State, Local Agencies Widen Anti-Virus Tech to Scrutinize Behavior

Theo Douglas | August 1, 2018

Realizing malware's growing sophistication and seemingly endless capacity for change, state and local governments are diversifying their security solutions against the evolving threat to one of their most vulnerable areas — the endpoint.

"The fast-moving nature of attacker tools, techniques and procedures means that an organization's endpoint security strategy must be continually assessed and adapted," writers at the technology research company Gartner said in the " Magic Quadrant for Endpoint Protection Platforms" report earlier this year. Malware's malleability is a central issue in endpoint security, as bad actors write myriad variants into its code, altering its once unique digital signatures or enabling it to run fileless, without ever writing any code to a drive.

The public sector remains at high risk and this year has seen some of the most resilient and devastating attacks ever against governments from Atlanta to Alaska. But information security officials at state and local agencies are mindful of the threat they face and are taking steps to guard against multiple types of malware. In Montana, Chief Information Security Officer Andy Hanks described the state's cybersecurity posture as “very fluid, based on the evolving threat landscape,” and said its philosophy is that it will always have both “ signature-based and behavior-based” anti-virus technology.

“The big difference I’ve found between the private sector and the public sector is that in private sector, you’re generally focused on (protecting) one or two areas, whereas in public sector, you pretty much need to focus on all of them,” said Hanks, who came to the state in January from IBM where he had been global security program manager.

“You put multiple locks on the doors of things you want to keep safe,” said Kevin Haley, director of product management for security technology and response at the cybersecurity firm Symantec. “Endpoints should have multiple locks. Organizations should have multiple locks throughout the organization.”

Symantec has long included behavioral- and signature-based technology in its endpoint protection. In its report, Gartner rated the company one of three leaders, a designation signifying “ balanced and consistent progress and effort” across “all execution and vision categories.”

A tech official in Charlotte, N.C., said government, like other sectors, is increasingly aware the traditional perimeters once protected by network firewalls and security controls have shifted dramatically with the advent of online work.

“Over the past several years, that perspective has shifted to the realization that, with an increasingly mobile workforce, that perimeter often gets basically broken down to the endpoint being the perimeter. And so, the role of security on an endpoint has become increasingly important for us,” said Cal Queener, information security supervisor for the Innovation & Technology department in Charlotte.

Both Charlotte and the state of Montana deployed behavior-based anti-virus endpoint protection last year from SentinelOne, one of 12 companies Gartner’s report called visionaries for delivering “ leading-edge features” that will be “significant in the next generation of products.” In Montana, the state did months of research, including consulting with other governments before choosing it based on its protection, remediation, forensics and cost. Officials in Charlotte did a broad search as well, considering technology from Carbon Black, Cylance and CrowdStrike before selecting SentinelOne for its behavioral focus, integration of cloud-based threat intel and open application programming interface (API) that allowed customization.

SentinelOne CEO Tomer Weingarten said a lack of maintenance and updates across broad enterprises combines with the human tendency to click through questionable emails to make governments a sometimes easy target. His company’s solution, Weingarten said, utilizes machine learning with static AI to analyze malware files; and behavioral AI to scrutinize memory, network, file and registry operations for anomalies and exploits at work as malware takes hold. Deployed directly onto endpoint machines, it’s automated, autonomous and works in the background.

“What we call ‘behavioral AI’ is the ability to really detect something and protect from an attack. Not by looking at signatures or at static indicators of compromise, it’s by actually looking at the nature of what it does,” Weingarten said.

In Charlotte, Queener said the agency used SentinelOne across its more than 20 departments; and, while it has resulted in some false positives, has caught threats “we are absolutely certain would not have been caught by our legacy anti-virus vendor that we had in place before.”

Officials in Montana agreed, praising the solution’s ease of installation, deep visibility for staff with varying skill levels and powerful potential against ransomware.

“The bad actors have evolved and gotten smarter on how to bypass security controls. We have researched and found that it’s very easy to bypass traditional-based (anti-virus). That’s why we felt the need to improve our security posture and pursue a next-generation (anti-virus) solution,” said James Zito, incident response and technical security supervisor for the state of Montana.

http://www.govtech.com/pcio/State-Local-Agencies-Widen-Anti-Virus-Tech-to-Scrutinize-Behavior.html