What are Autonomous Security Systems?

The next time you visit your grandma's house, airport or sports arena, don't be alarmed if you cross paths with a roving sentinel that resembles a character from Disney's Wall-E or confuse a mini drone actively taking rounds around the house with an alien invasion. This is because these sophisticated products have just come out from a series of meaningless ideas and patents to mass production thanks to a number of autonomous security startups and a few big tech companies looking for opportunities to advance in the security field.

When we think about security systems, the first thing that comes to mind are: Remote Cameras for monitoring and viewing, Entrance locks, verification systems, your average car lock & keys, etc, though what Autonomous Security Systems are is a much greater succession or advancement in security systems technology, coupled with Artificial Intelligence from PISIQ, Autonomous Security Systems are an incredibly capable security solution to rely on.

Autonomous Security Systems have become one of the greatest applications of AI and advanced tech for the good of humankind. With the help of these systems, we have been able to revolutionize home, office and industry security. Autonomous Security Systems generally consist of Artificial Intelligence, which is an autonomous entity that acts and directs said activity towards achieving security and safety, managing systems and taking necessary measures for achieving this through understanding (Machine Learning/Deep Learning) it's environment and using AI to use knowledge to achieve these objectives.

Effective AI Guided Autonomous Security requires that the system be able to do the following:

- **Understand and Interpret various data streams.**
- **Intelligently predict the necessary action and strategy to take next and make an effective plan.**
- **Enable measures when it is safe to do so, avoiding any potential situations that pose a risk or danger to human property, safety, the environment or the system itself.**
- **Sense the environment, obstacles and various, accurately monitor and track the system's current state and location.**

Security that is self governed and bulletproof. PISIQ's Security services include Autonomous Security, Enhanced Security, Government Level Security, Bank Level Security, Smart Security Solutions & Cyber Automation[/caption]

This is all you need to know about Autonomous Security Systems

Types of Autonomous Security Systems

Cyber Automation

Automating the process of developing secure infrastructure with zero hour vulnerability response systems aiming to build a guarded technical environment by intelligent software.

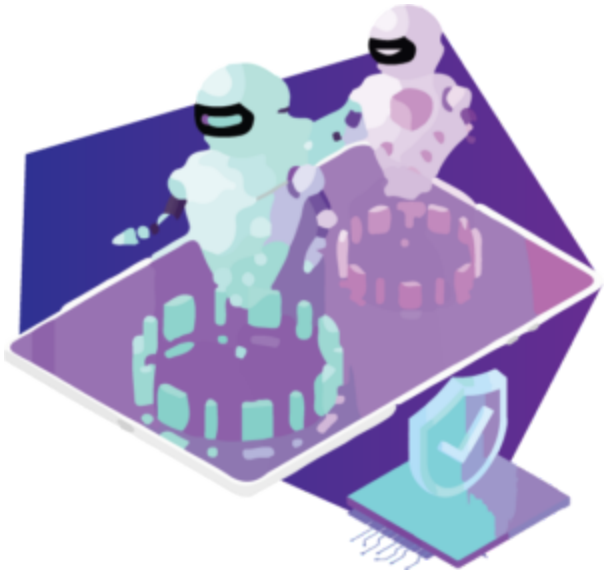
in Cyber Automation, Security comes from proper design, operation and maintenance of security architectures and infrastructures which provide up to date protection. An acceptable network security environment includes built-in high security engineered into the architecture, at the same time allowing operators, supervisors and administrators the ability to interact with the system without constantly getting into arduous, tedious and prolonged procedures. If it's too difficult, knowledgeable people will quickly find a way around the system – the well-intentioned, honest but impatient insider.

Well thought out network security architectures provide the mechanisms necessary to prioritize and manage traffic, restrict outside traffic, and give preferential treatment to control traffic. Systems pertaining around Cyber Automation must have the ability to recognize broadcast attacks that can create denial of service conditions, to prevent problem situations before they occur. When anything happens outside the bounds established for the control network, it must be captured as an auditable event as part of the Autonomous Systems, the event logs must be reviewed regularly to determine if unauthorized changes are made.

