www.pipelinepub.com
Volume 19, Issue 1

Automating the Future of Data Center Security

By: Wes Swenson

From distributed denial of service (DDoS) attacks on some of the world's biggest names in business, including Amazon and Google, to ransomware, phishing, and domain name system (DNS) breaches that count CNN and PayPal as victims, and cyberattacks of all sizes—the methods and sophistication of these threats continue to prove the importance of an ironclad data center security plan. Physical threats, too, like overheating servers and unauthorized visitors, are top-of-mind considerations for data center security professionals.

Like the attacks they're designed to protect against, data center security methods need to constantly evolve to keep pace with cunning criminals who only get smarter and more calculated in their attempts to derail data centers' operations. Inevitably, threats to data centers will continue to rise, posing a threat to physical and digital security for data centers, which can't afford the cost breaches—in reputation and budget. Data breach costs reached a new all-time high in 2022, netting out to an average of $4.35 million USD (a 12.7 percent increase from 2020, when the average data breach cost came in at $3.86 million USD).

To combat risks, the adoption of robotics and artificial intelligence (AI) to improve efficiency, operations, and security in data centers is at an all-time high. The 2021 AFCOM State of the Data Center Report finds that 40 percent of surveyed respondents expect robotics and automation to soon become a regular piece of the data center landscape. Additionally, 16 percent of those surveyed are already leveraging robotics and autonomous systems in their centers, while another 35 percent indicated they plan to deploy similar solutions in the next three years. Data centers aren't alone: 76 percent of enterprises prioritized AI and machine learning (ML) over other IT initiatives in 2021, with 86 percent of these organizations reporting increased AI/ML spending between 2019 and 2020.

The two primary burdens to data center security are threats to facility infrastructure and cybersecurity threats to data and applications housed by the infrastructure itself. When it comes to security automation, effective strategies must consider what digital and physical barriers need to be constructed between looming threats and the infrastructure and data that needs to be protected. In both cases, some combination of robots, AI, and machine learning represent the path to eliminating human error, saving time and money, and optimizing task monitoring.

Automation in virtual data center security

Despite being massive buildings housing critical infrastructure, data centers that approach security solely by equipping every door with an access keypad and an armed guard won't be able to effectively protect against what remains their biggest threat: virtual security. Applications that run on data center infrastructure operate on code that can be vulnerable to hacking. With the surge in hybrid work in recent years, remote access tools like virtual private networks (VPNs) can lead to compromised credentials and malware planting within systems.

In 93 percent of cases, an external attacker can breach an organization's network perimeter and gain access to local network resources. On top of this, when considering that the World Economic Forum (WEF) reports that 95 percent of cybersecurity issues are caused by human error, the case for automation becomes clear.

To help identify unusual network activity and secure any bad traffic, AI can help automate data center security by appropriately managing firewall rules and processing data. The sheer amount of data that needs to be sorted in order to spot anomalies is simply too massive and complicated for complete human sorting and interpretation. Even skilled analysts would be hard pressed to predict where data center functionality failures may occur in order to reduce downtime or accurately spot an incoming cybersecurity risk. AI-based security solutions, however, are able to analyze incoming and outgoing data to spot threats.

AI is also able to learn what normal network behavior looks like and identify cyber threats when that behavior deviates from the norm. With AI, it's also easier for data centers to detect malware or spot system loopholes. And, of course, with AI technology, better false positive rates are possible, singling out potentially damaging traffic in the most efficient way possible so that data center operators can respond with accuracy, precision, and speed.

When countless hours of data tracking and monitoring are being taken care of by AI-enabled computers, human employees are then free to examine the anomalies in that data, plot better security strategies, and utilize expanded skills and capabilities to fill other roles that work in tandem with their more repetitive-task performing counterparts.

Automation in physical data center security

When it comes to physical security, many data centers are looking to robotics to aid in automation efforts. According to Gartner, half of cloud data centers will leverage advanced robots with AI and machine learning capabilities by 2025, which will reportedly increase data center operating efficiency by 30 percent. With a growing gap between the number of servers and storage volumes at data centers vs. the number of capable workers to oversee them, deploying robots will be critical for facilities in the coming years.

Robots have long been explored for a variety of uses in data centers. From IBM's iRobot designed to track the data center's temperature to the Scout bot created to monitor KAIST's iCubeCloud Data Center, the use of robotics to streamline operations by passing off monotonous processes has a long history. Only now, however, is the technology reaching an inflection point in sophistication. In part, we can point to the COVID-19 pandemic as a catalyst, as it is suggested to have boosted the idea of "lights-out," or unmanned data centers. The thought of a completely autonomous data center is intriguing, but also brings up the fact that operating systems remain a major vulnerability.

To ensure that the data center infrastructure management (DCIM) systems that enable prime performance, like thermal and cooling management dashboards, humidity controllers, rack monitors, and more remain secure, robotics can play a major role.

Use case: The first robotic dogs deployed in data centers

Recent technological advances have provided the opportunity to use robotics to improve security measures. To this end, Novva Data Centers employs robotic dogs—created by Boston Dynamics—that can serve several security functions. From greeting guests just like their furry, flesh and blood counterparts, to monitoring day-to-day functions, the Boston Dynamics robots are some of the first functioning technology of their kind deployed in a data center. After all, who better can we trust to sniff out threats than man's best friend?

The robots are able to run predetermined missions throughout the data center to collect data, monitor equipment, and report any unusual activity or abnormalities, such as overheating machines, thanks to the robots' heat sensing capabilities. The robots are equipped with facial recognition technology—so that they can report any unwelcome visitors to the control room—and are programmed with walking, object avoidance, and autonomous route navigation capabilities. On the hardware side, the robots use a thermometer to assess the atmospheric temperature in the computer rooms.

The robots are taught the current layout of the data center, and then, using a QR code system that sits about three feet above the floor throughout the building, they're able to navigate to the correct location to perform their predefined monitoring missions.

Many leaders in the data center space point to AI technology that can integrate with DCIM systems as the next frontier in AI implementation for data center security, even though many older data centers would be hard-pressed to adopt similar technology due to a lack of mechanical equipment that can accommodate modern AI technology. However, as new buildings are constructed with the goal of employing AI and robots in similar ways, newer data center construction is expected to evolve, and physical security automation should pick up pace in the coming years as a result. This is expected to lead to multiple benefits:

- Greater ability to process massive amounts of video data to identify visitors or spot threats inside the data center or on the physical perimeter of the facility

- Reduced risk of human error in facilities
- Energy efficiencies with smarter routing of energy sourcing to servers as dictated by data being processed
- Predictive maintenance due to irregular machine or server behavior that is flagged by AI
- Prolonged use of machines due to immediate machine servicing or operational adjustments as needed
- Detection of physical anomalies, such as an employee performing a suspicious task within the data center, or a physical perimeter anomaly, such as a revisiting car or person on the street

In the fight against increasingly complex threats to data center security, modern solutions are required. Unlocking the potential of AI/ML and robotics will lead to data center security strategies that only continue to get smarter, more efficient, and cost-effective.