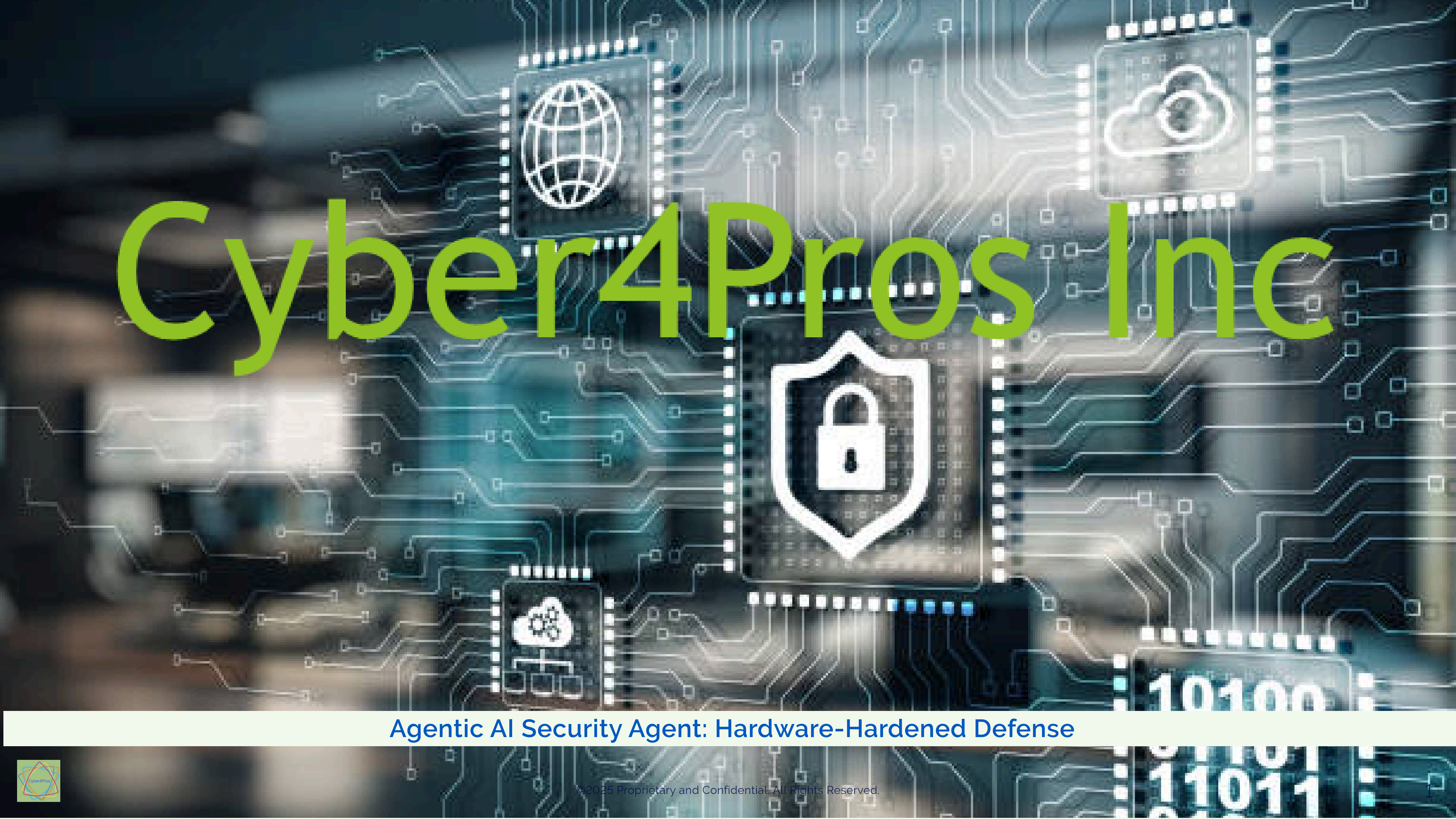
Cyber4Pros Inc



Agentic AI Security Agent: Hardware-Hardened Defense

Our Unique Approach

Introducing **Cyber4Pros**, the first company to deploy an **Agentic AI Security Agent,** ***"R^{2}IS^{2}E",*** embedded in secure firmware and chip-level infrastructure — delivering proactive, quantum-repellant cybersecurity beyond what today's ubiquitous software tools can achieve. ***R^{2}IS^{2}E*** stands for Receiving & Routing Internet Signals Securely Everytime.

