Can Siometrix arrest the increase in high-profile hacks?

JANUARY 2023

SHANTANU BHATTACHARYA, FOUNDER AND CEO, SIOMETRIX

INTRODUCTION – THE CONTEXT

Would you benefit if you had more reaction time before damage to your infrastructure due to a cyber-attack? What if you could prevent some types of cyber-attacks while reducing the impact of others?

If your organization might benefit from the above, continue reading the white paper. I might have a solution of the kind described above.

For “Stranger Things”, fans where plotline kept everyone guessing which teenagers across the town started getting killed, one by one. But before each demise, they started acting strangely - experiencing headaches and nightmares suggesting that Vecna, the mysterious evil, was beginning to take hold. Similarly, is there any solution that rings alarm bells that indicate a possible attack and provide you with time to remediate the attacks? Read on to find out.

SOME RECENT PROMINENT DIGITAL IDENTITY HACKS

In December 2022, an individual lost control of their myGov account (an Australian government-provided account for various services) without any particular error or risky behaviour from the individual. Instead, it appears to be an error from the government department.

Optus, a multi-national telecom operator owned by SingTel, was the subject of a ransomware attack in September 2022. Although online sources indicate that as many as 10 million customer accounts were exposed, solid information about what happened has been scarce. However, reports suggest Optus had an application programming interface (API) available online that did not require authorization or authentication to access customer data. In the instance where a public API endpoint did not require authentication, anyone on the Internet with knowledge of that endpoint [URL] could use it to see sensitive data.

Entrust is a major — and highly credible — player in the global identity and encryption market. The company has confirmed, in July 2022, an ongoing ransomware attack that has seen data from its internal systems stolen. The breach bears similarities to an attack earlier this year on another digital ID provider, Okta, and could have serious consequences. Entrust is a solutions provider for various organizations, including US government agencies, such as the Department of Homeland Security (DHS), Treasury, Health & Human

Services, Energy, Agriculture, and Veterans Affairs. The company claims about 10,000 customers in 150 countries, including high-profile private and public companies like Microsoft and VMWare. These organizations entrust the security vendor with critical services such as identity management, user and machine authentication, issuance of IDs, secure online payments, and encrypted communications. A breach in third-party software vendors is suspected here.

A ransomware cyberattack hit Accenture in August 2021 from the LockBit ransomware gang. Accenture is an IT giant that serves various industries, including automobiles, banks, government, technology, energy, telecoms, and many more. Valued at $44.3 billion, Accenture is one of the world's largest tech consultancy firms employing around 569,000 employees across 50 countries. 6 TB of files stolen; $50 million ransom demanded. The threat actors claim access to Accenture's network via a corporate "insider."

Ransomware attacked Colonial Pipeline, USA's refined product pipeline from Texas to New York, in May 2021. The attack vector is not available in the public domain. However, the suspects are combined vulnerabilities in IoT infrastructure, lack of segregation of IT and OT networks, phishing attacks and privilege escalation. The result affected the billing system, halted the IT & OT networks and compromised the PII of 6000 individuals. It started with the compromise of an unused VPN account.

Bulgaria's tax revenue office lost 5 million citizens' data in July 2019. The country's population is 7 million, indicating the entire adult population lost their data. The attacker exploited vulnerabilities in the third-party software providers' arsenal.

More than 85% of all cyberattacks begin with a phishing attack that, most of the time, culminates into a digital identity hack. Even though we have not established that these hacks started with identity hacks, their analysis indicates so. In most cyber-attacks, it is almost impossible to confirm the attack's origin with 100% certainty.

For the rest of the discussion, we would explore all the commonly used digital identity technologies and solutions from a technology standpoint, not necessarily a vendor standpoint. So, we would not differentiate different vendor solutions using the same technology, except where necessary, due to its popularity or visibility.

Let us check out some of the widely used existing technologies available and predominantly used with their strength and weaknesses.

EXISTING TECHNOLOGIES – STRENGTHS AND WEAKNESSES

Passwords: This is a commonly used technology and one of the oldest technologies. It is easy to implement and has minimal effect on usability. Also, due to the technology's age, most users understand its usage process.

Even though it is easy to use and implement, if one could have a long and strong password, say 25 characters long, it is still difficult to crack using brute force or dictionary attacks. The definition of a good length and its strength is well known. So, it is still the most popular authentication methodology.

