MPRISE

Merritt Enterprise Software
& Applied Sciences

The Future of Cyber Security
Protecting your data with love!

About Us

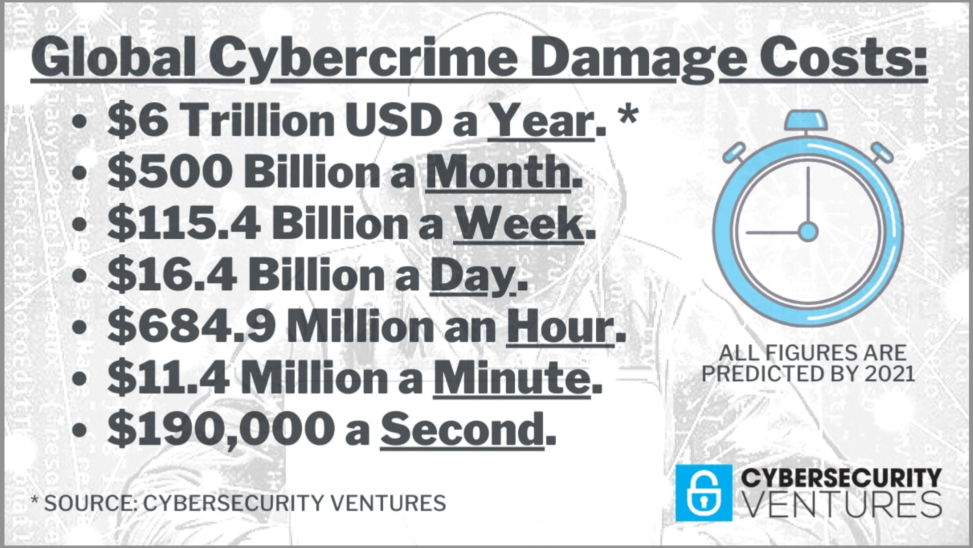
MPRISE (Merritt Enterprise) is an innovative startup focused on providing cutting edge security solutions for businesses. Through our advanced use of artificial intelligence and blockchain technology, we offer products that protect and secure your valuable data.

The Problem

Cybercrime Complaints

• Each year, approximately 15 million Americans are identity theft victims with financial losses totaling close to $50 billion. On April 4, 2018 Facebook Inc. said data on most of its 2 billion users could have been accessed improperly.

•Eighty-seven million Facebook users around the world were victims to one of the social network's largest data breaches. How can today's society feel safe with more and more cyber attacks against our privacy?



Global Cybercrime Damage Costs:

- **$6 Trillion USD a Year. ***
- **$500 Billion a Month.**
- **$115.4 Billion a Week.**
- **$16.4 Billion a Day.**
- **$684.9 Million an Hour.**
- **$11.4 Million a Minute.**
- **$190,000 a Second.**

ALL FIGURES ARE PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY VENTURES

- DATA BREACHES- April 04, 2018 Facebook Inc. said data on most of its 2 billion users could have been accessed improperly, giving fresh evidence of the ways the social- media giant failed to protect people's privacy while generating billions of dollars in revenue from the information. Eighty-seven million Facebook users around the world were victims to one of the social network's largest data breaches. About 70 million were affected in the US, 1.1 million people in the UK, Philippines and Indonesia may also have had their personal information harvested, and as well as 310,000 Australian Facebook users. With MPRISE Software we can totally solve both of these problems.

Cybercrime Complaints

- Nearly 42 million Americans were victims of identity fraud in 2021, costing consumers $52 billion in total losses, according to a new report cosponsored by AARP. The study, produced by Javelin Strategy & Research, notes that with so many more people relying on the internet due to the pandemic, criminals had plenty of opportunities to harvest their victims' personally identifiable information (PII). Thieves were especially eager to capitalize on the billions of dollars in stimulus funds that many people received as federal economic impact payments last year.

