DEEP-LEARNING-BACKED SECURITY TOOLS ARE THE NEXT STEP ON THE PATH TO MORE SECURE FEDERAL ENDPOINTS

As the internet of things continues to mature and workforces become more mobile, hackers and other malicious actors now find themselves in a world with a wealth of endpoints to exploit. This proliferation of endpoints can more difficult than ever for agencies and IT teams to pinpoint and to respond to attacks.

In fact, malware intelligence is on the rise, growing in "intensity, significance and malice," HP Federal Chief Technology Officer Tommy Gardner wrote earlier this year. By finding new entry points, attackers are opening the floodgates for malware to incorporate "Zero-Day" attacks, the term used to describe the threat of an unknown security vulnerability in computer software or application for which IT teams have not yet released patches, or have missed entirely.

"Bad guys don't announce they've found cyber-passages into networks. Rather, they penetrate their security perimeters and then either spy on an organization's activities or quietly make off with its data and money," said Gardner in an August 2019 LinkedIn post.

According to a state of security endpoint survey from the Ponemon Institute, Zero-Day attacks are four times more likely to compromise organizations compared with existing or known attacks. In addition, when it comes to antivirus solutions in place, respondents to the survey reported that their current antivirus solutions are effective at blocking only 43% of attacks. Last, attacks are pricey. The costs associated with successful attacks has increased from $5 million to $7.1 million, with the average cost per compromised endpoint at a price tag of $440.

Agencies are at a critical point where they need to strategically think through the tools that they adopt. This is particularly true when it comes to legacy systems, which often prove to be inefficient and riddled with security vulnerabilities.

Rising risk and costs signals demand for more investment in out-of -the-box virus protection that can not just respond to attacks, but predict their first moves, even for the unknown.

Updated National Institute of Standards and Technology guidelines (Special Publication 800-193) call for stronger, more resilient platforms that make use of "fundamental hardware and firmware components needed to boot and operate a system."

According to NIST guidelines, security mechanisms need to detect and prevent against unauthorized changes that occur and promote rapid recovery by layering security architectures for comprehensive protection. As government becomes more mobile and Zero-Day attacks become more common, security partners should look to prioritize adherence to NIST guidelines and keep up with the demand for flexible and adaptable security, providing updated and maintained protection without the stopgaps, hassle and hindrance of laborious updates and antiquated systems.

Deep Learning Tools Detect New Attacks Before the Damage is Done

By integrating advanced artificial intelligence and machine learning into security solutions and strategies, government agencies can reallocate protection attention to endpoints through resilient AI modeling that stays ahead of persistent evolving threats. By leveraging advanced forms of AI known as deep learning to fight against Zero-Day attacks, AI-backed software tools can head off and crack down on evolving and unknown malware attacks before they are able to take root in vulnerable government systems.

Unlike legacy tools, or even tools that feed off of less-advanced machine learning techniques, which can only recognize a few new forms of attacks, protection systems that use deep learning can recognize almost all malware instinctively.

Deep learning neural networks use over a billion samples of code to train and instinctively learn how to detect malicious code and raw data. These instincts then compress into lightweight, powerful, agents that systems then deploy to scan for malware, known or unknown, within the hardware. The fast and agile agents navigate within the hardware's system without affecting the user experience.

Deep-learning-based tools work more like the human mind, Gardner notes.

HP has released its own deep-learning-based tool, HP Sure Sense[1], which Gardner notes aims to inject powerful security capabilities into public sector tools and endpoints, "whether it's for our PCs, our laptops, workstations printers or 3-D printers," says Gardner.

[1] For HP Elite and Workstation PCs, HP Sure Sense requires Windows 10. See product specifications for availability.

The tool aims to alleviate the burden placed on IT admins and teams as they seek to protect against constantly evolving forms of malware.

"This recognition of the advanced persistent threat is using minor modifications to old malware and detections from new malware to do a springboard equation to figure out how to detect things for the first time so you don't have to wait until the damage is done."

Gardner notes that in this day and age, every decision chief executives and IT leaders make is a security consideration, as well.

"Whenever you buy something that goes on the network, you're making a security decision. You can't just choose on a low price, because you have a range of choices and those choices have consequences. If you think you just saved $5 million in the tools you bought, but have to pay $15 million to recover from an attack later on, you didn't save any money and put your data at risk in the process," he says.

Essentially, Gardner notes that cyberattacks are evolving, and cybersecurity systems need to evolve along with them.

"If you're not buying the most secure products on the market today, then you're taking a risk," he says. "You should be taking informed risks if you're taking risks at all."

Learn more about how HP Sure Sense's AI-backed technology can help keep your hardware safe.

Visit https://www8.hp.com/us/en/solutions/computer-security.html