Executive Summary

Our Mission

Greengrass Enterprises has created Secure Enterprise Connect™, a military grade security solution that will revolutionize how IT security is architected and implemented.

Secure Enterprise Connect™ leverages existing and proven technologies in one fully integrated seamless solution: trusted computing[1], software defined perimeter[2], blockchain technology[3], big data[4], analytics[5] and artificial intelligence[6]. This concept creates a *device centric* model for operations that *eliminates user credentials* while tracking and controlling *device identity*.

It is already clear that the user centric model is not an effective security control in today's world, yet the IT security industry continues to focus on adding layers of security controls to this already failing paradigm.

Our approach: tear up the rule book, throw out old paradigms, philosophies of thinking and self-imposed constraints, utilize that in which we've already invested and apply new methods to derive value for our customers. In short, we implement Secure Enterprise Connect™, the first key solution to make the leap to the future event horizon while directly addressing the current security crisis.

What Is Special About Secure Enterprise Connect™?

Greengrass Enterprises has invented a new paradigm for IT security architecture. The Company has scrutinized the deficiencies in current architectures, the resulting outcome of breaches and the products that were used to protect the perimeters where breaches occurred. Our conclusion is that it is vital to eliminate user credentials and open networks (such as exist within a perimeter focused environment). Our paradigm is to create a device centric model where key exchange replaces network authentication and where users authenticate to their devices (using biometrics embedded in trusted execution) and those devices, in turn, subscribe to needed resources.

Our simple and highly effective solution focuses on mobility and basically turns every company into its own telecom. Tracking and controlling known and trusted devices that communicate over dynamically created connections that are invisible and only exist while in use is the solution to the current dilemma. Add big data, analytics and AI and personas for devices; how, when, when and for what they are being used is automatically created. User authentication to the device instead of to the network means that only rightful users of a device will be able to access it.

Enterprises have always been about 'known users' and NOT 'known devices'. What is special about Secure Enterprise Connect™ is that it will migrate this thinking away from the user to the

[1] Every computer has within the Central Processing Unit a "Trust Zone" which is called the Trusted Execution Environment or TEE. Anything running within the TEE has complete control over the operating system while the operating system has no access at all to the TEE.
[2] Software Defined Perimeter is a standard in computing that uses a special type of connection that is invisible over the Internet and in being invisible is not able to be hacked.
[3] Explained in detail on page 2.
[4] Extremely large data sets that may be analyzed computationally to reveal patterns, trends and associations, especially relating to human behavior and interactions.
[5] Information resulting from the structured analysis of other data
[6] The theory and development of computer systems able to perform tasks that normally require human intelligence.

known device itself. Focusing on the known device will allow the users of those devices to become 'attributes of the device' instead of the reverse. Years of teleworking, VPN's[7], mobility, BYOD[8], and other technologies have eroded the old controls on individual user access. It is nearly impossible to retrain users to recall better passwords or use other more secure means of connecting to their resources. We also want to make security invisible to improve the user experience and make it friendly and easy. It is a relatively simple concept to allow a user to log into a device and then let the device log the user into the rest of the world.

How Does It All Work?

1) First, users authenticate to the devices they wish to use instead of to the networks they want to access. This will be accomplished from within the trusted execution environment (TEE), which is built into every processor built within the last ten years. When a device is initially turned on (or after a preset amount of time) the user will be required to enter a PIN known only to the user. The PIN will either be a sequence created by the user or a hard or soft token used in multi-factor authentication[9]. This PIN is entered into software running within the TEE. The TEE has complete control over the operating system while the operating system (and anything running within it) has no access to the TEE. If the PIN is legitimate, a biometric user scan and an IP geo-location scan are both performed from software also running within the TEE which authenticates the user to the device. Only the rightful user of a device will be able to access that device.

2) Once the user is authenticated to the device that device becomes known but not yet a *trusted* device. Both are required before it can be connected to a network resource. To become known and trusted, the device reaches out to an Orchestrator, which is a server located in a public cloud. The Orchestrator first reads data from a blockchain, (defined in detail below), which stores a public key. The private key, similar to a SIM chip, is virtual and is only located within the device's TEE. The Orchestrator encrypts an alphanumeric sequence using the public key from the blockchain and sends it to the device which decrypts it within the TEE, sending it back to the Orchestrator in the clear. If the two match, the Orchestrator declares the device *trusted*. This takes place in a fraction of a second.

   Blockchains are inherently secure databases, because the data stored within them cannot be changed. Once recorded, the data in a block cannot be altered retroactively. Secure Enterprise Connect manages the blockchain database autonomously. Blockchains are an open, distributed ledger that can record transactions between devices efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically. Due to the secure nature of Blockchains it makes them ideal for storage of identity management (which in this case consists of device identity), public keys, and the list of resources that specify what known and trusted device has access to what company resource, such as what servers a known and trusted device is allowed to access.

   Once the Orchestrator knows the device is Known and Trusted, it then reaches out to an analytics engine which assesses device identity information, also stored within the

[7] Virtual Private Networks have been the primary means that a remote user has used to access company resources while out of the office.
[8] Bring Your Own Device refers to companies that allow their users to use their own devices to access company resources.
[9] Multi-Factor Authentication uses either a pin created by software installed on one's device or a pin generated by a hard device such as a key fob that one would carry on their keychain.

Blockchain to provide an extra layer of security that the known and trusted device has a list of accessible locations stored in the Blockchain and combined with an AI that tracks and controls the devices identity, the AI then decides whether or not to create connectivity for that device. Because devices are subscribing to one another there are physical rules as to what can and cannot be done; the AI determines the correct course of action and passes that information to the Orchestrator. This big data / analytics environment also tracks what is being done by what device and stores that information in the Blockchain as well. This is all forensic compliance information that can be used to prove the state that a device was in when a transaction occurred should a future problem be identified that requires past forensics of what occurred, when, and by which device.

A control module for the analytics engine will be available to key staff to configure various access permissions and other options.

3) The Orchestrator then sets up a connection from the device to the network resources that are required using software defined perimeter (SDP) as the transport. Based loosely on the publicly available Software Defined Perimeter as published by the Cloud Security Alliance, this feature of Secure Enterprise Connect™ creates a dynamic secure encrypted multi-point connection from the end user device to the company resources that the device is authorized to access. SDP implementations require an SDP gateway to be placed in front of every corporate resource, or in some cases groups of resources. These are layer 2 devices that do not have IP addresses. Only the Blockchain in combination with the AI and the Orchestrator can setup SDP connections. SDP is dynamic in nature so these connections only exist while they are in use. They are highly encrypted, and torn down every few minutes then re-established. At layer 2[10] they are also invisible connections to invisible resources. Our motto is "you can't hack what you can't see."

   Once the SDP connection is established, the Orchestrator informs the gateways to open a pinhole in their firewalls and accept an incoming data stream from the IP address of a specific device. At the same time the Orchestrator contacts our Virtual SIM chip in the device's TEE and assures that this connection occurs. The orchestrator also communicates to the gateways the total number of allowed connections on that specific SDP. The Orchestrator then steps back from the process and the user then has access to all their allowed resources. This entire process occurs in under a second.

   Subscription of the device to its allowed network resources is now complete and the device's operating system boots. Simultaneously, the device is still running end user device protection software within the TEE. During the subscription process, the Orchestrator also collected a specific set of attributes that must be met in terms of the configuration of the device in order for the device to perform transactions. This includes software that is allowed to run on the device and other parameters as defined by the company or end user. This information was fed the end user device protection system, which has already scanned the operating system for compliance. Should anything that is non-compliant attempt to run, it would be stopped before it even started. This includes malware, viruses or anything not on the approved list. In this scenario, even a badly infected device can access a network resource without any concern that the infection can spread.

[10] There are seven layers in the OSI Network Model that defines how local and wide area networks work. Only at certain layers is an IP Address required and layer 2 networking is not one of them. Connections that are established at layer 2 are basically invisible over the Internet.

Leveraging the advanced mechanisms of hardware device integrity both internal and external, Secure Enterprise Connect™ will assure that all devices are in a known healthy state. Devices that have been compromised will be returned to a healthy state without any user intervention. Our solution will assure that a predetermined risk score on the device is satisfied prior to allowing it to subscribe to any network resources. Greengrass Enterprises' threat management solution will negate the use of third party anti-virus and anti-malware systems installed within the operating system on any device.

Greengrass Enterprise Differentiator

Reliability, Predictability, Mobility and Ease of Use of the User Experience are the goals of today's users. Trusted computing defines the model for achieving these goals and complicated sets of instructions sent between devices for access to corporate resources can be automated in software with a cloud based controller moderating that communication; an automatically timestamped Blockchain server handling the requests. An AI, data analytics and the Blockchain top off this solution with the ability to track and control all the devices in this device centric environment. This model is effective because of the existence of Known and Trusted Devices and device to device subscription.

Secure Enterprise Connect™ represents a game changing method that deploys intrinsically secure connections from any device to any device regardless of location or purpose. Secure Enterprise Connect™ has the dual uniqueness of being both infrastructure protecting and business enabling.

What are the Benefits for Users?

Secure Enterprise Connect™ operates the same way modern day wireless phone networks operate. Users authenticate to their devices and those devices then authenticate to the network to which they are assigned. There are companies today attempting to build secure voice and messaging applications based on specific configurations made to specific wireless devices. With Secure Enterprise Connect™, anyone utilizing this solution can communicate using voice or data in every possible way and achieve the same result. It is device and network independent.

Secure Enterprise Connect™:

- Invisible Networking using only device identity to establish connections over any utility connectivity available from mesh networks[11] to hard lines. Creating a private carrier grade network for every enterprise from 10 to 10 million users.
- Every company becomes their own telecom in terms of managing the subscription process of trusted devices.
- Fast to provision, easy to use, and highly scalable. Supports attribute based access control for any cloud service.
- Brings military-grade security to applications by hiding them within invisible networks.
- Quickly established and exists for a limited time.

[11] A mesh network is a local network topology in which the infrastructure nodes (i.e. bridges, switches and other infrastructure devices) connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients. This lack of dependency on one node allows for every node to participate in the relay of information.

- A totally effective means to eliminate all network-based attacks.
- Meets all 20 security requirements of the SANS 20. Over time will be fully supported by all compliance and governance standards.

No matter how we define what Secure Enterprise Connect™ does in *every instance* it is simple: ***You Can't Hack What You Can't See.***

The Benefits for Greengrass Enterprises

Greengrass Enterprises will own the cloud based Multi-Tenant Orchestrator as well as the Blockchain, analytics and AI components, charging a per use fee (see the next section on the Token Plan) that will be determined by how many applications are accessed within a given month by how many users. This will be setup in a federated multi-tenant model.

Conclusion: What Makes Secure Enterprise Connect™ Unique

There are three primary differentiators:

1. The Solution is built entirely in software upon existing technologies and requires a small effort to implement, making it a highly adaptable security solution for almost any business.
2. After investigation, we believe that there are no commercially available end-to-end solutions that currently exist that compete with Secure Enterprise Connect™.
3. It is extremely cost effective due to its speed of implementation, low operational impact, and great reduction of required support infrastructure and personnel.

Confidentiality and Risk Statements

The information, data and drawings embodied in this business plan are strictly confidential and are supplied on the understanding that they will be held confidentially and not disclosed to third parties without the prior written consent of Greengrass Enterprises, Inc.

This business plan represents management's best current estimate of the future potential of the business. It must be recognized that no business is free of major risks and few business plans are free of errors of omission or commission.

Point of Contact

Your questions and comments are most welcome. Please forward to Adam Greengrass, CEO, Greengrass Enterprises, Inc., 610-793-1474 (adam@greengrassent.com).

Token Plan

An ICO is an unregulated means of crowdfunding, via the use of Cryptocurrency, which can be a source of capital for start-up companies. In an ICO, a percentage of the newly issued cryptocurrency is sold to investors in exchange for legal tender or other cryptocurrency such as Bitcoin.

Over the last several years, as cryptocurrencies like Bitcoin and Ethereum have become popular, thousands of groups of developers have attempted to launch digital assets. In the last year or so, the number being issued in crowdsales, called initial coin offerings, accelerated to the point that, in 2017, according to data by CoinDesk, $1.5 billion has so far been raised from the crowd — more than twice the $695 million in venture capital funding into blockchain startups.

Now is the time to run an ICO for funding a startup, especially in the cyber security space. Cyber security is more interesting to cryptocurrency holders than any other tech sector product.

But one question hovered over these token sales: In the United States, would such offerings be deemed securities and be applicable to SEC securities oversight?

In July, the Securities and Exchange Commission issued a report stating that some crypto tokens may fit the definition of securities and would therefore be subject to certain investor disclosure and registration requirements. But the report left many questions unanswered, particularly around what the crypto community has taken to calling “utility tokens” — multidimensional coins which function only partially as a sort of equity in a network, whose value results from a mix of speculation in the asset and the demand for their use in that network. For instance, a token that powers a decentralized storage network, if it’s structured correctly, should grow in value as usage of storage on the network increases. However, unlike company stock, its value would not derive from any one corporate entity but from all the activity by a variety of actors on this open source network. In contrast to utility tokens, security tokens — coins that, like traditional securities, represent shares in an entity like company stock or shares in a limited partnership — don’t have any additional utility beyond representing the value of the fund and the profits would depend on the promoter.

There is still much debate over whether utility tokens are exempt from SEC regulations; for now, they seem to be.

The Secondary Market

All cryptocurrencies ultimately become part of the secondary market which resembles the OTC market for stocks and bonds but is currently an unregulated one that trades 24x7 worldwide. The reason this market has been successful is because a lot of people have made a lot of money with various ICO’s and are looking for new ICO’s to diversify their holdings. The bulk of ICO’s will not fulfill their promises and their Tokens will lose value because of it. Some, however, will fulfill their commitments, begin selling to the public and their Token values will soar. People are willing to risk cryptocurrency funds on the possibility that a company will fulfill its commitments however they are still actively seeking out ICO’s that have a clear business model, a well-defined core team and management team (Board of Directors) with people who are clearly assets and not just decoration, and who have already risen the amount of money necessary to spend to be successful before the ICO starts. Companies that go ICO without

these things will have limited success in the funds that are raised and may find themselves having to give it all back depending on how low they set the soft bar[12] at.

The Secure Enterprise Connect Token (SCT) is a utility token. Its purpose is to power the connectivity created by the Secure Enterprise Connect solution. In each step of the solution a transaction takes place which pays for that step in the solution with a token. To accomplish this the Secure Enterprise Connect solution would be pre-charged with a certain number of tokens to accomplish the necessary number of transactions that the customer would require over a predetermined amount of time. From time to time the customer would then be required to purchase additional tokens to recharge the Secure Enterprise Connect solution so that it would continue to function.

How Do Tokens Work in Secure Enterprise Connect

1) First, users authenticate to the devices they wish to use instead of to the networks they want to access. The TEE will be pre-charged with a certain number of tokens and every time a user authenticates to their device, one token will be utilized.
2) Once the user is authenticated to the device that device becomes known but not yet a *trusted* device. The Orchestrator Server will also be pre-charged with tokens and the process of turning a device into a known and *trusted* device will also utilize a token.
3) Once the Orchestrator knows the device is Known and Trusted, it then reaches out to an analytics engine which assesses device identity information, stored within the Blockchain to provide an extra layer of security that the known and trusted device has a list of accessible locations stored in the Blockchain and combined with an AI that tracks and controls the devices identity, the AI then decides whether or not to create connectivity for that device. The analytics engine and the AI will also be pre-charged with tokens and the process of engaging the analytics engine and the AI will use a third token.
4) The Orchestrator then sets up a connection from the device to the network resources that are required using software defined perimeter (SDP) as the transport. Based on the number of devices that are necessary to be included in the SDP, the Orchestrator will further charge 1 to 3 tokens for these services as well.

