# Securing Civilian Cyberspace

# Beyond DoD Specifications

**Two-Factor Authentication (2FA)** - Is in fact Multi-Factor Authentication and the reality of every solution in this area is that they are only One-Factor when used on the Internet. When secure activity was introduced to the internet the recommendation was to use two unique factors. This would inconvenience customers from using websites, so the term multi-factor was introduced to mask the decision not to follow the most basic security protocol.

**'Today Multi-Factor' and 'Two-Factor'** have come to mean a process the gathers data in multiple steps at the endpoint and transfers the data to a secure environment for authentication. At the secure environment there must also be two or more factors for a multi-factor model to be valid, however, currently only data is presented. Data is only One-Factor, because of this corruption of the English language I have described the process as proof-of-presence.

Multi-factor authentication when properly implemented is only half the problem into securing the cyberspace domain: Ensuring data is not accessible without true establishment of presence is key to maintaining access of control over digital system and information systems.

Our patented solution combines Hardware Unique Factor technology in etching complex signature into silicon, this by way of chip - cannot be replicated. The Secure Execution Environment, which isolates secure information delivered from client servers onto external memory modules prevents access from rouge processes - while naturally destroying any trace of the session once USB IsoNuclei are removed from machine/computer.

> In cyber security “...today we can only use indirect assertions of identity. Until a direct assertion [solution] is available [identity] will just be an informed guess."
>
> - *Dr. Daniel R. Ford – Title Here*

Cyber Safety Harbor (CSH)'s products are a quantum leap in securing sensitive transactions on the Internet. Our patented system engages a new mindset in security; instead of reactive "patch-and-repair," CSH takes a new approach of reducing the universe of users, then engaging security before the portal is created, not after as is current methodology. This "disruptive technology" with incredible market potential. The primary product hardware, IsoNuclei, currently in USB form factor, contains both a Hardware Unique Factor (HUF) and a Secure Execution Environment (SEE) used to establish PRESENCE over cyber.