- These factors and others caused losses through traditional identity fraud to increase by 79 percent over 2020, for a total of $24 billion stolen, according to the study. The number of people affected by traditional identity fraud also increased by an additional 5 million in 2021, for a total of 15 million people. Javelin defines traditional identity fraud as "the unauthorized use of some portion of another's personal information to achieve illicit financial gain." Many victims of this type of identity fraud may never find out how or when their personal information was compromised.

The Problem Conti.

Cybercrime Complaints, 2015-2021

- Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the numbers. Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined. The cybercrime prediction stands, and over the past year it has been corroborated by hundreds of major media outlets, universities and colleges, senior government officials, associations, industry experts, the largest technology and cybersecurity companies, and cybercrime fighters globally.

- The damage cost projections are based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation state sponsored and organized crime gang hacking activities, and a cyber attack surface which will be an order of magnitude greater in 2021 than it is today. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm." (Source- https://cybersecurityventures.com/hackerpocalypse-cybercrime- report-2016/)

Data on Identity Theft

Not so long ago, when we thought about theft, we imagined a house being robbed or someone getting mugged in the street. These crimes are far from harmless, but the devil was at least visible. The problem with identity theft is that you don’t know you’re in danger until the crime has already been committed.

As tech advances to keep people safe, criminals evolve in parallel, becoming more adept at stealing data. While far from pleasant, this is something you need to be aware of. We’re here with the latest identity theft stats to keep you vigilant.

- **33% of citizens in the US have experienced identity theft.**
- **The FTC handled 2.2 million fraud reports in 2020.**
- **One million child identity theft incidents occurred in 2020.**
- **Every year, 15 million Americans become victims of identity theft.**

1. Identity theft cost people in the US $56 billion in 2020.(Javelin)

Well over 49 million people were victims of identity theft in 2020. This resulted in $13 billion in damages from “traditional” identity theft, i.e., people losing their info through data breaches and similar attacks. On the other hand, one of the strangest statistics is that the majority of the losses ($43 billion) stemmed from direct-interaction scams, such as phishing emails. In other words, bad actors are getting bolder and are willing to target people directly.

2. **2.2 Million fraud reports were filed with the FTC in 2020. (FTC)**

Consumers have also stated that they lost $3.3 billion in fraud in the same year. That's nearly double the money lost the same way in 2019 - $1.8 million. When you look at the statistics released by the FTC, you will soon see that imposter scams were the most common type of fraud, as mentioned, this is one of the most shocking ID theft stats.

3. **Someone becomes the victim of identity fraud every 14 seconds.(FTC)**

Studies have also shown that every 14 seconds, someone becomes a victim of identity theft in the US. In light of the sharp rise in attacks we've seen in recent years, more and more people are calling for online data to be better protected.

4. **Identity theft affected around 0.6% of the US population in 2020.(FTC)**

Identity theft also disproportionately affects the older population. One explanation for this is that the elderly aren't always tech-savvy and often cannot tell the difference between a legitimate site or email and those that are fake.

5. **33% of Americans have been the victim of identity theft.(Proof Point)**

ID theft statistics show that 33% of Americans have been the victim of identity theft at some point in their lives. This is three times higher than the numbers from Germany or even France. It is also double the world average. US respondents leave their social media more open than worldwide users, making them vulnerable by exposing their information to cyber thieves.

Data on Identity Theft Cont.

6. Credit card fraud is the most common kind of identity theft. (FTC)

The FTC has found that credit card theft was the most common type of identity fraud in 2020 and 2021. The FTC has received nearly 18,000 reports from various individuals who have stated that their information has been used to gain access to their credit card accounts illegally.

7. People active on social media are more likely to have their details stolen. (Business News Daily)

People who are active on social media are 30% more likely to have their details stolen when compared to other people. These are the main channels where attackers seek out targets. Identity theft statistics also show that Facebook, Snapchat, and Instagram are exposed to an even higher level of risk, which propels the statistic to 46%.