A utilized token is one that has been recorded to the blockchain as having been employed for a specific purpose. It is subsequently removed from the server that used it. From time to time as token numbers diminish the Company utilizing the service will be required to re-charge their servers with more Tokens. Tokens will be available to those companies either from the secondary market or, at a premium, directly for Greengrass Enterprises.

[12] The soft bar is the minimum amount of capital that an ICO sets. If at the end of the ICO the soft bar is not met all the money raised must be returned to investors. This is opposed to the hard bar that is also set which is the minimum amount that the Company will accept and keep for funding purposes. One the hard bar is reached the ICO is not required to return any of its funding.

Marketing Plan

Market Opportunity

Everyone agrees that the market for cyber security solutions is huge and growing at an astounding rate; there are a lot of technologies from which to choose. Most, however, are about analyzing every packet that traverses a network: identifying risks, and responding to threats in real time. Secure Enterprise Connect™ is the first solution to completely eliminate the risks and the threats.

History of the Solution

Think of Perimeter Security as a wall that surrounds your crown jewels. This wall is visible to hackers who constantly besiege it, creating a never-ending battle that costs a great deal of time and money in order to maintain the integrity of your perimeter. Even the most innocuous slip gives an attacker all that is needed to penetrate your defenses and, once this occurs, the battle is over. The attacker is through the wall.

Breaches today do not generally occur from brute force attacks. Companies are targeted, and hackers spend a great deal of time attacking the perimeter until they get a piece of their rogue code inside. Once that occurs it is only a matter of time before they can acquire everything. A large portion of breaches today also occur from authorized users accessing information. Secure Enterprise Connect™ allows only known and trusted devices to subscribe to network resources with the ability to track and control every device. It is a much simpler task to identify devices that are doing something suspicious even if they are authorized. Plus, with a Blockchain and a big data/analytics/AI environment at the core it will be simple to track exactly what was done and by which device. Since only rightful users can utilize devices, once the device is identified so is the user.

Business Value & Market Demand

There are five prominent drivers that create significant attention on how individuals, small businesses, corporations and government can protect their interests and intellectual property. They include heightened awareness of:

- Increasing complexity in technology infrastructure and services
- Rapidly growing security exploitations
- Widespread adoption of mobility and business trends toward BYOD, which means companies are allowing their employees to Bring their Own Devices, or to utilize their personally owned equipment for business purposes. While reducing cost to those companies that allow this, it also increases risk. Secure Enterprise Connect™ directly mitigates this type of risk.
- The revolution in moving to cloud based services
- “The Internet of Things” connecting planes, trains and automobiles to buildings, signs and even your dog’s GPS

Not every connection is lifesaving or business critical; ultimately, the more ‘connected’ we become the more exploitable surfaces exist. Market demand will likely gravitate toward capabilities that are robust, affordable, and simple.

Risk Evaluation

Strengths

- There is no Secure Enterprise Connect™ like solution in the market. The field is ready and waiting for a company like Greengrass Enterprises to provide the Secure Enterprise Connect™ solution as a service provider.
- PC networking is rapidly failing to function as needed because of the continued use of an ineffective security model. The new model suggested in this plan is based on changing the security architecture of PC networks to that which has been used successfully in the wireless market for the last 20 years. PCs, Servers and Workstations support the hardware technology that allows device subscription to replace user authentication as the primary protection model. Enterprises today are already talking about the need for a new paradigm as everyone wants a solution that supports a higher degree of mobility and flexibility for workflows while remaining confident that their data will be completely secure.
- The current day timing is optimal for creating value added propositions for sales to directly address new threats and breaches, whether they are first identified by us or are reported by the media. Each is an opportunity to score a quick win while building out the company's core product portfolio into new industries with new value propositions.
- Strategic partnerships with technology providers that offer critical components for the Greengrass Enterprises strategy.
- Greengrass Enterprises builds on existing security models, tried and true technologies and DoD level architecture in use today. No introduction of 'new' models; instead it fully automates their execution or implementation.