However, some vendors do not implement it in the best possible way. For example, some implementations restrict password length to 6 characters, which is easily crackable. Others do not encrypt the password when stored, making it easy to obtain. Further, as numerous websites and agencies require passwords, they are often repeated across vendors or handle forgetfulness by using easy passwords.

The above scenario has given rise to a call for passwordless systems. We will see some of them discussed here.

Human Biometrics: Many human traits are unique, like fingerprints, faceprints, iris scan prints, etc. Due to its novelty, humankind has started treating it as the gold authentication standard. However, even the most accurate human biometrics, like Iris Scan print, when taken from both eyes, have an error rate of 0.77% - around seven errors in every thousand. Is this good enough? Of course not. In addition, it isn't easy to take an Iris Scan print and implement it. In short, human biometrics has significant perceptions of accuracy within humans but fails in the test of accuracy.

Short Messaging Service One Time Password: Many vendors suggest customers provide their mobile numbers so that the vendor can send a Short Message Service (SMS) with a One Time Password (OTP). This is good as this uses a different channel to send an OTP code than the primary authentication. However, like the Internet, the mobile network was designed assuming that all parties and components are trustworthy. However, we know that does not hold in current circumstances. There are well-known techniques to hack a mobile phone remotely without physical access and with very little detail about the mobile phone.

There are other mechanisms of authentication discussed in this white paper that has similar vulnerabilities due to the use of mobile phones.

Authenticator Apps: Several authenticator apps are available in the authentication market. They all provide One Time Password (OTP) on a mobile app. They have the same strengths as SMS OTP. However, there are known attack vectors for each. I will describe the overall attack vectors for each and leave you to research further if interested. Google and Microsoft authenticators are the most popular ones. Google authenticator is prone to Cerberus attacks, while Microsoft authenticator's default configuration is insecure. Not convinced that a wrong configuration can be harmful? Insecure configuration breached NASA and Amazon S3. Most end users are unaware of the secure configuration settings and can easily fall victim. These attack vectors are in addition to the mobile phone remote hack I discussed earlier.

FIDO Alliance: FIDO Alliance is a candidate solution for passwordless authentication. It uses a mechanism similar to PKI (at least some PKI algorithms) for authentication. However, FIDO uses unauthenticated Diffie Hellman (a commonly used algorithm in PKI key exchange) as part of the process. In addition, some other vulnerabilities make the solution a little weak.

Passkeys: Apple, Microsoft, and Google launched Passkeys in the second half of 2022. However, Passkeys have the following vulnerabilities in addition to the FIDO Alliance vulnerabilities:

- Sharing Passkeys can be exploited by phishing attackers, and
- Passkeys use cryptographic keys without expiry, giving rise to a possible attack on their strength. The reason why PKI certificates have an expiry date is.

International Mobile Equipment Identity (IMEI) number: manufacturers assign an IMEI number to each physical mobile phone for unique identification. The uniqueness of IMEI lasted for some time till some Chinese experts demonstrated that duplication was possible. Unfortunately, that destroyed the uniqueness of the IMEI number and its potential use for authentication.

Internet Protocol (IP) address: IP is a pillar protocol for the Internet we use. When a device wants to connect to another on the Internet, both need IP addresses for identification. However, there are straightforward ways of spoofing IP addresses. Hence a device's IP address cannot be considered unique and, therefore, cannot be used for reliable authentication.

Media Access Control (MAC) address: Every Internet device also has a MAC address and an IP address. Layer 2 uses MAC address to communicate at the 7-layer ISO (International Standards Organisation). The network card manufacturer assigns the MAC address on the device from their allocated quota.

ECCMA Shared Item Master (eSIM) identifier --- eSIM is a 32-digit embedded UICC (eUICC) Identifier for the SIM cards within mobile phones. eSIM is an excellent unique identifier for the SIM card, but the attacker can change it when they get physical access to the phone.

WHY DID THEY FAIL TO PREVENT THE HACKS?

So, why are such critical hacks a cakewalk for attackers despite the existence of varied technologies? Are there no technologies that can protect against these attacks? Or are the technologies ineffective? Or is it the incorrect deployment of the technologies?

The answer is all of the above. Some attacks are due to ineffective technology, and others are where the technology deployment is incorrect. But one thing is sure. New approaches are available that turn this position of weakness into the position of strength in all of the scenarios discussed here.