8. Most stolen identities were used to apply for government documents and benefits in 2020. (FTC)

The second most common target of stolen ID use is credit card fraud. Following that, you have bank fraud and utility fraud. The millions of people who have been affected by these crimes often experience considerable financial, psychological, and reputational damage.

9. 15 million US citizens experience identity theft every year. (Crime Museum)

15 million people in the US experience identity theft every single year. This results in $50 billion in financial losses. This equates to 4.5% of all US residents, with an average loss of $3,500.

10. 2.5 million identities are stolen every year. (Time)

Identity theft statistics also show that the dead can become victims of cybercrime. There have been over 800,000 incidents where criminals have exploited the identities of the deceased to open credit cards or even get a cell phone plan. Studies have also shown that twice as many thieves used a fake Social Security number belonging to those who have passed away.

11.One out of five people in the EU have experienced identity theft. (GRC World)

When you look at the latest cybercrime statistics for Europe, you will soon find that more than half of Europeans (56%) have been the victim of cybercrime at least once in the last two years. Identity theft is the second-most common type of cyber-attack, with one-third of the 56% mentioned above being victims. The UK is the most vulnerable, with 53% of respondents from this country having reported some kind of ID theft. Ireland has a rate of 50%, and France comes in third, at 45%.

12.Californians are the main target for identity theft.(FTC)

The FTC has found that Californians are the primary target for identity theft, with recent statistics showing that 147,382 complaints were filed from this state alone. This makes the state one of the top targets for cybercrime. If you look at the statistics for the top five worst US states by identity theft, you will see that Illinois comes in second with 135,038 cases, Texas has 134,788 cases, Florida is at 101,367 cases, and Georgia comes last at 69,487 cases.

13.Millennials account for around 35% of fraud cases in the US.(FTC)

The FTC received 2.2 million reports of fraud in 2020. People between the ages of 20 and 40 account for 35% of those reports. On the other hand, people over 70 only accounted for 8% of reports. However, the average financial losses experienced by the older population were much higher compared to the younger generations, despite the totals being bigger for Millennials.

Data on Identity Theft Conti.

14. The 60 to 69 age group lost the most in fraud-induced expenses. (FTC)

Baby Boomers lost the most to identity theft in 2020 and 2021. However, identity theft statistics for 2021 also show that they are in fourth place in terms of report numbers. This means scams are particularly costly per person for this age group.

15. Over 1.3 million children have fallen victim to identity theft. (Michigan State University)

Over 1.3 million young children become the victims of identity theft every year. Studies have also shown that 50% of those youngsters are the age of six or younger, and that the average age is decreasing.

16. Families are expected to pay $540 million out of pocket to account for fraud damage from scammed children. (GIZMODO)

Data from 2017 shows that $2.6 billion in damages may be attributed to cybercrime involving children. Only 7% of adults know the person responsible for identity theft. However, when you look at children, you will see that this percentage skyrockets to 60%. More often than not, crimes involving children are perpetrated by someone who knows them.

17. 3% to 10% of the annual health budget in the US is lost to fraud (NHCAA)

While that number is alarming in itself, it’s worsened by the fact that medical identity theft accounts for 2 million cases of fraud to date. Considering the price of health insurance in the US, this is a life-threatening figure for many.

18. **113,593 employment and tax-related fraud cases were reported in 2020.(FTC)**

According to online fraud statistics, this type of fraud was the fifth most commonly reported in 2020. It had the most significant spike in the second quarter of 2020 - when the pandemic first hit - and has been on a slow decline since.

19. **Credit card account fraud accounted for 48% of all fraud complaints in the UK in 2019. (UKFinance)**

The same percentage represents the annual increase from 2018 to 2019 in personal losses incurred by police and bank impersonation scams. The sheer number of cases increased by 112% in the same period.

20. **Gross losses from gift card fraud in 2021 exceed $148 million.(FTC)**

Unfortunately, cybercrime statistics account for the dark side of gift-giving too. Gross losses from fraudulent gift card redeeming saw a sharp uptick in the first three quarters of 2021, already surpassing the numbers for all of 2020. This can be traced back to over 40,000 consumers who used gift cards to pay criminals.