Our Mission

Our mission is to secure the digital future by delivering advanced cybersecurity solutions across all applications via the use of NextGen secure firmware and smart chips we design for Secure Network Infrastructure (SNI) devices.

R^{2}IS^{2}E - AI-Powered Hardware Security That Rises Above Every Threat

Problem

Why Traditional Cybersecurity Is No Longer Enough

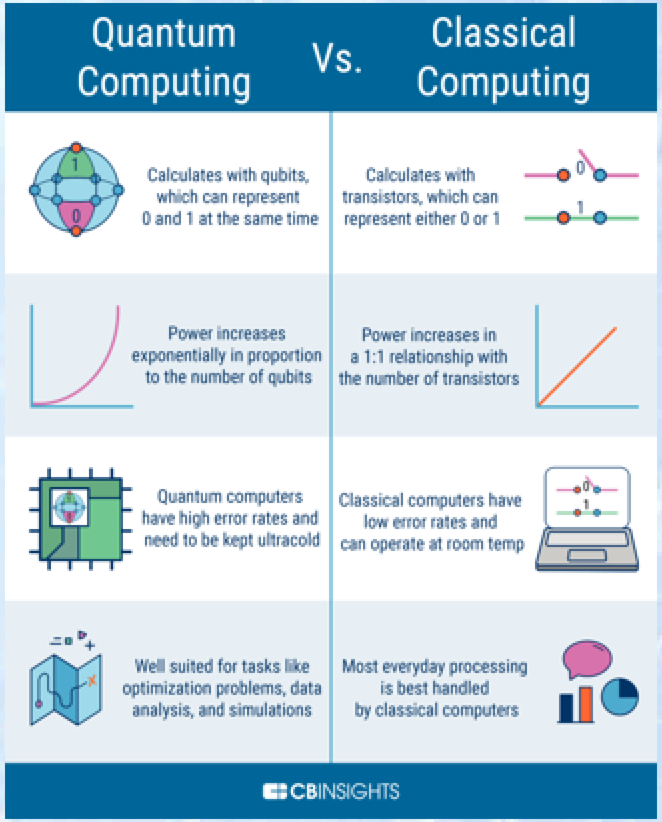
- **Legacy tools like encryption, VPNs, and firewalls are reactive, outdated, and require constant updates** to address emerging threats. They typically focus **only on OSI layers 3 through 7**, leaving the physical and data link levels exposed and unaddressed.

- **Adversaries now target every system tier** — from hardware and ISPs to DNS and IoT — exploiting zero-day vulnerabilities and supply chain entry points.

- **Quantum computing will soon make traditional encryption, the backbone of current cybersecurity tools, obsolete.** It can efficiently solve mathematical problems that underpin many public-key cryptosystems. For instance, Shor's algorithm enables quantum computers to factor large integers and compute discrete logarithms in polynomial time, rendering **RSA and elliptic-curve cryptography** insecure (Radanliev, 2024). Adding NIST's quantum-resistant - not repellent - algorithms require full hardware, software, and cyber tool overhauls creating more vulnerabilities in the process.

- **While NIST 800 compliance** still mandates the use of encryption standards, it is preferable to implement these requirements within a hardware-hardened system. **R^2IS^2E can be additional to current defenses** as it is specifically designed to block emerging quantum and AI-based threats before they can penetrate systems. This permits existing security standards in place to continue to function effectively inside a strong shield.

- **SMEs are especially unprotected**, lacking the resources to keep up with complex, manual patching and security tools becoming obsolete.



Quantum Computing	Classical Computing
Calculates with qubits, which can represent 0 and 1 at the same time	Calculates with transistors, which can represent either 0 or 1
Power increases exponentially in proportion to the number of qubits	Power increases in a 1:1 relationship with the number of transistors
Quantum computers have high error rates and need to be kept ultracold	Classical computers have low error rates and can operate at room temp
Well suited for tasks like optimization problems, data analysis, and simulations	Most everyday processing is best handled by classical computers

Cybersecurity must evolve from reactively patching vulnerabilities to proactively stopping all malware in internet signals before the breach of a system.

