Zero Trust for 21st Century Automotive Applications

Overview

StealthPath's zero trust security innovation made us a 2020 PACEpilot honoree. In the year since, we have continued to evolve, supercharging our digital fingerprinting enforcement with an AI-enabled Behavioral Configuration Management Database (BCMDB). The enhanced functionality speeds time to value with cost reductions and increased ease of use. Based on client demand, the company has developed zero trust training and consulting services.

Ongoing delivery to government/defense clients validates our approach. Solutions are currently in pilot projects protecting US critical infrastructure. We provide a leading US Defense entity with training, strategic planning, and mentoring based on our Zero Trust Capability and Maturity Models.

StealthPath's zero trust approach is purpose-built for security challenges faced by the automotive sector. Digital fingerprints ensure identity integrity. BCMDB leverages artificial intelligence and human feedback to create and optimize rules for expected behaviors and anomaly responses within a continuously monitored environment. This functionality can be implemented without a change to legacy environments or by providing targeted policy enforcement for distributed, offline endpoints. The result is easy, seamless integration with existing investments, delivering high value with minimal disruption or economic impact.

To date we have delivered two of three solution offerings. All are aligned to our staged adoption path. Our current GTM model is for direct sales, but we have built a reseller model into midterm plans. The company is on track for $12M in revenue by 2023.

Pilot Program Specifics

Since receiving the 2020 PACEpilot Honoree award StealthPath has been investing heavily in developing and maturing every aspect of our business. Exclusively focused on zero trust, we built out training programs to support executive teams and practitioners. We brought forward professional services to provide zero trust gap analysis and strategic planning. We released two solution offerings that are currently in use by two major entities:

- A financial organization with over $400B in assets under its management.
- A US Government entity with more than 32,000 employees, a $5B budget, and a focus on critical infrastructure.

A senior government official said adopting this model would save them two years of mandated effort. Their solution adoption was enhanced by StealthPath’s passive, agentless methodology requiring zero changes to hardware, software, or networks, and operating in environments ranging from the Cloud to a highly secure, air-gapped deployment.

-
- StealthPath believes the applications for zero trust are relevant across multiple verticals. We project market penetration within:

- Defense - Protecting critical assets like drones and service vehicles; Securing Defense Industrial Bases; Securing biomechanics such as robotic weapon sleeves
- Utility – Securing energy and water supplies
- Manufacturing – Securing OT/IoT assets and ensuring all communications are authorized
- Healthcare – Securing patient data and medical devices, ransomware protection
- Pharmaceutical – Ensuring vaccine and drug developments are secure

Specific to the automotive industry we see numerous use cases where zero trust can impact the bottom line. StealthPath solutions can be leveraged in any of the following areas:

- OT/Manufacturing
- Over-the-air communications and software update
- Onboard systems – batteries, sensors, autonomous vehicle controls
- Autonomous vehicle environmental awareness – smart cities interfaces
- Charging (EV)
- Vehicle servicing
- Supply chain integrity

Investment to date has been through angel investors. We are actively engaged in additional funding discussions including a firm focused specifically on electrification and sustainable investing.

Innovation Narrative

The world has changed significantly since COVID. Businesses have accelerated their efforts in virtualization and remote support services. During this same period the number of smart, network attached devices has increased exponentially, permitting remote support and work from home. This explosion of connected devices, most often now being supported remotely, has increased business and home vulnerability to attacks across their networks. Zero trust security is the necessary response. It's starting assumption is that all environments are compromised, and verification must precede granting access or permissions to the supported devices.

The automotive sector relies extensively on computerized components and over the air diagnostics and software updates. Leading manufacturers are committed to becoming carbon-neutral, converting to electronic drive-by-wire vehicles (EV) and investing heavily in the continued potential of autonomous vehicle control in the near future. We have already seen the beginnings of this with Tesla and more and more cars offering autonomous parking. The potential is great, but increasingly sophisticated cyberattacks threaten everything from the supply chain, to manufacturer production, to connected vehicles already on the road.

