

20 + YEARS EXPERIENCE
PATENT TECHNOLOGY
CERTIFIED TECHNOLOGY
WE'RE GENIUSES!

OUR MISSION

Our mission at CyberIntel is to revolutionize cybersecurity on a global scale. Through the launch of our innovative commercials, we aim to communicate a powerful message to hackers worldwide. With our unparalleled, patent-pending technology, CyberGuard Hacker & Ransomware Locator is not only capable of thwarting cyberattacks but also tracing the exact location of potential perpetrators. This capability allows us to swiftly identify and apprehend hacker suspects, effectively diminishing their anonymity and impunity.

The awareness created by our groundbreaking technology will act as a strong deterrent against cybercrime. Criminal elements will come to realize that their attempts at ransomware and other malicious hacks now carry a significant risk of detection and capture. By instilling fear and apprehension among hacker communities, we anticipate an immediate reduction in the incidence of hacking by over 80%. CyberGuard's seal stands as a singular commitment to safeguarding digital landscapes worldwide, heralding a new era where cybercriminals are held accountable and cyber integrity is staunchly protected.

The cyber war is critical and only getting worse!

*The first line of cyber defense is struggling in the cyber war; it's time for the experts—the **SPECIAL FORCES** of cyber defense—to take charge! CyberIntel. We're smarter!"*

CyberIntel
Cybersecurity



CYBERINTEL

Hacker
Suspect
Locator

Patent
Technology

CyberIntel

Powered by PC Logic

32565 GOLDEN LANTERN ST
UNIT 163
DANA POINT CA 92629-3247
www.pcllogic.com



CyberGuard Hacker & Ransomware Locator

WE DON'T JUST DETECT AND BLOCK HACKERS, WE TRACE AND LOCATE PRECISE LOCATIONS

CyberGuard is our patented technology. It leverages sophisticated algorithms and advanced artificial intelligence to proactively identify and block cyber-criminal hackers.

One of the distinguishing features of our technology is its ability to not only guard against cyber threats but also to trace the sources of these attacks. When a potential threat is identified, our AI systems employ advanced traceback techniques to follow the digital footprints left behind by hackers.

With our groundbreaking capabilities of CyberIntels' cutting-edge product, CyberGuard. In today's digital world, where cybersecurity threats have become increasingly sophisticated and pervasive, our reliance on robust solutions to protect sensitive data and infrastructure has never been more critical. CyberGuard stands at the forefront of this challenge, boasting the **remarkable ability to trace hackers' precise locations, even when they employ Virtual Private Networks (VPNs) to shield their activities. We're geniuses!**



CUSTOM SOLUTIONS

CyberIntel experts possess extensive capabilities in tailoring bespoke solutions to meet the specific requirements of governmental agencies, casinos and businesses. Leveraging our profound expertise in cybersecurity and software development, we employ a systematic approach to ensure the delivery of innovative and intelligent solutions without constraints on possibilities.



PROPRIETARY SOLUTIONS

At CyberIntel, innovation is embedded in our DNA. Our cutting-edge patented technology and proprietary algorithms have been refined and perfected over years of relentless development.

This enables us not only to predict hacker behavior but also to outthink and outmaneuver them at every turn. Our intelligence-driven approach ensures that we stay ahead of cybercriminals, protecting our clients with unmatched precision.



SMART SOLUTIONS

CyberIntel doesn't just respond to threats—we preempt them. Our commitment to staying smarter than hackers is evident in our proactive measures and groundbreaking methodologies. Trust CyberIntel to safeguard your digital future with the expertise and dedication that only decades of experience can provide.

WHY US?

- PATENT TECHNOLOGY
- DETECT, BLOCK AND APPREHEND
- TRACE AND LOCATE HACKERS IN REAL-TIME
- CONSTANT IMPROVEMENTS
- CUSTOMIZED CYBERSECURITY SOLUTIONS
- A TEAM OF OVER 20+ YEARS EXPERIENCE
- CERTIFIED CYBERSECURITY SOLUTIONS
- REDUCING HACKER ATTACKS WORLDWIDE
- REDUCING VICTIMS REVENUE LOSS
- ELIMINATE WEEK SECURITY SOLUTIONS

Patent technology your business needs

WE'RE SMARTER THAN HACKERS. PERIOD!

Our goal #1 goal at CyberIntel is to out smart the hacker to simply protect the victims and immediately apprehend the suspect hackers!

Over the past two years, the activities of cyber criminals have escalated significantly, posing a severe threat to individuals, businesses, and governments worldwide. The sophistication of attacks has grown, with hackers employing advanced techniques such as ransomware, phishing, and APTs (Advanced Persistent Threats). According to various reports and studies, cybercrime has resulted in staggering financial losses. In 2022 alone, global losses due to cybercrime were estimated at over \$6 trillion, up from around \$3 trillion in 2020.

Cyber Crime Magazine report provides a breakdown of the cybercrime damage costs predicted in 2023:

- \$8 trillion USD a Year.
- \$667 billion a Month.
- \$154 billion a Week.
- \$21.9 billion a Day.
- \$913 million an Hour.
- \$15.2 million a Minute.
- \$255,000 a Second.

Ransomware attacks have become particularly prevalent, with criminals demanding exorbitant sums for the safe return of stolen data.

GROUNDBREAKING TECHNOLOGY THAT CAN PUT A STOP TO THE GROWING CYBER WAR

OTHER SECURITY SOLUTIONS ARE WEAK

In 2023, MGM Resorts lost an estimated \$100 million in revenue due to a cyberattack on its casinos and hotels:

The Impact

The attack disrupted MGM's operations, causing a reduction in daily revenue and cash flow by 10–20%. The company also saw its market cap decrease by nearly \$2 billion.

The attack compromised the private data of some customers who used MGM services before March 2019. The data included names, contact information, gender, date of birth, driver's license numbers, and, for a limited number of customers, Social Security numbers and/or passport numbers.

The cyber-attack also caused a \$100 million hit to the company's third-quarter results, as it had to shut down certain systems and restore its operations. The FBI is investigating the breach, which is believed to have started with a social engineering attack on the company's IT service desk.

