Why AI transforms cybersecurity

With the help of AI, cybersecurity can scale up to meet the demands of a changing threat landscape

Tomer Weingarten
Co-Founder and CEO, SentinelOne

THE COVID-19 PANDEMIC has accelerated how distributed the workforce is in terms of the devices we use and where we use them. We're seeing a dramatic shift from on-premises networks to a distributed workforce model that enables people to work from anyplace, use any device they want and even access cloud-based resources directly.

The focus becomes protecting the devices employees use to access data. The IT world is moving toward better securing those endpoints rather than trying to build a virtual wall around them. The risks of ransomware and cyberattacks are increased in this new paradigm, and legacy antivirus isn't built for today's realities.

The new approach involves embedding security into devices and infusing them with identity protection. Agencies need to authenticate the person using the device but also make sure the device is not compromised. And they need to continue to validate that the device is safe to use and the security portal is intact.

Monitoring endpoints via the cloud

The focus of protection has long been moving to the endpoint, but now that move is more pronounced than ever. However, agencies can no longer rely on a network to gain visibility into those end-user devices and know whether they are protected and what resources users are accessing. All that insight now happens via the endpoint rather than the firewall.

The distributed nature of the workforce makes it harder to control where devices are and sometimes even to provision them. Along with allowing remote work, agencies must also allow remote security. That means they need to be able to monitor all those endpoints via the cloud, and devices need to have embedded mechanisms that deliver real-time protection regardless of cloud connectivity.

Real-time response to threats

The proliferation in endpoint devices extends to the internet of things as well. When combined with the rapid influx of attacks, the volume of data that security teams need to process is increasing exponentially. At some point, it becomes impossible for a human team to monitor all those devices and sift through all that data.

Instead, a good part of that activity must be automated so that agencies can respond to threats and secure their resources in real time. Artificial intelligence has a key role to play in scaling cybersecurity and enhancing the human operator. Ideally, an AI algorithm should be deployed to take autonomous actions — deflecting attacks, analyzing events and making decisions in real time.

That scalable level of cybersecurity is the only way for agencies to ensure that their distributed networks are protected from attack. ■

Tomer Weingarten is co-founder and CEO of SentinelOne.