Global study finds AI is a key cybersecurity weapon

Research from Aruba and Ponemon Institute shows security teams view machine learning and network visibility for users and IoT devices essential for battling stealthy threats inside IT infrastructures.

Larry Ponemon, chairman, Ponemon Institute.

As businesses struggle to combat increasingly sophisticated cyber security attacks, the severity of which is exacerbated by both the vanishing IT perimeters in today's mobile and IoT era, coupled with an acute shortage of skilled security professionals, IT security teams need both a new approach and powerful new tools to protect data and other high-value assets.

Increasingly, they are looking to artificial intelligence (AI) as a key weapon to win the battle against stealthy threats inside their IT infrastructures, according to a new global research study conducted by the Ponemon Institute on behalf of Aruba, a Hewlett Packard Enterprise company.

Network security 101 - cyber security basics

The Ponemon Institute study, entitled "Closing the IT Security Gap with Automation & AI in the Era of IoT," surveyed 4,000 security and IT professionals across the Americas, Europe and Asia to understand what makes security deficiencies so hard to fix, and what types of technologies and processes are needed to stay a step ahead of bad actors within the new threat landscape.

The research revealed that in the quest to protect data and other high-value assets, security systems incorporating machine learning and other AI-based technologies are essential for detecting and stopping attacks that target users and IoT devices. The majority of respondents agree that security products with AI functionality will help to:

- Reduce false alerts (68%)
- Increase their team's effectiveness (63%)
- Provide greater investigation efficiencies (60%)
- Advance their ability to more quickly discover and respond to stealthy attacks that have evaded perimeter defense systems (56%)

Taking a 'human-centric' approach to security
13 Sep 2018

Twenty-five percent of respondents said they currently use some form of an AI-based security solution, with another 26% stating they plan on deploying these types of products within the next 12 months.

Current security tools are not enough

"Despite massive investments in cybersecurity programs, our research found most businesses are still unable to stop advanced, targeted attacks – with 45% believing they are not realising the full value of their defence arsenal, which ranges from 10 to 75 security solutions," said Larry Ponemon, chairman, Ponemon Institute.

"The situation has become a 'perfect storm,' with nearly half of respondents saying it's very difficult to protect complex and dynamically changing attack surfaces, especially given the current lack of security staff with the necessary skills and expertise to battle today's persistent, sophisticated, highly trained, and well-financed attackers. Against this backdrop, AI-based security tools, which can automate tasks and free up IT personnel to manage other aspects of a security program, were viewed as critical for helping businesses keep up with increasing threat levels."

IoT and cloud adds significant risk

Ponemon researchers found that the majority of IT security teams believe that a key gap in their company's overall security strategy is their inability to identify attacks that use IoT devices as the point of entry.

In fact, more than three-quarters of respondents believe their IoT devices are not secure, with 60% stating even simple IoT devices pose a threat. Two-thirds of respondents admitted they have little or no ability to protect their "things" from attacks. Continuous monitoring of network traffic, closed-loop detection and response systems, and detecting behavioural anomalies among peer groups of IoT devices, were cited as the most effective approaches to better protect their environments.

Report unveils predictions for the future of multi-cloud

21 Sep 2018

Even the ownership model for IoT security presents a potential risk. When asked who inside their organisation was responsible for IoT security, responses ranged from the CIO, CISO, CTO, and line-of-business leaders, with no majority consensus. Only 33% identified the CIO, with no other executive or functional group achieving response totals above 20%. Surprisingly, "No Function" was the third-highest answer (15%).

Survey results also highlighted the importance of visibility and the ability to define which resources that people and IoT devices can access, with 63% of respondents stating network access control is an important element of their company's overall security strategy and critical for reducing the reach of inside exploits. Also cited as important was having detailed information about applications (71%), endpoints (69%), cloud (64%), and networks (63%), with more than half saying they currently deploy network access control solutions for enabling visibility and control across both wired and wireless networks.

Additionally, more than half of respondents said it's hard to protect expanding and blurring IT perimeters resulting from requirements to concurrently support IoT, BYOD, mobile, and cloud initiatives (55%).

A data breach can lead to job loss

17 Sep 2018

"Partnering with the Ponemon Institute helps us to improve customer experiences by better understanding security teams' challenges, and then arming them with advanced solutions that enable quick identification and responses to an ever-changing threat landscape," said Larry Lunetta, vice president of security solutions marketing for Aruba. "The insight gained from this study enables us to continually improve our ability to provide an enterprise wired and wireless network security framework with an integrated and more comprehensive approach for gaining back visibility and control."

Ponemon findings parallel other Aruba research

The Ponemon Institute study parallels findings from an Aruba global study conducted in June 2018 of 7,000 employees across 15 countries. That study revealed that cybersecurity is a challenge for employers, especially for those working in smart buildings.

The report found that although employees reported higher levels of cybersecurity awareness, with 52% thinking about security often or daily, they also admitted to taking more risks with company data and devices. Seventy percent admitted to risky behaviours such as sharing passwords and devices.

It also showed that 25% of employees have connected to potentially unsafe open Wi-Fi networks in the past 12 months. Additionally, 20% said they use the same password across multiple applications and accounts, and 17% admitted to writing

down passwords in order to remember them.