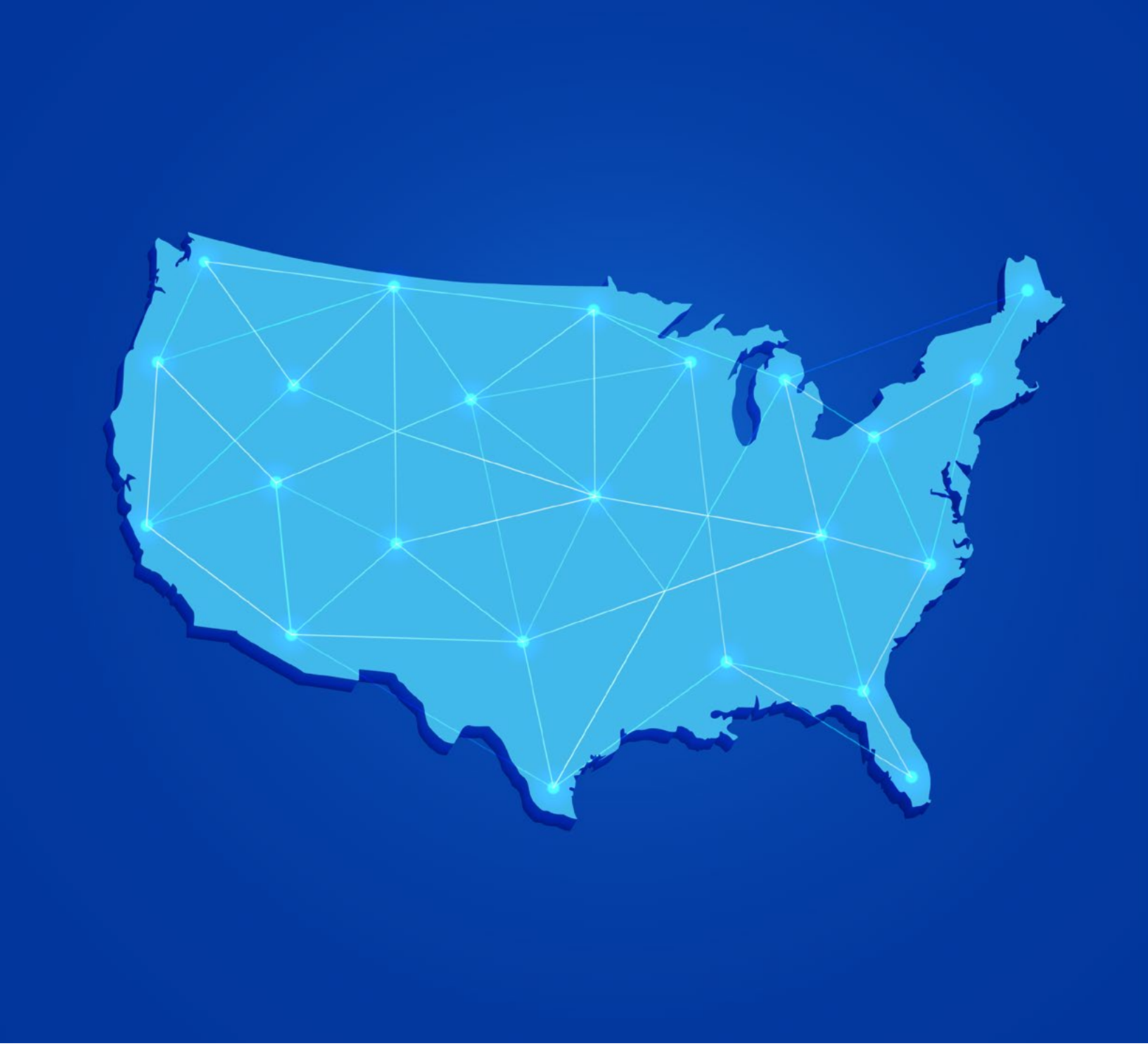


Smart Move: Why Government Agencies Need AI-Powered Cybersecurity

MARKET TRENDS REPORT

govloop BlackBerry carahsoft

Executive Summary

Security teams can feel outnumbered against the sheer volume, velocity and variety of cyberthreats that take aim at government agencies every day. But they're also being outsmarted — by zero-day exploits and other advanced threats that bypass the signature-based security measures in place to stop attacks. Those attacks slip by unrecognized by traditional antivirus (AV) programs and undetected by overwhelmed cybersecurity teams who lack the staff and possibly the skills to spot the attacks before they get into and damage networks.

To make matters worse, a range of advanced attacks has hit government agencies at every level, which are expensive to remediate while further straining the IT and security teams.

