

INFORMATION PAPER ON

Infiltron Software Suite

25 October 2020

Infiltron will replace the CAC card or any keyless system with one that integrates all forms of sign in information into one single sign in. For example, instead having to insert CAC card, password, and biometrics to access a classified laptop, Infiltron will streamline this process into one sign in with our extra secure verification and authentication function. If the power, satellite signal, or internet connectivity goes down, Infiltron will still provide security for connected devices and data by inserting a SIM card, circuit card, or hardwired cabling. These hardware devices can still be updated manually to provide Infiltron's latest security solutions in real time. Infiltron will implement any system rules such as HIPAA for healthcare, NIST for every system, Cybersecurity Maturity Model Certification for government contractors, legislation for industries such as finance and cannabis to make sure they follow their industry rules in real time. Infiltron watches how users behave within the systems it is installed on to give information to the business on how they can cut cost, improve system processes for better efficiency, and use innovative technology to improve cybersecurity posture. Out of this user behavior information, Infiltron creates fun, animated cybersecurity training modules that keeps the end user engaged to remember what they have learned this decreases insider cybersecurity threats as most threats come from employees mostly unintentional and sometimes intentional ex. Disgruntled employee. Infiltron can create this training per user, per location, and per device. Infiltron can also make sure other cybersecurity hardware and software are up to date. For our military airplane and communications people, we can detect if China is trying to jam or stop our communication signals and block them from carrying this action out in a fourth of a second. Infiltron can do similar detecting and blocking for credit/debit/procurement card transactions before the bank alerts you, transportation such as aircraft, ships, and other modes of transportation manned and unmanned. Infiltron also provides an emergency alert system for Air and Space crews through washable, wearable fabrics built into their uniforms. This allows the crews to speak back and forth to command. They can also text back and forth to command via their Velcro name patch that we have turned into a simple, encrypted, smartphone. Infiltron's services reduce bandwidth, increase encryption of ALL types of data, and speeds up how fast that data moves regardless of size. With military installations being turned into smart cities that will use facial recognition, Infiltron is the only Internet of things company that resolves issues where facial recognition does not accurately detect people of color or women. We are currently testing this at voting polls to improve overall accuracy detection of people of color and women.

A recent technological advancement is called the Internet of Things (IoT). Businesses have invested tremendous amount of money into utilizing these devices. IoT allows businesses to capture sophisticated information that allows them to view how consumers behave and use their products. IoT devices are connected back to businesses through network communications and the internet. In September, the House of Representatives passed a bill requiring that all internet of things (IoT) devices purchased by the government meet minimum security requirements. Some

studies suggest that as much as 98% of traffic from IoT devices are unencrypted today, and clearly that number has to become near zero.

There is an ongoing battle between hackers and information holders. To minimize risk, businesses, government agencies, and consumers require sophisticated security software, passwords, and extensive training. Infiltron meets the NSF program's focus because it is proactively seeking to provide security for latency technology and its entire network of devices, data, and signal transmissions. The Infiltron software suite will help all organizations mitigate risk, sustain consumer trust, and comply with government regulations.

We are DFARS compliant and CMMC compliant. Infiltron can reduce bandwidth, increase redundancy, and reliability because of the beyond the edge capabilities of our solutions.

Infiltron's patented internet of things cybersecurity technology will provide best-in-class security verification platforms that can be deployed to a variety of operations and situations. These include 5G, smart-systems, hybrid, and legacy systems. Infiltron's platform can be easily adapted to fulfill the needs of these environments by creating user verification systems for sensitive computers, which enhances the operational security of business and government systems. The following list captures the reasons Infiltron's cybersecurity suite is best-in-class:

The Infiltron Software Suite leverages artificial intelligence, blockchain, quantum, and deep learning to provide compliance and reduced bandwidth with our quantum function. Infiltron's technology audits and monitors employee behavior with data and devices connected to the system for compliance in Transportation, DoD, Healthcare, Insurance, and Financial Systems in real-time.

- The Infiltron Software Suite provides a minimum of protected 3 Factor Authentication. It secures data and devices regardless of connectivity.
- The suite enables real-time SMART compliance and governance. It helps your agency meet HIPAA, GDPR, NIST, POPI compliance guidelines.
- The system can be customized to an individual business's needs for strategic platform or dashboard integration.
- Infiltron's software analyzes user behavior for compliance to provide data analytics to give the business to solve problems facing the organization. It can help cost reduction efforts, improve system protection, and help improve efficiency of business processes.
- It can audit technology software and hardware for cybersecurity posture and biases.
- Infiltron's solution is socially aware to defend against racial and gender bias. Internet of things (IoT) sensors in smart ecosystems, such as smart cities, smart transportation, and smart offices, will check you and your device activities in real-time. That very same technology is used against you if you are black, brown, a woman, or transgender. We

protect our black and brown military and civilian personnel as military installations are gearing up to use facial recognition.

- Our solution integrates with IaaS [internet as a service], SaaS[software as a service], PaaS[platform as a service], CaaS[containers as a service], FaaS [Function as a service], SIM Cards, and secure FPGAs [Field-programmable gate array].
- Create real-time cybersecurity training modules for individuals and organizations per device, system, and location.

DoD Solutions:

- Infiltron will leverage Artificial Intelligence (AI) to pull actual biometric data to verify for authentication and verification. Our technology can be used to confirm and identify pilots before they take off to avoid hijacking or any unauthorized use of equipment, procurement cards, base/building access, and more. For example, with the Smart Base initiative, Infiltron can integrate biometrics with DS Login, CAC Cards into a single sign in and to provide added cyber posture.
- Protects, verifies, and authorizes procurement card and signal transactions across networks to prevent fraud/jamming in real time. Our patented, unique encryption methods enhance confidence knowing Infiltron is working behind the scenes during signal transmissions, protecting proprietary data, proactively detecting jamming and connected devices.
- Access Air Force and connected systems (ex. Government contractor or Remote civilians). Infiltron's technology would securely identify the user and grant appropriate access. This could also be adapted for airmen and civilians working from home networks. The software works for government issued smartphones. One example is CE Group who are mobile and could use Infiltron SIM for protection and object recognition for efficiency.
- Smart Base Facial Recognition Mitigation. 11 USAF Smart Bases rollouts – Infiltron's solution is socially aware to defend against racial and gender bias. Internet of things sensors in smart ecosystems will check you and your device activities in real-time. That very same technology is used against you if you are black, brown, a woman. Our solution can protect our black and brown military and civilian personnel as military installations are gearing up to use facial recognition.
- The capabilities of Infiltron software support the objectives related to cybersecurity: security tools, test bed concepts, intrusion detection or AI-based malicious behavior detection). Infiltron's innovative solution emphasizes confidentiality, authenticity,

integrity, availability, and non-repudiation, which improves the capabilities of current military communication systems and avionics.

Chasity Wright
Title: Founder/CTO
Telephone Number: (478) 978-9779
E-Mail: cto@infiltron.net