Weaknesses

- The Secure Enterprise Connect™ Solution is a difficult concept to convey. Marketing and customer/consumer education will require creativity and innovation. "Experiencing" Secure Enterprise Connect™ has proven more effective in communicating what it is, how it can be used and why it is important.
- Additional due diligence is required to accurately scope, assess and prioritize target markets, solution sets and revenue projections.
- As of the completion of this business plan, Secure Enterprise Connect™ is a concept and not a working software deployment, though components of it such as key entry within the Trusted Execution Environment are functional and demonstrable today. Before Secure Enterprise Connect™ can be brought to market the Company must build a functional model in a lab and fully test it, a process that will take 3-4 months for creation of the initial demonstration followed by 6-8 months of development prior to initial sales. To mitigate this the company will focus more heavily initially on small to mid-size companies where the sales cycle will be faster once we can demonstrate the product and its capabilities.
- Vidder, Inc. is already selling an SDP solution and other companies today sell the various components that the company will uniquely bundle into Secure Enterprise Connect™. However, the CTO of Vidder may be joining the core team of the Company to build Secure Enterprise Connect.

Opportunities

- FIRST TO MARKET Advantage. This represents the first opportunity to provide military grade, secure networking capability to the public. This approach eliminates the complexity and cost associated with hardware based security, dedicated network infrastructure and technical customer-side knowledge requirements.
- The design supports extensive opportunity for repeatability; maximizing investment capital and affording opportunities to generate multiples on return.
- The Company's intellectual property will generate new opportunities for data sales to existing software publishers.
- The Company intends to patent the workflow and the new use of these technologies as soon as it is possible to do so.
- Secure Enterprise Connect™ can easily be implemented as a bolt on to the SDP sold by Vidder or any future company and the same is true of the other technologies as well. No one is selling a fully integrated end-to-end device centric solution today; everyone is focused on the user centric model.

Threats

- The most significant threats are likely to emerge from micro-innovator or specialty / boutique security companies. These threats, as far as we know, do not yet exist.
- In absence of a leading industry competitor with executable vision focused on solving the Internet evolution gaps, other motivated entities may apply a deterministic approach to creating an "80% solution". This would mostly be mitigated through first to market advantage and a continued effort to build additional value into the Secure Enterprise Connect™ Solution.

Sandbox Solution

At the start of Year 1 the company will make available a "sandboxed" environment within which demonstrations will be performed and customers will be provided with access to an environment in order to test the Secure Enterprise Connect™ solution. There will be no charge to customers for use of this test environment.

Potential Target Markets

Aerospace	Automotive	Financial Services
Biotechnology	Chemical	Consumer Products
Education	Energy, Oil & Gas	Entertainment
Government	High Technology	Hospitality
Industrial Automation	Insurance	Manufacturing
Pharmaceuticals	Real Estate	Retail
Health Care	Transportation	Telecommunications

A multitude of application or use cases have been identified within each of these target markets. The company's initial focus, however, will be on providing remote access that eliminates many existing products that are designed to protect the security perimeter. This will reduce cost and increase the security for all remote users and the data to which they connect. IOT is a logical initial step as well.

Market Growth Potential

It is anticipated that major growth areas will emerge within financial services, healthcare, telematics and the machine-to-machine verticals. Further, E-Commerce and Internet based transaction services will need to find more secure and cost competitive alternatives to methods employed today. Lastly, any business where regulatory or compliance requirements are tied to data security is a natural for a Secure Enterprise Connect™ solution.