A zero-day exploit initiated the 2020 SolarWinds attack, which spread to government agencies, major corporations and other organizations in the company's supply chain. In February 2021, a Chinese attack group dubbed Hafnium used a zero-day attack to exploit flaws in Microsoft's Exchange Server email software, and within a couple of weeks, had infected more than 30,000 U.S. organizations — including a significant number of city, town and local governments — and thousands of other organizations in more than 115 countries.

Leaders' favorite phrase — "work smarter, not harder" — may at times elicit eyerolls, but in cybersecurity, it is truly what's necessary today. And with properly deployed artificial intelligence (AI), it is very possible. The key is to focus not just on protection, but on prevention.

To learn more about how agencies can leverage AI to make dramatic gains in cybersecurity, GovLoop teamed with BlackBerry, a software company that provides AI-driven predictive security, on this report. We look at the key ways in which agencies can apply AI to cybersecurity and discuss best practices and case studies that show how to do it.

By The Numbers

No. 1

The rank of cybersecurity and risk management among the National Association of State Chief Information Officer's (NASCIO) State CIO Top 10 Priorities for 2021.

$18.9 billion

is the total cost in downtime and recovery costs from 79 ransomware attacks against U.S. government organizations in 2020.

70%

of cybersecurity pros say their organizations have a cyber skills shortage.

21%

is how much longer it takes to fill cybersecurity jobs, compared to jobs in other fields.

3.5 million jobs

is the estimated size of the worldwide cybersecurity skills gap.

61%

of malware cases in the public sector involved ransomware in 2020, as did 80% of malware cases in education.

67%

of all cyberthreats in the second fiscal quarter of 2020 involved zero-day malware.

"Under-resourced and under-staffed local governments continue to remain an easy target for cyberattacks."

– NASCIO President Denis Goulet in testimony before Congress, December 2020

Getting Smart About Cyber Prevention

The Challenge: A Job Too Big for Traditional Tools

The challenge security teams face is that the traditional approach to defending against malware can't keep up with the daily barrage of new malware in circulation, no matter how diligently security companies update their software.

"The traditional AV world has known for probably 15 years or more that they can't keep up with creating signatures for every single type of malware or attack that there is," said Brian Robison, Chief Evangelist at BlackBerry.

Attackers continually create new malware, variations on malware and new techniques for gaining access to networks. Between 300,000 and 500,000 samples of new malware are created every single day. "You'd have to employ thousands of researchers writing signatures to keep on top of even Monday's threats, let alone Tuesday's and Wednesday's and Thursday's," he said.

Cybersecurity providers have addressed the evolving malware threats by adding layers of security, such as host-intrusion protection and behavioral analysis, to generally good, though limited, effect.

"Signature-based, traditional AV does very, very well against known malware," Robison said. But it's the unknown malware, the zero days, behind many of today's most pernicious threats.

For example, zero-day attacks — which exploit previously unknown vulnerabilities — have become increasingly common. WatchGuard reported that 67% of all cyberthreats in the second quarter of 2020 were zero-day exploits.

"For all the improvements the cybersecurity industry has made," Robison said. "We are still stuck in a detect-and-respond paradigm based on getting hit first, then initiating an endless loop of getting a sample, analyzing it, assigning a signature and releasing a software update."

For state and local agencies with limited staff and resources, it's impossible to keep up.

The Solution: Working Smarter (Not Harder) with AI

Agencies need a new approach based on prevention.

"The only way to stay ahead of malware-based attacks is to create a predictive capability where you can learn from history to predict the future," Robison said. "And that is precisely what machine learning and artificial intelligence are absolutely fantastic at doing."

Many high-profile attacks — such as the recent ones involving SolarWinds and Microsoft, or even going back to the infamous Office of Personnel Management (OPM) attack of 2015 — have involved systems that traditional security products and services protected, albeit with some holes in how they were implemented. But they also didn't see the attacks coming.

"Those products failed to predict the malware that was used to exploit the system because the world had never seen it before — until there's a sacrificial lamb," Robison said. An AI-driven system would have made a difference.

AI systems can review and analyze millions of features instantly and recognize patterns and draw on historical behaviors to discern good from bad — even if it's something that has never been seen before. This makes it possible for AI to recognize previously unknown threats and prevent them from executing.

"As demonstrated in the report, AI could have prevented the OPM attack had it been in place before the attack rather than after," Robison said. The same is true for other major ransomware attacks, such as WannaCry , REvil, and more recently, DarkSide, that have plagued state and local governments.

AI's automation and learning capabilities also help relieve some of the workload and stress in managing IT security. In addition to requiring substantially fewer updates, its ability to detect threats, sort alerts and even initiate a response automatically, removes many manual duties that security personnel handle.

"We see these attacks happening essentially on a daily basis, whether in federal government, state government, local governments, school districts, whatever," Robinson said. "We see ransomware attacks constantly. And if there's a better way to prevent those things, there's really no excuse for not doing that."