Anti Virus software from companies like McAfee or Symantec could be part of a good security strategy, but this is not sufficient. Standard anti-virus and anti-spam packages were developed for typical PC users, not for sophisticated, real-time control systems. They need to be adapted specifically for use with automation control systems.

Good Autonomous Systems should provide preconfigured security settings for files, directories, and registry keys to protect against viruses, malicious users, and inadvertent actions. There should be preconfigured groups and group policies that define desktop and console behavior: Operators should be limited to say just auto start applications, supervisors could be very secure, engineers could be restricted to relevant engineering functions, and administrators could have unlimited access with secure settings. Clearly the administrative procedures (password protection, etc.) should be subject to maximum security procedures.

Smart Security Solutions



Offering hardware and software based on AI innovation and autonomous vulnerability testing to ensure an environment that is secure, robust and ever developing by self-programmed systems and defense solutions and privacy enhancement

Bank Level Security

Creating systems that allow organizations to secure sensitive information by using architectural methods inspired by world class financial organizations, It would involve using deep machine learning algorithms, smart cyber automation & powerful Artificial Intelligence (AI) Technology to provide smart security solutions and to effectively learn best the system operations, Whilst the

Artificial Intelligence Machine itself may take a some time to identify the issues, it's nature allows for near constant and complete exploration of such systems.

This also means that important personal information is encrypted and protected using the same industry-leading technology that artificial intelligence uses, other uses may also be in the assistance of cracking down on criminals such as in the case of the JP Morgan hack case.

Developed as a useful approach by the Department of Homeland Security of the United States, it is the application of AI technology to identify exploitable vulnerabilities and close any possible loopholes before they can be exploited. similar approaches to bank level security and smart security solutions can be useful in the total prevention of cyber security related crimes altogether.

Government Level Security

Sandboxing organizations and using technical architecture used by governments to ensure the safety and protection of information by facilitating multiple layers of access through multiple secured sandboxes that are custom to each organization and department's needs.

Government facilities face a challenging and ever-changing risk profile. PISIQ's Smart security solutions are paramount to increase safety for employees, area citizens and elected officials. But many government facilities, especially those in small cities and towns, are not staffed with a full-time staff so technology becomes an even more important piece of the puzzle.

Traditional analog-based systems are not effective enough to secure these critical facilities but the promise of IP technology can help facilities manage and control risks. Governments need advanced networked tools such as Cyber Automation tools that leverage the power of the IT backbone to correlate information from traditionally separate subsystems — video surveillance, analytics, access control, alarm management and VoIP, for example — into one platform to

increase situational awareness and help government staffs identify violence or threats before an event occurs.

What makes these Autonomous security systems so impressive? Autonomy.

How does this work?

In short- using machine learning and deep learning. PISIQ's Machine Learning involves collecting large amounts of data related to a problem, training a model using this data and employing this model to process new data. Recently, there have been huge advances in a branch of Machine Learning called Deep Learning. This describes a family of algorithms based on neural networks. These algorithms are able to learn efficiently from example, and subsequently apply this learning to new data.With deep learning, you can show a computer many different images and it will "learn" to distinguish the differences. This is the "training" phase. After the neural network learns about the data, it can then use "inference" to interpret new data based on what it has learned. For example, if it has seen enough cats before, the system will know when a new image is a cat. In effect, the system “learns” by looking at lots of data to achieve artificial intelligence (AI). Larry Anderson explores how new computer hardware - the Graphic Processing Unit (GPU) – is making artificial intelligence accessible to the security industry.

With the abilities afforded by AI, robots can navigate any designated area autonomously to keep an eye out for suspicious behaviour or alert first responders to those who may need aid. This also means that fewer law enforcement and/or security personnel will have to be pulled from surrounding areas.

Machine Learning

Machine learning is a type of artificial intelligence used mainly to prevent cyber attacks. It is a method of data analysis that uses the application of artificial technology to do so. It allows machines to learn without being explicitly programmed. It focuses on developing computer programs that have the ability to change when exposed to new data. Through the incorporation of algorithms that learn from data, machine learning allows computers to find hidden figures without being specifically programmed where to look.