THE WAY FORWARD

We have seen a gamut of technologies with their strengths and weaknesses. Before we surmise the way forward, we should analyze the attack vectors used against the digital identity solutions in the market.

THE ATTACK VECTORS THAT VICTIMIZE DIGITAL IDENTITY SOLUTIONS

It is time to discuss some commonly used attack vectors that attackers leverage.

Account Hack

Account hacking is by far the most popular attack vector. Most other attack vectors generally also culminate into account hacks. We have seen that around 85% of all cyberattacks start with phishing (a social engineering attack) and target account compromise. Account hacks could consist of users, customers or admin professionals.

Operational Technology (OT) Network Hack

OT network is mainly used by building, utilities and manufacturing (heavy and light engineering) industries. Examples are water and electricity distribution networks in utilities. Aircraft engine manufacturing, factory floors and conveyer belt-based manufacturing are examples of OT networks. The biggest worry of OT networks is the vulnerability of the parts constituted by the Internet of Things (IoT) devices. Many IoT devices are cheap, making it difficult to secure them as the cost of security will surpass the device cost. However, they are critical for critical infrastructure and other vital industries. The attacks can be taking admin control, replacing an IoT device in the supply chain with a fraudulent part, illegitimate change in the IoT device configuration and harming the factory operations.

Border Gateway Protocol (BGP) Hack

Border Gateway Protocol (BGP) is a protocol for intermediate routers that form the Internet infrastructure. Consider you were sending an email from London destined for an individual located in California. Your machine in London does not directly connect to the device in California. Many intermediate machines operate 24x7 to enable connectivity from the London machine to the California machine. BGP is one of the many protocols that facilitate that automated connectivity. Corrupting the BGP-delivering devices can lead to the email destined for the California machine going to Delhi, for example. The BGP attacks can affect the participants in a communication or even a transaction, financial or otherwise, stock or crypto exchanges or other routing changes for the data transferred. It is important to note that the source or the destination machines do not control BGP machines. So, any amount of security cannot prevent attacks of this type.

Transaction server hack

Let assumes a retailer operates online and transacts over the Internet. If the retailer's server machine that facilitates the transaction is hacked, the transaction participants' validity and the transaction's integrity could be compromised. Moreover, the compromised server can lead to hacking other machines in the retailer's infrastructure. This attack is similar to the BGP hack, except the server is within the retailer's control.

External software hack

Again, consider the example of the retailer in the previous case. Generally, the retailer will use a payment gateway from a third party, a database from a third party and many other software components that third parties provide. If the hacker successfully compromises the payment gateway, all transactions could be compromised. Here again, the third-party software is outside the retailer's control but has a hard dependency on it. Attacks of this kind can affect the supply chain software, the software Application Programming Interface (API) or even a virtual machine that the retailer uses.

Mobile hack

Nowadays, mobile phones perform a lot of Internet activities. However, as we have seen before, mobile phone hacks are very much possible that can compromise the mobile telephone by remote hacking, SMS hacking or even SIM swapping hacks. SIM swapping hacks are instances where the attacker transfers the victim's mobile network from the victim's mobile device to the attacker's mobile device.

We have now seen the variety of attack vectors that attackers can use. It is worth noting that there are many options for the attackers, while the victim needs to protect against all of the attack vectors – a much more complex undertaking.

IS THERE ANY BETTER SOLUTION?

The challenge is to detect and block "strange" user behaviour before time runs out. It is critical to race against time and complete remediation before harm occurs. It is very challenging, considering the attacker would try their best to cover up their tracks. So, detecting and then remediating in time is not for the faint-hearted.

So, can solutions address some of the challenges discussed here? Unfortunately, the existing solutions in the market rejig the already known technologies and hence have limited effect.

However, some solutions track the hardware in operation more accurately, thereby removing the current technologies' inaccuracy issues. However, the hardware tokens like RSA tokens available in the market are expensive to manufacture, distribute, maintain and run.

Two emerging technologies solve the hardware token problems. They are Physically Unclonable Functions (PUFs) and Silicon Metrics (Siometrix).

PUFs add hardware to your existing hardware producing non-replicating circuitry uniquely identifying the devices. Siometrix, on the other hand, derives the hardware uniqueness from existing devices without any hardware change required. So in that sense, Siometrix has some apparent advantages over PUFs.