Source- https://fortunly.com/statistics/identity-theft-statistics/#gref

The Solution

MTECT: Cyber & Homeland Real-Time Data Breach Detection

- At the forefront of our offerings is MTECT, our flagship product. A powerful tool that combines AI and blockchain to detect viruses, hackers, and payment card data breaches swiftly and effectively. With MTECT, organizations can confidently monitor and manage multi-channel transactions with enhanced security and efficiency. Experience enhanced security and efficiency with MPRISE, your trusted partner in safeguarding your business.

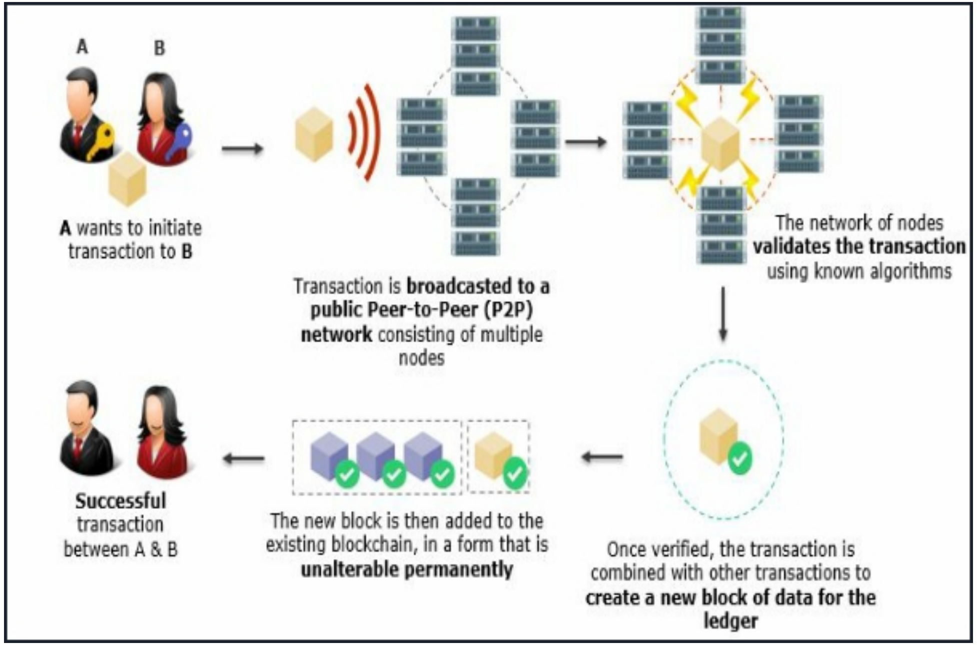
- Enhanced Security: MTECT leverages blockchain technology, encryption, and behavioral profiling to ensure the integrity of transactions. Our hybrid encryption approach combines AES-GCM and RSA, providing robust data protection.

- Real-Time Analysis: MTECT employs machine learning to predict transaction risk scores, allowing organizations to stay one step ahead of potential threats. With real-time data processing, you can proactively mitigate risks and safeguard your operations.
- Seamless Integration: MTECT provides comprehensive error handling, efficient database operations, and documentation to streamline integration and maintenance processes. We put simplicity and ease-of-use at the forefront.
- Trustworthy Solution: Our software offers a reliable and scalable platform, giving users confidence in the safety and security of their multi-channel transactions. MTECT is the solution for organizations seeking powerful monitoring and management capabilities.

The Solution Cont.

- MPRISE combines blockchain with Artificial Intelligence to create decentralized security products. Blockchain is a data structure that distributes trust across many nodes(Servers) instead of one (Glorified Singly linked List that lives on everyone’s computers). Even a super computer would have trouble hacking Blockchain because it will propagate into a Tree like structure to protect and organize each transaction and file(data). MPrise will store Code in a single node(Server) on Blockchain. And can change the code anytime to protect your data.