Sales Plan

Greengrass Enterprises has re-written the rulebook in relation to IT Security and has the creativity, relationships and business acumen needed to succeed. We will run a multi-faceted sales program that will include the following:

- **Sales Focus** – The Company's sales team will initially and primarily focus on sales to larger targeted enterprise customers. The purpose is to focus on quick wins that will bring customers in quickly. As we build a renewable monthly positive income we will focus more on larger and more complex customers.
- **Channel Sales** – The Company believes that the SMB and Consumer markets will also contribute to sales. To this end we intend to quickly build an inside sales organization to aggressively address this market, primarily through reseller agreements with partners who have established large customer bases in their respective channels. The Company's product will be rebranded for these markets and will respectively be called Secure SMB Connect and Secure Consumer Connect.
- **Development of API's and SDK's** with leading application providers and in leading vertical markets to "Secure Enterprise Connect™ Enable" specific public and industry specific applications.
- **Extensive use of the web to drive lead flow.** The Company intends to use Inbound Marketing instead of paying for traffic with search ads. Specifically, the Company intends to utilize SEO to build a remarkable website while simultaneously and professionally utilizing social media like Twitter, Facebook, LinkedIn, Digg, StumbleUpon, etc., to get the word out. Our goal is to get other bloggers to link to our site and to have people tweet on our content.
- **Use of a free product or service to attract web visitors, and aim for a viral spread as they tell their friends.** Examples of free products include Open Source software, services like HubSpot's Website Grader, free versions of a SaaS service that have limited, but still valuable, feature sets, etc. For instance, the first milestone in the Company's growth is to establish a sandbox (or free online demonstration) that can be used by anyone to fully examine and test our product.
- **Use of a free trial.** At product launch the Company will provide a downloadable version of the product. In combination with the demonstration version running from the sandbox this will be all any customer needs to fully test the product.
- **Use of the touchless conversion** to convert trials to paying customers.
- **Using low cost inside sales** when the touchless conversion is not possible (see Channel Sales above).
- **Extensive use of software to automate all processes** such as SEO, SEM, social networking, lead scoring, lead nurturing, CRM, etc. The Company will also build a portal site for administration and collection of metrics that will be able to be ebonded to, so that customers with existing systems that provide this information can take feeds directly from ours.
- **Metrics on all aspects of the customer acquisition process** will be tracked on an ongoing basis to find out what can be improved. ITIL focused Continuous Service Improvement will also be implemented.

- **Sponsorships/Co-Branding** – We will sponsor specific opportunities, products and services that bring incremental value to our Secure Enterprise Connect™ users. Additionally, we will co-brand other products and/or services and build them into the Secure Enterprise Connect™ Solution. These sponsorships and co-branded opportunities will generate additional income from the programs that will be setup with these partners.

- **OEM Licensing** – We will provide licenses of our proprietary technology for use by retailers, manufacturer's, financial institution's or any OEM that will be approved for this purpose.

Organization & Operations

Core Management Team

The Company's management team consists of individuals with unique and specific skillsets as well as extensive experience in various aspects of business strategies.

- Founder and CEO – Adam Greengrass: With a 30-year track record in Enterprise Security Architecture solution development, sales, and delivery, Adam brings outstanding technical sales abilities, organizational management, strategic business planning and development, solutions delivery and creativity. An expert in multi-disciplinary, cross platform IT solutions, Adam has also been an ICO consultant for the last year and has taken several companies through their ICO's. Adam has the expertise, technical leadership, and IT Process Expertise needed to establish long term customer relationships and successful ICO's. Throughout his career Adam has held executive and senior technical leadership roles with Unisys, Computer Associates, IBM and Verizon. Adam is a graduate of New York University.
- Chief Operations Officer – John Caserotti. With 30+ years of Business and Technology Leadership, John has held positions in both corporate and startup enterprises. He has served as a Chief Operations Officer at Perot Systems, Chief Technology Officer at Experian, and Senior Vice President at Bank of America. John's professional and leadership style is one of relationship management, team work, collaboration, professional growth, education, revenue generation, cost controls, quality services and delivery achieved by continuous process and efficiencies improvement, effective strategic goals alignment and focused on strategic and tactical action.
- Chief Technology Officer – Junaid Islam. Junaid Islam was the CTO and founder of Vidder and has over 25 years of experience in developing network and security protocols. Prior to founding Vidder, Junaid founded Bivio Networks which was the first Gigabit speed software-based security platform in the industry. Earlier in his career Junaid helped create networking protocols such as Frame Relay, ATM and MPLS while at StrataCom and Cisco. Currently, Junaid is the Co-chair of the Software Defined Perimeter (SDP) Working Group at the Cloud Security Alliance. Junaid will lead the software development team for the Company.
- VP of Business Development – Jay Dowling. Jay is a veteran of the telecommunications and high-technology industry with extensive executive level experience & training in direct sales, sales management, sales engineering, marketing, sales operations and business development. Over his career Jay has managed large multi-state sales regions with sales, engineering & service teams handling over $725 Million in revenue responsibility for Tier-1 telecommunications providers such as MCI & Verizon. Jay has also worked for smaller next-generation CLEC's such as Citizen Communications Subsidiary Electric Lightwave, and was a founding executive team member of BroadRiver Communications. In these roles he built sales teams from the ground up & helped a pre-revenue start-up raise venture capital funding and negotiate underlying service provider contracts for the company's IP network infrastructure and subsequent launch. Jay has direct sales and management experience with enterprise voice, data, mobility, machine-to-machine (M2M) and data center services as well as next-generation platforms such as cloud and virtual service offerings.