What if I told you Siometrix could increase your available time before any harm? Yes, Siometrix can keep the integrity of the transactions even after the attack and will start declining the fraudulent transactions, provided you have protected your transaction participants using Siometrix. Thus, you not only get alarm bells ringing due to declined transactions but can also start remediation work before any fraudulent transactions occur.

STRENGTHS AND WEAKNESSES OF NEW SOLUTIONS

PUFs and Siometrix leverage the same principle of physics – the analogue part of hardware can uniquely identify the hardware – PUFs introduce new hardware for the purpose. In contrast, Siometrix extracts uniqueness from existing hardware and calls it Silicon Metrics (Siometrix).

Physically Unclonable Functions (PUFs):

PUFs have the following advantages:

Key Encryption Key: The most popular use case for PUF technology is creating and storing the cryptographic root key for a device. The cryptographic root key created by the PUF does not require key insertion/storage and is hence not replicable to a new gadget as it is never stored. Instead, it is reconstructed from the device's silicon fingerprint whenever needed. Since this fingerprint is different for every chip, there is no way for an attacker to copy the key across devices.

Secure Vault: What if an IoT device stores sensitive data that needs to be protected? The data could be valuable IP that contains proprietary secrets or measurement data that is privacy sensitive or system critical. That is when the device requires a secure vault. A secure vault can securely store and physically bind to the device's hardware. This uniqueness can be achieved easily with a PUF by encrypting all sensitive data with a key derived from the PUF root key. Combining this encryption with message authentication code (MAC) functionality enables IP and validates data before use.

Chip-to-Cloud Authentication: To set up a secure channel between an IoT device and the cloud based on a public key infrastructure (e.g., a transport layer security (TLS) connection with a cloud service), the device and cloud exchange certificates. These certificates authenticate each party. A public/private key pair is made from the PUF fingerprint to produce a certificate for authenticating a device. Authentication is performed through the steps illustrated in the figure below.

Once the device obtains a public/private key pair certificate, it can start mutual authentication with the cloud by exchanging certificates. After mutual authentication, a key agreement protocol for cryptographic key

exchange runs. Finally, the exchanged keys apply end-to-end encryption and data authentication. End-to-end encryption ensures attackers cannot eavesdrop on the communication between two entities. Data authentication (with hash/MAC functions) assures that received data comes from a trusted source and has not been tampered with in transit.

The private key used to create the device certificate in this scenario is generated and securely stored by the PUF. Likewise, the session key the devices receive from the cloud during the key exchange is also stored securely by encrypting them with keys derived from the PUF.

Now let us delve into some disadvantages of PUF:

Requires additional hardware introduction: For the PUF-based workflow, introducing new PUF hardware is a must to make it functional. That is not possible in many of the use cases.