This means big news for cyber security. As cyber threats evolve with the industry and adjust to get around overprotective mechanisms, security professionals have to focus on the more severe risks first. Artificial intelligence is the key to allowing cyber security systems to carry out human-like tasks and provide first-hand protection.The industry is quickly evolving and with the addition of artificial intelligence, machine-learning can be a step in the right direction towards improved cyber security.

Limitations of AI in security

AI and ML are not magic wands that you can wave to suddenly secure your organization. Security personnel must work closely with these models to train and hone them, and these professionals are neither cheap nor easy to find.

Another challenge is data and cost: We need to amass enough clean data to build a robust algorithm we can trust. Clean data doesn't just happen – it must be analyzed and verified for accuracy.

The cost of storing massive amounts of data and purchasing the necessary compute time to run hefty ML algorithms is significant, and implementing an all-encompassing AI security solution may be too costly for some. According to the Harvard Business Review, 40 percent of executives reported that the technology and required expertise of AI initiatives are too expensive.

Traditional anti-virus and firewall solutions can't keep pace with zero-day threats and the wave of malware variants. AI and ML provide a proactive solution. They can find behavioral patterns from the user community to stop threats before they start. AI can help security professionals digest mountains of data to pinpoint problems. They can help us keep pace with an AI-powered hacking community intent on doing us harm.

AI still has some maturing to do before it becomes the security solution for all businesses, but it's progressing quickly. It's difficult to imagine the future of IT security without AI and machine learning at the center of it.

How are these systems better than their human counterparts?

Regarding the question of what is better - autonomous security systems or their human parts, we have a clear winner.

Though autonomous systems as a whole have the aspect of malfunctioning and taking over human jobs the main advantages that are -

- **They are cost efficient,**
- **Commit far fewer errors and**
- **Are capable of modification according to the needs, which far outweigh the disadvantages**

Major Examples of Autonomous Security Systems

- **Ring**

1. Ring is a California based home security startup that recently got acquired by Amazon. Ring manufactures home security products that incorporate outdoor motion-detecting cameras, including Ring Video Doorbell. It hosts an app, Neighbors, for online social sharing of captured footage among users. Ring also provides video footage from its cameras and data from its Neighbors app to law enforcement agencies on request.
2. Ring had recently launched the Ring Always Home Cam. Unlike Amazon's other security cameras, the Always Home Cam is a flying camera drone that docks when it isn't in use. The Ring Always Home Cam will be available in 2021 for $250.

- **Aegis AI**

1. Aegis AI is a startup using computer vision software to turn security cameras into gun-detecting smart cameras.Aegis AI sells to U.S. corporations and school district its technology, which scans thousands of video feeds for brandished weapons and provides threat-detection alerts to customers within one second, for $30 per camera, per month. Coupling AI and cloud computing, Aegis integrates with existing camera hardware and video management software, requiring no on-site installation or maintenance.
2. To teach its software to identify weapons, Aegis began by scrubbing the web for photos of weapons, then they reached out to key influencers in the personal safety space, who proved to be essential resources throughout the process. To complete the data collection process, they got their hands on real security footage and even took their own posed photos holding weapons to fill in any of the AI's blind spots.
3. They take an "aggressive" data augmentation approach to develop the AI, as opposed to just scraping the web for images of weapons to feed to the platform.

- **Evolv Technology**

1. Evolv Technology is the leader in human security dedicated to making the world a safer place to live, work, learn and play by helping to protect innocent people from mass shootings and terrorist attacks.
2. Evolv's mission is to return confidence and peace of mind to people visiting public spaces by changing the paradigm of how security professionals can assure venues are safe from the most serious threats without compromising visitor experience. They have accomplished this by fusing the latest sensors and AI technology to consistently and reliably scan every visitor without the hassle and the gaps presented by century-old metal detector technology.
3. Similar to the TSA's body scanners, the Evolv Edge solution combines millimeter-wave technology and a number of other sensors to non-intrusively screen people as they walk through the machine for threats. Unlike those airport body scanners that require people to enter, turn 90 degrees and put their arms in the air while columns scan the entirety of their body to create an image, the Edge system screens subjects as they walk between

two columns and can produce an analysis of what someone may be carrying in about a hundredth of a second.