Solutions - R^{2}IS^{2}E Platform with Agentic AI Security

- R^{2}IS^{2}E is a proprietary cybersecurity platform powered by our Agentic AI Security Agent — a fusion of TrustLinkShield secure firmware and CyberGuard smart chips — delivering intelligent, hardware-level threat prevention. It will autonomously detect and neutralize AI-powered, quantum, polymorphic malware, zero-day exploits, and other cyber threats in real-time, without external dependencies. By identifying malicious activity before it breaches networks, R^{2}IS^{2}E will enhance data integrity and stop attacks at the edge or across enterprise, IoT, cloud, & other critical networks. It also protects all 7 OSI layers, ensuring end-to-end security from the physical infrastructure to the application layer.

- TrustLinkShield (TLSd) secure firmware protects Secure Network Infrastructure (SNI) devices from external threats by ensuring data integrity, preventing tampering, and directing signal flow to the chip for processing. It also eliminates vulnerabilities by minimizing attack surfaces.

- CyberGuard (CG) smart chips analyze packet headers, metadata, and payloads in real-time without latency bottlenecks, use AI-driven heuristics and signature-less anomaly detection identifying threats before they breach, and redirect malware into an isolated “Malware Vault” for safe containment and subsequent forensic analysis.

- Our chips use real-time AI-driven threat detection — they do not rely on virus databases, making them effective even against Zero-Day threats and unknown malware.

- Our solutions are hardware-based, future-ready, and seamlessly integrate with a wide range of devices-including CPUs, GPUs, laptops, tablets, IoT sensors, SCADA systems, network equipment, printers, robotics, and medical devices. They can be deployed as gateway or edge devices, and serve as an overlay to enhance enterprise, hybrid, and cloud environments by blocking all hardware-level attacks & strengthening cloud provided or other internal security measures.

- Quantum-repellent by design, our solutions protect the weaknesses of encryption-only models vulnerable to next-gen computing threats.

- Our partnerships to date, listed below, add significant value to our process as suppliers of start-up and cloud services, software & hardware devices, and chip design, testing, & fabrication services:

NVIDIA INCEPTION PROGRAM | Microsoft for Startups | aws startups aws activate | Barracuda | IC ENABLE DESIGN SERVICES | tp-link | skywater

Why Now ?

Beyond Resistance: Repelling Quantum Threats

Quantum computers look like chandeliers due to the complex cooling systems. The quantum chip must remain at near absolute zero degrees.

In 2024, global cybercrime costs were estimated at $9.5T (Cybercrime Magazine, 2024). In the first half of 2024, the use of AI in cyberattacks increased by 600% compared to the latter half of 2023 (Cinco Días, 2024), amplifying the speed, scale, and complexity of breaches.

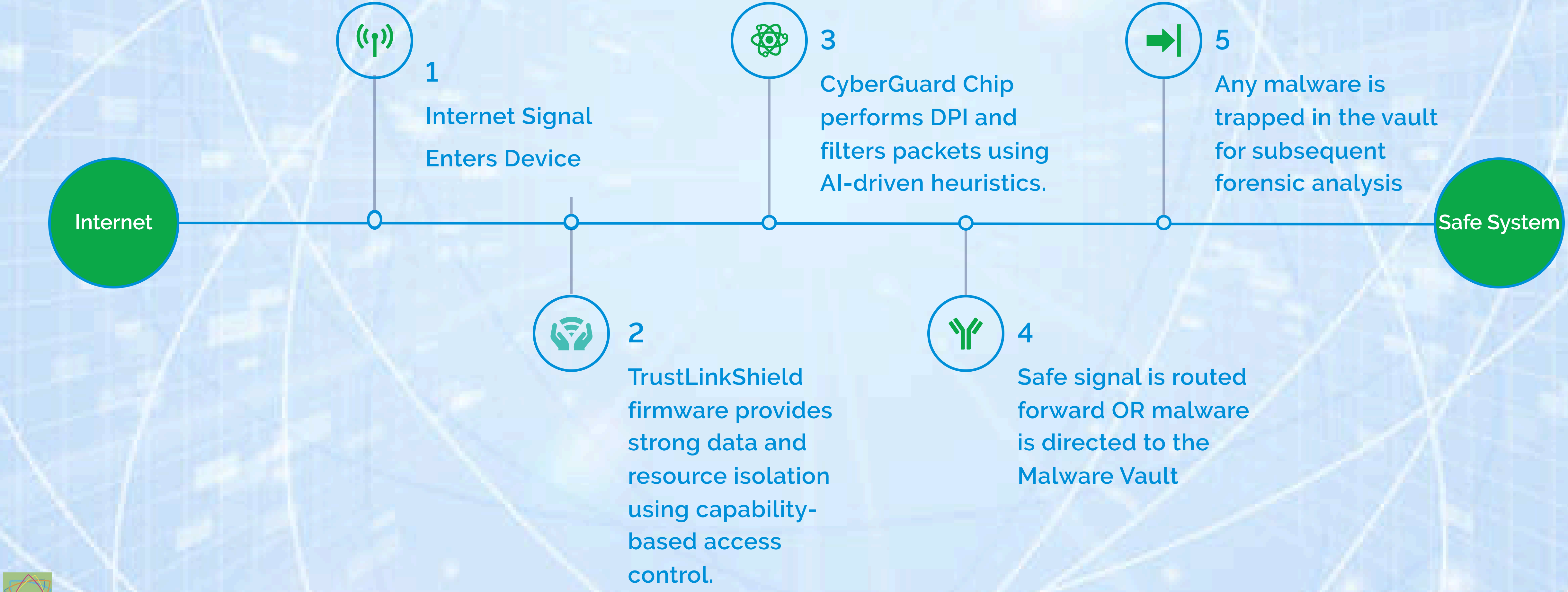
- Traditional tools are failing in many AI-powered attacks and will fail in future quantum-powered attacks.