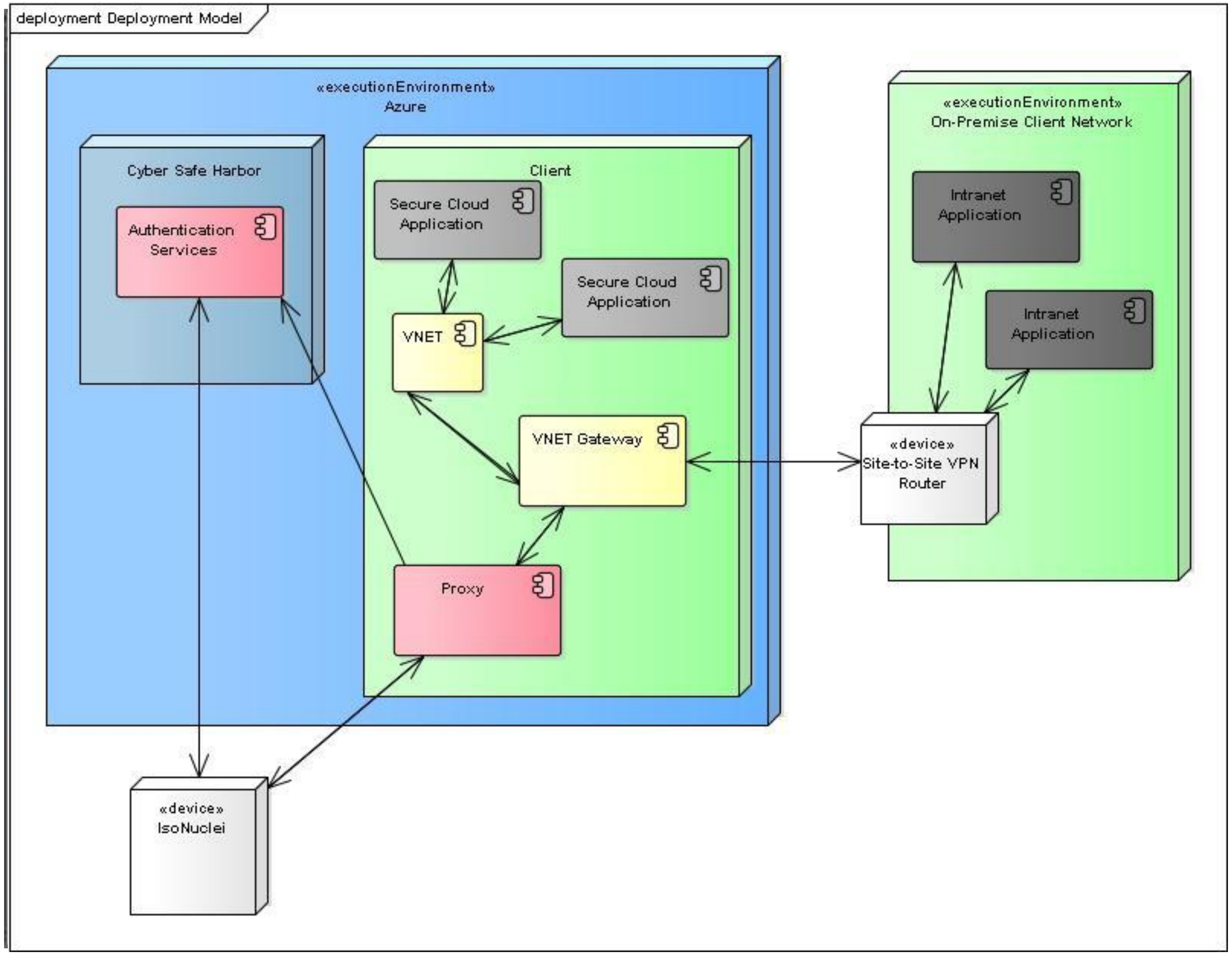
Originally designed for US Military Command and Control, CSH holds the patent on SimulNuclei which defines a set of IsoNucleis with authorization to perform a set of actions and then a subset of those whose presence must be established in order to perform one of those actions.Our HUF is an Atmel encrypted chip that is theorticaly physically impossible to duplicate once etched meaning, once registered with CSH's authentication services, only that specific IsoNuclei has the ability to authenticate. SEE's enable software to run in the memory space on the IsoNuclei itself, not on the Host OS, and therefore, since nothing is in RAM on the underlying computer, once the IsoNuclei is removed the session implodes and not only does the user lose access to the application but also there is no evidence of their session on the host computer, since there was none to begin with.

## Applications in the Legal Field

The initial market for IsoNuclei is projected to be Law Firms, particularly those in Mergers & Acquisitions. M&A Firms have increasingly been targeted for their documents, which are regularly accessible through "secure" web portals that this technology would eliminate. The cost-benefit ratio is high here as a single leak could costs billions and implementing this solution on top of something like SharePoint is trivial from both a technical and logistics standpoint.

## Applications in Private Banking

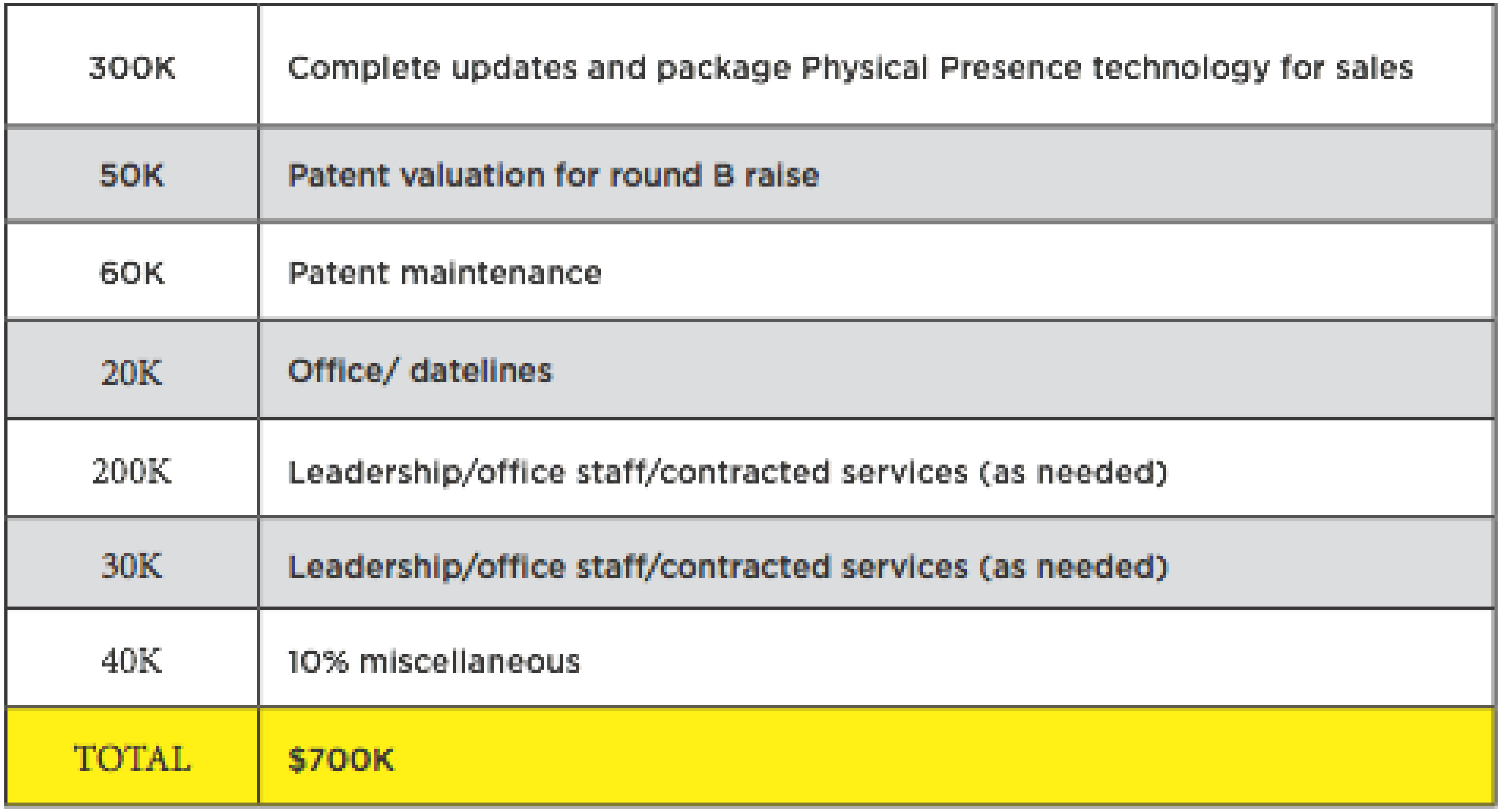
In private banking SimulNuclei could be applied to account actions like wire transfers where both the account holder and a banker both need to establish presence, perhaps the banker even at a physical location. This maintains the human authentication element many banks now require for some transactions while the transactions remain available in cyberspace.



The solution on the left is a next-generation implemention of CSH’s original co-located plan. In this CSH’s Authentication Services are deployed on Azure, first in a Virtual Machine and later as true PaaS solution where private authentication providers can deployed.The client then has deployment in Azure including a Proxy specifically designed to talk to the authentication services and relay web application back to the

IsoNuclei. Behind the proxy will sit a VNET that connects Site-to-Site with the client’s physical infrastructure for the proxy to access. The Proxy will be a packaged network component so that the client can be deployed, and marketed, under a true IaaS model.

COST BREAK DOWN FOR INITIAL START-UP



| | |
|---|---|
| 300K | Complete updates and package Physical Presence technology for sales |
| 50K | Patent valuation for round B raise |
| 60K | Patent maintenance |
| 20K | Office/ datelines |
| 200K | Leadership/office staff/contracted services (as needed) |
| 30K | Leadership/office staff/contracted services (as needed) |
| 40K | 10% miscellaneous |
| TOTAL | $700K |