Best Practices in AI-Enabled Security

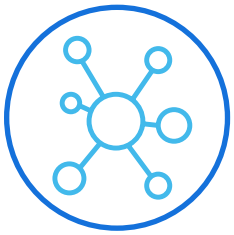
Not all AI is created equal, so government agencies looking to adopt a predictive security posture should look for features that benefit them. That includes:

Offline Ability

Most traditional AV systems depend on a constant flow of information and updates to stay up to speed and constant connectivity to the cloud services, which can leave them ineffective (or not working at all) when connectivity is lost. Because an AI-driven security solution does not rely on signature-based detection, it can continue functioning as long as it has power. AI-driven technology can often be extremely effective, even when years out of date.

Lower Overhead

AI handles its processing locally on the device, which requires fewer resources than traditional solutions that need a regular flow of updates and a steady transmission of data from a central location followed by a response from the IT center. That all adds to the traffic and latency on a network. And because AI can handle its job via a single AI process compared with traditional AV, which could be working with multiple products from different vendors, it often requires less memory to run. In some cases, AI only needs 50 to 70 megabytes as opposed to 700 megabytes or a gigabyte with typical AV.



Securing a Range of Systems

The Internet of Things is full of outdated medical devices, manufacturing devices, kiosks and point-of-sale machines with limited amounts of memory and running older operating systems, such as Microsoft Windows 7 or even Windows XP. They aren't updated often but are still part of the network and must be protected. An AI system's tiny footprint allows it to fit comfortably in those devices, delivering malware and attack prevention without requiring steady updates and management, and will continue to work seamlessly whenever that device's OS is upgraded.

Update Independence

The key factor in a solution's ability to work offline is its ability to function effectively without a constant flow of updates from a central location via an internet connection. That requires continual uptime and effort from the IT staff. An AI solution's ability to learn as it goes and think independently allows it to function without the need for signature-based updates, because it doesn't use them. A mature solution can go a year or more without needing a new version pushed out to a network's endpoints.

HOW BLACKBERRY® HELPS

BlackBerry has an extensive history of providing security services to local, state and federal agencies. Their services do everything from enabling secure communications to supporting emergency response, to a full range of cybersecurity services that can be tailored depending on an agency's needs. For example, endpoint protection platform and endpoint detection and response are applicable for all organizations regardless of size, while higher-level services such as a security operations center and threat hunting may be necessary only for large organizations with an international presence.

The company's AI-driven security portfolio and its ability to continue working while offline can benefit agencies at any level. BlackBerry® Protect and the company's other solutions provide not just malware protection, but malware prevention, combined with features such as application and script control, memory protection, and device policy enforcement.

"We are a prevention-first company," Robison said. "We focus on preventing the event from happening in the first place, rather than monitoring or cleaning it up after."

For more information: BlackBerry Protects Against Nobelium Malware Attacks

> "The results speak for themselves. For over seven years now, we have had zero incidents of malware of any type, including zero-day threats and ransomware. BlackBerry's solution is proactive, frees up our resources, and provides us with peace of mind when it comes to security threats in our environment. No other vendor can claim to do what BlackBerry Protect does."
>
> *- Michael Dent, Chief Information Security Officer for Fairfax County, Virginia*

Conclusion

The threat environment has outstripped signature-based AV solutions' abilities to defend networks, leaving critical government data and operations vulnerable to costly attacks, such as ransomware, that erode the public's trust and affect agencies' ability to deliver critical functions.

Agencies need to get away from the outdated detect-and-respond paradigm and move toward preventing attacks. And prevention is possible with a mature AI-powered solution that can stop malware before it can penetrate and damage a network. AI solutions are cost-effective and proven to improve both return on investment and productivity among IT personnel, a particular benefit for state and local agencies that feel the pinch of limited budgets and the IT skills shortage.

AI security represents the future of network defense, not just augmenting traditional protections, but making them unnecessary. "This is essentially the next generation or the future generation of that," Robison said. "We are using AI to replace signature-based AV."

ABOUT BLACKBERRY

BlackBerry provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions and is a leader in the areas of endpoint security management,encryption, and embedded systems. BlackBerry's vision is clear—to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry.

ABOUT CARAHSOFT

Carahsoft is the trusted government IT solutions provider, combining technological expertise with a thorough understanding of the government procurement process to help public sector organizations select and implement the best solution at the best possible value. As a top-ranked GSA Schedule Contract holder, Carahsoft is the largest government partner, serving as the master government aggregator for many of its best-of-breed vendors and driving value for an extensive ecosystem of IT manufacturers, resellers, system integrators, and consulting partners. Our dedicated solutions teams support proactive sales, marketing, and delivery of strategic solutions to help improve the efficiency and productivity of government IT.

For more information please visit www.carahsoft.com/

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop