# Executive Summary

## Our Mission

Secure Enterprise Connect, LLC 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]](#footnote-1), software defined perimeter[[2]](#footnote-2), blockchain technology[[3]](#footnote-3), big data[[4]](#footnote-4), analytics[[5]](#footnote-5) and artificial intelligence[[6]](#footnote-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™?

Secure Enterprise Connect, LLC 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, where 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 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]](#footnote-7), mobility, BYOD[[8]](#footnote-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 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]](#footnote-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 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.

1. 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]](#footnote-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.

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. Secure Enterprise Connect, LLC’ threat management solution will negate the use of third party anti-virus and anti-malware systems installed within the operating system on any device.

## 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]](#footnote-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.
* 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 Secure Enterprise Connect, LLC

Secure Enterprise Connect, LLC 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 Secure Enterprise Connect, LLC, 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, Secure Enterprise Connect, LLC, Inc., 610-793-1474 (adam@secureenterpriseconnect.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 another 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 crowd sales, 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](https://www.sec.gov/litigation/investreport/34-81207.pdf) 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 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]](#footnote-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 Secure Enterprise Connect, LLC.

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. [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)
3. Explained in detail on page 2. [↑](#footnote-ref-3)
4. Extremely large data sets that may be analyzed computationally to reveal patterns, trends and associations, especially relating to human behavior and interactions. [↑](#footnote-ref-4)
5. Information resulting from the structured analysis of other data [↑](#footnote-ref-5)
6. The theory and development of computer systems able to perform tasks that normally require human intelligence. [↑](#footnote-ref-6)
7. Virtual Private Networks have been the primary means that a remote user has used to access company resources while out of the office. [↑](#footnote-ref-7)
8. Bring Your Own Device refers to companies that allow their users to use their own devices to access company resources. [↑](#footnote-ref-8)
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. [↑](#footnote-ref-9)
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. [↑](#footnote-ref-10)
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. [↑](#footnote-ref-11)
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. [↑](#footnote-ref-12)