

Cybersecurity in the Federal Government

How Artificial Intelligence Provides Predictive Protection

CYLANCE™

Introduction

Federal agencies face many of the same cybersecurity challenges as private-sector organizations. These include a barrage of attacks such as malware, phishing emails used to spread malware or steal credentials, and distributed denial of service attacks that can be generated by malware-infected systems elsewhere.

Agencies also must deal with issues that businesses typically do not encounter, however, and that require a new approach to protecting data assets. For example, many agencies need to protect themselves against nation-state actors that are specifically targeting them using malware built solely for that purpose. Nation states continue to recruit highly skilled people whose main focus is to carry out these attacks.

In addition, a number of agencies utilize an air gap strategy, in which many of their networks are physically isolated from unsecured networks such as the Internet. That means the systems on these networks do not have easy access to the malware signatures pushed out by antivirus vendors after they identify and analyze new malware.

To address these challenges and better protect data resources, federal agencies must transition from traditional security solutions based on signature technologies to newer machine-learning capabilities designed to stop the latest attacks.

More and more businesses and local, state, and federal government agencies are beginning to learn and see the value of predictive cybersecurity that exceeds traditional benchmarks. By employing new methods and technologies, federal agencies can provide better security to both their own employees and the public they serve.

Feds Face Daunting Challenges

A number of security threats plague the federal government on an ongoing basis, and perhaps the most daunting and damaging of these are attacks sponsored by nation states. Launched by people recruited or hired by foreign governments, these attacks access systems and networks of specific U.S. government agencies. The attackers are highly skilled and well financed, and they spend time and resources developing schemes that take advantage of the latest vulnerabilities to compromise federal agencies.

They base their attacks on detailed knowledge they have gained through research about the security infrastructure and vulnerabilities of a particular agency, which technologies the agency uses, what the agency's work processes are, how employees gain access to data, etc. They conduct a significant amount of surveillance, often over a period of months, to gather all the information they need prior to launching an attack. They do this so that their attacks can have the maximum effectiveness — and go completely undetected by the agencies they target.



What makes these attacks so difficult to defend against? They involve pieces of malware that attackers have created or modified specifically to execute on an endpoint of a particular agency. Because the malware has never been seen before and will likely only be used once or twice by the attacker, the signature-based security tools deployed by many agencies will not be effective at detecting and stopping it. The malware will breach traditional signature-based defenses and adversely affect federal systems.

Many signature-based anti-malware products are designed only to stop malware that the product vendors have previously seen. These malware samples are analyzed in depth so that vendors can develop and test signatures that are distributed to customers. This approach is time consuming and oftentimes ineffective at stopping malware that is being used for the first time. Given that the federal government has made substantial investments in signature-based security technologies over the past 25 years, these types of attacks create a significant and sustained risk for most federal agencies. Many agencies are simply not prepared to defend against new malware, putting their systems and data at risk.

Another big challenge that many federal agencies face is the presence of air-gapped networks. Certain government organizations with extremely high security requirements run air-gapped networks, which are completely disconnected from the Internet. They do this as a precautionary measure that isolates their networks and the systems connected to them from Internet-based threats.

But because signature-based solutions rely on the Internet to push out signature updates when they are needed, this lack of connectivity renders the security products far less useful and effective for the agencies that have air-gapped networks in place. Government agencies would have to manually provide the updates at the endpoints for protection against new malware in air-gapped environments, which is not at all practical. Many times, traditional anti-malware solutions require multiple signature updates in a single day.

Another option the air-gapped agencies have is to set up a server on each air-gapped network for internal signature distribution. But getting updates from the Internet several times a day and manually transferring them to the distribution server on each air-gapped network could be a significant effort requiring large expenditures of human capital. Any time people are involved in lengthy and sometimes tedious processes, the possibility of errors increases, which can lead to additional risks as well as increased support costs.

Furthermore, this option has its own security risks. Assuming that the updates would be transferred using removable media, agencies would then need to scan the removable media each time to make sure it does not contain any known malware. This, in itself, is not effective if the media is infected with malware that has not been seen before.

Moreover, federal agencies face an ever-growing volume of signature files being generated by anti-malware products. Many agencies operate expansive networks with many systems connected, and the distribution of signature file updates to all these systems several times a day can consume considerable network capacity, especially given how large the signature files often are.

This also affects the air-gapped networks if there is a dedicated server for internal signature distribution. All the systems on the air-gapped network have to transfer the signatures from that server several times a day. That consumes a tremendous amount of time, effort, and resources.

In some cases, agencies might have to acquire additional network capacity in order to support anti-malware software signature file distribution. At a time when many agencies are looking to rein in technology costs, this is an unnecessary financial hardship.

Artificial Intelligence and Machine Learning

It's clear that federal agencies need a better solution than signature-based technology in order to properly protect systems and data against the growing number and increased sophistication of threats. The legacy, signature-based approach to identifying malware attacks does not effectively secure agency assets, particularly in the context of well-resourced, highly capable nation-state threat actors. Time and time again, this approach allows malware to exfiltrate precious data from agencies or otherwise harm agency systems.