- Invest in MTECT today and join the future of secure multi-channel transactions. Experience the power of enhanced security, real-time analysis, and seamless integration. Empower your organization with MTECT.



A wants to initiate transaction to **B**

Transaction is **broadcasted to a public Peer-to-Peer (P2P) network** consisting of multiple nodes

The network of nodes **validates the transaction** using known algorithms

Once verified, the transaction is combined with other transactions to **create a new block of data for the ledger**

The new block is then added to the existing blockchain, in a form that is **unalterable permanently**

Successful transaction between A & B

The Team

CEO/Founder - Ranzel Merritt

As the sole founder of Mprise, I'm uniquely qualified to solve the problem we are addressing. With my background in product management and project management, along with a solid understanding of software development through agile methodologies, I bring a unique set of skills to the table for solving the problem at hand.

CTO - Still being Recruited

COO- Still being Recruited

Product Manager- Still being Recruited

MPRISE SECURITY PRODUCTS:

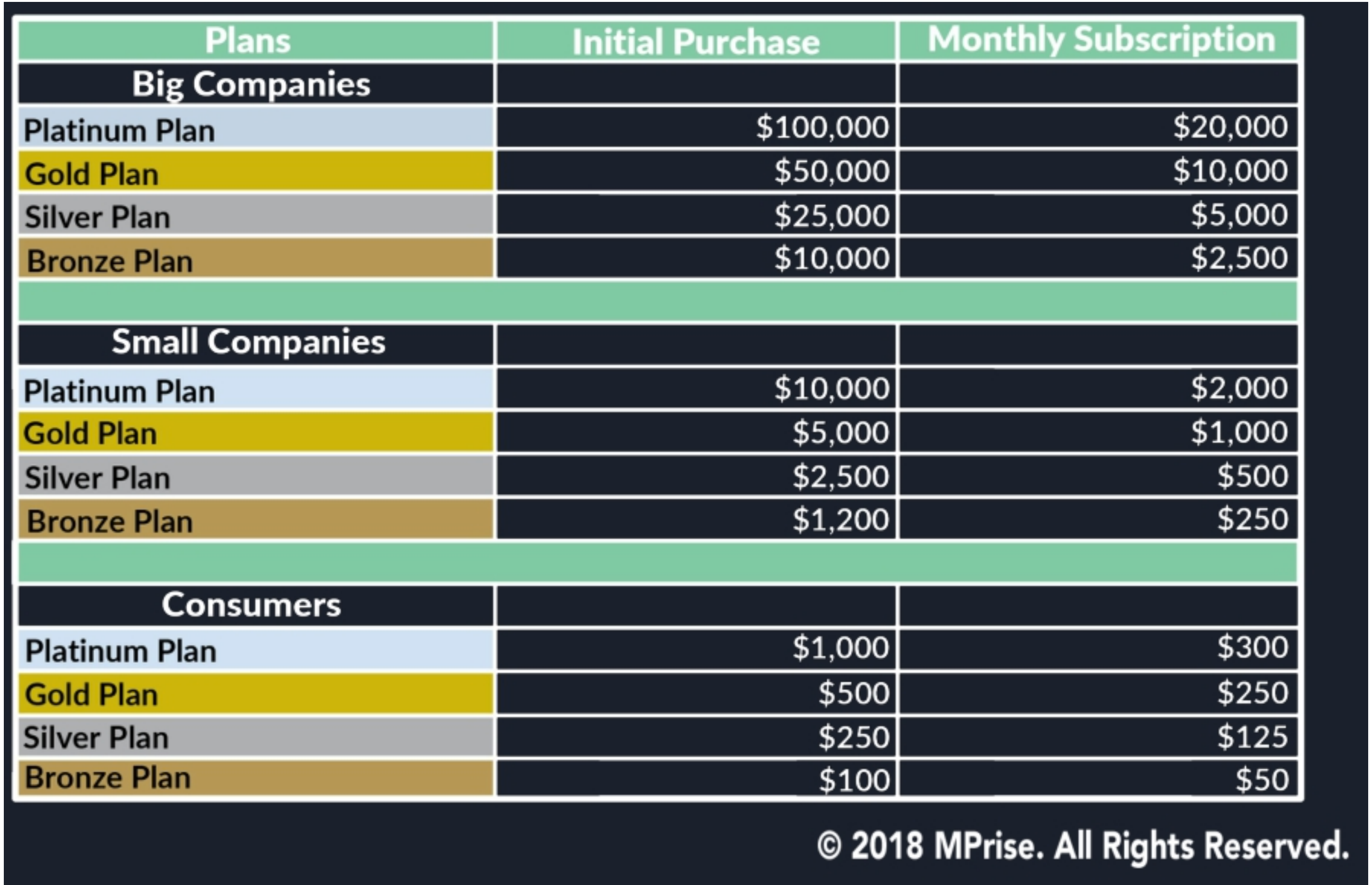
MTECT: CYBER & HOMELAND REAL-TIME DATA BREACH DETECTION

MTECT is an advanced software tool that securely analyzes and controls multi-channel transactions. It utilizes blockchain-based data storage, cross-channel behavioral profiling, real-time data processing, and hybrid encryption. With machine learning algorithms, comprehensive error handling, and efficient database operations, MTECT ensures transaction integrity and minimizes risks. Benefit from its robust security measures and efficient data processing capabilities for effective multi-channel transaction monitoring and management.

MCOMPLY: GLOBAL ANTI-MONEY LAUNDERING PREDICTION

MComply leverages a sophisticated predictive analysis system that harnesses the power of cutting edge AI technologies, particularly unsupervised learning, to detect and identify potential instances of money laundering. By intelligently analyzing patterns and anomalies within financial transactions, MComply automatically identifies suspicious behaviors and generates Suspicious Activity Reports (SAR) in compliance with regulatory requirements. Stay compliant, secure, and safeguarded with MComply as your partner in combating money laundering threats.