- **DarkTrace**

1. The application of artificial intelligence to the cyber defense challenge has marked a fundamental shift in our ability to protect critical data systems and digital infrastructures. For strained security teams, it offers the possibility to keep pace with an ever-evolving threat landscape.
2. While rule and signature-based solutions offer some protection against pre-identified threats, the reality is that attacks consistently evade these and get inside your network. Powered by unsupervised machine learning, Cyber AI responds to these threats before they become a crisis.
3. Cyber AI is a self-learning technology – like the human immune system, it learns 'on the job', from the data and activity that it observes in situ. This means making billions of probability-based calculations in light of evolving evidence.
4. As a new generation of cyber-threats, powered by offensive AI, emerge, Autonomous Response AI will be critical to fight back with the precision and speed necessary. These machine-speed attacks will only be countered by AI defenses that can stay one step ahead – allowing humans precious time to catch up.
5. Darktrace has identified a new form of cyber security that moves the whole industry forward beyond current defense models. By applying advanced machine learning methods to a novel software application, it has established a world-beating company that has no significant

- **Webroot**

1. Webroot Inc. is an American privately-held cybersecurity software company that provides Internet security for consumers and businesses.
2. SecureAnywhere uses machine learning to defend against modern attacks. Machine learning makes it predictive and adaptive, so it's able to keep up with the evolving landscape of cybersecurity threats.
3. Webroot SecureAnywhere is a cloud-based solution that includes:

- **Offline protection and automatic remediation**. Webroot's technology can monitor endpoints, even when they are offline. It uses proprietary technology to track data and system changes, allowing compromised local drives to be restored without reimaging.
- **More uptime and fewer slowdowns**. Since Webroot's heavy processing activities take place in the cloud, its resource usage is very low, even when it's doing full scheduled scans and updates.
- **Advanced threat intelligence**. Webroot's BrightCloud Threat Intelligence uses machine-learning to classify and isolate threats, even when they've never been seen before. It stops phishing attacks, analyzes files in real time and stops malware in real time.

Autonomous Security Systems and AI's Future

The future of autonomous security systems is beyond our imagination. Here below are some technology advancements of AI in autonomous home security that we can foresee in the near future.

- AI is going to have better recognition soon

It is a sure thing that AI vision will recognize more types of things due to the exponential growth of big data. AI can even be trained to recognize human's behaviors. For example, AI security camera can determine that a stranger is criminal when he is carrying a guy or beating the homeowner.

- AI security systems will be able to make their own decisions upon an emergency.

Because AI can judge the level of a threat, it can automatically and immediately take action without humans intervene. Imagine when a burglar tried to break into your house, not only can an AI security camera set off an alarm and lights to deter the burglar, but even sent the captured image to the police or a monitoring center by itself. AI computer vision will work like a virtual security guard that relentlessly watches your camera 24/7.

- Two-way interaction with both AI vision and AI voice.

An AI-powered security camera can not only detect a person in the video, but also use voice to communicate with the person. The voice can greet guests with their names or handle package delivery for you when you are not available.

In addition to voice, vision AI can be another way to interact with your home security system.

No matter what the future holds for AI and autonomous security systems in general - one thing seems clear - because of the uprising of numerous innovative tech startups and big tech paying attention to the security industry, we can claim that we are headed towards a safe future.

To Learn more about Artificial Intelligence and other technologies here are few recommended articles you should read:

1: Is Artificial Intelligence Capitalized?

2: Artificial Intelligence as a necessary tool

You might have come across Internet of Things (IOT), we have an article that explains about an emerging field called Industrial Internet of Things (IIOT)

3: Read about it here

4: How Artificial Intelligence could change Dubai