A much better approach is to utilize security technology on each endpoint — whether it's a desktop, laptop, server, or virtual machine — that applies artificial intelligence (AI) and a mathematical approach using machine learning. Such an approach provides instantaneous identification and prevention of many types of malware and other cyberattacks. This enables agencies to protect their systems and data without the need for signatures.

What makes security technology like this possible is the progress that researchers have made in algorithmic science, as well as the rise of big data analytic processing capabilities. With the centralized analysis of hundreds of millions of file binaries (both known 'good' and 'bad' samples) collected from public and private malware repositories, this solution then extracts millions of features from each of these files and applies artificial intelligence and machine learning techniques to build highly accurate mathematical models. The models identify what are statistically good and bad features and combinations of features.



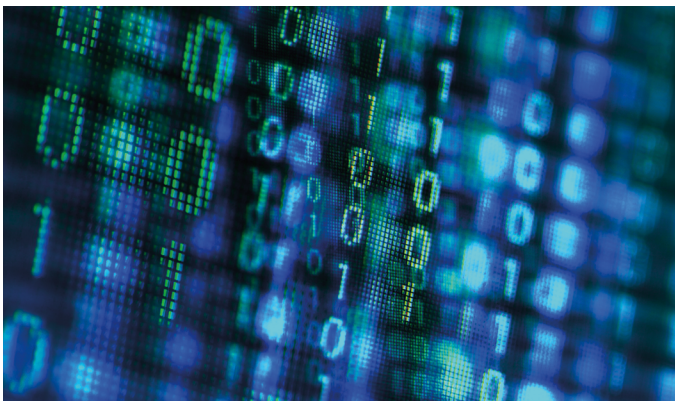
Before any binary can be executed on a host, real-time static analysis and predictive modeling determines if the binary contains malicious features. If the binary is deemed a threat, the solution stops it from executing, and thus prevents the system from becoming compromised. This is an incredible difference from the current threat environment at most agencies and other organizations; when a threat is detected, that usually means the organization has already been compromised.

This new type of security solution is ideal for addressing the problem of nation-state actors. The AI and machine learning capabilities can quickly identify and stop the highly-targeted, custom-made malware created by these attackers — even if the malware has never been seen before in any other environment. That's something signature-based products cannot do.

The machine learning capability enables agencies to identify and prevent the execution of all types of malicious content, including zero-day activity, malware related to the implementation of advanced persistence mechanisms, BIOS malware, master boot record (MBR) malware, hypervisor malware, and malware capable of injecting into memory at any time. This can stop many nation-state attacks that rely on malicious code execution.

As for the challenge of dealing with an abundance of signature files that consume significant network capacity, that is no longer an issue. The newer security solution does not have signature files, so it does not require the constant updating of traditional anti-malware software. Updates can be far less frequent, and as a result, this type of solution greatly reduces the bandwidth and administrative burdens on agencies. They can push updates through their standard software distribution practices.

In terms of addressing the issues of updating systems on air-gapped networks and requiring systems to have Internet access most or all of the time, this type of solution does not require frequent updates and does not rely on constant Internet access. It runs entirely on the host endpoint and requires no Internet connection to be able to analyze malware, predict its intent, and prevent it from executing. Each binary executable is analyzed locally by the solution's self-contained prediction and prevention model. The solution's defenses remain effective even after months of not being updated because the analysis is not dependent on signature files or other knowledge of specific instances of malware.



The agencies that rely on air-gapped networks will be able to block malware without having to update the security solutions more than a few times a year. This is different than traditional security products that rely heavily on constant signature lookups in the cloud or frequent signature downloads.

The adoption and use of newer security solutions for endpoints can lead to greatly reduced costs. By taking advantage of advanced mathematical approaches to cybersecurity instead of using signature-based scanning, newer security solutions minimize the requirements for resource consumption such as CPU usage. This is of particular importance to federal agencies that have legacy systems that might struggle to run signature-based technologies because of the extensive system resources they require.

With newer, smarter security solutions, federal agencies can stay ahead of the bad actors who are constantly trying to break into their systems. They can be more effective in preventing the execution of malware, advanced persistent threats, and other forms of attack at each endpoint, which means they can more effectively protect federal agencies against attacks. The process of identifying and stopping a malicious executable is extremely fast, taking less than 100 milliseconds. That's a major advantage, given how quickly malware can inflict damage on agency systems.

Summary and Conclusion

The U.S. federal government is a major target for highly resourced, well funded, and skilled threat actors. And when it comes to cybersecurity and the government, the stakes are extremely high. U.S. residents — as well as millions of people around the world — rely on many of the services the government provides, supports, or regulates.

Any attack on a federal agency, even one that brings systems down for a matter of hours, can potentially have significant repercussions. Furthermore, a successful attack on one agency could give further impetus for other bad actors to conduct similar assaults on other agencies.

Government agencies are highly popular targets for cyber espionage, in which attackers are looking for sensitive data. According to Verizon's 2016 Data Breach Investigations Report, which examined cybersecurity threats in 20 industries, public sector organizations were top on the list of targets of espionage-related attacks.

