MAR 01 2021

SECURITY

5 Key Capabilities Next-Generation Endpoint Security Offers for Enhanced Cybersecurity

Advanced recognition, analysis and response resources are helping government agencies obtain robust, layered protection.

by Erin Brereton

Erin Brereton has written about technology, business and other topics for more than 50 magazines, newspapers and online publications.

Years ago, state and local governments relied on reactive methods such as signature detection to protect against cyberthreats.

Attackers' techniques, however, have grown more complex. Government entities have also become more frequent targets: Attacks on local governments rose over 58 percent between 2018 and 2019, according to data from security training provider KnowBe4.

These factors, along with the increase in employees working remotely due to the coronavirus pandemic, have prompted the need for a complex and nuanced cybersecurity approach.

Over the past several years, next-generation endpoint security tools have become a popular option, according to Michael Suby, IDC research vice president for security and trust. Instead of looking for hashes that represent a sequence of code related to a bad actor, today's endpoint security solutions utilize behavioral monitoring, threat intelligence and other protective methods to rapidly detect and block attacks.

"Threat actors are smart; they just accelerated their process of creating malware variations," Suby says. "Their behaviors have become more subtle and difficult to discern from appropriate behaviors. Organizations' approach is, 'Let's be clearer about what we'll allow to happen, what applications we'll allow to be on endpoints and what application behaviors we find acceptable.'"

A number of next-generation endpoint protection tools can help organizations identify, assess and ultimately deal with potential threats. Here are five key features to consider in a next-generation endpoint security system and how they can help government agencies prevent and respond to cyberattacks.

1. Next-Generation Anti-Virus

In the past, anti-virus tools required organizations to frequently update a signature database. While signature file detection is often still a cyberattack prevention component, next-generation anti-virus solutions incorporate advanced features, such as artificial intelligence, offering dynamic, proactive protection.

"Next-gen antivirus has moved from looking for just code to looking for malicious behavior," Suby says. "That's a big difference."

Endpoint security software provider SentinelOne's Singularity Core cloud-native next-generation antivirus product, for instance, scans files and scripts, monitors behavior and utilizes AI to identify and stop malware, script misuse and other attacks.

"We've eliminated the need to have a signature database and any prior knowledge of the attack," says Jared Phipps, senior vice president of worldwide sales engineering at SentinelOne. "We can tell if something is good or bad using AI and behavioral analysis, and we can remove something from a machine if we need to. It's a dramatic difference over legacy anti-virus tech."

2. Endpoint Detection and Response (EDR)

Organizations want to quell attacks as soon as possible to minimize their effects. In addition to detection capabilities, endpoint detection and response technology can provide a fast automated response.

EDR solutions, according to Gartner, generally have several common attributes. They record endpoint-level behaviors, use data analytics to detect suspicious system behavior, contain security incidents at the endpoint and provide remediation guidance to restore affected systems.

Essentially, EDR capabilities will complement modern anti-virus solutions, according to Suby, which can often confidently identify a number of malicious activity indications but may not always be able to gather enough evidence to confidently reach a verdict.

"In some cases, next-gen anti-virus can react with a high level of certainty," he says. "When that's not the case, we're looking at EDR to help us uncover more subtle threat actors. It provides another layer of defense."

LEARN MORE: Find out how agencies can gain visibility by centralizing logs.

3. Mobile Threat Defense (MTD)

A third of IT and security professionals identified attacks involving employee mobile devices as one of their top three cybersecurity concerns as of mid-2020, according to a Check Point survey. Forty-three percent said they planned to implement mobile security solutions within months.

Touching on applications, networks and devices, mobile-focused defense products can include protective techniques such as monitoring network traffic and analyzing code.

Palo Alto Networks' Cortex XDR, for instance, utilizes a mobile agent that can prevent known malware and unknown malicious APK files from running on Android endpoints while also enforcing an organization's security policy, according to Elton Fontaine, senior director of systems engineering at Palo Alto Networks, which has worked with state and local government entities for over a decade.

"The security policy determines whether to block known malware and/or unknown files, upload unknown files for in-depth inspection and analysis to Palo Alto Networks' cloud-based WildFire malware prevention service, treat malware as grayware or perform local analysis to determine the likelihood of an unknown file containing malware," Fontaine says. "Administrators can also whitelist trusted signers to enable unknown apps to run before Cortex XDR receives an official verdict."

4. Sandboxing

Isolating unknown objects from key system resources to analyze how they'll function in a controlled environment can prevent threats from reaching the network. Sandboxing, or advanced malware analysis, was the most frequently installed network security technology in 2019, used by 62 percent of organizations, a 12 percent increase from the year before.