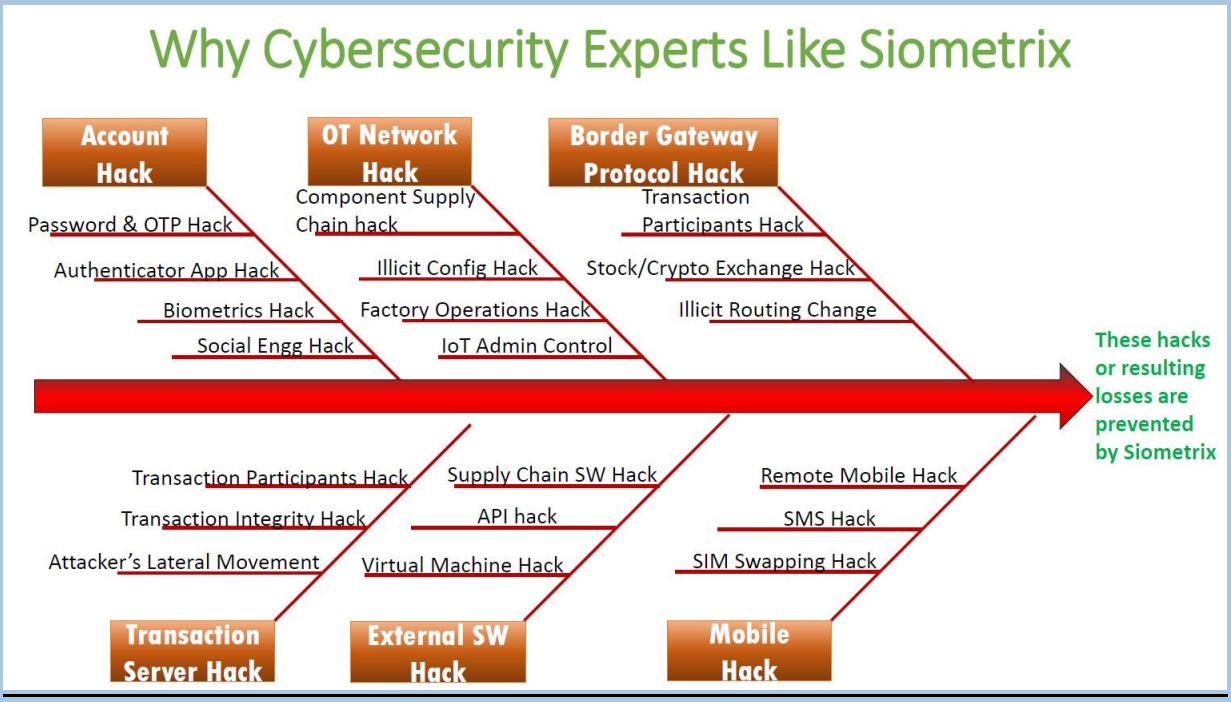
Still relies on Public Key Infrastructure (PKI): As you might have realized by now, PUFs provide you with a key that can leverage PKI. However, PKI is very expensive, complex and technology with many moving parts. The complexity and multitude of moving parts give rise to incorrect implementations with bugs. And as a system is only as secure as the weakest link, that does not make it very secure.

PUF can work without PKI, but technology solutions focus on leveraging PKI, resulting in unnecessary drawbacks.

Silicon Metrics (Siometrix):

As we have seen, Siometrix also leverages the unique nature of the hardware to derive Silicon Metrics that we call Siometrix. However, we have built a solution and business model around the technology that does not use PKI. So, let us see some of the advantages of Siometrix:

Resists against all attack vectors discussed in this white paper: Siometrix can either prevent the attack vectors or reduce their impact when deployed.



Benefits of Siometrix for businesses: So why will senior executives be interested in deploying Siometrix?

There is a multitude of reasons.

It is no secret that cyber insurance premiums are going up by the hour due to the high regularity and frequency of high-profile attacks. Therefore, it is natural that cyber insurers carefully consider their risk when they insure an organization.

Identity and Access Management has many security components. They are securing employee, customer and administrator accounts. In addition, security controls must exist to ensure that any attack on them can be detected before harm occurs. Then a team needs to monitor to ensure that the attacks are detected. If the monitoring team gets many false alarms, they are fatigued and will miss actual attacks. Finally, if the attack did happen, a separate team is required to recover from it. Any efficiency in the strength of the account protection can trigger considerable savings down the line. Siomterix can significantly strengthen account security, thereby bringing in much-needed savings.

Are you wondering how much you could save?

