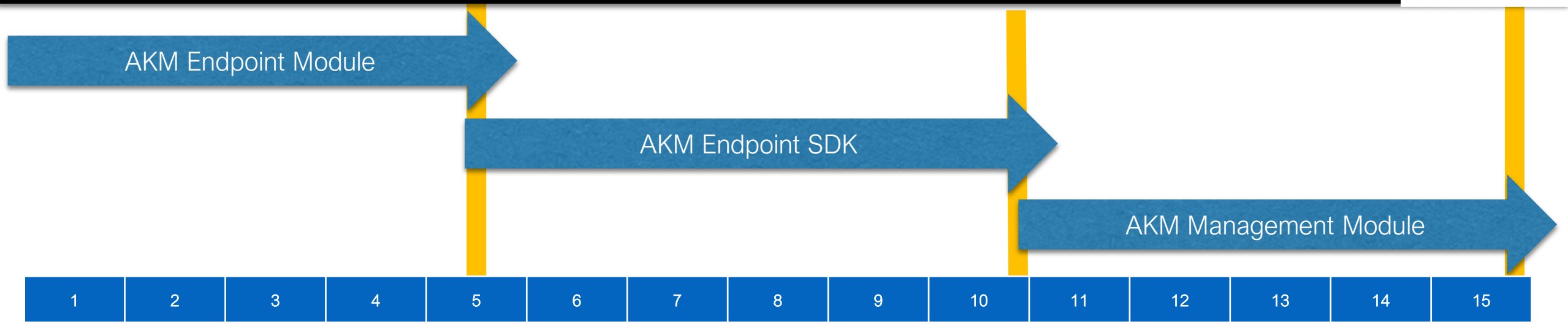
TAM	SAM	SOM
$84.2B	$16.84B	$1.3B

What is more impressive is that the OT cybersecurity CAGR is projected to be 15.7%, outpacing the general cybersecurity CAGR of 13.4%.

1) Straits Research: Industrial Cybersecurity Market Size, Share & Trends Analysis Report By Component (Software, Service), By Type (Network Security, Application Security, Endpoint Security, Wireless Security, Cloud Security, Others), By Application (Energy and Utilities, Manufacturing, Oil and Gas, Chemicals, Aerospace and Defense, Healthcare, Transportation and Logistics, Others) and By Region(North America, Europe, APAC, Middle East and Africa, LATAM) Forecasts, 2024-2032
2) Allied Market Research: Operational Technology (OT) Security Market Size, Share, Competitive Landscape and Trend Analysis Report, by Component, by Deployment Mode, by Organization Size, by End-User : Global Opportunity Analysis and Industry Forecast, 2023-2032
3) Markets and Markets: Operational Technology (OT) Security Market by Offering (Solutions & Services), Deployment Mode (On-premises & Cloud), Organization Size (SMEs & Large Enterprises), Vertical (Manufacturing, Oil & Gas, Others), End User & Region - Global Forecast to 2029
4) Global News Wire: Cyber Security Market Exhibits 13.4% CAGR to Hit USD 376.32 Billion by 2029

Investment Ask For Seed (15-Months) => $375K

AKM CYBER CORP
AUTOMATING CYBERSECURITY



Expenses ($400K)

- Personnel: 4, $300K
- Overhead: $12K
- Hardware & Software: $35K
- Miscellaneous: $3K
- Marketing: $50K

Products & Revenue ($111K)

- OS Agnostic AKM SDK Revenue: $3.1K
- AKM HW Endpoint: $48K
- AKM HW Management Module: $60K

Breakeven Indicator

- Monthly Burn: $25K (M0) to 25K (M15)
- Revenue: $0K (M0) to $37K (M15)
- **Breakeven Month 14**

Competitors

Competitive Landscape:

Top Five Competitors (all solutions based on 30+ year old PKI approach):

U.S. Patents & Competitive Advantages of AKM:

- Technology backed by 3 U.S. patents (plus another filed in June of 2024)
- Explicitly Designed to protect against Man-in-the-Middle and Replay Attacks
- Designed to scale, regardless of network size
- Spoofing Protection of physical device and associated firmware by implicitly authenticating endpoints, creating an Implicit Zero-Trust Architecture and foundation for Micro-Segmentation
- Explicitly Authenticating every data frame
- Minimum code size and processing power overhead, easily runs on small microcontrollers
- Autonomous management of cybersecurity credentials is a perfect defense against AI-based attacks

Go-To-Market Strategy

AKM CYBER CORP
AUTOMATING CYBERSECURITY

Marketing Strategy – Existing Legacy Systems First, Then New Designs

- Target growing endpoint cybersecurity needs within existing legacy OT systems.
- Partner with VARS/Integrators to sell, install, and service AKM hardware modules.
- Offer AKM SDKs to OEMs for both legacy and future products

Open Source for "Core AKM Software" and Documentation (GPLv2, Evaluation) or Commercial for B2B

- This is the same license model Linux uses and enables companies like Red Hat to create their own distribution model and sell commercial licenses, while still being part of the open-source community. The primary purpose of this is that AKM is competing against PKI & TLS, both of which are open standards, thus, the same will be expected of us in addition to this affording AKM Cyber to gain traction with developers and small companies, thus providing both credibility as well as verifying our approach.