The recent SolarWinds breach revealed inadequate precautions in ensuring service patches were not compromised, exposing their customers to great risk. This will not be the last attack leveraging trusted updates. StealthPath's zero trust approach is purpose-built for these challenges.

Our multi-factor digital fingerprinting of data exchanged between nodes on a network and profile management/enforcement (specified in last year's application) is now supercharged by new Behavioral Configuration Management (BCM) functionality. StealthPath BCM leverages artificial intelligence (AI) and human feedback to evolve rules for expected behavior and anomaly response within a continuously monitored environment. This functionality can be implemented without any change in legacy environments.

Zero trust presents significant opportunity for both automotive manufacturing and onboard vehicle systems, proving both security and operational integrity. These are convergent challenges, driven by the rise of connected smart devices. Factories manage the communications between robots, conveyors, forklifts, picking stations, etc. Vehicles contain their own ecosystem of computers and sensors responsible for all functional elements, from continuous engine diagnostics to entertainment systems.

The StealthPath BCM inventories digital patterns of behavior within systems and then continues to monitor them, building a baseline of nominal connections and commands. The BCM reliably adapts to individual use cases with situation awareness. This data can be aggregated and shared with product engineering for future enhancements and provide feedback to owners on vehicle performance and their driving patterns.

Thought Leadership

While first proposed in 2010, there is no consensus on zero trust implementation. NIST has established a framework but has not issued a deployment roadmap or even a defined set of capabilities.

StealthPath has created both. From its inception in 2017, we have focused on developing a holistic zero trust strategy and purpose-built zero trust solutions.

Our Zero Trust Capability and Maturity Model (ZTCMM), developed by a leading global security practitioner and former White House Executive Fellow with roots in nuclear command and control and the automotive industry, provides a real-world, risk-based methodology for practitioners.

The ZTCMM is the foundation of our strategy, training, consulting, and solution offerings. It provides a comprehensive architectural blueprint for zero trust assessment and implementation. Our model is a bridge between the massive detail of NIST 800-53 Security & Privacy Controls and the high-level approach of NIST 800-207 Zero Trust Architecture. The model is holistic and practical, a step-by-step guide to a phased adoption and implementation. It provides value in both IT and operational contexts, with defined approaches and metrics for both.

The end goal is a coherent environment with the ability to detect and contain malicious traffic that would elude traditional protections, with the flexibility to continuously adapt to emerging threats.

Product Innovation

The ZTCMM is vendor-agnostic because a comprehensive zero trust implementation strategy requires more than one product. The optimal approach most likely combines multiple software and hardware products, along with risk-based policies and processes.

StealthPath solutions are purpose-built to be complementary. They are agentless and can be retrofitted into legacy environments with no changes to networks or solutions, and no impacts to ongoing operations or current risk. They supercharge rather than displace existing cybersecurity solutions. They function equally well in cloud, hybrid, or air-gapped (offline) deployments.

The StealthPath Zero Trust Capability and Maturity Model (ZTCMM) provides a new, practical methodology and roadmap to zero trust. It enables organizations to assess their security and operational integrity posture against their own acceptable risk definitions within a continuous assessment framework.

ZAlert, StealthPath's flagship product, uses AI and advanced analytics of Behavioral Configuration Management (BCM) to build a model of a systems acceptable connections and actions. The BCM engine flags unusual events, providing immediate context for classification and response. Real-world feedback continuously improves its understanding of nominal behavior and its sensitivity to potentially threatening anomalies.

Market Value

There is strong market demand for our solutions.

Effective implementation of StealthPath's zero trust solutions could have stopped the most damaging cyberattack in recent history - the penetration SolarWinds popular product and the subsequent spread across customer systems. ZAlert's capabilities could have detected suspicious activity as early as the preliminary "reconnaissance" phase of the attack. The hacker's initial probing for vulnerabilities inevitably required new connections between internal and external devices that ZAlert could have flagged for investigation.