The attacks against government agencies will not likely abate any time soon, according to consulting firm PwC's Global State of Information Security Survey 2016. Government agencies detected 137% more cybersecurity incidents in 2015 than in the prior year, the report said.

Perhaps because of the increased threat levels, government agencies are showing a willingness to invest in security technologies. After a decline in spending on security in 2014, agencies increased their cybersecurity budgets by 23% in 2015, according to PwC.

They will need stronger security because threats continue to become more dangerous and unpredictable. Today's threat environment is similar to an asymmetric digital conflict. The threat actors are able to create and distribute highly customized and sophisticated malware. They are also able to take nearly any instance of malware and mutate it into new, undetectable variants within a matter of minutes. The legacy approach of using signature-based technology that essentially relies on a malware blacklist is simply not adequate for protecting federal agencies.

Consider that a single piece of malware can be mutated many times over by a single bad actor. There could potentially be an exponential factor behind malware incidents. For each piece of malware, it could take researchers days to analyze it and develop signatures. There is simply no effective manner to scale this up.

The endpoint is the new battleground. With the expansion of commercial cloud applications, a highly mobile workforce, the growth of telecommuting, and the expanding use of portable media, the endpoint has become the extended perimeter of an agency. As such, the extended perimeter is also the key target of adversaries and needs to be protected with the most advanced set of capabilities available on the market today.

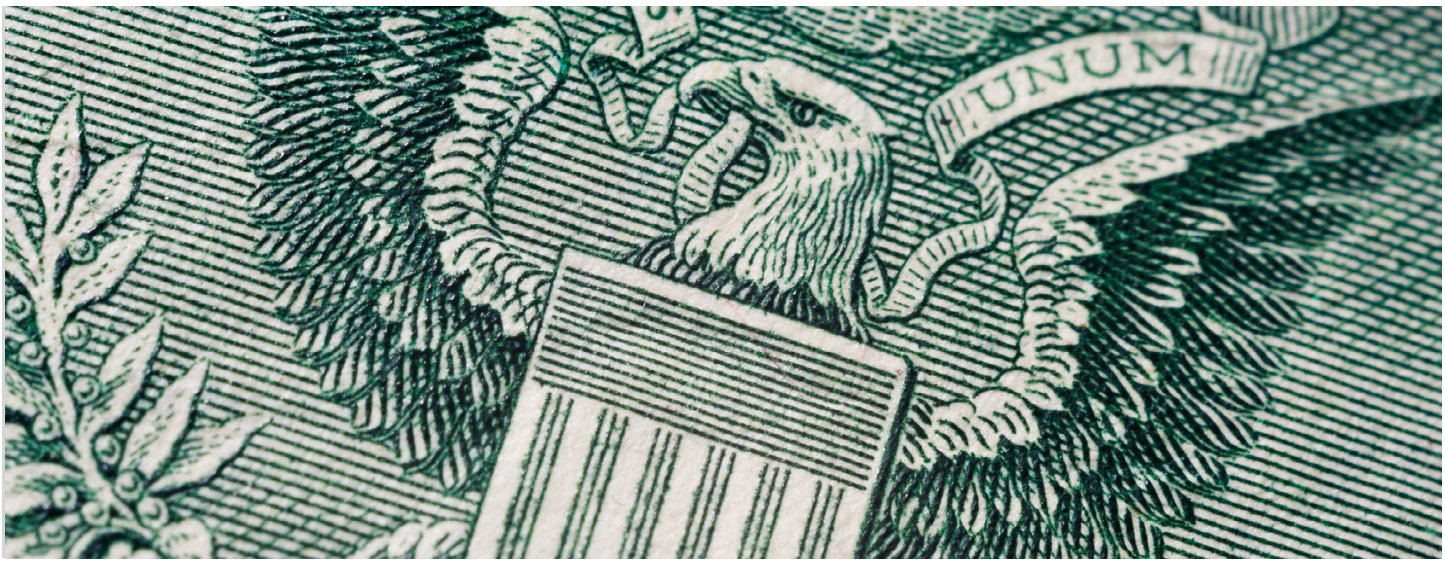
In looking for security solutions, agencies should consider three key questions:

- Does the solution truly secure the agency's endpoint population, preventing malware and other threats from doing damage?
- Does it simplify the security environment of the agency, removing signature-based technologies at the endpoint that are no longer as effective in stopping attacks and actually cause network traffic to keep rising?
- Does it drive down the total costs of security technology for the agency?

If the answer to any of these questions is "no," it's time to look for another solution. Total protection of the endpoint is essential for ensuring that federal agencies can continue to operate effectively. At the same time, that protection must not come at the cost of increased complexity of security environments, and result in ever-increasing expenses for security.

IT and security executives at federal agencies need to take a hard look at how they are protecting their agencies' systems today. If they continue to rely on aging, ineffective methods of defending against malware and other malicious content, they are essentially inviting the bad actors and nation-state sponsors to exploit the inherent weaknesses of those legacy solutions.

For more information about new cybersecurity technologies that transform federal government threat protection, visit www.cylance.com.



+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170228-2769