Board of Directors

- Steven Sprague – with 25 years of building and leading the growth of trusted computing technologies, Steven has been a key figure in driving the growth and penetration of open hardware security in billions of devices. He has served as a CEO and board member of Wave Systems Corp and is the founder of Rivetz Corp., a leading provider of TEE based security tools. Steven brings the highest level of expertise and practical business knowledge in the application of trusted computing to the project. Further, Steven's company, Rivetz, will be hired to assist in the ICO and provide the toolkit which will lead to the first version of Secure Enterprise Connect.
- Andrew Tarbox. Andrew is CEO of Thornebrook, LLC and brings more than 30 years of experience in the identity and smart card industry working with financial services, telecommunications, and government sectors. His cross-sector expertise and experience is particularly valuable to pragmatic approaches to large identity and payment deployments to consumers, business and government users. Currently he is leading the transformation of Identity and Access Control systems of a major hospital network with over 12,000 employees and over 1 million patients. He has supported the efforts of a number of companies including IDW, Wave, PRIVO, and TSCP as they worked with the NSTIC program office, a White House initiative to improve Internet privacy and security.
- Heather Wilson – Chief Data Officer and Head of Analytics and Artificial Intelligence, L Brands. Prior to L Brands, Heather worked at AIG as the Chief Data Officer and prior to that at Citigroup and Kaiser Permanente as Chief Data Officer, Global Head of Analytics, and Head of Innovation and Information Strategy.

Advisory Board

- Ari Singer. Ari is an energetic and experienced strategist, high-tech product manager, entrepreneur and security specialist. He is co-founder and CTO of TrustiPhi, LLC, where he leads technical strategy and solution delivery for enabling hardware-based security in next-generation devices. He is a former VP of Trusted Computing at Digital Management, Inc. and at NTRU Cryptosystems, where he was integral to helping to define the US Department of Defense's Trusted Computing technical strategy and enabling industry leaders to deploy Trusted Computing technologies. Ari has frequently served in leadership roles in standards organization including as chair of the Trusted Computing Group (TCG) Trusted Platform Module (TPM) and TPM Software Stack (TSS) working groups, as chair of the IEEE P1363 working group for public key cryptography and as security editor for IEEE 802.15.3, IEEE 802.15.4 and Efficient Embedded Security Standard (EESS) #1. Ari received a BS in Mathematics and a BA in Music from The Ohio State University, an MBA from Babson College and holds five U.S. issued patents.
- Jeff Schweitzer – with 30+ years of experience in IT Security and other complex IT solutions, Jeff is the current Chief Innovation Architect at Verizon and the inventor of the Software Defined Perimeter. Jeff's vision has helped the Company to invent Secure Enterprise Connect and his continued support will be invaluable to the success of the company.