Even if a vulnerability were identified and exploited, any abnormal behavior would have set off alarms that would have directed them to the source device of the anomaly. ZAlert' s functionality goes beyond detecting new connections. It can also alert on atypical payloads, including unusual transaction size, frequency, or timing. ZAlert's situational awareness can completely resolve every outlying anomaly down to the individual device and transaction. The result is an early warning of abnormal behaviors, providing the context and detail to respond quickly and precisely before damaging exploitation or operational compromise.

For example, consider the interactions between two "smart devices." Under zero trust, each device is authenticated, and their connections authorized before communications can take place. That authorization would expire when communication ceased and would require a new approval process at the next interaction. There is no persistent implicit trust. Additional layers provided by advanced identification techniques, AI pattern recognition, and behavioral baselines can tighten access even further, potentially to the level of individual commands, source of command, and even the size and response based upon established behavioral patterns.

Development Flexibility

StealthPath anticipates new requirements arising from client and prospect engagements. In the case of the automotive industry, we expect new requirements for both digital and analog fingerprints / behavior patterns, as well as external data such as weather, temperature, etc. Our solutions are designed to accommodate extended functionality wherever system interactions can be characterized.

Competitive Impact

With COVID-19, cybersecurity breaches are up 300%. Phishing attacks are up 14,000%. Legacy perimeter defenses are not addressing today's sophisticated attacks. Zero trust hardens operational aspects to ensure all business elements are secure, from OT and business operations to the supply chain.

StealthPath's innovative Zero Trust Capability and Maturity Models establish a consistent methodology and metrics baseline in the mostly undefined zero trust security space. The company's complementary approach to solutions allows frictionless implementation with existing or legacy security solutions and avoids the "rip and replace" mentality of typical new solution implementations.

StealthPath is strategically positioned to take advantage of organizational imperatives to move toward continuous monitoring and assurance of product and service security and operational integrity. The ZTCMM incorporates the principal tenets of zero trust security within the context of a holistic implementation strategy to monitor and validate system integrity continuously, at a granular level.

Customers can use our solutions as little, or as much as they choose. By reducing the barriers to entry, we establish strong beachheads for a "land and expand" client penetration approach. Because we complement legacy products, we can integrate with them and, through partnerships, leverage existing vendor market positions.

No other firm that we have found in our ongoing monitoring of the competitive landscape offers the StealthPath’s full range of zero trust services and solutions, or the equivalent granularity of device/transaction-level detail. With the addition of Behavioral Configuration Management tools to our intuitive user interface, we identify threats and update the policies required to make zero trust environments more transparent and manageable.

Pilot Performance Measures

NDAs limit revelation of current StealthPath pilot programs

Innovation Challenges

Change is difficult. Even with its apparent flaws, there is a lot of inertia in the status quo. The most significant challenge that we face in commercialization is building awareness.

Zero trust's growing market recognition has spawned a cacophony of vendor claims. Choosing the right mix to deliver zero trust security can be confusing, resulting in incomplete implementations. It is not that the claims are misleading; most of these solutions provide some value in moving towards zero trust. However, they lack the required holistic perspective for coherent realization at the enterprise level.

StealthPath is engaged in initiatives with US Department of Defense entities. In this environment means that we need to conform to an ever-changing superset of compliance requirements unique to government oversight and high-value assets. Our challenge is to deliver robust solutions, able to rapidly adapt to new demands without significant impact to ongoing missions.

Ultimately, our main challenge is the sophisticated and dedicated cyber opponent. Whether a criminal or a nation-state attacker, they are highly adaptable and dedicated to eluding whatever obstacles impede their successful breach. It is a race that we can't afford to lose. Zero trust is the most effective strategy and StealthPath provides the solution and service vehicles to win.

Patents & Awards

- StealthPath Zero Trust Capability Model
- StealthPath Zero Trust Maturity Model
- StealthPath Behavioral Configuration Management Database
- 7 US/Global patents on Zero Trust technologies (See attached presentation)
- 2020 PACEpilot Honoree
- 2020 IBM Think, Build, Grow Winner (Global)