- Effective quantum-resistant algorithms are years away and still struggle against evolving threats. Today's systems require extensive manual intervention for patching, configuration & privilege management, compliance, etc., while still leaving unidentified security gaps.

- R^{2}IS^{2}E stops threats at the signal entry point for all 7 OSI layers.

- No one else is offering this type of autonomous, preventive, hardware-hardened defense.

How it Works: Our Secure Flow Engine



Internet

1

Internet Signal

Enters Device

2

TrustLinkShield firmware provides strong data and resource isolation using capability-based access control.

3

CyberGuard Chip performs DPI and filters packets using AI-driven heuristics.

4

Safe signal is routed forward OR malware is directed to the Malware Vault

5

Any malware is trapped in the vault for subsequent forensic analysis

Safe System

Market Opportunity

Growing Cybersecurity Market

The global cybersecurity market is expected to grow at a CAGR of 14.3% from 2025 to 2032, reaching $563 billion. Within that, the AI driven cybersecurity market is expected to grow by a CAGR of 30%. The edge security market is expected to grow by a CAGR of 22.2%, reaching $148 billion during the same time frame. 30+Billion connected devices are forecast by 2030.

Emerging Cyber Threats and Evolving Regulatory Landscape

Stringent data privacy regulations and a rise of sophisticated cyber attacks are fueling demand for advanced, impenetrable security solutions.

Shift from Software-Centric to Hardware-Hardened Approach

The market must move away from traditional software-based security solutions towards a more effective embedded, hardware-hardened approach to cybersecurity.

Increasing Demand for More Robust Security

Businesses are turning to more robust cybersecurity solutions to strengthen their security posture, defend against evolving threats, and keep pace with rising compliance demands.

The substantial growth of the global cybersecurity market presents a significant opportunity for Cyber4Pros to capitalize on the increasing demand for innovative security solutions.

Competition

Our apparent competitors are cybersecurity companies (Akamai Tech, Broadcom, Cisco, Crowdstrike, Fortinet, Palo Alto Networks, Trellix, Zscaler, etc.) that focus on encryption, VPN, and firewall solutions that are reactionary, often identifying malware after a breach has occurred. However, our front-end solutions not only complement but also enhance the offerings of our competitors. TrustLinkShield and CyberGuard chips deliver an advanced, proactive layer of defense that operates ahead of—and exceeds—the protection provided by traditional encryption methods, which are still required for NIST compliance. Meanwhile, R^2IS^2E is specifically designed to block emerging quantum and AI-based threats before they can penetrate systems, ensuring that existing security standards continue to function effectively.

In the first half of 2024, cybersecurity startups raised $7.1B across 327 deals with the vast majority of them offering only software-based solutions.

There are eight other companies in the market now with hardware devices on offer that rely on traditional methods for security.

There are a further twelve companies in the capital raising stages for network security hardware products according to Pitchbook as of August 2024.

Cyber4Pros cannot find any other companies that are using secure firmware combined with AI-driven smart chips for security.

Why Do Business with Cyber4Pros?

Unique Hardware-Based Cybersecurity Solution

Cyber4Pros's proprietary hardware-based security platform provides unparalleled protection against the latest cyber threats, setting it apart from traditional software-based solutions. Our Agentic AI Security Agent R^2IS^2E delivers proactive, quantum-repellant cybersecurity beyond what today's ubiquitous software tools can achieve.