CyberEdge Group, the research firm that sponsored the study, attributed the rise to the tools maturing and being incorporated into cloud-based security suites — and malware being perceived as the single most dangerous tool a hacker has.

Ransomware in particular, according to Phipps, has been a prevalent state and local government threat for the past two years; those governments can be targets because a number don't have next-generation solutions in place, he says, and could be motivated to pay the ransom to get critical services like a 911 system back online quickly.

"We've seen a lot of high-profile cases go public," Phipps says. "That's what sparked people to have a strong interest in endpoint security, because they've seen it happen enough to other people to realize it's only a matter of time."

> "Next-gen antivirus has moved from looking for just code to looking for malicious behavior. That's a big difference."
>
> Michael Suby, Research Vice President for Security and Trust, IDC

Some security professionals, however, have expressed concerns about sandbox evasion technology in recent years, due to attackers finding ways to recognize their malware isn't running in a live environment and potentially terminating its execution to conceal the incident.

SentinelOne's behavioral analysis capabilities, Phipps says, essentially establish sandboxlike protective measures on every endpoint to detect concerns, analyzing elements of items such as Microsoft's PowerShell, which administrators can utilize in legitimate ways but hackers also use as a key ransomware component.

"We know when someone or a system process is accessing the Local Security Authority Subsystem Service (LSASS) properly, and when a hacker is trying to dump passwords from it," Phipps says. "We determine it and block it right there, on the spot. We're trying to take the decision a security team would have to make and do it at runtime so they can focus on more complex security aspects."

EXPLORE: What is the state of local government cybersecurity?

5. Next-Generation Firewalls

The fundamental defining characteristics of a next-generation firewall, according to Fontaine, involve the ability to leverage deep packet inspection and enforce policy based on Layer 7 identification of an application and its users.

Palo Alto Networks' next-generation firewall platform delivers security capabilities, Fontaine says, that would traditionally require their own standalone hardware, such as URL filtering, Internet of Things security, data loss prevention and software-defined WAN.

"The automated integration and collaboration of these capabilities has helped our local and state government customers markedly increase their security posture and reduce the administrative burden of manually coordinating intelligence between disparate solutions, while reducing the spend required to maintain several standalone solutions," Fontaine says.

Next-Generation Tools Facilitate Workplace Security

Although remote environments have become the norm for many government employees in the past year, eventually, a number will return to working on-premises. Although it may seem as if that will reduce some of the need for MTD, firewalls and other protective measures, IT and security professionals aren't so sure.

Three-quarters said they fear a further increase in cyberattacks and exploits as offices reopen and employees at the same time work remotely.

With the increased probability that governments, like many organizations, will operate under a hybrid work environment, established perimeter-based security technologies may have less relevance, according to Suby.

Today's next-generation endpoint solutions could potentially provide some protection.

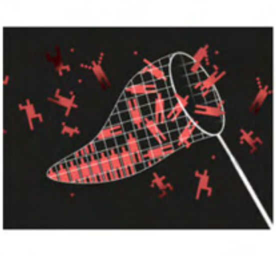
"The perimeter needs to be more at the endpoint," Suby says. "Endpoints have always been a popular initial point of attack; that continues to be the case. Endpoint security is not a stagnant solution. Products will continue to expand the methods they have to identify threats and take action. We're entering a period of evolution in endpoint security."

MORE FROM STATETECH: How do SIEM tools enhance government cybersecurity?

BORCHEE/GETTY IMAGES

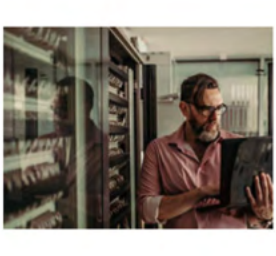
More On ANTI-MALWARE ANTI-VIRUS ENDPOINT SECURITY FIREWALLS THREAT PREVENTION SECURITY SOFTWARE

Related Articles



Security

3 Stages of Building an Identity and Access Management Program for Government



Security

Ransomware, Phishing Top Cybersecurity Concerns for State and Local IT Leaders

Security

Infrastructure Legislation Could Improve State and Local Government Cybersecurity

Latest Articles

- Hyperconverged Infrastructure Empowers Cities To Scale Citizen Services
- Social Service Agencies Turn To The Cloud And AI To Serve Families In Crisis
- 3 Stages Of Building An Identity And Access Management Program For Government
- State Government Enterprise Systems Benefit From Business Relationship Management

CLOUD

Social Service Agencies Turn to the Cloud and AI to Serve Families in Crisis

INTERNET

30 State and Local Government IT Influencers Worth a Follow in 2021