MPRISE Subscription Plan



Plans	Initial Purchase	Monthly Subscription
Big Companies		
Platinum Plan	$100,000	$20,000
Gold Plan	$50,000	$10,000
Silver Plan	$25,000	$5,000
Bronze Plan	$10,000	$2,500
Small Companies		
Platinum Plan	$10,000	$2,000
Gold Plan	$5,000	$1,000
Silver Plan	$2,500	$500
Bronze Plan	$1,200	$250
Consumers		
Platinum Plan	$1,000	$300
Gold Plan	$500	$250
Silver Plan	$250	$125
Bronze Plan	$100	$50

Why MPRISE?

With MPRISE, both large enterprises and small businesses can swiftly go live in just 5-6 weeks. Our software is designed to be highly adaptable, running seamlessly on off-the-shelf computers and entry-level servers. This streamlined approach not only expedites the return on investment but also optimizes operational costs, offering an exceptional value proposition to all potential buyers and users of MPRISE Software.

The Conclusion

In an age where fraud looms as a pervasive threat, taking proactive steps to protect yourself is paramount. Begin by acquainting yourself with the telltale signs of identity fraud in its early stages. Complement this knowledge with regular credit report assessments, the adoption of two-step verification whenever possible, the use of diverse and secure passwords, and a vigilant approach to safeguarding your privacy on social media. By diligently implementing these strategies, you can significantly diminish the likelihood of becoming a target for criminal exploitation.

MPRISE envisions evolving into a Decentralized Autonomous Organization (DAO) in the future. Currently, we are in the prototype phase, diligently working towards this goal. MPRISE is committed to delivering cutting-edge security products tailored to assist both businesses and individuals in safeguarding their valuable data. We firmly believe in your right to own your data and the peace of mind that it remains unaltered. At MPRISE, we spare no effort in ensuring your protection.

Invest in MPRISE today and join the future of secure multi-channel transactions. Experience the power of enhanced security, real-time analysis, and seamless integration. Empower your organization with MPRISE.

Thank you for entrusting us with your security!