Experienced and Seasoned Team

Cyber4Pros was founded by a team of industry veterans with extensive experience in cybersecurity, AI, embedded systems, secure hardware design, network protocols, real-time data processing, firmware, chip design, and risk management, continuing their proven track record of successes.

Rapidly Growing Market Opportunity

The global cybersecurity market is expected to grow at a CAGR of 14.3% from 2025 to 2032, reaching $563 billion. Within that, the AI-driven cybersecurity market is expected to grow by a CAGR of 30%. The edge security market is expected to grow by a CAGR of 22.2%, reaching $148 billion during the same time frame, providing a substantial and expanding addressable market for Cyber4Pros.

Robust Financial Outlook

Cyber4Pros has a strong financial model that demonstrates solid growth potential and a clear path to profitability. We expect to maintain gross margins over 40% and a five-year CAGR of 36.5%, compared to the industry's average of 14%. The average profit margin forecast for years 3-5 is 38.1% vs. the industry average of 17.5%.

You can have the opportunity to be part of a transformative company that is redefining the future of cybersecurity. Join us. Secure the future. Let's make the world safe together.

The Team

Lee Waite is the CEO and CTO of Cyber4Pros and a seasoned entrepreneur with over 25 years of experience. A recognized cybersecurity expert and artificial intelligence strategist, Ms. Waite specializes in cyber risk and resiliency management as well as AI/ML technologies. Earlier in her career, she led the development of the U.S. Navy's Physical Access Smart Detection System and Virtual Access Smart Detection System networks, which were delivered on time and under budget, using her skills in cyber risk, embedded systems, secure hardware design, network protocols, real-time data processing, and firmware. After exiting that start-up, cybersecurity has been Ms. Waite's primary focus, building upon her further expertise in AI, firmware development, chip design, risk management, modeling, and simulation. Her current research focuses on Hardware Security in Gateway and Edge Devices.   Ms. Waite earned an MPA from Harvard University and a BA in Economics from Boston College. She also holds an MS in Digital Forensics and a Graduate Certificate in Behavioral Cybersecurity from the University of Central Florida's (UCF) School of Engineering and Computer Science (CECS). She has completed the coursework for her PhD (ABD) in Modeling & Simulation - Behavioral Cybersecurity at UCF's CECS, and her dissertation is on secure cyber technologies for SNI devices. While small and focused, her M&S program has earned acclaim from their partner Nvidia for being the most advanced university group researching digital twin technologies. She is a Life Member of Tau Beta Pi, the Engineering Honor Society.

Bob Chomut is the MD and Technical Project Manager of Cyber4Pros with over thirty years of expertise in leading complex, global projects within the treasury and securities industry. Specializing in FX trading, back-office settlement systems, cybersecurity, and related IT services, Mr. Chomut has a proven track record of driving product innovation, managing large-scale product portfolios, and delivering secure, impactful solutions across diverse sectors. Prior to joining Cyber4Pros, he held key leadership roles at industry giants such as Finastra, SWIFT, Misys, and Citibank, where he managed the development and implementation of flagship products. He was responsible for Finastra's cross border payment system and invented Citibank's early FX trading systems, ensuring secure, scalable solutions. Mr. Chomut earned a BS in Computer Science from the City College of New York, following his education at NYC's prestigious Brooklyn Technical High School. He has extensive hands-on project management experience and is also an award-winning innovator. He holds US Patent (No. US5787402A) for a method and system that performs automated financial transactions involving foreign currencies, demonstrating his ability to drive technological advancements. He was awarded Citibank's Service Excellence Award in 2000.

Vision

Cyber4Pros’ NextGen Cybersecurity technology platform R^{2}IS^{2}E is poised to revolutionize the way businesses protect their networks by offering a simple, proactive, intelligent approach to cybersecurity. Our SNI devices with Cyber4Pro's Agentic AI Security Agent, powered by proprietary firmware TrustLinkShield and CyberGuard smart chips, provide real-time protection without relying on outdated methods like encryption, VPNs, and firewalls. Our secure chip hardware solution is not vulnerable to cyber intrusions fueled by AI- or Quantum-driven attacks. By isolating and analyzing threats before they can cause damage, our disruptive, future-proof solutions offer organizations peace of mind in an increasingly dangerous digital world.