Artificial Intelligence: A Smarter Way to Approach Enterprise Security

Companies today face an onslaught of cybersecurity challenges, from data breaches and the resulting loss of sensitive data to malware that can take down an organization's network at the press of a button. By all accounts, these threats are becoming much more sophisticated and much more prevalent. Thus, security measures must also grow more sophisticated to respond to these threats and keep up with—if not get ahead of—hackers and other cybercriminals bent on doing harm to organizations.

Companies of all sizes are considered fair game, but enterprises in particular are under constant threat, especially as mobile devices proliferate on the corporate network and expand the potential attack surface well beyond the four walls of the organization.

These days, cybersecurity strategies must leverage every tool available to protect digital assets and ensure every device attached to a network is secure. An increasing number of security-related technologies are incorporating AI to help bolster traditional security efforts by helping cybersecurity professionals detect, deter and destroy threats to data and networks.

The Need for Artificial Intelligence in Cybersecurity

In 2018, companies experienced more than 53,308 security incidents, of which 2,216 resulted in data breaches,[1] and more than two-thirds of those breaches took six months or longer to discover.[2] In addition, organizations pay on average $40 million for a data breach that involves 1 million records.[3]

Companies grappling with cybersecurity have more to lose than their sensitive data and potential profits; they also risk losing their customers. In fact, 78 percent of U.S. consumers taking part in a recent poll said a company's ability to keep their data private is extremely important and 75 percent said they will not do business with companies they do not trust to protect their data.[4]

At the same time, the security industry is facing a skills gap, with a current shortage of almost 3 million cybersecurity professionals globally.[5] The dearth of qualified security specialists is impacting how well organizations are able to react to existing threats and head off new ones. More than half of respondents taking part in a recent poll said their company is at moderate or extreme risk for cybersecurity attacks because of a lack of IT staff dedicated to cybersecurity.[6]

AI is providing much-needed insight into cyberthreats and helping fill the gaps in current IT security strategies. The market for AI in security is expected to reach more than $35 billion by 2024,[7] as organizations increasingly understand the threats are too great to manage without advanced technology.

When used in conjunction with security information and event management (SIEM) solutions, AI can spot anomalies in behavior patterns—of people, data, applications or devices—and predict attacks on the network, enabling organizations to defend themselves appropriately.

AI-enabled technologies provide a plethora of services related to managing a successful security posture, from network monitoring and risk management to detecting emerging cyberthreats and identifying fraud. Indeed, there are a seemingly endless number of solutions available addressing all manner of threats. Three areas in particular, however, show great promise for enterprise security: real-time threat detection, malware detection and software vulnerability detection.

Real-Time Threat Detection

AI has the ability to sift through massive amounts of data and spot trends faster than any human could. For that reason alone, a number of companies in various industries have adopted AI to improve the customer experience and be nimbler against their competitors.

In security, the ability to sift through large data sets and spot trends means attacks can be thwarted before they start. When used in conjunction with security information and event management (SIEM) solutions, AI can spot anomalies in behavior patterns—of people, data, applications or devices—and predict attacks on the network, enabling organizations to defend themselves appropriately. Such information also can be collected for historical reference to further detect patterns that could indicate potential attacks.

Malware Detection

There are few cyberthreats as pervasive as malware. Botnets, ransomware, cryptominers and more are impacting networks in myriad ways, overwhelming computer resources and potentially compromising network security by installing backdoors or scraping data. AI provides the necessary insight to detect malware by spotting events that aren't considered normal, such as a spike in power consumption every night between midnight and 4 a.m., which might indicate the presence of cryptomining malware.

AI can also stop malware immediately by shutting down any activity it sees as deviating from normal behavior—such as the aforementioned spike in power consumption. It can also quarantine unrecognized apps to prevent them from accessing other systems or processes to prevent possible malware infections.

In addition, AI can "learn" from older malware codes to detect new or mutated versions of malware, further protecting organizations even as cyberthreats evolve.

Software Vulnerability Detection

As more organizations take a software-centric stance in the market—even going so far as to call themselves a software company that happens to make athletic shoes, in the case of Nike, for example—a growing number are adopting DevOps principles to build better-quality software and release it faster. For some organizations, that can mean code releases weekly or even daily.

Ensuring software and application code is free from any errors that make it prone to vulnerabilities is a near-impossible task for humans to accomplish. The average iPhone game app has about 50,000 lines of code, while the 2.2.0 version of the open source operating system Linux Kernel has more than a million lines of code,[8] for example. AI, however, can do accurately in minutes what would take developers weeks to do, with debatable results.

Augmenting, Not Replacing, Humans

As helpful as AI is in helping organizations improve their security posture through analysis and detection, it needs human assistance to be most effective.

Security professionals are critical for monitoring and managing alerts, providing a historical and operational perspective that AI systems can't. Indeed, that "human touch" is important for many aspects of decision-making in security, from determining false-positives in testing to understanding the scope of threats uncovered by AI systems and then acting upon those threats accordingly.

Taking Advantage of Artificial Intelligence and Other Tech Trends in 2019

The technology landscape for security in 2019 is rife with solutions designed to help organizations approach IT security in a more intelligent manner. However, AI and other new and emerging technologies can't be sustained on legacy networks and IT architecture. To reap the benefits of these technologies, companies need sufficient bandwidth as well as smart, software-defined architecture to enable more capacity, flexibility and control of business applications running across an enterprise—from headquarters to the edges at the branch level—to enable higher security and improve the user experience at all points on the network.

In addition, to take advantage of AI, organizations need an environment that supports digital technologies in every location. Hybrid cloud and network environments, SD-WAN and high-speed broadband are just some of the technologies that can enable companies to better manage their business applications across all locations, while networking components such as WiFi and unified communications ensure employees can work anytime, anywhere, with no impact on productivity.

Managed services, meanwhile, can help organizations as they adopt new technologies without overly stressing their current network and help streamline processes for IT managers, by tying disparate systems together and "filling in the gaps" as companies update current infrastructure and after networks have been upgraded.

Working with a network service provider can help IT leaders as they embrace new services for their organization. Organizations can leverage virtual and physical private Ethernet connectivity to assure there are no issues regarding network performance and availability for critical applications at all company locations. They also can receive all or some of their most critical connectivity functions as a managed service, including managed connectivity, WiFi, security, voice and business continuity, among others.

Conclusion

Enterprise security will continue evolving to protect against threats that are increasingly sophisticated and have the potential to do even greater harm to an organization. AI can help IT organizations bolster their security efforts by augmenting the work of cybersecurity professionals and filling the gaps in current IT security strategies.

To learn more about how Comcast Business can help, click here.

---

1 "2018 Hiscox Small Business Cyber Risk Report," Hiscox, 2018 https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

2 Ibid

3 "2018 Cost of a Data Breach Study," Ponemon Institute, 2018 https://www.ibm.com/security/data-breach/

4 "New Survey Finds Deep Consumer Anxiety over Data Privacy and Security," press release, IBM, April 16, 2018 https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html

5 "Cybersecurity Skills Shortage Soars, Nearing 3 Million," press release, ISC2, Oct. 18, 2018 https://blog.isc2.org/isc2_blog/2018/10/cybersecurity-skills-shortage-soars-nearing-3-million.html

6 Ibid

7 "Artificial Intelligence in Security Market By Application," research report, Market Research Engine, May 2018 https://www.marketresearchengine.com/artificial-intelligence-in-security-market

8 Jeff Desjardins, "How Many Millions of Lines of Code Does It Take?" infographic, Visual Capitalist, Feb. 8, 2017 https://www.visualcapitalist.com/millions-lines-of-code/