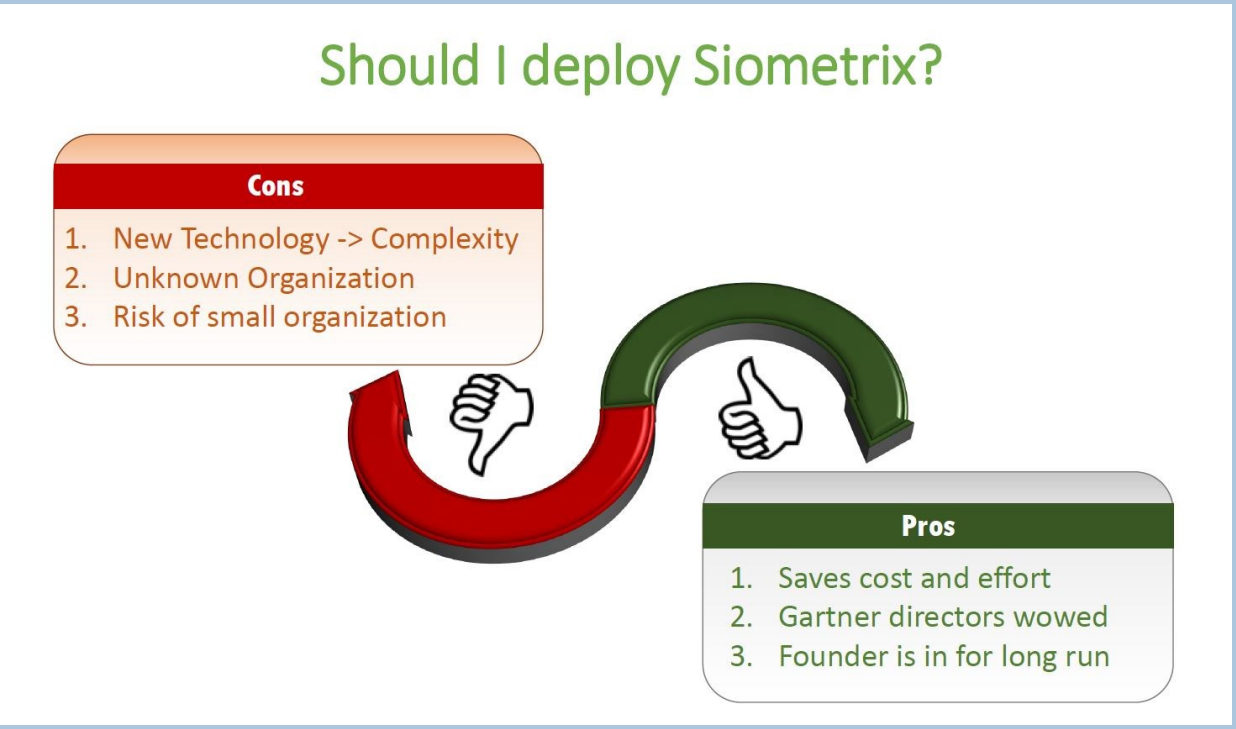
Here is a calculator that computes your potential annual savings in Identity and Access Management (in-house or outsourced) by deploying Siometrix.

Siometrix increases your organization's security by SIX TIMES. This claim is extraordinary that demands great proof. Siometrix can keep any fraudulent transaction at bay even if one or more of these are hacked - employee's password, customer's password, admin's password, transaction server, supply chain software and BGP node. That is FULL SIX BREACHES!

As inferred from this discussion, Siometrix has some unique benefits that none of the existing digital identity technologies or solutions can deliver. I treat technology and solution differently as they can be very different in the business context. Not all technologies can be easily used by businesses as is. Siometrix is a solution with components other than the technology and is discussed in this white paper.

SIOMETRIX – PROS AND CONS

Like any other technology, Siometrix is not free from pros and cons in the business context. The associated figure shows you the overall picture. Let me delve a bit deeper into the factors.



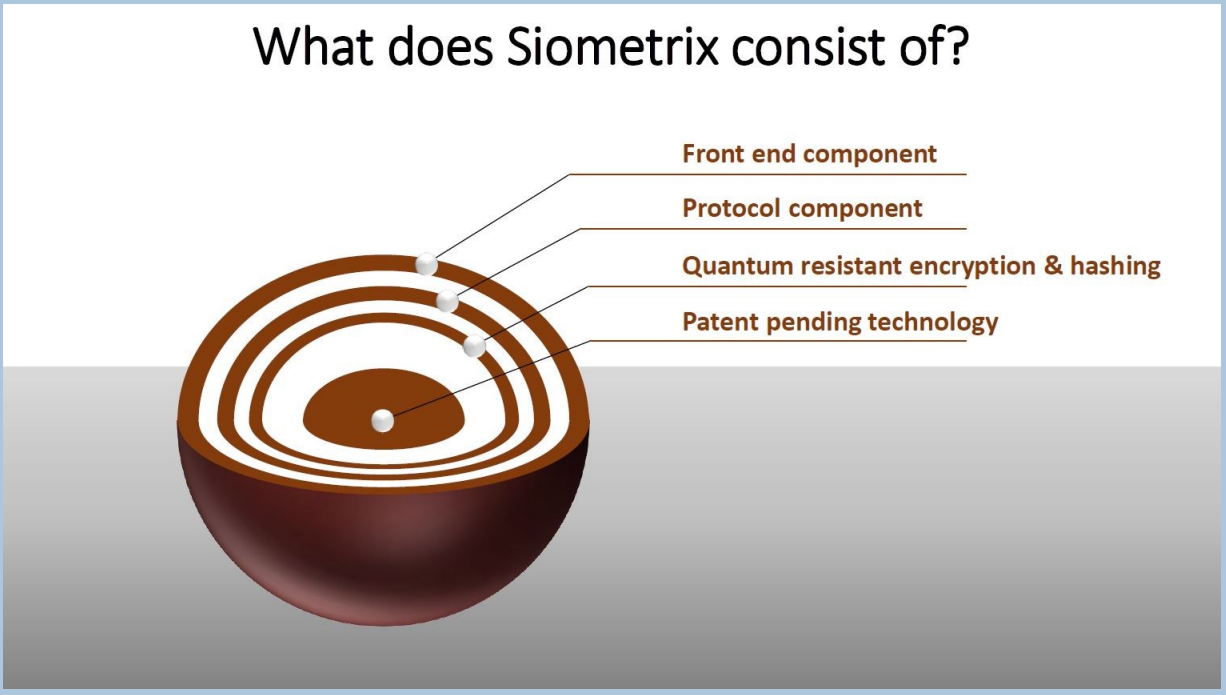
Let us discuss the cons first to ensure businesses like yours can deploy with their eyes wide open. We have simplified the technology deployment of Siometrix. So much so that no specialized skills are needed to deploy, maintain and run the technology. But there is some complexity by virtue of its newness. Siometrix is a new technology, and so is our business. Hence you might find it challenging to rely on it. However, I must say that the founding and advisory teams have extensive experience in the cybersecurity and IT industry. Hence, they have been on the other side of the table earlier. They have tried to plug every hole that they knew would concern adopters.