Sales Channels:

- VARS and Integrators, such as:
  - Engineering Industries Excellence: https://www.indx.com/
  - TIGA, https://www.tiga.us/about-tiga
  - Revere Control, https://www.reverecontrol.com/
  - TDC Systems Integration, https://www.tdcsi.com/
- Direct sales to OT Equipment OEMs

Seed Funding Go-To Market

AKM CYBER CORP
AUTOMATING CYBERSECURITY

Phase our Go-To Market Execution with Product Availability

1.Continue Market Outreach	2. Sales Demo & SDK	3. Kubernetes Sidecar & SDK	4. Endpoint Module, Kubernetes Sidecar & SDK
P1 – Prepare	**P2 – Ramp-up**	**P3 – MVP & Sell**	**P4 – Drive Revenue**
Fill out Ambassador ranks – Referral Program Update AKM website Product Literature for Endpoint SDK & COTS HW Continue building funnel Activate LinkedIn Posts Place industry articles	Move funnel to EP SDK & HW Continue building market awareness Continue to add & work opportunities Opportunistic OT with the SDK to sell NOW Identify OT/Critical Infrastructure opportunities for P3	Move Management Module prospects through funnel Add more Management Module Leads Close OT SDK opportunities Develop OT Endpoint Module Opportunities for P4 Continue building market awareness	#1 Drive OT Opportunities Highlight Client Successes Publish Case Studies Select a few industry exhibits Prepare for Series A funding

AKM Cyber Core Team

AKM CYBER CORP
AUTOMATING CYBERSECURITY

Bart Shields

CEO

- Product Architect with significant experience, concept through deployment across multiple verticals, including Aerospace, Rail, Automotive, Wireless, Data Communications, and cybersecurity for the past 10+ years.
- Inventor of Autonomous Key Management (AKM) and Asset Integrity Management (AIM, the AKM Integrity Management extension for authenticating assets).
- Multiple Start-ups.
- Multiple Patents, including 3 issued for AKM, 1 filed for AKM in May, and another one for AKM is in process.
- 27+ years of Technical Leadership.
- B.S. & M.S. in Computer Science

Larry Butler

VP Engineering

- Experienced System Architect & Software Engineer with over 30-years of experience.
- Extensive experience bringing up boards, writing drivers and real-time embedded programming from bare metal up to the application layers.
- Extensive experience in implementing both storage communication & data communication (TCP/IP) protocols.
- Experience with multiple real-time embedded operating systems, Linux, and Windows.
- Multiple Patents.
- Extensive Leadership Experience in both management and engineering.
- B.S. Mathematics/Computer Science
- U.S. Army Veteran

Bruce McIndoe

Strategic Advisor

Bruce McIndoe is the President of McIndoe Risk Advisory and a recognized leader in risk management, security, intelligence, and travel industries, dedicated to helping organizations achieve Agile Operational Resiliency™. As a founder/CEO of WorldAware (iJET), he played a crucial role in its growth into a global leader in intelligence and operational risk management until its 2022 acquisition. Previously, he founded and led CSSi, an Inc. 500 and four-time Washington Technology FAST 50 company that developed systems and cryptologic software for the intelligence community. Bruce holds a BS in Physics and an MS in Computer Science from Johns Hopkins University. His accolades include: Global Top 40 Thought Leader by the Life Safety Alliance, President's Award from the Global Business Travel Association, and one of the Top 25 Most Influential Executives by Business Travel News (BTN).

Bill Basser

COO

- Embedded System Architect, with a strong focus on secure wireless devices. Bill is passionate about focusing on designing and manufacturing reliable, secure embedded products.
- Former Executive Director of Engineering/Distinguished Architect for StrongArm Technologies
- Senior System Architect for Guardhat, where he architected and designed the HC1 Communicator, which was recognized as one of The Best Inventions of 2020, by Time Magazine in 2020
- Bill also architected an innovative Data Product concept at GE Aerospace, which reduced the overall NRE from 10Million to 500K.
- Multiple Start-ups (multiple successful exits)
- Prior experience includes software, firmware, HW, FPGA & ASIC design.
- U.S.M.C. Combat Veteran