Now let us explore the pros. We have already discussed some significant wins that are available with Siometrix deployment. In addition, cost and effort savings will make it worthwhile. Finally, we have demonstrated the technology to several Gartner directors worldwide, who all thought Siometrix could be one of the world's most innovative solutions.

You can also find the areas your organization will benefit from by filling out the details here.

COMPONENTS OF SIOMETRIX

The solution built around Siometrix has four components that the diagram below shows:



BUILDING SUSTAINABLE BUSINESS USING SIOMETRIX

I have been questioned by several industry experts about the status of Siometrix – whether it is still a technology or a solution. That will change how adopters will look at Siometrix. Though adopters will not directly benefit from Siometrix's success, they would like to understand how stable it is and if Siometrix will go out of the market as soon as it surfaces.

We are open to adding clauses in the sales agreement to support it for at least a predetermined number of years. Further, the technical risk of the solution has been significantly reduced and hence will be able to provide the benefits outlined in this white paper.

We would monetize the solution by charging organizations a small fee per year for each user. As a result, online retailers would derive maximum benefit from Siometrix deployment in their transaction workflows.

However, Siometrix can create wonders in many use cases other than authentication. A few examples are securing water or electricity distribution networks. It ensures the distributors and end consumers can act out their roles without any fear of fraud. For example, a car rental company can benefit from using mobile phone-driven cars. Mobile phones can start or shut down cars instead of physical key fobs. Furthermore,

mobile phone operation would enable the rented vehicle to be dropped off or picked up from any point – not necessarily the offices of the car rental company, increasing efficiency and bringing down costs significantly.

Consider manufacturing an aircraft or car engine. Aviation accidents have occurred, including one in a helicopter, due to fraudulent parts made into the engine. Each of these engines comprises of hundred thousand IoT devices. It is a nightmare to track and ensure that each IoT device comes from authorized suppliers. In short, they are detecting supply chain fraud and ensuring supply chain integrity. Siometrix can help in reducing supply chain fraud.

Many other areas can see dramatic improvements due to the deployment of Siometrix. However, a detailed discussion is absent in this white paper due to a lack of space, as the focus of the white paper is digital identity fraud addressing.

CONCLUSION

Siometrix is a solution that can bring many advantages to its adopters. It can be a game-changing solution needed in the digital identity space.

ABOUT SIOMETRIX

Siometrix is a patent-pending technology that addresses digital identity fraud in a world where high-profile attacks starting with digital identity hack, is becoming increasingly frequent. Siometrix provides its adopters with some unique benefits unheard of in this space – resilience despite successful attacks and attack resistance not seen before are some of them. Interested in finding the fantastic benefits you can get? Check this out. Visit us at www.siomterix.com